



Guia do Desenvolvedor

Amazon MQ



Amazon MQ: Guia do Desenvolvedor

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o Amazon MQ?	1
Como o Amazon MQ é diferente da Amazon ou da SQS Amazon? SNS	1
Como posso começar a usar o Amazon MQ?	1
Deixe seu comentário	2
Configuração	3
Etapa 1: pré-requisitos	3
Inscreva-se para um Conta da AWS	3
Criar um usuário com acesso administrativo	4
Crie um usuário e obtenha suas AWS credenciais	5
Etapa 3: Preparar-se para usar o código de exemplo	6
Próximas etapas	7
Começando: Criando e conectando-se a um corretor ActiveMQ	8
Etapa 1: Criar um corretor ActiveMQ	8
Etapa 2: Conectar um aplicativo Java ao seu corretor	10
Pré-requisitos	11
Criar um produtor de mensagem e enviar uma mensagem	13
Criar um consumidor de mensagem e receber a mensagem	14
Etapa 3: (opcional) conectar-se a uma AWS Lambda função	16
Começando: Criando e conectando-se a um corretor RabbitMQ	19
Etapa 1: Crie um corretor RabbitMQ	19
Etapa 2: Conecte um aplicativo JVM baseado ao seu corretor	21
Pré-requisitos	21
Etapa 3: (opcional) conectar-se a uma AWS Lambda função	26
Gerenciando um agente	29
Definindo configurações adicionais do corretor	29
Agendamento da manutenção do corretor	31
Atualizar a versão do mecanismo	35
Atualizar manualmente a versão do mecanismo	36
Atualizar automaticamente a versão do mecanismo espelho	38
Status do agente	40
Listando corretores	41
Para listar os agentes e visualizar os detalhes	41
Acessando o console web do Amazon MQ broker sem acessibilidade pública	42
Pré-requisitos	42

Para acessar o console web de um agente Amazon MQ sem acessibilidade pública	43
Reiniciando um agente	44
Para reinicializar um agente do Amazon MQ	44
Excluindo um agente	44
Excluindo um agente do Amazon MQ	45
Tipos de instância	45
Tipos de instância do Amazon MQ para ActiveMQ	45
Amazon MQ para tipos de instância RabbitMQ	46
Tags	47
Adicionar tags no console do Amazon MQ	48
Amazon MQ para ActiveMQ	49
Amazon MQ para corretores ActiveMQ	49
Agente	49
Usuário	52
Implantando um corretor	53
Agente de instância única	53
Corretor ativo/em espera	54
Rede de agentes	55
Como funciona uma rede de agentes?	57
Como uma rede de agentes lida com as credenciais?	57
Esquemas de exemplo	58
Topologias das redes de agentes	59
Dentro da região	64
Failover dinâmico com conectores de transporte	66
Configurações do agente	67
Atributos	67
Usando arquivos de XML configuração do Spring	68
Criando uma configuração	69
Editar uma revisão de configuração	72
Elementos permitidos	74
Atributos permitidos	77
Coleções permitidas	89
Atributos de elementos filho	96
Replicação entre regiões	103
Agentes primários e de réplica	103
Criação de um CRDR corretor	104

Excluindo um corretor CRDR	108
Promovendo um CRDR corretor	109
Métricas	111
Tutoriais ActiveMQ	113
Criação e configuração de uma rede de agentes	114
Conectar uma aplicação Java ao seu agente	120
Integração de agentes ActiveMQ com LDAP	125
Criando um usuário do ActiveMQ broker	141
Editar um usuário do ActiveMQ broker	142
Excluir um usuário do ActiveMQ broker	143
Exemplos de Java funcional	144
Gerenciamento de versão	156
Versões de motor suportadas no Amazon MQ para ActiveMQ	156
Atualizações da versão do motor	157
Listando as versões compatíveis do mecanismo	157
Armazenamento	157
Diferenças entre tipos de armazenamento	158
Práticas recomendadas do Amazon MQ para ActiveMQ	159
Nunca modifique ou exclua a interface de rede elástica do Amazon MQ	159
Sempre usar pooling de conexão	160
Sempre usar o transporte de failover para conectar-se a vários endpoints de operador	161
Evite usar seletores de mensagens	162
Preferir destinos virtuais a assinaturas duráveis	162
Se estiver usando o Amazon VPC Peering, evite clientes ao IPs alcance CIDR 10.0.0.0/16	162
Desativar o armazenamento e a expedição simultâneos para filas com consumidores lentos	162
Selecionar o tipo de instância de agente correto para obter a melhor taxa de transferência .	163
Escolha o tipo de armazenamento de agente correto para obter a melhor taxa de transferência	164
Configurar sua rede de agentes corretamente	164
Evite reinicializações lentas recuperando transações XA preparadas	165
Amazon MQ para RabbitMQ	167
Amazon MQ para corretores RabbitMQ	167
Agente	167
Usuários do Broker	169

Padrões do agente	171
Tipos de instâncias de agente	174
Diretrizes de dimensionamento	175
Plug-ins	178
Políticas	181
Implantando um corretor RabbitMQ	186
Agente de instância única	186
Implantação de clusters	187
Configurações do agente	189
Atributos	67
Criando uma configuração	190
Editando uma revisão de configuração	193
Políticas de configuração	194
Filas de quórum	195
Migração para filas de quórum	196
Configuração da política	197
Práticas recomendadas	198
Tutoriais do RabbitMQ	199
Editar as preferências de agente	199
Como usar Python Pika com o Amazon MQ para RabbitMQ	200
Resolvendo a sincronização de fila pausada	207
Gerenciamento de versão	214
Versões de mecanismo compatíveis no Amazon MQ para RabbitMQ	214
Atualizações da versão do motor	215
Listando as versões compatíveis do mecanismo	216
Práticas recomendadas do Amazon MQ para RabbitMQ	216
Ativar atualizações automáticas de versões secundárias	217
Usando recursos obsoletos	217
Escolha o tipo correto de instância do broker para obter a melhor taxa de transferência	218
Use vários canais	218
Habilitar filas lazy	218
Use mensagens persistentes e filas duráveis	219
Mantenha as filas curtas	220
Configurar reconhecimento e confirmação	221
Configurar pré-busca	222
Configurar o Celery	223

Recuperação automática de falhas de rede	224
Habilite o Classic Queue v2 para seu agente do RabbitMQ	224
Segurança	226
Proteção de dados	227
Criptografia	228
Criptografia em repouso	228
Criptografia em trânsito	237
Gerenciamento de identidade e acesso	239
Público	239
Autenticando com identidades	240
Gerenciando acesso usando políticas	243
Como o Amazon MQ funciona com IAM	246
Exemplos de políticas baseadas em identidade	252
Autorização e autenticação da API	255
AWS políticas gerenciadas	259
Uso de funções vinculadas a serviço	260
Solução de problemas	266
Validação de conformidade	268
Resiliência	270
Segurança da infraestrutura	270
Práticas recomendadas de segurança	271
Preferir agentes sem acessibilidade pública	271
Sempre configurar um mapa de autorização	271
Bloquear protocolos desnecessários	272
Logging e monitoramento	273
Acessando CloudWatch métricas	273
Acessando CloudWatch métricas usando o AWS Management Console	274
Métricas do ActiveMQ	274
Métricas do Amazon MQ para ActiveMQ	274
Métricas de destino do ActiveMQ (fila e tópico)	280
Métricas para RabbitMQ	284
Métricas do agente RabbitMQ	284
Dimensões para métricas de agente RabbitMQ	288
Métricas do nó RabbitMQ	288
Dimensões para métricas de nó RabbitMQ	289
Métricas de fila RabbitMQ	290

Dimensões para métricas de fila RabbitMQ	291
Configurar logs do Amazon MQ for RabbitMQ	291
Registrando API chamadas usando CloudTrail	291
Informações sobre o Amazon MQ em CloudTrail	292
Exemplo de entrada do arquivo de log do Amazon MQ	294
Configurar logs do Amazon MQ for ActiveMQ	296
Entendendo a estrutura do registro em CloudWatch Logs	297
Adicionar a permissão CreateLogGroup ao seu usuário do Amazon MQ	297
Configure uma política baseada em recursos para o Amazon MQ	298
Prevenção contra o ataque do “substituto confuso” em todos os serviços	300
Solução de problemas	302
Grupos de registros não aparecem em CloudWatch	302
Os fluxos de registros não aparecem nos grupos de CloudWatch registros	302
Cotas	303
Operadores	303
Configurações	304
Usuários	305
Armazenamento de dados	306
APILimitação	308
Solução de problemas	309
Solução de problemas: Amazon MQ geral	309
Não consigo me conectar ao console da Web ou endpoints do agente.	309
SSLexceções	315
Criei um agente, mas a criação falhou.	315
Meu agente reiniciou e não sei por quê.	316
Solução de problemas do Amazon MQ para ActiveMQ	316
Recuperando registros CloudWatch	317
Conectar ao agente após uma reinicialização	317
Alguns clientes não conseguem se conectar	318
Exceção JSP no console da Web	319
Solução de problemas: Amazon MQ para RabbitMQ	319
Não consigo ver as métricas das minhas filas ou dos meus hosts virtuais em CloudWatch. .	320
Como faço para habilitar plugins no Amazon MQ para RabbitMQ?	320
Não consigo alterar a VPC configuração da Amazon para o corretor.	320
RABBITMQ_MEMORY_ALARM	320
Diagnosticar alarme de alta memória com o console da Web do RabbitMQ	322

Diagnosticar o alarme de alta memória usando métricas do Amazon MQ	322
Solucionar o alarme de alta memória	324
Reduzir o número de conexões e canais	325
Solucionar sincronizações de filas pausadas em implantações de cluster	326
Solucionar loops de reinicialização em agentes de instância única	327
Evitar alarmes de alta memória	327
RABBITMQ_INVALID_KMS_KEY	328
Diagnosticando e abordando INVALID __ KMS KEY	329
BROKER_ENI_DELETED	329
BROKER_OOM	330
RABBITMQ_DISK_ALARM	331
Diagnostico e solução do alarme de limite de disco	332
RABBITMQ_QUORUM __ QUEUES NOT _ SUPPORTED CURRENT _EM_ _ VERSION	333
Recursos relacionados	334
Recursos do Amazon MQ	334
Recursos do Amazon MQ para ActiveMQ	335
Recursos do Amazon MQ para RabbitMQ	335
Notas de lançamento	337
.....	ccclxxii

O que é o Amazon MQ?

O Amazon MQ é um serviço de agente gerenciado que facilita a migração para um agente de mensagem na nuvem. Um agente de mensagem permite que aplicações de software e componentes se comuniquem usando várias linguagens de programação, sistemas operacionais e protocolos de sistemas de mensagens formais. [Atualmente, o Amazon MQ oferece suporte aos tipos de mecanismo Apache ActiveMQ Classic e RabbitMQ.](#)

O Amazon MQ funciona com as aplicações e serviços existentes sem a necessidade de gerenciar, operar e manter seu próprio sistema de mensagens.

Tópicos

- [Como o Amazon MQ é diferente da Amazon ou da SQS Amazon? SNS](#)
- [Como posso começar a usar o Amazon MQ?](#)
- [Deixe seu comentário](#)

Como o Amazon MQ é diferente da Amazon ou da SQS Amazon? SNS

O Amazon MQ é um serviço de agente de mensagens gerenciado, que fornece compatibilidade com muitos agentes de mensagens populares. Recomendamos o Amazon MQ para migrar aplicativos de agentes de mensagens existentes que dependem da compatibilidade com protocolos APIs como JMS AMQP 0-9-1, 1.0., e. AMQP MQTT OpenWire STOMP

[A Amazon SQS e a Amazon SNS](#) são serviços de filas e tópicos que são altamente escaláveis, simples de usar e não exigem a configuração de agentes de mensagens. Recomendamos esses serviços para novos aplicativos que podem se beneficiar de uma escalabilidade quase ilimitada e simples APIs.

Como posso começar a usar o Amazon MQ?

- Para criar seu primeiro corretor com o Amazon MQ, consulte ou [Começando: Criando e conectando-se a um corretor ActiveMQ](#) [Começando: Criando e conectando-se a um corretor RabbitMQ](#)

- Para conhecer as diretrizes e advertências que ajudarão você a aproveitar ao máximo o Amazon MQ, consulte [Working with Amazon MQ for ActiveMQ](#) e [Working with Amazon MQ for RabbitMQ](#).
- Para saber mais sobre o Amazon MQ REST APIs, consulte a Referência do [Amazon REST API MQ](#).
- Para saber mais sobre os AWS CLI comandos do Amazon MQ, consulte [Amazon MQ na AWS CLI Referência de comandos](#).

Deixe seu comentário

Os seus comentários são bem-vindos. Para entrar em contato conosco, visite o [Fórum de discussão do Amazon MQ](#).

Configuração do Amazon MQ

Antes de usar o Amazon MQ, é necessário executar as etapas a seguir.

Tópicos

- [Etapa 1: pré-requisitos](#)
- [Etapa 2: criar um usuário e obter suas AWS credenciais](#)
- [Etapa 3: Preparar-se para usar o código de exemplo](#)
- [Próximas etapas](#)

Etapa 1: pré-requisitos

Inscriva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a <https://portal.aws.amazon.com/billing/inscrição>.
2. Siga as instruções online.

Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar [tarefas que exigem acesso de usuário-raiz](#).

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando <https://aws.amazon.com/e> escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login [AWS Management Console](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira sua senha.

Para obter ajuda ao fazer login usando o usuário raiz, consulte [Fazer login como usuário raiz](#) no Guia do usuário do Início de Sessão da AWS .

2. Ative a autenticação multifator (MFA) para seu usuário root.

Para obter instruções, consulte [Habilitar um MFA dispositivo virtual para seu usuário Conta da AWS root \(console\)](#) no Guia IAM do usuário.

Criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

Para obter instruções, consulte [Habilitar AWS IAM Identity Center](#) no Guia do usuário do AWS IAM Identity Center .

2. No IAM Identity Center, conceda acesso administrativo a um usuário.

Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte [Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM](#) no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para entrar com seu usuário do IAM Identity Center, use o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte [Como fazer login no portal de AWS acesso](#) no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

Para obter instruções, consulte [Create a permission set](#) no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

Para obter instruções, consulte [Add groups](#) no Guia do usuário do AWS IAM Identity Center .

Etapa 2: criar um usuário e obter suas AWS credenciais

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho (Usuários gerenciados no IAM Identity Center)	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	<p>Siga as instruções da interface que deseja utilizar.</p> <ul style="list-style-type: none"> • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferramentas e AWS APIs, consulte Autenticação do IAM Identity Center no Guia de referência de ferramentas AWS SDKs e ferramentas.

Qual usuário precisa de acesso programático?	Para	Por
IAM	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções em Uso de credenciais temporárias com AWS recursos no Guia do IAM usuário.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitações programáticas para o AWS CLI, AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. <ul style="list-style-type: none"> • Para o AWS CLI, consulte Autenticação usando credenciais de IAM usuário no Guia do AWS Command Line Interface usuário. • Para ferramentas AWS SDKs e ferramentas, consulte Autenticar usando credenciais de longo prazo no Guia de referência de ferramentas AWS SDKs e ferramentas. • Para AWS APIs, consulte Gerenciamento de chaves de acesso para IAM usuários no Guia IAM do usuário.

Etapa 3: Preparar-se para usar o código de exemplo

Os tutoriais a seguir mostram como você pode trabalhar com corretores Amazon MQ usando AWS Management Console o e como se conectar programaticamente aos corretores Amazon MQ para ActiveMQ e Amazon MQ para RabbitMQ. Se você quiser usar o código de exemplo ActiveMQ de

Java, será necessário instalar o [Java Standard Edition Development Kit](#) e fazer algumas alterações de configuração no código de exemplo.

Você também pode criar e gerenciar corretores de forma programática usando o Amazon MQ e [RESTAPI AWS SDKs](#)

Próximas etapas

Agora que você está preparado para trabalhar com o Amazon MQ, comece [criando um agente](#). Dependendo do tipo de mecanismo do seu agente, você pode então [conectar um aplicativo Java ao seu agente Amazon MQ for ActiveMQ](#) ou [usar a biblioteca cliente Java do RabbitMQ para conectar um aplicativo baseado JVM ao seu agente Amazon MQ for RabbitMQ](#).

Começando: Criando e conectando-se a um corretor ActiveMQ


Um agente é um ambiente de agente de mensagens em execução no Amazon MQ. É o bloco de criação básico do Amazon MQ. A descrição combinada da classe (m5, t3) e do tamanho (large, micro) da instância do agente é um Tipo de instância de agente (por exemplo, mq.m5.large). Para obter mais informações, consulte [O que é um corretor Amazon MQ for ActiveMQ?](#).

Etapa 1: Criar um corretor ActiveMQ

A tarefa inicial e mais comum do Amazon MQ é a criação de um agente. O exemplo a seguir mostra como você pode usar o AWS Management Console para criar um corretor básico.

1. Faça login no [console do Amazon MQ](#).
2. Na página Select broker engine (Selecionar mecanismo de agente), selecione Apache ActiveMQ (Apache ActiveMQ).
3. Na página Select deployment and storage (Selecionar implantação e armazenamento), na seção Deployment mode and storage type (Modo de implantação e tipo de armazenamento), faça o seguinte:
 - a. Selecione o Deployment mode (Modo de implantação) (por exemplo: Agente ativo/em espera). Para obter mais informações, consulte [Opções de implantação do Amazon MQ para agentes ActiveMQ](#).
 - Um agente de instância única é composto por um agente em uma Zona de disponibilidade. O corretor se comunica com seu aplicativo e com um volume de EFS armazenamento da Amazon EBS ou da Amazon. Para obter mais informações, consulte [Opção 1: corretores de instância única do Amazon MQ](#).
 - Um agente ativo/em espera de alta disponibilidade é composto por dois agentes em duas zonas de disponibilidade diferentes, configuradas em um par redundante. Esses corretores se comunicam de forma síncrona com seu aplicativo e com a Amazon. EFS Para obter mais informações, consulte [Opção 2: corretores ativos/em espera do Amazon MQ para alta disponibilidade](#).
 - Para obter mais informações sobre os esquemas de amostra de uma rede de agentes, consulte [Esquemas de exemplo](#).

- b. Escolha o tipo de armazenamento (por exemplo, EBS). Para obter mais informações, consulte [Storage](#).

 Note

A Amazon EBS replica dados dentro de uma única zona de disponibilidade e não suporta o modo de implantação ativo/em espera do [ActiveMQ](#).

- c. Escolha Próximo.
4. Na página Definir configurações, faça o seguinte na seção Detalhes:
 - a. Digite o Broker name (Nome do agente).

 Important

Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nos nomes dos corretores. Os nomes dos corretores podem ser acessados por outros AWS serviços, incluindo CloudWatch registros. Nomes de agente não devem ser usados para dados privados ou sigilosos.

- b. Selecione o Tipo de instância de agente (por exemplo, m5.large). Para obter mais informações, consulte [Broker instance types](#).
5. Na seção ActiveMQ Web Console access (Acesso ao console da Web ActiveMQ), forneça um Username (Nome de usuário) e Password (Senha). As seguintes restrições se aplicam a nomes de usuário e senhas de agente:
 - Seu nome de usuário pode conter somente caracteres alfanuméricos, traços, pontos, sublinhados e tils (- . _ ~).
 - Sua senha deve ter pelo menos 12 caracteres, deve conter pelo menos 4 caracteres exclusivos e não deve conter vírgulas, dois pontos ou sinais de igual (,:=).

 Important

Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nos nomes de usuário da corretora. Os nomes de usuário dos corretores podem ser acessados por outros AWS serviços, incluindo CloudWatch

registros. Nomes de usuário do agente não devem ser usados para dados privados ou sigilosos.

6. Escolha Implantar.

Enquanto o Amazon MQ cria seu agente, ele exibe o status Criação em andamento.

A criação do agente leva cerca de 15 minutos.

Quando o seu agente é criado com sucesso, o Amazon MQ exibe o status Running (Em execução).

7. Escolha **MyBroker**.

Sobre o **MyBroker** página, na seção Connect, anote o URL console [web ActiveMQ do seu corretor, por exemplo:](#)

```
https://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:8162
```

Além disso, observe os [Endpoints de protocolo de nível de conexão](#) do seu agente. Veja a seguir um exemplo de um OpenWire endpoint:

```
ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:61617
```

Etapa 2: Conectar um aplicativo Java ao seu corretor

Depois de criar um agente do Amazon MQ ActiveMQ, você pode conectar sua aplicação a ele. Os exemplos a seguir mostram como você pode usar o Java Message Service (JMS) para criar uma conexão com o broker, criar uma fila e enviar uma mensagem. Para obter um exemplo completo e funcional do Java, consulte [Working Java Example](#).

Você pode se conectar a agentes do ActiveMQ usando [vários clientes de ActiveMQ](#). Recomendamos usar o [Cliente ActiveMQ](#).

Pré-requisitos

Ativar VPC atributos

Note

Não é possível desativar a acessibilidade pública para os agentes do Amazon MQ existentes.

Para garantir que seu corretor esteja acessível dentro de vocêVPC, você deve habilitar os `enableDnsSupport` VPC atributos `enableDnsHostnames` e. Para obter mais informações, consulte [DNSSupport VPC em seu](#) Guia do VPC usuário da Amazon.

Habilitar conexões de entrada

Em seguida, use as instruções a seguir para habilitar conexões de entrada para seu corretor.

1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, escolha o nome do seu corretor (por exemplo, MyBroker).
3. Sobre o **MyBroker** página, na seção Conexões, anote os endereços e portas do console web URL e dos protocolos de nível de fio do broker.
4. Na seção Details (Detalhes), em Security and network (Segurança e rede), escolha o nome do seu grupo de segurança ou



A página Grupos de Segurança do EC2 Painel é exibida.

5. Na lista de security group, escolha seu security group.
6. Na parte inferior da página, escolha Inbound (Entrada) e a seguir selecione Edit (Editar).
7. Na caixa de diálogo Editar regras de entrada, adicione uma regra para cada terminal URL ou endpoint que você deseja que seja acessível ao público (o exemplo a seguir mostra como fazer isso em um console web do broker).
 - a. Escolha Add Rule.
 - b. Em Tipo, selecione Personalizado TCP.
 - c. Para o Intervalo de Portas, digite a porta do console da Web (8162).

- d. Para Source (Origem), deixe Custom (Personalizado) selecionado e, depois, digite o endereço IP do sistema ao qual deseja ser capaz de acessar o console da Web (por exemplo, 192.0.2.1).
- e. Escolha Salvar.

Agora seu agente pode aceitar conexões de entrada.

Adicionar dependências de Java

Adicione os pacotes `activemq-client.jar` e `activemq-pool.jar` ao caminho da classe Java. O exemplo a seguir mostra essas dependências em um arquivo `pom.xml` do projeto Maven.

```
<dependencies>
  <dependency>
    <groupId>org.apache.activemq</groupId>
    <artifactId>activemq-client</artifactId>
    <version>5.15.16</version>
  </dependency>
  <dependency>
    <groupId>org.apache.activemq</groupId>
    <artifactId>activemq-pool</artifactId>
    <version>5.15.16</version>
  </dependency>
</dependencies>
```

Para obter mais informações sobre `activemq-client.jar`, consulte [Initial Configuration](#) (Configuração inicial) na documentação do Apache ActiveMQ.

Important

No código de exemplo a seguir, os produtores e consumidores são executados em um único thread. Para sistemas de produção (ou para testar o failover de instância do agente), certifique-se de que seus produtores e consumidores sejam executados em hosts ou threads separados.

Criar um produtor de mensagem e enviar uma mensagem

Em seguida, verifique se seu corretor pode receber uma mensagem criando um produtor de mensagens e enviando uma mensagem.

1. Crie uma fábrica de conexões em JMS pool para o produtor de mensagens usando o endpoint do seu corretor e, em seguida, chame o `createConnection` método na fábrica.

Note

Para um agente ativo/em espera, o Amazon MQ fornece dois ActiveMQ Web ConsoleURLs, mas somente um está ativo por vez. URL Da mesma forma, o Amazon MQ fornece dois endpoints para cada protocolo de nível de conexão, mas apenas um endpoint está ativo em cada par de cada vez. Os sufixos -1 e -2 denotam um par redundante. Para obter mais informações, consulte [Opções de implantação do Amazon MQ para agentes ActiveMQ](#).

Para endpoints de protocolo de nível de conexão, você pode permitir que sua aplicação se conecte a qualquer endpoint usando o [Transporte de failover](#).

```
// Create a connection factory.
final ActiveMQConnectionFactory connectionFactory = new
    ActiveMQConnectionFactory(wireLevelEndpoint);

// Pass the sign-in credentials.
connectionFactory.setUsername(activeMqUsername);
connectionFactory.setPassword(activeMqPassword);

// Create a pooled connection factory.
final PooledConnectionFactory pooledConnectionFactory = new
    PooledConnectionFactory();
pooledConnectionFactory.setConnectionFactory(connectionFactory);
pooledConnectionFactory.setMaxConnections(10);

// Establish a connection for the producer.
final Connection producerConnection = pooledConnectionFactory.createConnection();
producerConnection.start();

// Close all connections in the pool.
pooledConnectionFactory.clear();
```

Note

Os produtores de mensagens devem sempre usar a classe `PooledConnectionFactory`. Para obter mais informações, consulte [Sempre usar pooling de conexão](#).

2. Crie uma sessão, uma fila chamada `MyQueue` e um produtor de mensagens.

```
// Create a session.
final Session producerSession = producerConnection.createSession(false,
    Session.AUTO_ACKNOWLEDGE);

// Create a queue named "MyQueue".
final Destination producerDestination = producerSession.createQueue("MyQueue");

// Create a producer from the session to the queue.
final MessageProducer producer =
    producerSession.createProducer(producerDestination);
producer.setDeliveryMode(DeliveryMode.NON_PERSISTENT);
```

3. Crie a string da mensagem "Hello from Amazon MQ!" e, em seguida, envie a mensagem.

```
// Create a message.
final String text = "Hello from Amazon MQ!";
TextMessage producerMessage = producerSession.createTextMessage(text);

// Send the message.
producer.send(producerMessage);
System.out.println("Message sent.");
```

4. Limpe o produtor.

```
producer.close();
producerSession.close();
producerConnection.close();
```

Criar um consumidor de mensagem e receber a mensagem

Depois de criar um produtor, crie um consumidor para verificar se ele pode receber a mensagem.

1. Crie uma fábrica de JMS conexões para o produtor de mensagens usando o endpoint do seu corretor e, em seguida, chame o `createConnection` método na fábrica.

```
// Create a connection factory.
final ActiveMQConnectionFactory connectionFactory = new
    ActiveMQConnectionFactory(wireLevelEndpoint);

// Pass the sign-in credentials.
connectionFactory.setUsername(activeMqUsername);
connectionFactory.setPassword(activeMqPassword);

// Establish a connection for the consumer.
final Connection consumerConnection = connectionFactory.createConnection();
consumerConnection.start();
```

Note

Os consumidores de mensagens nunca devem usar a classe `PooledConnectionFactory`. Para obter mais informações, consulte [Sempre usar pooling de conexão](#).

2. Crie uma sessão, uma fila chamada `MyQueue` e um consumidor de mensagens.

```
// Create a session.
final Session consumerSession = consumerConnection.createSession(false,
    Session.AUTO_ACKNOWLEDGE);

// Create a queue named "MyQueue".
final Destination consumerDestination = consumerSession.createQueue("MyQueue");

// Create a message consumer from the session to the queue.
final MessageConsumer consumer =
    consumerSession.createConsumer(consumerDestination);
```

3. Comece a aguardar mensagens e receba a mensagem quando ela chegar.

```
// Begin to wait for messages.
final Message consumerMessage = consumer.receive(1000);

// Receive the message when it arrives.
final TextMessage consumerTextMessage = (TextMessage) consumerMessage;
```



```
System.out.println("Message received: " + consumerTextMessage.getText());
```

Note

Ao contrário dos serviços de AWS mensagens (como a AmazonSQS), o consumidor está constantemente conectado à corretora.

4. Feche o consumidor, a sessão e a conexão.

```
consumer.close();  
consumerSession.close();  
consumerConnection.close();
```

Etapa 3: (opcional) conectar-se a uma AWS Lambda função

AWS Lambda pode se conectar e consumir mensagens do seu agente Amazon MQ. Quando você conecta um agente ao Lambda, você cria um [Mapeamento da origem do evento](#) que lê mensagens de uma fila e invoca a função [sincronicamente](#). O mapeamento da fonte de eventos que você cria lê mensagens do seu agente em lotes e as converte em uma carga Lambda na forma de um objeto. JSON

Para conectar seu agente a uma função do Lambda

1. Adicione as seguintes permissões de IAM função à sua função de [execução](#) da função Lambda.
 - [metros quadrados: DescribeBroker](#)
 - [ec2: CreateNetworkInterface](#)
 - [ec2: DeleteNetworkInterface](#)
 - [ec2: DescribeNetworkInterfaces](#)
 - [ec2: DescribeSecurityGroups](#)
 - [ec2: DescribeSubnets](#)
 - [ec2: DescribeVpcs](#)
 - [troncos: CreateLogGroup](#)
 - [troncos: CreateLogStream](#)
 - [troncos: PutLogEvents](#)

- [gerente de segredos: GetSecretValue](#)

Note

Sem as IAM permissões necessárias, sua função não conseguirá ler com sucesso os registros dos recursos do Amazon MQ.

2. (Opcional) Se você criou um agente sem acessibilidade pública, você deve fazer um dos seguintes procedimentos para permitir que o Lambda se conecte ao seu agente:
 - Configure um NAT gateway por sub-rede pública. Para obter mais informações, consulte [Acesso à Internet e aos serviços para funções VPC conectadas](#) no Guia do AWS Lambda desenvolvedor.
 - Crie uma conexão entre sua Amazon Virtual Private Cloud (AmazonVPC) e o Lambda usando um VPC endpoint. Seu Amazon também VPC deve se conectar aos endpoints AWS Security Token Service (AWS STS) e Secrets Manager. Para obter mais informações, consulte [Configurando VPC endpoints de interface para Lambda](#) no Guia do desenvolvedor.AWS Lambda
3. [Configure seu agente como uma origem do evento](#) para uma função do Lambda usando AWS Management Console. Você também pode usar o [create-event-source-mapping](#) AWS Command Line Interface comando.
4. Escreva algum código para sua função do Lambda para processar as mensagens consumidas pelo seu agente. A carga útil do Lambda recuperada pelo mapeamento da origem do evento depende do tipo de mecanismo do agente. Veja a seguir um exemplo de uma carga útil do Lambda para uma fila do Amazon MQ para ActiveMQ.

Note

No exemplo, testQueue é o nome da fila.

```
{
  "eventSource": "aws:amq",
  "eventSourceArn": "arn:aws:mq:us-
west-2:112556298976:broker:test:b-9bcfa592-423a-4942-879d-eb284b418fc8",
  "messages": {
    [
```

```
{
  "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-
west-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
  "messageType": "jms/text-message",
  "data": "QUJD0kFBQUE=",
  "connectionId": "myJMScoID",
  "redelivered": false,
  "destination": {
    "physicalname": "testQueue"
  },
  "timestamp": 1598827811958,
  "brokerInTime": 1598827811958,
  "brokerOutTime": 1598827811959
},
{
  "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-
west-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
  "messageType": "jms/bytes-message",
  "data": "3DT00W7crj51prgVLQaGQ82S48k=",
  "connectionId": "myJMScoID1",
  "persistent": false,
  "destination": {
    "physicalname": "testQueue"
  },
  "timestamp": 1598827811958,
  "brokerInTime": 1598827811958,
  "brokerOutTime": 1598827811959
}
]
}
```

Para obter mais informações sobre como conectar o Amazon MQ ao Lambda, as opções com as que o Lambda é compatível para uma origem de evento do Amazon MQ e erros de mapeamento da origem do evento, consulte [Usar o Lambda com o Amazon MQ](#) no Guia do desenvolvedor AWS Lambda .

Começando: Criando e conectando-se a um corretor RabbitMQ

Um agente é um ambiente de agente de mensagens em execução no Amazon MQ. É o bloco de criação básico do Amazon MQ. A descrição combinada da classe (m5, t3) e do tamanho (large, micro) da instância do agente é um Tipo de instância de agente (por exemplo, mq.m5.large). Para ter mais informações, consulte [O que é um corretor Amazon MQ para RabbitMQ?](#)

Etapa 1: Crie um corretor RabbitMQ

A tarefa inicial e mais comum do Amazon MQ é a criação de um agente. O exemplo a seguir mostra como você pode usar o AWS Management Console para criar um corretor básico.

1. Faça login no [console do Amazon MQ](#).
2. Na página Select broker engine (Selecionar mecanismo do agente), selecione RabbitMQ e, em seguida, selecione Next (Avançar).
3. Na página Select deployment mode (Selecionar modo de implementação), escolha o Deployment mode (Modo de implantação), por exemplo, Cluster deployment (Implantação de cluster) e, depois, escolha Next (Avançar).
 - Um agente de instância única é composto por um agente em uma zona de disponibilidade atrás de um Network Load NLB Balancer (). O corretor se comunica com seu aplicativo e com um volume de EBS armazenamento da Amazon. Para obter mais informações, consulte [Opção 1: agente de instância única Amazon MQ para RabbitMQ](#).
 - A implantação de cluster RabbitMQ para alta disponibilidade é um agrupamento lógico de três nós do agente RabbitMQ atrás de um Network Load Balancer (NLB), cada um compartilhando usuários, filas e um estado distribuído em várias Zonas de Disponibilidade (AZ). Para obter mais informações, consulte [Opção 2: Amazon MQ para implantação do cluster RabbitMQ](#).
4. Na página Definir configurações, faça o seguinte na seção Detalhes:
 - a. Digite o Broker name (Nome do agente).

Important

Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nos nomes dos corretores. Os nomes dos corretores

podem ser acessados por outros AWS serviços, incluindo CloudWatch registros. Nomes de agente não devem ser usados para dados privados ou sigilosos.

- b. Selecione o Tipo de instância de agente (por exemplo, m5.large). Para obter mais informações, consulte [Broker instance types](#).

Note

A seção Configurações adicionais fornece opções para habilitar CloudWatch registros e configurar o acesso à rede para seu corretor. Se você criar um broker RabbitMQ privado sem acessibilidade pública, deverá selecionar uma Virtual Private Cloud (VPC) e configurar um grupo de segurança para acessar seu broker.

5. Na página Configure settings (Definição de configurações), na seção RabbitMQ access (Acesso RabbitMQ), forneça um Username (Nome de usuário) e Password (Senha). As seguintes restrições se aplicam a credenciais de login do agente:
 - Seu nome de usuário pode conter somente caracteres alfanuméricos, traços, pontos e sublinhados (- . _). Este valor não deve conter quaisquer caracteres de til (~). O Amazon MQ proíbe o uso de guest como um nome de usuário.
 - Sua senha deve ter pelo menos 12 caracteres, deve conter pelo menos 4 caracteres exclusivos e não deve conter vírgulas, dois pontos ou sinais de igual (,:=).

Important

Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nos nomes de usuário da corretora. Os nomes de usuário dos corretores podem ser acessados por outros AWS serviços, incluindo CloudWatch registros. Nomes de usuário do agente não devem ser usados para dados privados ou sigilosos.

6. Escolha Próximo.
7. Na página Review and create (Revisar e criar), você pode revisar suas seleções e editá-las conforme necessário.
8. Escolha Criar agente.

Enquanto o Amazon MQ cria seu agente, ele exibe o status Criação em andamento.

A criação do agente leva cerca de 15 minutos.

Quando o seu agente é criado com sucesso, o Amazon MQ exibe o status Running (Em execução).

9. Escolha **MyBroker**.

Sobre o **MyBroker** página, na seção Connect, anote o [console web RabbitMQ](#) do seu corretorURL, por exemplo:

```
https://b-c8349341-ec91-4a78-ad9c-a57f23f235bb.mq.us-west-2.amazonaws.com
```

Além disso, observe o [AMQPendpoint seguro](#) do seu corretor. Veja a seguir um exemplo de endpoint amqps expondo a porta listener 5671.

```
amqps://b-c8349341-ec91-4a78-ad9c-a57f23f235bb.mq.us-west-2.amazonaws.com:5671
```

Etapa 2: Conecte um aplicativo JVM baseado ao seu corretor

Depois de criar um agente do RabbitMQ, você pode conectar sua aplicação a ele. Os exemplos a seguir mostram como usar a [Biblioteca de cliente Java](#) para criar uma conexão com seu agente, criar uma fila e enviar uma mensagem. Você pode se conectar a agentes RabbitMQ usando bibliotecas de cliente RabbitMQ compatíveis para vários idiomas. Para obter mais informações sobre bibliotecas de cliente RabbitMQ compatíveis, consulte [Bibliotecas de cliente e ferramentas de desenvolvedor RabbitMQ](#).

Pré-requisitos

Note

As etapas de pré-requisito a seguir são aplicáveis somente a agentes RabbitMQ criados sem acessibilidade pública. Se você estiver criando um agente com acessibilidade pública, pode ignorar essas etapas.

Ativar VPC atributos

Para garantir que seu corretor esteja acessível dentro de vocêVPC, você deve habilitar os `enableDnsSupport` VPC atributos `enableDnsHostnames` e. Para obter mais informações, consulte [DNSSupport VPC em seu](#) Guia do VPC usuário da Amazon.

Habilitar conexões de entrada

1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, escolha o nome do seu corretor (por exemplo, MyBroker).
3. Sobre o **MyBroker** página, na seção Conexões, observe os endereços e portas do console web URL e dos protocolos de nível de fio do broker.
4. Na seção Details (Detalhes), em Security and network (Segurança e rede), escolha o nome do seu grupo de segurança ou



A página Grupos de Segurança do EC2 Painel é exibida.

5. Na lista de security group, escolha seu security group.
6. Na parte inferior da página, escolha Inbound (Entrada) e a seguir selecione Edit (Editar).
7. Na caixa de diálogo Editar regras de entrada, adicione uma regra para cada terminal URL ou endpoint que você deseja que seja acessível ao público (o exemplo a seguir mostra como fazer isso em um console web do broker).
 - a. Escolha Add Rule.
 - b. Em Tipo, selecione Personalizado TCP.
 - c. Para Source (Origem), deixe Custom (Personalizado) selecionado e, depois, digite o endereço IP do sistema ao qual deseja ser capaz de acessar o console da Web (por exemplo, 192.0.2.1).
 - d. Escolha Salvar.

Agora seu agente pode aceitar conexões de entrada.

Adicionar dependências de Java

Se você estiver usando o Apache Maven para automatizar compilações, adicione a seguinte dependência a seu arquivo `pom.xml`. Para obter mais informações sobre os arquivos do Modelo de Objeto do Projeto no Apache Maven, consulte [Introdução ao POM](#).

```
<dependency>
  <groupId>com.rabbitmq</groupId>
  <artifactId>amqp-client</artifactId>
  <version>5.9.0</version>
</dependency>
```

Se você estiver usando o [Gradle](#) para automatizar compilações, declare a seguinte dependência.

```
dependencies {
    compile 'com.rabbitmq:amqp-client:5.9.0'
}
```

Importar **Connection** e classes **Channel**

O cliente Java RabbitMQ usa `com.rabbitmq.client` como seu pacote de nível superior, com `Channel` API classes `Connection` e representando uma conexão e um canal AMQP 0-9-1, respectivamente. Importe as classes `Connection` e `Channel` antes de usá-las, conforme mostrado no exemplo a seguir.

```
import com.rabbitmq.client.Connection;
import com.rabbitmq.client.Channel;
```

Crie um **ConnectionFactory** e conecte ao seu agente

Use o exemplo a seguir para criar uma instância da classe `ConnectionFactory` com os parâmetros fornecidos. Use o método `setHost` para configurar o endpoint do agente que você anotou anteriormente. Para conexões AMQPS de nível de conexão, use a porta 5671.

```
ConnectionFactory factory = new ConnectionFactory();

factory.setUsername(username);
factory.setPassword(password);

//Replace the URL with your information
```



```
factory.setHost("b-c8352341-ec91-4a78-ad9c-a43f23d325bb.mq.us-west-2.amazonaws.com");
factory.setPort(5671);

// Allows client to establish a connection over TLS
factory.useSslProtocol();

// Create a connection
Connection conn = factory.newConnection();

// Create a channel
Channel channel = conn.createChannel();
```

Publicar uma mensagem em uma troca

Você pode usar o `Channel.basicPublish` para publicar mensagens em uma troca. O exemplo a seguir usa a `AMQP.Builder` classe para criar um objeto de propriedades da mensagem com o tipo de conteúdo `plain/text`.

```
byte[] messageBodyBytes = "Hello, world!".getBytes();
channel.basicPublish(exchangeName, routingKey,
    new AMQP.BasicProperties.Builder()
        .contentType("text/plain")
        .userId("userId")
        .build(),
    messageBodyBytes);
```

Note

Observe que `BasicProperties` é uma classe interna da classe titular gerada automaticamente, `AMQP`.

Inscriver-se em uma fila e receber uma mensagem

Você pode receber uma mensagem inscrevendo-se em uma fila usando a Interface `Consumer`. Depois de inscrito, as mensagens serão entregues automaticamente à medida que chegarem.

A maneira mais fácil de implementar um `Consumer` é usar a subclasse `DefaultConsumer`. Um objeto `DefaultConsumer` pode ser transmitido como parte de uma chamada `basicConsume` para configurar a assinatura, conforme mostrado no exemplo a seguir.

```
boolean autoAck = false;
channel.basicConsume(queueName, autoAck, "myConsumerTag",
    new DefaultConsumer(channel) {
        @Override
        public void handleDelivery(String consumerTag,
            Envelope envelope,
            AMQP.BasicProperties properties,
            byte[] body)
            throws IOException
        {
            String routingKey = envelope.getRoutingKey();
            String contentType = properties.getContentType();
            long deliveryTag = envelope.getDeliveryTag();
            // (process the message components here ...)
            channel.basicAck(deliveryTag, false);
        }
    });
```

Note

Como nós especificamos `autoAck = false`, é necessário reconhecer as mensagens entregues ao `Consumer`, o que é feito de maneira mais conveniente no método `handleDelivery`, conforme mostrado no exemplo.

Fechar sua conexão e desconectar do agente

Para se desconectar do seu agente RabbitMQ, feche o canal e a conexão, conforme mostrado a seguir.

```
channel.close();
conn.close();
```

Note

Para obter mais informações sobre como trabalhar com a biblioteca cliente Java do RabbitMQ, consulte o Guia do cliente Java do [RabbitMQ](#). API

Etapa 3: (opcional) conectar-se a uma AWS Lambda função

AWS Lambda pode se conectar e consumir mensagens do seu agente Amazon MQ. Quando você conecta um agente ao Lambda, você cria um [Mapeamento da origem do evento](#) que lê mensagens de uma fila e invoca a função [sincronicamente](#). O mapeamento da fonte de eventos que você cria lê mensagens do seu agente em lotes e as converte em uma carga Lambda na forma de um objeto JSON

Para conectar seu agente a uma função do Lambda


1. Adicione as seguintes permissões de IAM função à sua função de [execução](#) da função Lambda.
 - [metros quadrados: DescribeBroker](#)
 - [ec2: CreateNetworkInterface](#)
 - [ec2: DeleteNetworkInterface](#)
 - [ec2: DescribeNetworkInterfaces](#)
 - [ec2: DescribeSecurityGroups](#)
 - [ec2: DescribeSubnets](#)
 - [ec2: DescribeVpcs](#)
 - [registros: CreateLogGroup](#)
 - [registros: CreateLogStream](#)
 - [registros: PutLogEvents](#)
 - [gerente de segredos: GetSecretValue](#)

Note

Sem as IAM permissões necessárias, sua função não conseguirá ler com sucesso os registros dos recursos do Amazon MQ.

2. (Opcional) Se você criou um agente sem acessibilidade pública, você deve fazer um dos seguintes procedimentos para permitir que o Lambda se conecte ao seu agente:
 - Configure um NAT gateway por sub-rede pública. Para obter mais informações, consulte [Acesso à Internet e aos serviços para funções VPC conectadas](#) no Guia do AWS Lambda desenvolvedor.

- Crie uma conexão entre sua Amazon Virtual Private Cloud (AmazonVPC) e o Lambda usando um VPC endpoint. Seu Amazon também VPC deve se conectar aos endpoints AWS Security Token Service (AWS STS) e Secrets Manager. Para obter mais informações, consulte [Configurando VPC endpoints de interface para Lambda](#) no Guia do desenvolvedor.AWS Lambda
3. [Configure seu agente como uma origem do evento](#) para uma função do Lambda usando AWS Management Console. Você também pode usar o [create-event-source-mapping](#) AWS Command Line Interface comando.
 4. Escreva algum código para sua função do Lambda para processar as suas mensagens consumidas pelo seu agente. A carga útil do Lambda recuperada pelo mapeamento da origem do evento depende do tipo de mecanismo do agente. Veja a seguir um exemplo de uma carga útil do Lambda para uma fila do Amazon MQ para RabbitMQ.

 Note

No exemplo, test é o nome da fila e / é o nome do host virtual padrão. Ao receber mensagens, a origem do evento lista as mensagens em test::/.

```
{
  "eventSource": "aws:rmq",
  "eventSourceArn": "arn:aws:mq:us-west-2:112556298976:broker:test:b-9bcfa592-423a-4942-879d-eb284b418fc8",
  "rmqMessagesByQueue": {
    "test::/": [
      {
        "basicProperties": {
          "contentType": "text/plain",
          "contentEncoding": null,
          "headers": {
            "header1": {
              "bytes": [
                118,
                97,
                108,
                104,
                105,
                118,
                49
              ]
            }
          }
        }
      }
    ]
  }
}
```

```
    },
    "header2": {
      "bytes": [
        118,
        97,
        108,
        117,
        101,
        50
      ]
    },
    "numberInHeader": 10
  }
  "deliveryMode": 1,
  "priority": 34,
  "correlationId": null,
  "replyTo": null,
  "expiration": "60000",
  "messageId": null,
  "timestamp": "Jan 1, 1970, 12:33:41 AM",
  "type": null,
  "userId": "AIDACKCEVSQ6C2EXAMPLE",
  "appId": null,
  "clusterId": null,
  "bodySize": 80
},
"redelivered": false,
"data": "eyJ0aW1lb3V0IjowLCJkYXRhIjoiQ1pybWYwR3c4T3Y0YnFMUXhENEUifQ=="
}
]
}
}
```

Para obter mais informações sobre como conectar o Amazon MQ ao Lambda, as opções com as que o Lambda é compatível para uma origem de evento do Amazon MQ e erros de mapeamento da origem do evento, consulte [Usar o Lambda com o Amazon MQ](#) no Guia do desenvolvedor AWS Lambda .

Gerenciando um agente do Amazon MQ

Depois de criar um agente, você pode gerenciar e manter os diferentes componentes do seu agente Amazon MQ.

Tópicos

- [Definir configurações adicionais do agente Amazon MQ](#)
- [Programando a janela de manutenção para um agente Amazon MQ](#)
- [Atualizando uma versão do mecanismo de agente do Amazon MQ](#)
- [Status de corretor Amazon MQ](#)
- [Listar os agentes do Amazon MQ e visualizar os detalhes dos agentes](#)
- [Acessando o console web do Amazon MQ broker sem acessibilidade pública](#)
- [Reinicializar um agente do Amazon MQ](#)
- [Excluindo um agente do Amazon MQ](#)
- [Tipos de instância do agente Amazon MQ](#)
- [Adicionar tags aos recursos do Amazon MQ](#)

Definir configurações adicionais do agente Amazon MQ


Talvez você queira definir configurações adicionais para seu corretor. Você pode definir configurações adicionais para sua corretora no console durante o processo de criação da corretora. Configurações adicionais podem incluir configurações e VPCs acessibilidade pública.

Important

- Sub-rede(s) – Um agente de instância única requer uma sub-rede (por exemplo, a sub-rede padrão). Um agente ativo/em espera requer duas sub-redes.
- Grupo(s) de segurança – os agentes de instância única e os agentes ativos/em espera requerem, pelo menos, um grupo de segurança (por exemplo, o grupo de segurança padrão).
- VPC— A (s) sub-rede (s) e o (s) grupo (s) de segurança de uma corretora devem estar na mesma VPC. EC2-Os recursos clássicos não são suportados. O Amazon MQ só oferece suporte VPC à locação padrão e não à locação dedicada. VPC

- Criptografia – Escolha a chave mestra do cliente para criptografar seus dados. Consulte [Criptografia em repouso](#).
- Acessibilidade pública — Desativar a acessibilidade pública torna o corretor acessível somente dentro do seu VPC. Para ter mais informações, consulte [Preferir agentes sem acessibilidade pública](#) e [Acessando o console web do Amazon MQ broker sem acessibilidade pública](#).


1. Expanda a seção Configurações adicionais.
2. Na seção Configuration (Configuração), selecione Create a new configuration with default values (Criar uma configuração com valores padrão) ou Select an existing configuration (Selecionar uma configuração existente). Para obter mais informações, consulte [Amazon MQ Broker Configuration Parameters](#).
3. Na seção Logs, escolha se deseja publicar registros gerais e registros de auditoria no Amazon CloudWatch Logs. Para obter mais informações, consulte [Monitoring and logging Amazon MQ brokers](#).

 Important

Se você não [adicionar a permissão CreateLogGroup ao seu usuário do Amazon MQ](#) antes que ele crie ou reinicialize o agente, o Amazon MQ não criará o grupo de logs. Se você não [configurar uma política baseada em recursos para o Amazon MQ](#), o agente não poderá publicar os registros no Logs. CloudWatch

4. Na seção Network and security (Rede e segurança), configure a conectividade do agente:
 - a. Execute um destes procedimentos:
 - Escolha Usar o padrão VPC, a (s) sub-rede (s) e o (s) grupo (s) de segurança.
 - Escolha Selecionar existente VPC, sub-rede (s) e grupo (s) de segurança.
 1. Se você escolher essa opção, poderá criar uma nova Virtual Private Cloud (VPC) no VPC console da Amazon, selecionar uma existente VPC ou selecionar a padrão VPC. Para obter mais informações, consulte [O que é a Amazon VPC?](#) no Guia do VPC usuário da Amazon.

2. Depois de criar ou selecionar uma VPC, você pode criar novas sub-redes no VPC console da Amazon ou selecionar as existentes. Para obter mais informações, consulte [VPCs Sub-redes no Guia VPC](#) do usuário da Amazon.
3. Depois de criar ou selecionar sub-redes, você poderá selecionar os Security group(s) (Grupos de segurança).
- b. Escolha a chave mestra do cliente (CMK) que será usada para criptografar seus dados. Consulte [Criptografia em repouso](#).
- c. Selecione a Public accessibility (Acessibilidade pública) do seu operador.
5. Na seção Maintenance (Manutenção), configure a programação de manutenção do agente:
 - a. Para atualizar o agente para novas versões à medida que são lançadas pelo Apache, selecione Enable automatic minor version upgrades (Habilitar atualizações automáticas de versões secundárias). As atualizações automáticas ocorrem durante a janela de manutenção definida pelo dia da semana, a hora do dia (no formato de 24 horas) e o fuso horário (UTC por padrão).

 Note

Para um agente ativo/em espera, se uma das instâncias do agente for submetida à manutenção, o Amazon MQ levará pouco tempo para tirar de serviço a instância inativa. Isso permite que a instância em espera saudável se torne ativa e comece a aceitar comunicações recebidas.

- b. Execute um destes procedimentos:
 - Para permitir que o Amazon MQ selecione a janela de manutenção automaticamente, selecione No preference (Sem preferência).
 - Para definir uma janela de manutenção personalizada, selecione Select maintenance window (Selecionar janela de manutenção) e especifique o Start day (Dia de início) e o Start time (Horário de início) das atualizações.

Programando a janela de manutenção para um agente Amazon MQ

Periodicamente, o Amazon MQ realiza manutenção no hardware, no sistema operacional ou no software do mecanismo de um agente de mensagens durante a janela de manutenção. Por

exemplo, se você ativou [atualizações automáticas de versões secundárias](#) ou alterou o tipo de instância do broker, o Amazon MQ aplicará suas alterações durante a próxima janela de manutenção programada. A duração da manutenção pode durar até duas horas, dependendo das operações programadas para seu agente de mensagens. Você pode minimizar o tempo de inatividade durante uma janela de manutenção selecionando um modo de implantação do agente com alta disponibilidade em várias zonas de disponibilidade (AZ).

[O Amazon MQ for ActiveMQ fornece implantações ativas/em espera para alta disponibilidade.](#) No modo ativo/em espera, o Amazon MQ executa operações de manutenção, uma instância por vez, e pelo menos uma instância permanece disponível. Além disso, você pode configurar uma [rede de corretores](#) com janelas de manutenção variadas ao longo da semana. O Amazon MQ para RabbitMQ fornece implantações de [cluster](#) para alta disponibilidade. Em implantações de cluster, o Amazon MQ executa operações de manutenção, um nó por vez, mantendo pelo menos dois nós em execução o tempo todo.

Ao criar seu corretor pela primeira vez, você pode programar a janela de manutenção para ocorrer uma vez por semana em um horário especificado. Você só pode ajustar a janela de manutenção de um agente até quatro vezes antes da próxima janela de manutenção programada. Depois que a janela de manutenção do corretor é concluída, o Amazon MQ redefine o limite e você pode ajustar a programação novamente antes que a próxima janela de manutenção ocorra. A disponibilidade do corretor não é afetada ao ajustar a janela de manutenção do corretor.


Para ajustar a janela de manutenção do corretor, você pode usar o AWS Management Console AWS CLI, o ou o Amazon MQAPI.

Agende a janela de manutenção do corretor usando o AWS Management Console

Para ajustar a janela de manutenção do corretor usando o AWS Management Console

1. Faça login no [console do Amazon MQ](#).
2. No painel de navegação à esquerda, selecione Brookers (Agentes) e depois escolha o agente que você deseja atualizar na lista.
3. Na página de detalhes do agente, selecione Edit (Editar).
4. Em Manutenção, faça o seguinte.
 - a. Para Start day (Dia de início), escolha um dia da semana, por exemplo, Sunday (domingo), da lista suspensa.

- b. Para Start time (Hora de início), escolha o horário (horas e minutos) do dia para o qual deseja agendar a próxima janela de manutenção do agente, por exemplo, 12:00.

 Note

As opções de horário de início são configuradas no fuso horário UTC +0.

5. Navegue até o final da página e selecione Salvar. A janela de manutenção é ajustada imediatamente.
6. Na página de detalhes do agente, em Maintenance window (Janela de manutenção), verifique se sua nova programação preferencial é exibida.

Agende a janela de manutenção do corretor usando o AWS CLI

Para ajustar a janela de manutenção do corretor usando o AWS CLI

1. Use o CLI comando [update-broker](#) e especifique os parâmetros a seguir, conforme mostrado no exemplo.
 - `--broker-id` — O ID exclusivo que o Amazon MQ gera para o agente. Você pode analisar o ID do seu corretor ARN. Por exemplo, considerando o seguinte ARN, `arn:aws:mq:us-east-2:123456789012:broker:MyBroker:b-1234a5b6-78cd-901e-2fgh-3i45j6k17819`, o ID do corretor seria `b-1234a5b6-78cd-901e-2fgh-3i45j6k17819`.
 - `--maintenance-window-start-time` — Os parâmetros que determinam a hora de início da janela de manutenção semanal fornecida na estrutura a seguir.
 - `DayOfWeek` — O dia da semana, na sintaxe a seguir: `MONDAY | TUESDAY | WEDNESDAY | THURSDAY | FRIDAY | SATURDAY | SUNDAY`
 - `TimeOfDay` — A hora, no formato de 24 horas.
 - `TimeZone` — (Opcional) O fuso horário, no País/Cidade ou no formato de UTC deslocamento. Definida como UTC por padrão.

```
aws mq update-broker --broker-id broker-id \  
--maintenance-window-start-time DayOfWeek=SUNDAY,TimeOfDay=13:00,TimeZone=America/  
Los_Angeles
```

2. (Opcional) Use o CLI comando [describe-broker](#) para verificar se a janela de manutenção foi atualizada com êxito.

```
aws mq describe-broker --broker-id broker-id
```

Agende a janela de manutenção do corretor usando o Amazon MQ API

Para ajustar a janela de manutenção do corretor usando o Amazon MQ API

1. Use a [UpdateBroker](#) API operação. Especifique `broker-id` como um parâmetro de caminho. Os exemplos a seguir pressupõem um agente na região `us-west-2`. Para ter mais informações sobre os endpoints do Amazon MQ disponíveis, consulte [Endpoints e cotas do Amazon MQ](#) na Referência geral da AWS.

```
PUT /v1/brokers/broker-id HTTP/1.1
Host: mq.us-west-2.amazonaws.com
Date: Wed, 7 July 2021 12:00:00 GMT
x-amz-date: Wed, 7 July 2021 12:00:00 GMT
Authorization: authorization-string
```

Use o parâmetro `maintenanceWindowStartTime` e o tipo de recurso [WeeklyStartTime](#) na carga útil da solicitação.

```
{
  "maintenanceWindowStartTime": {
    "dayOfWeek": "SUNDAY",
    "timeZone": "America/Los_Angeles",
    "timeOfDay": "13:00"
  }
}
```

2. (Opcional) Use a [DescribeBroker](#) API operação para verificar se a janela de manutenção foi atualizada com êxito. `broker-id` é especificado como um parâmetro de caminho.

```
GET /v1/brokers/broker-id HTTP/1.1
Host: mq.us-west-2.amazonaws.com
Date: Wed, 7 July 2021 12:00:00 GMT
x-amz-date: Wed, 7 July 2021 12:00:00 GMT
Authorization: authorization-string
```

Atualizando uma versão do mecanismo de agente do Amazon MQ

O Amazon MQ fornece regularmente novas versões de mecanismos de corretagem para todos os tipos de mecanismos de corretagem compatíveis. As novas versões do mecanismo incluem patches de segurança, correções de bugs e outras melhorias no mecanismo do corretor.

O Amazon MQ organiza os números de versão de acordo com a especificação semântica de controle de versão como. X.Y.Z Nas implementações do Amazon MQ, X indica a versão principal, Y representa a versão secundária e Z indica o número da versão do patch. Existem dois tipos de atualizações:

- Atualização da versão principal: ocorre quando os números de versão do mecanismo principal mudam. Por exemplo, a atualização da versão 1.0 para a versão 2.0 é considerada uma atualização de versão principal.
- Atualização de versão secundária: ocorre quando apenas os números de versão secundários do mecanismo mudam. Por exemplo, atualizando a partir da versão 1.5 até a versão 1.6 é considerado um pequeno upgrade de versão.

Você pode atualizar manualmente seu corretor a qualquer momento para a próxima versão principal ou secundária compatível. Quando você ativa as [atualizações automáticas de versões secundárias](#), o Amazon MQ atualiza seu corretor para a versão de patch mais recente compatível. [Para todos os corretores que usam a versão 3.13 e superior do mecanismo, o Amazon MQ gerencia as atualizações para a versão de patch mais recente suportada durante a janela de manutenção.](#) O Amazon MQ atualiza seu corretor para a próxima versão secundária quando a versão secundária atual chega ao fim do suporte. As atualizações de versões manuais e automáticas ocorrem durante a janela de manutenção agendada ou depois de [reiniciar seu agente](#).

Os tópicos a seguir descrevem como você pode atualizar manualmente a versão do mecanismo do agente e ativar atualizações automáticas de versões secundárias.

Tópicos

- [Atualizar manualmente a versão do mecanismo](#)
- [Atualizar automaticamente a versão do mecanismo espelho](#)

Atualizar manualmente a versão do mecanismo

Para atualizar manualmente a versão do mecanismo de um corretor para uma nova versão principal ou secundária, você pode usar o AWS Management Console AWS CLI, o ou o Amazon MQAPI.

AWS Management Console

Para atualizar a versão do mecanismo de um corretor usando o AWS Management Console

1. Faça login no [console do Amazon MQ](#).
2. No painel de navegação à esquerda, selecione Brokers (Agentes) e depois escolha o agente que você deseja atualizar na lista.
3. Na página de detalhes do agente, selecione Edit (Editar).
4. Em Especificações, para Versão do mecanismo de agente escolha o novo número de versão na lista suspensa.
5. Role até o final da página e selecione Programar modificações.
6. Em Programar modificações do agente, para Quando aplicar modificações, escolha uma das seguintes opções.
 - Selecione After the next reboot (Depois da próxima reinicialização) se você quiser que o Amazon MQ conclua a atualização da versão durante a próxima janela de manutenção programada.
 - Selecione Immediately (Imediatamente) se você quiser reiniciar o agente e atualizar a versão do mecanismo imediatamente.

Important

O agente estará offline durante a reinicialização.

7. Selecione Apply (Aplicar) para concluir a aplicação das alterações.

AWS CLI

Para atualizar a versão do mecanismo de um corretor usando o AWS CLI

1. Use o CLI comando [update-broker](#) e especifique os parâmetros a seguir, conforme mostrado no exemplo.

- `--broker-id` — O ID exclusivo que o Amazon MQ gera para o agente. Você pode analisar o ID do seu corretor ARN. Por exemplo, considerando o seguinte ARN, `arn:aws:mq:us-east-2:123456789012:broker:MyBroker:b-1234a5b6-78cd-901e-2fgh-3i45j6k17819`, o ID do corretor seria `b-1234a5b6-78cd-901e-2fgh-3i45j6k17819`.
- `--engine-version` — O número da versão do mecanismo para a qual o a atualização do mecanismo de agente será feita.

```
aws mq update-broker --broker-id broker-id --engine-version version-number
```

2. (Opcional) Use o CLI comando [reboot-broker](#) para reinicializar seu broker se você quiser atualizar a versão do mecanismo imediatamente.

```
aws mq reboot-broker --broker-id broker-id
```

Se você não quiser reiniciar seu agente e aplicar as alterações imediatamente, o Amazon MQ atualizará o agente durante a próxima janela de manutenção agendada.

Important

O agente estará offline durante a reinicialização.

Amazon MQ API

Para atualizar a versão do mecanismo de um corretor usando o Amazon MQ API

1. Use a [UpdateBroker](#) API operação. Especifique `broker-id` como um parâmetro de caminho. Os exemplos a seguir pressupõem um agente na região `us-west-2`. Para ter mais informações sobre os endpoints do Amazon MQ disponíveis, consulte [Endpoints e cotas do Amazon MQ](#) na Referência geral da AWS.

```
PUT /v1/brokers/broker-id HTTP/1.1
Host: mq.us-west-2.amazonaws.com
Date: Mon, 7 June 2021 12:00:00 GMT
x-amz-date: Mon, 7 June 2021 12:00:00 GMT
Authorization: authorization-string
```


Use o `engineVersion` na carga útil da solicitação para especificar o número da versão para a qual o agente será atualizado.

```
{
  "engineVersion": "engine-version-number"
}
```

2. (Opcional) Use a [RebootBroker](#) API para reinicializar seu broker, se quiser atualizar a versão do mecanismo imediatamente. `broker-id` é especificado como um parâmetro de caminho.

```
POST /v1/brokers/broker-id/reboot-broker HTTP/1.1
Host: mq.us-west-2.amazonaws.com
Date: Mon, 7 June 2021 12:00:00 GMT
x-amz-date: Mon, 7 June 2021 12:00:00 GMT
Authorization: authorization-string
```

Se você não quiser reiniciar seu agente e aplicar as alterações imediatamente, o Amazon MQ atualizará o agente durante a próxima janela de manutenção agendada.

 Important

O agente estará offline durante a reinicialização.

Atualizar automaticamente a versão do mecanismo espelho

Você pode controlar se a atualização automática da versão secundária é ativada para um agente quando você cria o agente pela primeira vez ou modificando as preferências do agente. Para ativar atualizações automáticas de versões secundárias para uma corretora existente, você pode usar o AWS Management Console, o AWS CLI, ou o Amazon API MQ.

AWS Management Console

Para ativar atualizações automáticas de versões secundárias usando o AWS Management Console

1. Faça login no [console do Amazon MQ](#).
2. No painel de navegação à esquerda, selecione **Brokers (Agentes)** e depois escolha o agente que você deseja atualizar na lista.

3. Na página de detalhes do agente, selecione Edit (Editar).
4. Em Maintenance (Manutenção), escolha Enable automatic minor version upgrades (Ativar atualizações automáticas de versões secundárias).

 Note

Se a opção já estiver selecionada, você não precisará fazer nenhuma alteração.

5. Escolha Salvar (Save) na parte inferior da página.

AWS CLI

Para ativar atualizações automáticas de versões secundárias por meio do AWS CLI, use o CLI comando [update-broker](#) e especifique os parâmetros a seguir.

- `--broker-id` — O ID exclusivo que o Amazon MQ gera para o agente. Você pode analisar o ID do seu corretor ARN. Por exemplo, considerando o seguinte ARN, `arn:aws:mq:us-east-2:123456789012:broker:MyBroker:b-1234a5b6-78cd-901e-2fgh-3i45j6k17819`, o ID do corretor seria `b-1234a5b6-78cd-901e-2fgh-3i45j6k17819`.
- `--auto-minor-version-upgrade` — Ativa a opção Atualização automática da versão secundária.

```
aws mq update-broker --broker-id broker-id --auto-minor-version-upgrade
```

Se você quiser desativar as atualizações automáticas de versão secundárias para o seu agente, use o parâmetro `--no-auto-minor-version-upgrade`.

Amazon MQ API

Para ativar atualizações automáticas de versões secundárias por meio do Amazon API MQ, use [UpdateBroker](#) API a operação. Especifique `broker-id` como um parâmetro de caminho. O exemplo a seguir pressupõe um agente na região `us-west-2`. Para ter mais informações sobre os endpoints do Amazon MQ disponíveis, consulte [Endpoints e cotas do Amazon MQ](#) na Referência geral da AWS.

```
PUT /v1/brokers/broker-id HTTP/1.1  
Host: mq.us-west-2.amazonaws.com
```



```
Date: Mon, 7 June 2021 12:00:00 GMT
x-amz-date: Mon, 7 June 2021 12:00:00 GMT
Authorization: authorization-string
```

Use a propriedade `autoMinorVersionUpgrade` na carga útil da solicitação para ativar a atualização automática da versão secundária.

```
{
  "autoMinorVersionUpgrade": "true"
}
```

Se quiser desativar as atualizações automáticas de versão secundárias para o seu agente, defina `"autoMinorVersionUpgrade": "false"` na carga útil da solicitação.

Status de corretor Amazon MQ

A condição atual do agente é indicada por um status. A tabela a seguir lista os status de um agente Amazon MQ.

Console	API	Descrição
Falha na criação	CREATION_FAILED	Não foi possível criar o agente.
Criação em andamento	CREATION_IN_PROGRESS	O agente está sendo criado no momento.
Exclusão em andamento	DELETION_IN_PROGRESS	O agente está sendo excluído no momento.
Reinicialização em andamento	REBOOT_IN_PROGRESS	O agente está sendo reinicializado no momento.
Running	RUNNING	O agente está funcionando.
Ação crítica obrigatória	CRITICAL_ACTION_REQUIRED	O agente está em execução, mas se encontra em um estado degradado e exige ação imediata. Você pode

Console	API	Descrição
		encontrar instruções para resolver o problema selecionando o código de ação necessário na lista em Solução de problemas .

Listar os agentes do Amazon MQ e visualizar os detalhes dos agentes

Quanto você solicita que o Amazon MQ crie um agente, o processo de criação pode levar cerca de 15 minutos.

O exemplo a seguir mostra como confirmar a existência do agente listando todos os agentes na região atual utilizando o AWS Management Console.

Para listar os agentes e visualizar os detalhes

1. Faça login no [console do Amazon MQ](#).

Seus agentes na região atual são listados.

As informações a seguir são exibidas para cada agente:

- Nome
- Data de Criação
- [Status](#)
- Deployment mode (Modo de implementação)
- [Tipo de instância](#)

2. Escolha o nome do agente.

Para corretores ActiveMQ, no **MyBroker** página, os detalhes [configurados](#) são exibidos para o seu corretor:

Para corretores do Amazon MQ para RabbitMQ, você pode visualizar as configurações selecionadas no **MyBroker2** página, na seção Detalhes, conforme mostrado a seguir.

Abaixo da seção **Details** (Detalhes), são exibidas as seguintes informações:

- Na seção **Conexões**, para Amazon MQ for ActiveMQ, corretores ActiveMQ, o console web e os endpoints do protocolo de nível de fio. URL

Na seção **Conexões**, para Amazon MQ para corretores RabbitMQ, o console web e o endpoint seguro. URL AMQP

- Para agentes do Amazon MQ para ActiveMQ, na sessão **Usuários**, os [usuários](#) associados com o agente

Important

O gerenciamento de usuários por meio do AWS Management Console e do Amazon MQ não API é suportado pelos corretores Amazon MQ for RabbitMQ.

Acessando o console web do Amazon MQ broker sem acessibilidade pública

Se você desativar a acessibilidade pública do seu corretor, deverá executar as etapas a seguir para acessar o console web do corretor.

Pré-requisitos

Para executar as etapas a seguir, você deve configurar o seguinte:

- VPCs
 - O VPC sem um gateway de internet, ao qual o agente Amazon MQ está conectado, chamado `private-vpc`
 - Um segundo VPC, com um gateway de internet, chamado `public-vpc`.
 - Ambos VPCs devem estar conectados (por exemplo, usando [VPC peering](#)) para que as EC2 instâncias da Amazon no público VPC possam se comunicar com as EC2 instâncias no privado VPC.
 - Se você usa VPC emparelhamento, as tabelas de rotas de ambos VPCs devem ser configuradas para a conexão de emparelhamento.
- Grupos de segurança

- O grupo de segurança costumava criar o agente do Amazon MQ, chamado `private-sg`.
- Um segundo grupo de segurança usado para a EC2 instância no `public-vpcVPC`, chamado `public-sg`.
- `private-sg` deve permitir conexões de entrada de `public-sg`. Recomendamos restringir esse grupo de segurança à porta 8162 para o ActiveMQ e à porta 443 para o RabbitMQ.
- `public-sg` deve permitir conexões de entrada da sua máquina na porta 22.

Para acessar o console web de um agente Amazon MQ sem acessibilidade pública

1. Crie uma EC2 instância Linux em `public-vpc` (com um IP público, se necessário).
2. Para verificar se você VPC está configurado corretamente, estabeleça uma `ssh` conexão com a EC2 instância e use o `curl` comando com o URI do seu broker.
3. Na sua máquina, crie um `ssh` túnel para a EC2 instância usando o caminho para seu arquivo de chave privada e o endereço IP da sua EC2 instância pública. Por exemplo:

```
ssh -i ~/.ssh/id_rsa -N -C -q -f -D 8080 ec2-user@203.0.113.0
```

Um servidor de proxy de encaminhamento é iniciado em sua máquina.

4. Instale um cliente proxy, como [FoxyProxy](#) em sua máquina.
5. Configure seu cliente proxy usando as seguintes configurações:
 - Para o tipo de proxy, especifique `SOCKS5`.
 - Para endereço IP, DNS nome e nome do servidor, especifique `localhost`.
 - Para a porta, especifique `8080`.
 - Remova todos os URL padrões existentes.
 - Para o URL padrão, especifique `*.mq.*.amazonaws.com*`
 - Para o tipo de conexão, especifique `HTTP(S)`.

Quando você habilita seu cliente proxy, é possível acessar o Console da Web em sua máquina.

Reinicializar um agente do Amazon MQ

Para aplicar uma nova configuração a um agente, você pode reiniciá-lo.

Note

Se o agente do ActiveMQ não responder, você poderá reiniciá-lo para fazer a recuperação de um estado com defeito.

O exemplo a seguir mostra como reiniciar um agente do Amazon MQ utilizando o AWS Management Console.

Para reinicializar um agente do Amazon MQ

1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, escolha o nome do seu corretor (por exemplo, MyBroker).
3. Sobre o **MyBroker** página, escolha Ações, Reinicialize o corretor.

Important

Os agentes de instância única ficarão offline durante a reinicialização. Os agentes de cluster estarão disponíveis, mas os nós serão reinicializados um por vez.

4. Na caixa de diálogo Reboot broker, escolha Reboot.

A reinicialização de um operador leva cerca de 5 minutos. Se a reinicialização incluir alterações no tamanho da instância ou for executada em um agente com alta profundidade de fila, o processo de reinicialização poderá levar mais tempo.

Excluindo um agente do Amazon MQ

Se você não usa um agente do Amazon MQ (e não prevê usá-lo em um futuro próximo), é uma prática recomendada excluí-lo do Amazon MQ para reduzir seus custos. AWS

O exemplo a seguir mostra como excluir um agente utilizando o AWS Management Console.

Excluindo um agente do Amazon MQ

1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, selecione seu corretor (por exemplo MyBroker) e escolha Excluir.
3. Na opção Excluir **MyBroker?** caixa de diálogo, digite delete e escolha Excluir.

A exclusão de um agente leva cerca de 5 minutos.

Tipos de instância do agente Amazon MQ

A descrição combinada da instância do agente classe (m5, t3) e tamanho (large, micro) é um tipo de instância de agente (por exemplo, mq.m5.large). A tabela a seguir lista os tipos de instância de agente do Amazon MQ disponíveis para cada tipo de mecanismo compatível.

Tópicos

- [Tipos de instância do Amazon MQ para ActiveMQ](#)
- [Amazon MQ para tipos de instância RabbitMQ](#)

Tipos de instância do Amazon MQ para ActiveMQ

Important

Você pode usar a Amazon EBS somente com a família de tipos de instância do mq.m5 broker. Para obter mais informações, consulte [Storage](#).

Tipo de instância	v CPU	Memória (GiB)	Performance de rede	Uso recomendado
mq.t2.micro	1	1	Baixo	Avaliação
mq.t3.micro	2	1	Baixo	Avaliação
mq.m4.large	2	8	Moderada	Produção
mq.m5.large	2	8	Alta	Produção

Tipo de instância	v CPU	Memória (GiB)	Performance de rede	Uso recomendado
mq.m5.xlarge	4	16	Alta	Produção
mq.m5.2xlarge	8	32	Alta	
mq.m5.4xlarge	16	64	Alta	


Para obter mais informações sobre considerações em relação à taxa de transferência, consulte [Selecionar o tipo de instância de agente correto para obter a melhor taxa de transferência.](#)

Amazon MQ para tipos de instância RabbitMQ

Important

Não é possível fazer downgrade de um agente de um tipo de instância mq.m5. para um tipo de instância mq.t3.micro.

Tipo de instância	v CPU	Memória (GiB)	Performance de rede	Caso de uso
mq.t3.micro	2	1	Baixo	Avaliação

 Important

O tipo de instância mq.t3.micro não é compatível com a

Tipo de instância	v CPU	Memória (GiB)	Performance de rede	Caso de uso
				implantação de cluster.
mq.m5.large	2	8	Alta	Produção
mq.m5.xlarge	4	16	Alta	Produção
mq.m5.2xlarge	8	32	Alta	
mq.m5.4xlarge	16	64	Alta	

Adicionar tags aos recursos do Amazon MQ

Para organizar e identificar seus recursos do Amazon MQ para alocação de custo, você pode adicionar etiquetas de metadados que identificam um objetivo ou configuração de um agente. Isso é especialmente útil quando você tem vários agentes. Você pode usar etiquetas de alocação de custos para organizar sua AWS fatura de forma a refletir sua própria estrutura de custos. Para fazer isso, inscreva-se para receber a fatura AWS da sua conta e incluir as chaves e os valores da tag. Para obter mais informações, consulte [Configuração de um relatório de alocação de custos mensal](#) no Manual do usuário do AWS Billing .

Por exemplo, você pode adicionar etiquetas que representam o centro de custos e o objetivo dos seus recursos do Amazon MQ:

Recurso	Chave	Valor
Broker1	Cost Center	34567
	Stack	Production

Recurso	Chave	Valor
Broker2	Cost Center	34567
	Stack	Production
Broker3	Cost Center	12345
	Stack	Development

Esse esquema de marcação permite que você agrupe dois agentes executando tarefas relacionadas no mesmo centro de custo e, ao mesmo tempo, etiquetar um agente não relacionado com outra etiqueta de alocação de custo.

Adicionar tags no console do Amazon MQ

Você pode adicionar tags rapidamente aos recursos que você está criando no console do Amazon MQ seguindo estas etapas:

1. Na página Criar um agente, selecione Configurações adicionais.
2. Em Tags, selecione Adicionar tag.
3. Insira um par de chave e valor.
4. (Opcional) Selecione Adicionar tag para adicionar várias tags ao agente.
5. Selecione Criar agente.

Para adicionar tags ao criar uma configuração:

1. Na página Criar configuração, selecione Avançado.
2. Em Tags na página Criar configuração, selecione Adicionar tag.
3. Insira um par de chave e valor.
4. (Opcional) Selecione Adicionar tag para adicionar várias tags à sua configuração.
5. Selecione Criar configuração.

Depois de adicionar tags, você pode visualizar, editar e remover as tags de seus recursos no console do Amazon MQ. Você também pode ver as tags dos seus recursos usando REST API o. Para obter mais informações, consulte a Referência do [Amazon MQ REST API](#).

Usando o Amazon MQ para ActiveMQ

O Amazon MQ facilita a criação de um agente de mensagem com os recursos de processamento e armazenamento que atendem às suas necessidades. Você pode criar, gerenciar e excluir corretores usando o AWS Management Console, Amazon REST API MQ ou o AWS Command Line Interface.

Os agentes do Amazon MQ para ActiveMQ podem ser implantados como agentes de instância única ou corretores ativos/em espera. Para ambos os modos de implantação, o Amazon MQ oferece alta durabilidade armazenando seus dados de forma redundante.

Note

O Amazon MQ usa o [Apache KahaDB](#) como seu armazenamento de dados. Outros armazenamentos de dados, como JDBC e LevelDB, não são suportados.

Você pode acessar seus corretores usando [qualquer linguagem de programação compatível com o ActiveMQ](#) e TLS habilitando explicitamente os seguintes protocolos:

- [AMQP](#)
- [MQTT](#)
- MQTTterminado [WebSocket](#)
- [OpenWire](#)
- [STOMP](#)
- STOMPterminado WebSocket

Para saber mais sobre o Amazon MQ REST APIs, consulte a Referência do [Amazon REST API MQ](#).

Amazon MQ para corretores ActiveMQ

O que é um corretor Amazon MQ for ActiveMQ?

Um agente é um ambiente de agente de mensagens em execução no Amazon MQ. É o bloco de criação básico do Amazon MQ. A descrição combinada da classe (m5, t3) e do tamanho (large, micro) da instância do agente é um Tipo de instância de agente (por exemplo, mq.m5.large). Para obter mais informações, consulte [Broker instance types](#).

- Um agente de instância única é composto por um agente em uma Zona de disponibilidade. O corretor se comunica com seu aplicativo e com um volume de EFS armazenamento da Amazon EBS ou da Amazon.
- Uma agente ativo/em espera é composto por dois agentes em duas zonas de disponibilidade diferentes, configuradas em um Par redundante. Esses corretores se comunicam de forma síncrona com seu aplicativo e com a Amazon. EFS

Para obter mais informações, consulte [Opções de implantação do Amazon MQ para agentes ActiveMQ](#).

É possível habilitar as atualizações secundárias de versão automáticas para novas versões secundárias do mecanismo de agente à medida que o Apache lança novas versões. As atualizações automáticas ocorrem durante a janela de manutenção definida pelo dia da semana, a hora do dia (no formato de 24 horas) e o fuso horário (UTC por padrão).

Para obter informações sobre a criação e o gerenciamento de agentes, consulte o seguinte:

- [Começando: Criando e conectando-se a um corretor ActiveMQ](#)
- [Operadores](#)
- [Broker statuses](#)

Protocolos de nível de conexão compatíveis

Você pode acessar seus corretores usando [qualquer linguagem de programação compatível com o ActiveMQ](#) e TLS habilitando explicitamente os seguintes protocolos:


- [AMQP](#)
- [MQTT](#)
- MQTTterminado [WebSocket](#)
- [OpenWire](#)
- [STOMP](#)
- STOMPterminado WebSocket

Atributos

Um agente ActiveMQ tem vários atributos, por exemplo:


- Um nome (MyBroker)
- Um ID (b-1234a5b6-78cd-901e-2fgh-3i45j6k17819)
- Um nome de recurso da Amazon (ARN) (arn:aws:mq:us-east-2:123456789012:broker:MyBroker:b-1234a5b6-78cd-901e-2fgh-3i45j6k17819)
- Um ActiveMQ Web Console () URL `https://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:8162`

Para obter mais informações, consulte o [console da Web](#) na documentação do Apache ActiveMQ.

 Important

Se você especificar um mapa de autorização que não inclua o `activemq-webconsole`, você não poderá usar o Console da Web do ActiveMQ porque o grupo não estará autorizado a enviar mensagens ou receber mensagens do agente do Amazon MQ.

- Endpoints de protocolos de nível de conexão:
 - `amqp+ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:5671`
 - `mqtt+ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:8883`
 - `ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:61617`

 Note

Esse é um OpenWire ponto final.

- `stomp+ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:61614`
- `wss://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:61619`

Para obter mais informações, consulte [Configuração de transportes](#) na documentação do Apache ActiveMQ.

Note

Para um agente ativo/em espera, o Amazon MQ fornece dois ActiveMQ Web Console URLs, mas somente um está ativo por vez. URL Da mesma forma, o Amazon MQ fornece dois endpoints para cada protocolo de nível de conexão, mas apenas um endpoint está ativo em cada par de cada vez. Os sufixos -1 e -2 denotam um par redundante.

Para obter uma lista completa dos atributos do agente, consulte o seguinte na Referência do Amazon MQ: REST API

- [RESTID da operação: Corretor](#)
- [RESTID da operação: Corretores](#)
- [RESTID da operação: Broker Reboot](#)

Usuários do Broker

Um usuário do ActiveMQ é uma pessoa ou uma aplicação que pode acessar as filas e tópicos de um agente ActiveMQ. Você pode configurar usuários para que tenham permissões específicas. Por exemplo, é possível permitir que alguns usuários acessem o [Console da Web ActiveMQ](#).

Um grupo é um rótulo semântico. Você pode atribuir um grupo a um usuário e configurar permissões para grupos para enviar, receber e administrar filas e tópicos específicos.

Important

Fazer alterações em um usuário não aplica as alterações ao usuário imediatamente. Para aplicar as alterações, você deve aguardar a próxima janela de manutenção ou [reiniciar o agente](#).

Para obter informações sobre usuários e grupos, consulte a documentação do Apache ActiveMQ a seguir:

- [Autorização](#)
- [Exemplo de autorização](#)

Para obter informações sobre a criação, edição e exclusão de usuários do ActiveMQ, consulte o seguinte:

- [Criando um usuário do ActiveMQ broker](#)
- [Usuários](#)

Atributos do usuário

Para obter uma lista completa dos atributos do usuário, consulte o seguinte na Referência do Amazon MQ: REST API

- [RESTID da operação: Usuário](#)
- [RESTID da operação: Usuários](#)

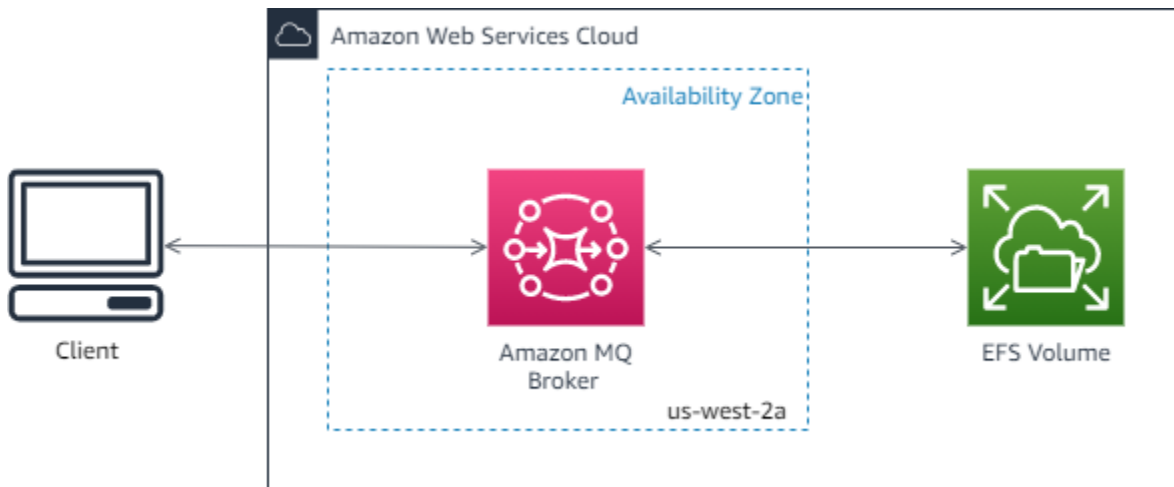
Opções de implantação do Amazon MQ para agentes ActiveMQ

O Amazon MQ oferece opções de implantação de instância única e cluster para corretores.

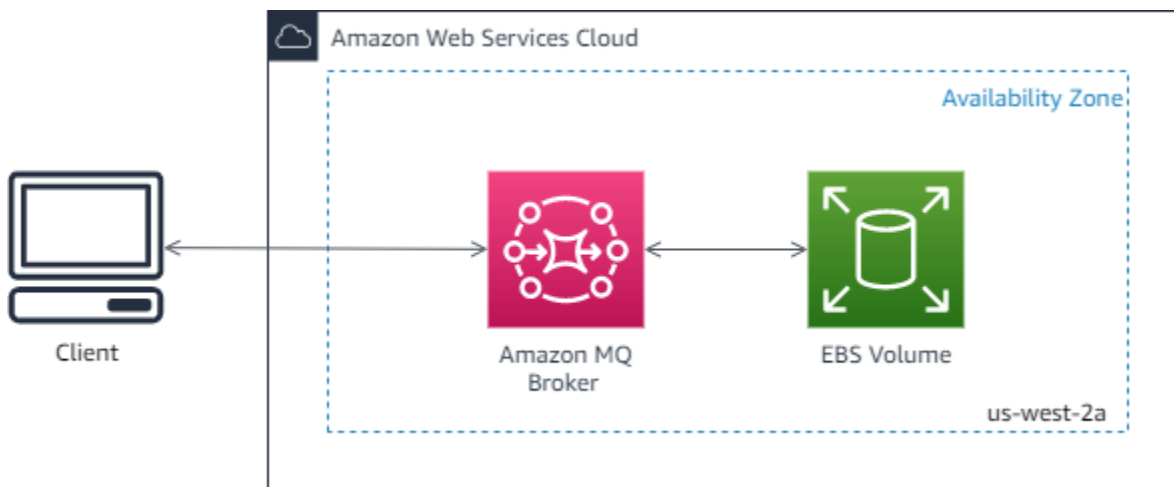
Opção 1: corretores de instância única do Amazon MQ

Um agente de instância única é composto por um agente em uma Zona de disponibilidade. O corretor se comunica com seu aplicativo e com um volume de EFS armazenamento da Amazon EBS ou da Amazon. Os volumes EFS de armazenamento da Amazon são projetados para fornecer o mais alto nível de durabilidade e disponibilidade, armazenando dados de forma redundante em várias zonas de disponibilidade (AZs). EBSA Amazon fornece armazenamento em nível de bloco otimizado para baixa latência e alta taxa de transferência. Para obter mais informações sobre opções de armazenamento, consulte [Storage](#).

O diagrama a seguir ilustra um agente de instância única com EFS armazenamento da Amazon replicado em várias. AZs



O diagrama a seguir ilustra um agente de instância única com EBS armazenamento da Amazon replicado em vários servidores em uma única AZ.



Opção 2: corretores ativos/em espera do Amazon MQ para alta disponibilidade

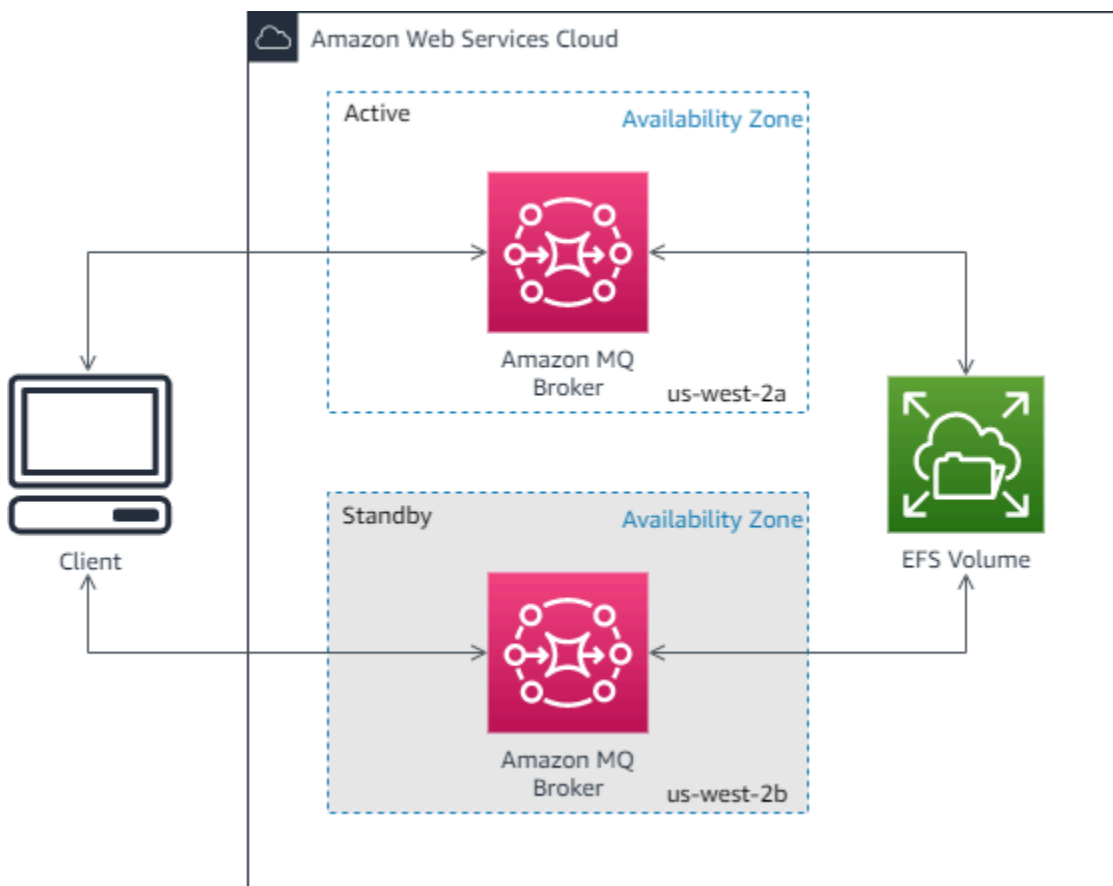
Uma agente ativo/em espera é composto por dois agentes em duas zonas de disponibilidade diferentes, configuradas em um Par redundante. Esses corretores se comunicam de forma síncrona com seu aplicativo e com a Amazon. EFS Os volumes EFS de armazenamento da Amazon são projetados para fornecer o mais alto nível de durabilidade e disponibilidade, armazenando dados de forma redundante em várias zonas de disponibilidade (AZs). Para obter mais informações, consulte [Storage](#).

Geralmente, apenas uma das instâncias do agente está sempre ativa, enquanto a outra está em espera. Se uma das instâncias do agente apresentar um defeito ou for submetida à manutenção, o Amazon MQ levará pouco tempo para tirar de serviço a instância inativa. Isso permite que a instância

em espera saudável se torne ativa e comece a aceitar comunicações recebidas. Quando você reinicia um operador, o failover leva apenas alguns segundos.

Para um agente ativo/em espera, o Amazon MQ fornece dois ActiveMQ Web Console URLs, mas somente um está ativo por vez. URL Da mesma forma, o Amazon MQ fornece dois endpoints para cada protocolo de nível de conexão, mas apenas um endpoint está ativo em cada par de cada vez. Os sufixos -1 e -2 denotam um par redundante. Para endpoints de protocolo de nível de conexão, você pode permitir que sua aplicação se conecte a qualquer endpoint usando o [Transporte de failover](#).

O diagrama a seguir ilustra um agente ativo/em espera com armazenamento da EFS Amazon replicado em vários. AZs



Rede de corretores Amazon MQ

O Amazon MQ é compatível com o recurso da rede de agentes do ActiveMQ.

A rede de agentes é composta por vários agentes ativos simultaneamente, [agentes de instância única](#) ou [agentes ativos/em espera](#). Você pode configurar redes de corretores em uma variedade

de [topologias](#) (por exemplo, concentrador hub-and-spokes, árvore ou malha), dependendo das necessidades do seu aplicativo, como alta disponibilidade e escalabilidade. Por exemplo, uma rede [hub-and-spokes](#) (hub-e-raios) de agentes pode aumentar a resiliência, preservando mensagens se um agente não estiver acessível. Uma rede de agentes com uma topologia de [concentrador](#) pode coletar mensagens de um número maior de agentes que aceitam mensagens recebidas, e concentrá-las em agentes mais centrais, para lidar melhor com a carga de muitas mensagens recebidas.

Para obter um tutorial e informações detalhadas de configuração, consulte o seguinte:

- [Creating and Configuring a Network of Brokers](#)
- [Configurar sua rede de agentes corretamente](#)
- [networkConnector](#)
- [networkConnectionStartAssíncrono](#)
- [Redes de agentes](#) na documentação do ActiveMQ

Veja a seguir os benefícios de usar uma rede de agentes:

- A criação de uma rede de agentes permite aumentar a taxa de transferência agregada e contagem máxima da conexão de produtor e consumidor, adicionando instâncias de agente.
- Você pode garantir melhor disponibilidade, permitindo que os produtores e os consumidores estejam cientes de várias instâncias de agente ativas. Isso permite que eles se reconectem a uma nova instância se aquela a qual estiverem conectados no momento se tornar indisponível.
- Como os produtores e os consumidores podem se reconectar a outro nó na rede de agentes imediatamente, e como não há necessidade de esperar que uma instância de agente em espera seja promovida, a reconexão do cliente dentro de uma rede de agentes é mais rápida do que para um agente [ativo/em espera de alta disponibilidade](#).

Tópicos

- [Como funciona uma rede de agentes?](#)
- [Como uma rede de agentes lida com as credenciais?](#)
- [Esquemas de exemplo](#)
- [Topologias das redes de agentes](#)
- [Dentro da região](#)
- [Failover dinâmico com conectores de transporte](#)

Como funciona uma rede de agentes?

O Amazon MQ é compatível com o recurso de rede de agentes do ActiveMQ de diversas maneiras. Primeiro, você pode editar os parâmetros dentro de cada configuração do agente para criar uma rede de agentes, da mesma forma que faria com o ActiveMQ nativo. Em segundo lugar, o Amazon MQ tem modelos de amostra que são usados AWS CloudFormation para automatizar a criação de uma rede de corretores. Você pode implantar esses exemplos de esquemas diretamente no console do Amazon MQ, ou você pode editar os respectivos modelos AWS CloudFormation para criar suas próprias topologias e configurações.

Uma rede de agentes é estabelecida por meio da conexão de um agente com outro usando os conectores de rede. Depois de conectados, esses agentes fornecem o encaminhamento de mensagem. Por exemplo, se Broker1 estabelece um conector de rede com Broker2, as mensagens no Broker1 são encaminhadas para o Broker2 se houver um consumidor nesse agente para a fila ou tópico. Se o conector de rede for configurado como `duplex`, as mensagens também serão encaminhadas do Broker2 para o Broker1. Os conectores de rede são configurados na configuração do agente. Consulte [Amazon MQ Broker Configuration Parameters](#). Por exemplo, aqui está um exemplo de entrada do `networkConnector` em uma configuração de agente:

```
<networkConnectors>
  <networkConnector name="connector_1_to_2" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-
east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

Uma rede de agentes garante que as mensagens passem de uma instância de agente para outra, encaminhe mensagens apenas para instâncias de agente que têm consumidores correspondentes. Para o benefício de instâncias de agente adjacentes dentro da rede, o ActiveMQ envia mensagens para tópicos de aviso sobre como os produtores e consumidores se conectam e se desconectam da rede. Quando uma instância de agente recebe informações sobre um consumidor que consome de um destino específico, a instância de agente começa a encaminhar mensagens. Para obter mais informações, consulte [Tópicos de aviso](#) na documentação do ActiveMQ.

Como uma rede de agentes lida com as credenciais?

Para o agente A se conectar ao agente B em uma rede, o agente A deve usar credenciais válidas, como qualquer outro produtor ou consumidor. Em vez de fornecer uma senha em uma configuração do `<networkConnector>` do agente A, você deve primeiro criar um usuário no agente A com os mesmos valores como outro usuário no agente B (esses são usuários separados e exclusivos

que compartilham os mesmos valores de nome de usuário e senha). Quando você especifica o atributo `userName` na configuração do `<networkConnector>`, o Amazon MQ adicionará a senha automaticamente no tempo de execução.

⚠ Important

Não especifique o atributo `password` para o `<networkConnector>`. Não recomendamos armazenar senhas em texto simples nos arquivos de configuração do agente, porque isso torna as senhas visíveis no console do Amazon MQ. Para obter mais informações, consulte [Configure Network Connectors for Your Broker](#).

Os corretores devem estar no mesmo lugar VPC ou em paresVPCs. Para obter mais informações, consulte [Pré-requisitos](#) no tutorial [Creating and Configuring a Network of Brokers](#).

Esquemas de exemplo


Para começar a usar uma rede de agentes, o Amazon MQ fornece esquemas de exemplo. Esses exemplos de esquemas criam uma implantação da Rede de Corretores e todos os recursos relacionados usando, . AWS CloudFormation Os dois esquemas de exemplo disponíveis são:

1. Rede de malha de agentes de instância única
2. Rede de malha de agentes ativos/em espera

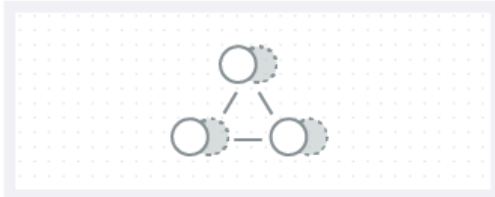
Sample blueprints for a network of brokers

Networks of brokers provide high availability and scalability, and are suitable for production workloads. These sample blueprints use AWS CloudFormation to automatically deploy a network of brokers in the specific topology. [Info](#)

Mesh network of single-instance brokers
Set of 3 single-instance brokers connected in a mesh network.



Mesh network of active/standby brokers
Set of 3 active/standby brokers connected in a mesh network. Each broker has automatic failover capability to a standby in another AZ.

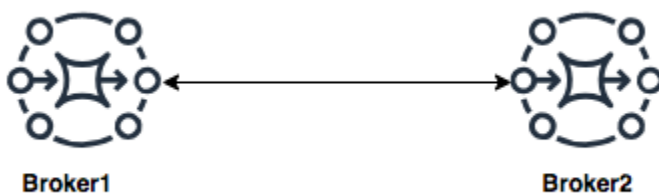


Na página Criar agentes, selecione um dos esquemas de exemplo e escolha Próximo. Assim que os recursos forem criados, revise os agentes gerados e suas configurações no console do Amazon MQ.

Ao criar agentes e configurar elementos `networkConnector` diferentes nas configurações de agente, você pode criar uma rede de agentes em muitas topologias diferentes. Para obter mais informações sobre como configurar uma rede de agentes, consulte [Redes de agentes](#) na documentação do ActiveMQ.

Topologias das redes de agentes

Ao implantar agentes e, em seguida, configurar entradas do `networkConnector` em suas configurações, você pode criar uma rede de agentes usando diferentes topologias de rede. Um conector de rede fornece o encaminhamento de mensagem sob demanda entre os agentes conectados. As conexões podem ser configuradas como duplex, nas quais as mensagens são encaminhadas de duas maneiras entre os agentes, ou não duplex, nas quais o encaminhamento apenas se propaga de um agente para o outro. Por exemplo, se uma conexão duplex entre o Broker1 e o Broker2, as mensagens serão encaminhadas de um para o outro se houver um consumidor.



Com um conector de rede duplex, as mensagens são encaminhadas de cada agente para o outro. Elas são encaminhadas sob demanda: se houver um consumidor no Broker2 para uma mensagem no Broker1, a mensagem será encaminhada. Da mesma forma, se houver um consumidor no Broker1 para uma mensagem no Broker2, a mensagem será encaminhada.

Para conexões não duplex, as mensagens são encaminhadas apenas de um agente para o outro. Neste exemplo, se houver um consumidor no Broker2 para uma mensagem no Broker1, a mensagem será encaminhada. Mas as mensagens não serão encaminhadas do Broker2 para o Broker1.



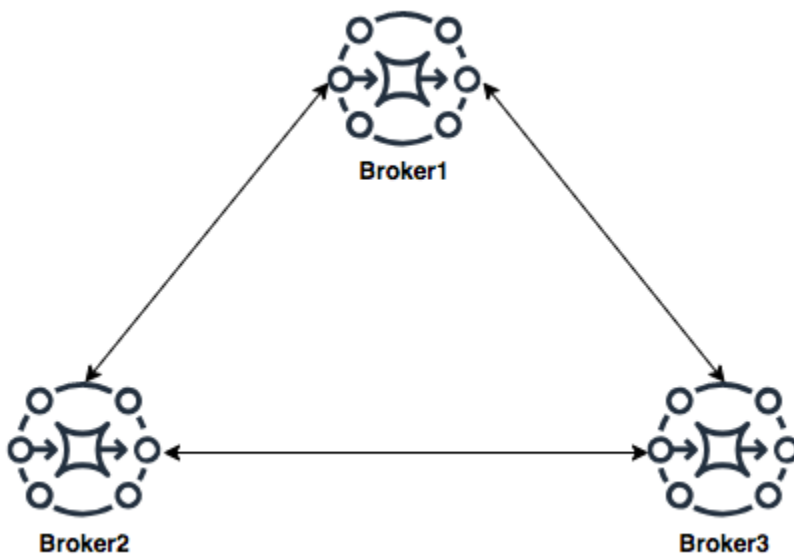
Usando os dois conectores de rede duplex e não duplex, é possível criar uma rede de agentes em qualquer número de topologias de rede.

Note

Em cada um dos exemplos de topologia de rede, os elementos do `networkConnector` fazem referência ao endpoint dos agentes aos quais eles se conectam. Substitua as entradas de endpoint do agente nos atributos `uri` com os endpoints dos seus agentes. Consulte [Listing brokers and viewing broker details](#).

Topologia de malha

Uma topologia de malha fornece vários agentes que estão conectados uns aos outros. Esse exemplo simples se conecta a três agentes de instância única, mas você pode configurar mais agentes como uma malha.



Essa topologia é uma que inclui uma malha de pares de agentes ativos/em espera, podem ser criadas usando esquemas de exemplo no console do Amazon MQ. Você pode criar essas implantações de esquemas de exemplo para ver uma rede de agentes funcionando e analisar como elas são configuradas.

Você pode configurar uma rede de malha de três agentes semelhante a essa adicionando um conector de rede ao Broker1 que faz conexões duplex com o Broker2 e o Broker3 e uma única conexão duplex entre o Broker2 e o Broker3.

Conectores de rede para o Broker1:

```
<networkConnectors>
  <networkConnector name="connector_1_to_2" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-987615k4-32ji-109h-8gfe-7d65c4b132a1-2.mq.us-
east-2.amazonaws.com:61617)"/>
  <networkConnector name="connector_1_to_3" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-743c885d-2244-4c95-af67-a85017ff234e-3.mq.us-
east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

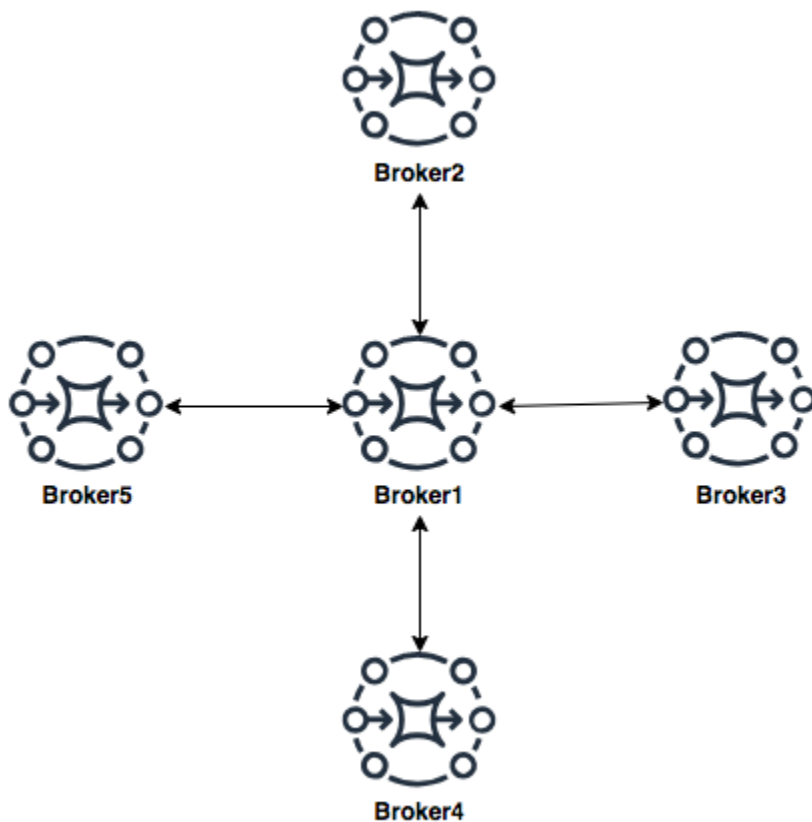
Conectores de rede para o Broker2:

```
<networkConnectors>
  <networkConnector name="connector_2_to_3" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-743c885d-2244-4c95-af67-a85017ff234e-3.mq.us-
east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

Ao adicionar os conectores acima às configurações do Broker1 e do Broker2, você pode criar uma malha entre esses três agentes que encaminha a mensagem entre todos os agentes sob demanda. Para obter mais informações, consulte [Amazon MQ Broker Configuration Parameters](#).

Topologia hub e spoke

Em uma topologia hub e spoke, as mensagens são preservadas se houver uma interrupção para qualquer agente em um raio. As mensagens são encaminhadas e apenas o Broker1 central é essencial para a operação da rede.



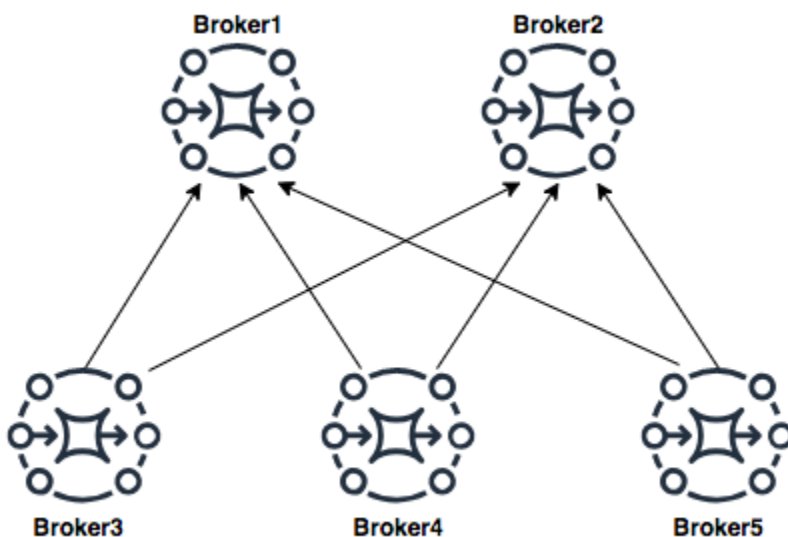
Para configurar a rede hub e spoke de agentes neste exemplo, você pode adicionar um `networkConnector` para cada um dos agentes nos raios da configuração do Broker1.

```
<networkConnectors>
  <networkConnector name="connector_hub_and_spoke_2" userName="myCommonUser"
duplex="true"
  uri="static:(ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
east-2.amazonaws.com:61617)"/>
  <networkConnector name="connector_hub_and_spoke_3" userName="myCommonUser"
duplex="true"
  uri="static:(ssl://b-9876l5k4-32ji-109h-8gfe-7d65c4b132a1-2.mq.us-
east-2.amazonaws.com:61617)"/>
  <networkConnector name="connector_hub_and_spoke_4" userName="myCommonUser"
duplex="true"
  uri="static:(ssl://b-743c885d-2244-4c95-af67-a85017ff234e-3.mq.us-
east-2.amazonaws.com:61617)"/>
  <networkConnector name="connector_hub_and_spoke_5" userName="myCommonUser"
duplex="true"
```

```
uri="static:(ssl://b-62a7fb31-d51c-466a-a873-905cd660b553-4.mq.us-east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

Topologia Concentrador

Nessa topologia de exemplo, os três agentes na parte inferior podem lidar com um grande número de conexões, e essas mensagens são concentradas para o Broker1 e o Broker2. Cada um dos outros agentes tem uma conexão não duplex com os agentes centrais. Para escalar a capacidade dessa topologia, você pode adicionar outros agentes para receberem mensagens e as concentrarem no Broker1 e no Broker2.



Para configurar essa topologia, cada um dos agentes na parte inferior conteria um conector de rede para cada um dos agentes para os quais estão concentrando as mensagens.

Conectores de rede para o Broker3:

```
<networkConnectors>
  <networkConnector name="3_to_1" userName="myCommonUser" duplex="false"
    uri="static:(ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-east-2.amazonaws.com:61617)"/>
  <networkConnector name="3_to_2" userName="myCommonUser" duplex="false"
    uri="static:(ssl://b-9876l5k4-32ji-109h-8gfe-7d65c4b132a1-2.mq.us-east-2.amazonaws.com:61617)"/>
</networkConnectors>
```


Conectores de rede para o Broker4:

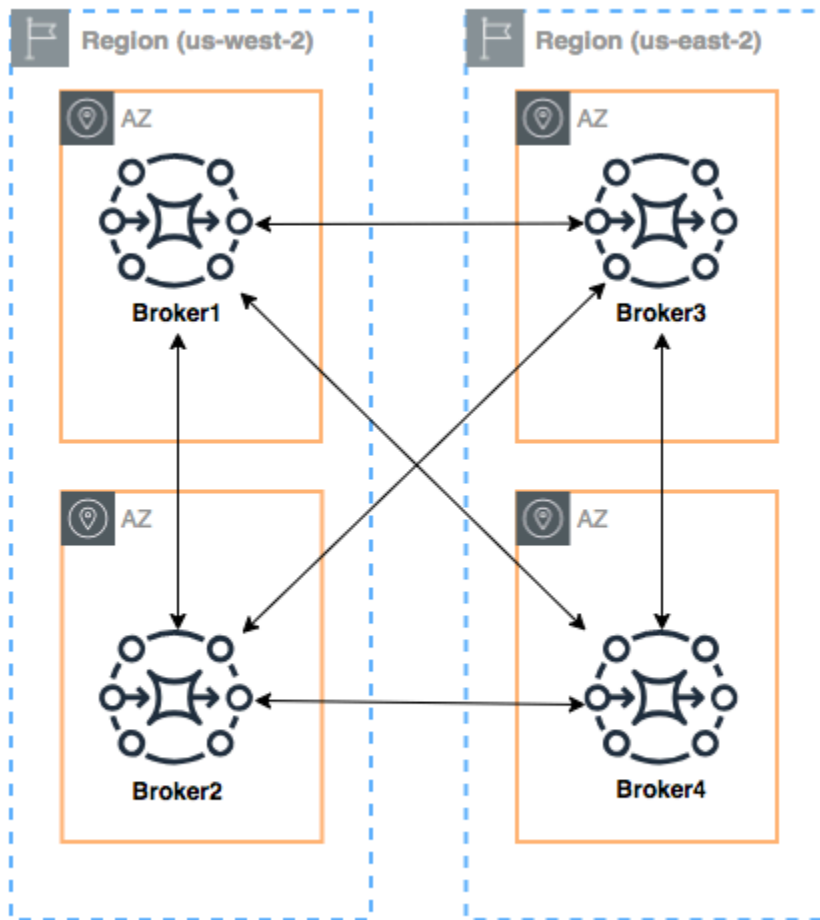
```
<networkConnectors>
  <networkConnector name="4_to_1" userName="myCommonUser" duplex="false"
    uri="static:(ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
east-2.amazonaws.com:61617)"/>
  <networkConnector name="4_to_2" userName="myCommonUser" duplex="false"
    uri="static:(ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

Conectores de rede para o Broker5:

```
<networkConnectors>
  <networkConnector name="5_to_1" userName="myCommonUser" duplex="false"
    uri="static:(ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
east-2.amazonaws.com:61617)"/>
  <networkConnector name="5_to_2" userName="myCommonUser" duplex="false"
    uri="static:(ssl://b-9876l5k4-32ji-109h-8gfe-7d65c4b132a1-2.mq.us-
east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

Dentro da região

Para configurar uma rede de corretores que abranja AWS regiões, implante corretores nessas regiões e configure conectores de rede para os endpoints desses corretores.



Para configurar uma rede de agentes, como nesse exemplo, você pode adicionar entradas do `networkConnectors` para as configurações do Broker1 e do Broker4 que fazem referência a endpoints de nível de conexão desses agentes.

Conectores de rede para o Broker1:

```
<networkConnectors>
  <networkConnector name="1_to_2" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-987615k4-32ji-109h-8gfe-7d65c4b132a1-2.mq.us-
east-2.amazonaws.com:61617)"/>
  <networkConnector name="1_to_3" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-743c885d-2244-4c95-af67-a85017ff234e-3.mq.us-
east-2.amazonaws.com:61617)"/>
  <networkConnector name="1_to_4" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-62a7fb31-d51c-466a-a873-905cd660b553-4.mq.us-
east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

```
</networkConnectors>
```

Conector de rede para o Broker2:

```
<networkConnectors>
  <networkConnector name="2_to_3" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-743c885d-2244-4c95-af67-a85017ff234e-3.mq.us-
east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

Conectores de rede para o Broker4:

```
<networkConnectors>
  <networkConnector name="4_to_3" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-743c885d-2244-4c95-af67-a85017ff234e-3.mq.us-
east-2.amazonaws.com:61617)"/>
  <networkConnector name="4_to_2" userName="myCommonUser" duplex="true"
    uri="static:(ssl://b-987615k4-32ji-109h-8gfe-7d65c4b132a1-2.mq.us-
east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

Failover dinâmico com conectores de transporte

Além de configurar elementos `networkConnector`, você pode configurar as opções `transportConnector` do agente para habilitar o failover dinâmico e para rebalancear as conexões quando os agentes são adicionados ou removidos da rede.

```
<transportConnectors>
  <transportConnector name="openwire" updateClusterClients="true"
    rebalanceClusterClients="true" updateClusterClientsOnRemove="true"/>
</transportConnectors>
```

Nesse exemplo, tanto `updateClusterClients` como `rebalanceClusterClients` estão definidos como `true`. Nesse caso, os clientes receberão uma lista de agentes da rede e solicitarão que eles façam um rebalanceamento se um novo agente ingressar.

Opções disponíveis:

- `updateClusterClients`: transmite informações aos clientes sobre alterações na rede de topologia do agente.

- `rebalanceClusterClients`: faz com que os clientes realizem um rebalanceamento em todos os agentes quando um agente novo é adicionado a uma rede de agentes.
- `updateClusterClientsOnRemove`: atualiza os clientes com informações sobre topologia quando um agente sai de uma rede de agentes.

Quando `updateClusterClients` é definido como `true` (verdadeiro), os clientes podem ser configurados para se conectarem a um único agente em uma rede de agentes.

```
failover:(ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:61617)
```

Quando um novo corretor se conectar, ele receberá uma lista URIs de todos os corretores da rede. Se a conexão com o agente falhar, ela poderá trocar de maneira dinâmica para um dos agentes fornecidos no momento da conexão.

Para obter mais informações sobre failover, consulte [Opções do lado do agente para failover](#) na documentação do ActiveMQ.

Configurações do agente do Amazon MQ para ActiveMQ

Uma configuração contém todas as configurações do seu broker ActiveMQ XML em formato (semelhante ao arquivo do ActiveMQ). `activemq.xml` Você pode criar uma configuração antes de criar qualquer agente. Em seguida, você pode aplicar a configuração a um ou mais agentes.

Important

Fazer alterações em uma configuração não aplica as alterações ao agente imediatamente. Para aplicar as alterações, você deve aguardar a próxima janela de manutenção ou [reiniciar o agente](#).

No momento, não é possível excluir uma configuração.

Atributos

A configuração de um agente tem vários atributos, por exemplo:

- Um nome (`MyConfiguration`)
- Um ID (`c-1234a5b6-78cd-901e-2fgh-3i45j6k17819`)

- Um nome de recurso da Amazon (ARN) (arn:aws:mq:us-east-2:123456789012:configuration:c-1234a5b6-78cd-901e-2fgh-3i45j6k17819)

Para obter uma lista completa dos atributos de configuração, consulte o seguinte na Referência do Amazon MQ: REST API

- [RESTID da operação: Configuração](#)
- [RESTID da operação: configurações](#)

Para obter uma lista completa de atributos de revisão de configuração, consulte o seguinte:

- [RESTID da operação: revisão de configuração](#)
- [RESTID da operação: revisões de configuração](#)

Usando arquivos de XML configuração do Spring

[Os corretores ActiveMQ são configurados usando arquivos Spring XML](#) É possível configurar vários aspectos do agente do ActiveMQ, como destinos pré-definidos, políticas de destino, políticas de autorização e plugins. O Amazon MQ controla alguns desses elementos de configuração, como transportes de rede e armazenamento. Outras opções de configuração, como a criação de redes de agentes, não são compatíveis atualmente.

O conjunto completo de opções de configuração suportadas está especificado nos esquemas do Amazon MQXML. Faça download de arquivos zip dos esquemas compatíveis usando os links a seguir.

- [amazon-mq-active-mq-5.18.4.xsd.zip](#)
- [amazon-mq-active-mq-5.17.6.xsd.zip](#)
- [amazon-mq-active-mq-5.16.7.xsd.zip](#)
- [amazon-mq-active-mq-5.15.16.xsd.zip](#)

Esses esquemas podem ser usados para validar e limpar seus arquivos de configuração. O Amazon MQ também permite que você forneça configurações por meio do upload de arquivos XML. Quando você carrega um XML arquivo, o Amazon MQ limpa e remove automaticamente parâmetros de configuração inválidos e proibidos de acordo com o esquema.

Note

Para os atributos, é possível usar apenas valores estáticos. O Amazon MQ limpa elementos e atributos que contenham expressões, variáveis e referências de elementos do Spring da configuração que você fez.

Criação de uma configuração do agente Amazon MQ para ActiveMQ

Uma configuração contém todas as configurações do seu broker ActiveMQ, XML em formato (semelhante ao arquivo do ActiveMQ). `activemq.xml` Você pode criar uma configuração antes de criar qualquer agente. Em seguida, você pode aplicar a configuração a um ou mais agentes. As configurações podem ser aplicadas imediatamente ou durante uma janela de manutenção.

Para obter mais informações, consulte as informações a seguir.

- [Amazon MQ Broker Configuration Parameters](#)

O exemplo a seguir mostra como criar e aplicar uma configuração de agente do Amazon MQ utilizando o AWS Management Console.

Tópicos

- [Criar uma configuração](#)
- [Criar uma revisão de configuração](#)
- [Aplicar uma revisão de configuração ao operador](#)

Criar uma configuração

Para criar uma nova configuração de agente, primeiro crie a nova configuração.


1. Faça login no [console do Amazon MQ](#).
2. Do lado esquerdo, expanda o painel de navegação e selecione Configurations (Configurações).

Amazon MQ ×

Brokers

Configurations

3. Na página Configurations (Configurações), selecione Create configuration (Criar configuração).
4. Na página Create configuration, na seção Details, digite o Configuration name (por exemplo, MyConfiguration) e selecione uma versão do Broker engine.

 Note


Para saber mais sobre as versões do mecanismo ActiveMQ compatíveis com o Amazon MQ para ActiveMQ, consulte [the section called “Gerenciamento de versão”](#).

5. Escolha Criar configuração.

Criar uma revisão de configuração

Depois de criar uma configuração de agente, você precisará editar a configuração usando uma revisão de configuração.


1. Na lista de configurações, escolha **MyConfiguration**.

 Note

A primeira revisão de configuração será sempre criada para você quando o Amazon MQ criar a configuração.

Sobre o **MyConfiguration** página, o tipo e a versão do mecanismo do broker que sua nova revisão de configuração usa (por exemplo, Apache ActiveMQ 5.15.16) são exibidos.

2. Na guia Detalhes da configuração, o número da revisão da configuração, a descrição e a configuração do broker em XML formato são exibidos.

 Note

Editar a configuração atual irá criar uma nova revisão da configuração.

Revision 1 Auto-generated default for MyBroker-configuration on ActiveMQ 5.15.0 Latest

Amazon MQ configurations support a limited subset of ActiveMQ properties. [Info](#)

```
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <broker xmlns="http://activemq.apache.org/schema/core">
3   <!--
4     A configuration contains all of the settings for your ActiveMQ broker, in XML format
     (similar to ActiveMQ's activemq.xml file).
5     You can create a configuration before creating any brokers. You can then apply the
     configuration to one or more brokers.
```

3. Escolha Editar configuração e faça alterações na XML configuração.
4. Escolha Salvar.

A caixa e diálogo Save revision (Salvar revisão) será exibida.

5. (Opcional) Tipo A description of the changes in this revision.
6. Escolha Salvar.

A nova revisão da configuração é salva.

⚠ Important

O console do Amazon MQ limpa automaticamente parâmetros de configuração inválidos e proibidos de acordo com um esquema. Para obter mais informações e uma lista completa dos XML parâmetros permitidos, consulte [Amazon MQ Broker Configuration Parameters](#).

Aplicar uma revisão de configuração ao operador

Depois de revisar a configuração, você pode aplicar a revisão da configuração ao seu broker.

1. Do lado esquerdo, expanda o painel de navegação e selecione Brokers (Agentes).

Amazon MQ ×

Brokers

Configurations

2. Na lista de corretores, selecione seu corretor (por exemplo MyBroker) e escolha Editar.
3. Na edição **MyBroker** página, na seção Configuração, selecione uma Configuração e uma Revisão e, em seguida, escolha Programar Modificações.
4. Na seção Schedule broker modifications (Programar modificações no operador), escolha se deseja aplicar as modificações During the next scheduled maintenance window (Durante a próxima janela de manutenção programada) ou Immediately (Imediatamente).

Important

O agente estará offline durante a reinicialização.

5. Selecione Apply (Aplicar).

Sua revisão de configuração será aplicada ao agente no horário especificado.

Editar uma revisão de configuração do Amazon MQ para ActiveMQ

Talvez você queira editar uma revisão de configuração depois de aplicá-la ao seu corretor. Use as instruções a seguir para editar uma revisão de configuração.

1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, selecione seu corretor (por exemplo MyBroker) e escolha Editar.
3. Sobre o **MyBroker** página, escolha Editar.
4. Na edição **MyBroker** página, na seção Configuração, selecione uma Configuração e uma Revisão e, em seguida, escolha Editar.

Note

A menos que você selecione uma configuração ao criar um agente, a primeira revisão de configuração será sempre criada para você quando o Amazon MQ criar o agente.

Sobre o **MyBroker** página, o tipo e a versão do mecanismo do broker que a configuração usa (por exemplo, Apache ActiveMQ 5.15.8) são exibidos.

- Na guia Detalhes da configuração, o número da revisão da configuração, a descrição e a configuração do broker em XML formato são exibidos.

Note

Editar a configuração atual irá criar uma nova revisão da configuração.

Revision 1 Auto-generated default for MyBroker-configuration on ActiveMQ 5.15.0 Latest

Amazon MQ configurations support a limited subset of ActiveMQ properties. [Info](#)

```

1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <broker xmlns="http://activemq.apache.org/schema/core">
3   <!--
4     A configuration contains all of the settings for your ActiveMQ broker, in XML format
4     (similar to ActiveMQ's activemq.xml file).
5     You can create a configuration before creating any brokers. You can then apply the
5     configuration to one or more brokers.

```

- Escolha Editar configuração e faça alterações na XML configuração.
- Escolha Salvar.

A caixa e diálogo Save revision (Salvar revisão) será exibida.

- (Opcional) Tipo A description of the changes in this revision.
- Escolha Salvar.

A nova revisão da configuração é salva.

Important

O console do Amazon MQ limpa automaticamente parâmetros de configuração inválidos e proibidos de acordo com um esquema. Para obter mais informações e uma lista completa dos XML parâmetros permitidos, consulte [Amazon MQ Broker Configuration Parameters](#).

Elementos permitidos nas configurações do Amazon MQ

Veja a seguir uma lista detalhada dos elementos permitidos nas configurações do Amazon MQ. Para obter mais informações, consulte [XMLConfiguração na documentação](#) do Apache ActiveMQ.

Elemento
<code>abortSlowAckConsumerStrategy</code> (atributos)
<code>abortSlowConsumerStrategy</code> (atributos)
<code>authorizationEntry</code> (atributos)
<code>authorizationMap</code> (elementos de conjunto de filhos)
<code>authorizationPlugin</code> (elementos de conjunto de filhos)
<code>broker</code> (atributos) (elementos de conjunto de filhos)
<code>cachedMessageGroupMapFactory</code> (atributos)
<code>compositeQueue</code> (atributos) (elementos de conjunto de filhos)
<code>compositeTopic</code> (atributos) (elementos de conjunto de filhos)
<code>constantPendingMessageLimitStrategy</code> (atributos)
<code>discarding</code> (atributos)
<code>discardingDLQBrokerPlugin</code> (atributos)
<code>fileCursor</code>
<code>fileDurableSubscriberCursor</code>
<code>fileQueueCursor</code>
<code>filteredDestination</code> (atributos)
<code>fixedCountSubscriptionRecoveryPolicy</code> (atributos)

Elemento

fixedSizedSubscriptionRecoveryPolicy [\(atributos\)](#)

forcePersistencyModeBrokerPlugin [\(atributos\)](#)

individualDeadLetterStrategy [\(atributos\)](#)

lastImageSubscriptionRecoveryPolicy

messageGroupHashBucketFactory [\(atributos\)](#)

mirroredQueue [\(atributos\)](#)

noSubscriptionRecoveryPolicy

oldestMessageEvictionStrategy [\(atributos\)](#)

oldestMessageWithLowestPriorityEvictionStrategy [\(atributos\)](#)

policyEntry [\(atributos\)](#) | [elementos de conjunto de filhos](#)

policyMap [\(elementos de conjunto de filhos\)](#)

prefetchRatePendingMessageLimitStrategy [\(atributos\)](#)

priorityDispatchPolicy

priorityNetworkDispatchPolicy

queryBasedSubscriptionRecoveryPolicy [\(atributos\)](#)

queue [\(atributos\)](#)

redeliveryPlugin [\(atributos\)](#) | [elementos de conjunto de filhos](#)

redeliveryPolicy [\(atributos\)](#)

redeliveryPolicyMap [\(elementos de conjunto de filhos\)](#)

retainedMessageSubscriptionRecoveryPolicy [\(elementos de conjunto de filhos\)](#)

Elemento`roundRobinDispatchPolicy``sharedDeadLetterStrategy` ([atributos](#) | [elementos de conjunto de filhos](#))`simpleDispatchPolicy``simpleMessageGroupMapFactory``statisticsBrokerPlugin``storeCursor``storeDurableSubscriberCursor` ([atributos](#))`strictOrderDispatchPolicy``tempDestinationAuthorizationEntry` ([atributos](#))`tempQueue` ([atributos](#))`tempTopic` ([atributos](#))`timedSubscriptionRecoveryPolicy` ([atributos](#))`timeStampingBrokerPlugin` ([atributos](#))`topic` ([atributos](#))`transportConnector` ([atributos](#))`uniquePropertyMessageEvictionStrategy` ([atributos](#))`virtualDestinationInterceptor` ([elementos de conjunto de filhos](#))`virtualTopic` ([atributos](#))`vmCursor``vmDurableCursor`

Elemento

vmQueueCursor


Elementos e atributos permitidos nas configurações do Amazon MQ

A seguinte é uma lista detalhada dos elementos e de seus atributos permitidos nas configurações do Amazon MQ. Para obter mais informações, consulte [XMLConfiguração na documentação](#) do Apache ActiveMQ.

Elemento	Atributo
abortSlowAckConsumerStrategy	abortConnection
	checkPeriod
	ignoreIdleConsumers
	ignoreNetworkConsumers
	maxSlowCount
	maxSlowDuration
	maxTimeSinceLastAck
	name
abortSlowConsumerStrategy	abortConnection
	checkPeriod
	ignoreNetworkConsumers
	maxSlowCount
	maxSlowDuration
	name

Elemento	Atributo
authorizationEntry	admin
	queue
	read
	tempQueue
	tempTopic
	topic
	write
broker	advisorySupport
	allowTempAutoCreationOnSend
	cacheTempDestinations
	consumerSystemUsagePortion
	dedicatedTaskRunner
	deleteAllMessagesOnStartup
	keepDurableSubsActive
	enableMessageExpirationOnActiveDurableSubs
	maxPurgedDestinationsPerSweep
	maxSchedulerRepeatAllowed
	monitorConnectionSplits
networkConnectorStartAsync	

Elemento	Atributo
	<code>offlineDurableSubscriberTaskSchedule</code>
	<code>offlineDurableSubscriberTimeout</code>
	<code>persistenceThreadPriority</code>
	<code>persistent</code>
	<code>populateJMSXUserID</code>
	<code>producerSystemUsagePortion</code>
	<code>rejectDurableConsumers</code>
	<code>rollbackOnlyOnAsyncException</code>
	<code>schedulePeriodForDestinationPurge</code>
	<code>schedulerSupport</code>
	<code>splitSystemUsageForProducersConsumers</code>
	<code>taskRunnerPriority</code>
	<code>timeBeforePurgeTempDestinations</code>
	<code>useAuthenticatedPrincipalForJMSXUserID</code>
	<code>useMirroredQueues</code>
	<code>useTempMirroredQueues</code>
	<code>useVirtualDestSubs</code>
	<code>useVirtualDestSubsOnCreation</code>


Elemento	Atributo
	useVirtualTopics
cachedMessageGroupMapFactory	cacheSize
compositeQueue	concurrentSend
	copyMessage
	forwardOnly
	name
	sendWhenNotMatched
compositeTopic	concurrentSend
	copyMessage
	forwardOnly
	name
	sendWhenNotMatched
conditionalNetworkBridgeFilterFactory	rateDuration
	rateLimit
	replayDelay
	replayWhenNoConsumers
	selectorAware
	<div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e1f5fe;">  Compatível com Apache ActiveMQ 5.16.x </div>

Elemento	Atributo
constantPendingMessageLimitStrategy	limit
discarding	deadLetterQueue
	enableAudit
	expiration
	maxAuditDepth
	maxProducersToAudit
	processExpired
	processNonPersistent
discardingDLQBrokerPlugin	dropAll
	dropOnly
	dropTemporaryQueues
	dropTemporaryTopics
	reportInterval
filteredDestination	queue
	selector
	topic
fixedCountSubscriptionRecoveryPolicy	maximumSize
fixedSizedSubscriptionRecoveryPolicy	maximumSize
	useSharedBuffer

Elemento	Atributo
<code>forcePersistencyModeBrokerPlugin</code>	<code>persistenceFlag</code>
<code>individualDeadLetterStrategy</code>	<code>destinationPerDurableSubscriber</code>
	<code>enableAudit</code>
	<code>expiration</code>
	<code>maxAuditDepth</code>
	<code>maxProducersToAudit</code>
	<code>processExpired</code>
	<code>processNonPersistent</code>
	<code>queuePrefix</code>
	<code>queueSuffix</code>
	<code>topicPrefix</code>
	<code>topicSuffix</code>
	<code>useQueueForQueueMessages</code>
	<code>useQueueForTopicMessages</code>
<code>messageGroupHashBucketFactory</code>	<code>bucketCount</code>
	<code>cacheSize</code>
<code>mirroredQueue</code>	<code>copyMessage</code>
	<code>postfix</code>
	<code>prefix</code>
<code>oldestMessageEvictionStrategy</code>	<code>evictExpiredMessagesHighWatermark</code>

Elemento	Atributo
<code>oldestMessageWithLowestPriorityEvictionStrategy</code>	<code>evictExpiredMessagesHighWatermark</code>
<code>policyEntry</code>	<code>advisoryForConsumed</code>
	<code>advisoryForDelivery</code>
	<code>advisoryForDiscardingMessages</code>
	<code>advisoryForFastProducers</code>
	<code>advisoryForSlowConsumers</code>
	<code>advisoryWhenFull</code>
	<code>allConsumersExclusiveByDefault</code>
	<code>alwaysRetroactive</code>
	<code>blockedProducerWarningInterval</code>
	<code>consumersBeforeDispatchStarts</code>
	<code>cursorMemoryHighWaterMark</code>
	<code>doOptimizeMessageStorage</code>
	<code>durableTopicPrefetch</code>
	<code>enableAudit</code>
	<code>expireMessagesPeriod</code>
	<code>gcInactiveDestinations</code>
<code>gcWithNetworkConsumers</code>	
<code>inactiveTimeoutBeforeGC</code>	
<code>inactiveTimeoutBeforeGC</code>	

Elemento	Atributo
	<code>includeBodyForAdvisory</code>
	<code>lazyDispatch</code>
	<code>maxAuditDepth</code>
	<code>maxBrowsePageSize</code>
	<code>maxDestinations</code>
	<code>maxExpirePageSize</code>
	<code>maxPageSize</code>
	<code>maxProducersToAudit</code>
	<code>maxQueueAuditDepth</code>
	<code>memoryLimit</code>
	<code>messageGroupMapFactoryType</code>
	<code>minimumMessageSize</code>
	<code>optimizedDispatch</code>
	<code>optimizeMessageStoreInFlightLimit</code>
	<code>persistJMSRedelivered</code>
	<code>prioritizedMessages</code>
	<code>producerFlowControl</code>
	<code>queue</code>
	<code>queueBrowserPrefetch</code>
	<code>queuePrefetch</code>

Elemento	Atributo
	reduceMemoryFootprint
	sendAdvisoryIfNoConsumers
	sendFailIfNoSpace
	sendFailIfNoSpaceAfterTimeout
	<div style="border: 1px solid #007bff; border-radius: 10px; padding: 10px; background-color: #e6f2ff;">  Compatível com Apache ActiveMQ 15.16.4 e posterior </div>
	sendDuplicateFromStoreToDLQ
	storeUsageHighWaterMark
	strictOrderDispatch
	tempQueue
	tempTopic
	timeBeforeDispatchStarts
	topic
	topicPrefetch
	useCache
	useConsumerPriority
usePrefetchExtension	
prefetchRatePendingMessageLimitStrategy	multiplier

Elemento	Atributo
queryBasedSubscriptionRecoveryPolicy	query
queue	DLQ
	physicalName
redeliveryPlugin	fallbackToDeadLetter
	sendToDlqIfMaxRetriesExceeded
redeliveryPolicy	backOffMultiplier
	collisionAvoidancePercent
	initialRedeliveryDelay
	maximumRedeliveries
	maximumRedeliveryDelay
	preDispatchCheck
	queue
	redeliveryDelay
	tempQueue
	tempTopic
	topic
	useCollisionAvoidance
	useExponentialBackOff
sharedDeadLetterStrategy	enableAudit
	expiration

Elemento	Atributo
	maxAuditDepth
	maxProducersToAudit
	processExpired
	processNonPersistent
storeDurableSubscriberCursor	immediatePriorityDispatch
	useCache
tempDestinationAuthorizationEntry	admin
	queue
	read
	tempQueue
	tempTopic
	topic
tempQueue	DLQ
	physicalName
tempTopic	DLQ
	physicalName
timedSubscriptionRecoveryPolicy	zeroExpirationOverride
timeStampingBrokerPlugin	recoverDuration
	futureOnly

Elemento	Atributo
	processNetworkMessages
	ttlCeiling
topic	DLQ
	physicalName
transportConnector	•
	name
	updateClusterClients
	rebalanceClusterClients
	updateClusterClientsOnRemove
uniquePropertyMessageEvictionStrategy	evictExpiredMessagesHighWatermark
	propertyName
virtualTopic	concurrentSend
	local
	dropOnResourceLimit
	name
	postfix
	prefix
	selectorAware
	setOriginalDestination

Elemento	Atributo
	transactedSend

Atributos de elementos pai do Amazon MQ

A seguinte é uma explicação detalhada dos atributos de elementos pai. Para obter mais informações, consulte [XMLConfiguração na documentação](#) do Apache ActiveMQ.

Tópicos

- [agente](#)

agente

`broker` é um elemento de coleção pai.

Atributos

`networkConnectionStartAssíncrono`

Para reduzir a latência da rede e permitir que outras redes para iniciar em tempo hábil, use a tag `<networkConnectionStartAsync>`. A tag instrui o agente a usar um executor para iniciar conexões de rede em paralelo, assíncrona para um agente iniciar.

Padrão: `false`

Exemplo de configuração

```
<broker networkConnectorStartAsync="false"/>
```

Elementos, elementos de conjunto secundários e elementos secundários permitidos nas configurações do Amazon MQ

A seguinte é uma lista detalhada dos elementos, elementos do conjunto de filhos e de seus elementos filho permitidos nas configurações do Amazon MQ. Para obter mais informações, consulte [XMLConfiguração na documentação](#) do Apache ActiveMQ.

Elemento	Elemento de coleção filho	Elemento filho
authorizationMap	authorizationEntries	authorizationEntry
		tempDestinationAuthorizationEntry
	defaultEntry	authorizationEntry
		tempDestinationAuthorizationEntry
	tempDestinationAuthorizationEntry	tempDestinationAuthorizationEntry
authorizationPlugin	map	authorizationMap
broker	destinationInterceptors	mirroredQueue
		virtualDestinationInterceptor
	destinationPolicy	policyMap
	destinations	queue
		tempQueue
		tempTopic
		topic
	networkConnectors	networkConnector
persistenceAdapter	kahaDB	
plugins	authorizationPlugin	
	discardingDLQBrokerPlugin	

Elemento	Elemento de coleção filho	Elemento filho
		forcePersistenceModeBrokerPlugin
		redeliveryPlugin
		statisticsBrokerPlugin
		timeStampingBrokerPlugin
	systemUsage	systemUsage
	transportConnector	name
		updateClusterClients
		rebalanceClusterClients
		updateClusterClientsOnRemove
compositeQueue	forwardTo	queue
		tempQueue
		tempTopic
		topic
		filteredDestination
compositeTopic	forwardTo	queue
		tempQueue
		tempTopic

Elemento	Elemento de coleção filho	Elemento filho
		topic
		filteredDestination
policyEntry	deadLetterStrategy	discarding
		individualDeadLetterStrategy
		sharedDeadLetterStrategy
	destination	queue
		tempQueue
		tempTopic
		topic
	dispatchPolicy	priorityDispatchPolicy
		priorityNetworkDispatchPolicy
		roundRobinDispatchPolicy
		simpleDispatchPolicy
		strictOrderDispatchPolicy
		clientIdFilterDispatchPolicy

Elemento	Elemento de coleção filho	Elemento filho
	messageEvictionStrategy	oldestMessageEvictionStrategy
		oldestMessageWithLowestPriorityEvictionStrategy
		uniquePropertyMessageEvictionStrategy
	messageGroupMapFactory	cachedMessageGroupMapFactory
		messageGroupHashBucketFactory
		simpleMessageGroupMapFactory
	pendingDurableSubscriberPolicy	fileDurableSubscriberCursor
		storeDurableSubscriberCursor
		vmDurableCursor
	pendingMessageLimitStrategy	constantPendingMessageLimitStrategy
		prefetchRatePendingMessageLimitStrategy
	pendingQueuePolicy	fileQueueCursor
		storeCursor

Elemento	Elemento de coleção filho	Elemento filho
		vmQueueCursor
	pendingSubscriberPolicy	fileCursor vmCursor
	slowConsumerStrategy	abortSlowAckConsumerStrategy abortSlowConsumerStrategy
	subscriptionRecoveryPolicy	fixedCountSubscriptionRecoveryPolicy fixedSizedSubscriptionRecoveryPolicy lastImageSubscriptionRecoveryPolicy noSubscriptionRecoveryPolicy queryBasedSubscriptionRecoveryPolicy retainedMessageSubscriptionRecoveryPolicy
timedSubscriptionRecoveryPolicy		
policyMap	defaultEntry	policyEntry
	policyEntries	policyEntry

Elemento	Elemento de coleção filho	Elemento filho
redeliveryPlugin	redeliveryPolicyMap	redeliveryPolicyMap
redeliveryPolicyMap	defaultEntry	redeliveryPolicy
	redeliveryPolicyEntries	redeliveryPolicy
retainedMessageSubscriptionRecoveryPolicy	wrapped	fixedCountSubscriptionRecoveryPolicy
		fixedSizedSubscriptionRecoveryPolicy
		lastImageSubscriptionRecoveryPolicy
		noSubscriptionRecoveryPolicy
		queryBasedSubscriptionRecoveryPolicy
		retainedMessageSubscriptionRecoveryPolicy
sharedDeadLetterStrategy	deadLetterQueue	queue
		tempQueue
		tempTopic
		topic
virtualDestinationInterceptor	virtualDestinations	compositeQueue

Elemento	Elemento de coleção filho	Elemento filho
		compositeTopic
		virtualTopic

Atributos de elementos filho do Amazon MQ

A seguinte é uma explicação detalhada dos atributos de elementos filho. Para obter mais informações, consulte [XMLConfiguração na documentação](#) do Apache ActiveMQ.

Tópicos

- [authorizationEntry](#)
- [networkConnector](#)
- [kahaDB](#)
- [systemUsage](#)

authorizationEntry

authorizationEntry é um filho do elemento do conjunto de filhos authorizationEntries.

Atributos

admin|read|write

As permissões concedidas a um grupo de usuários. Para obter mais informações, consulte [Sempre configurar um mapa de autorização](#).

Se você especificar um mapa de autorização que não inclua o activemq-webconsole, você não poderá usar o Console da Web do ActiveMQ porque o grupo não estará autorizado a enviar mensagens ou receber mensagens do agente do Amazon MQ.

Padrão: null

Exemplo de configuração

```
<authorizationPlugin>
    <map>
```

```
        <authorizationMap>
            <authorizationEntries>
                <authorizationEntry admin="admins,activemq-
webconsole" read="admins,users,activemq-webconsole" write="admins,activemq-webconsole"
queue=""/>
                <authorizationEntry admin="admins,activemq-
webconsole" read="admins,users,activemq-webconsole" write="admins,activemq-webconsole"
topic=""/>
            </authorizationEntries>
        </authorizationMap>
    </map>
</authorizationPlugin>
```

networkConnector

`networkConnector` é um filho do elemento do conjunto de filhos `networkConnectors`.

Tópicos

- [Atributos](#)
- [Exemplos de configuração](#)

Atributos

conduitSubscriptions

Especifica se uma conexão de rede em uma rede de agentes trata vários consumidores que se inscreveram para o mesmo destino como um consumidor. Por exemplo, se `conduitSubscriptions` estiver definido como `true` e dois consumidores se conectarem ao agente B e consumirem a partir de um destino, o agente B combina as assinaturas em uma única assinatura lógica pela conexão de rede para o agente A, para que apenas uma única cópia de um agente de mensagem seja encaminhado do agente A para o B.

Note

Configurar `conduitSubscriptions` como `true` pode reduzir o tráfego de rede redundante. No entanto, o uso desse atributo pode ter implicações no balanceamento de carga das mensagens entre os consumidores e pode causar um comportamento incorreto em determinados cenários (por exemplo, com seletores de JMS mensagens ou com tópicos duradouros).

Padrão: `true`

`duplex`

Especifica se a conexão na rede de agentes é usada para produzir e consumir mensagens. Por exemplo, se o agente A cria uma conexão para o agente B no modo não duplex, as mensagens podem ser encaminhadas apenas do agente A para o agente B. No entanto, se o agente A cria uma conexão duplex para o agente B, então, o agente B pode encaminhar mensagens para o agente A sem a necessidade de configurar um `<networkConnector>`.

Padrão: `false`

`name`

O nome da ponte na rede de agentes.

Padrão: `bridge`

`uri`

O endpoint do protocolo de nível de conexão para um dos dois agentes (ou para vários agentes) em uma rede de agentes.

Padrão: `null`

`username`

O nome de usuário comum aos agentes em uma rede de agentes.

Padrão: `null`

Exemplos de configuração

Note

Ao usar um `networkConnector` para definir uma rede de agentes, não inclua a senha de usuário comum para os agentes.

Uma rede de agentes com dois agentes

Nesta configuração, dois agentes são conectados em uma rede de agentes. O nome do conector de rede é `connector_1_to_2`, o nome de usuário comum aos corretores é `myCommonUser`, a conexão

éduplex, e o OpenWire endpoint URI é prefixado porstatic:, indicando uma one-to-one conexão entre os corretores.

```
<networkConnectors>
    <networkConnector name="connector_1_to_2"
      userName="myCommonUser" duplex="true"
        uri="static:(ssl://
b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:61617)"/>
    </networkConnectors>
```

Para obter mais informações, consulte [Configure Network Connectors for Your Broker](#).

Uma rede de agentes com vários agentes

Nesta configuração, vários agentes são conectados em uma rede de agentes. O nome do conector de rede éconnector_1_to_2, o nome de usuário comum aos corretores émyCommonUser, a conexão éduplex, e a lista de OpenWire endpoints separados por vírgulas URIs é prefixada pormasterslave:, indicando uma conexão de failover entre os corretores. O failover do agente para o agente não é aleatório e tentativas de reconexão continuam indefinidamente.

```
<networkConnectors>
    <networkConnector name="connector_1_to_2"
      userName="myCommonUser" duplex="true"
        uri="masterslave:(ssl://
b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:61617,
        ssl://
b-987615k4-32ji-109h-8gfe-7d65c4b132a1-2.mq.us-east-2.amazonaws.com:61617)"/>
    </networkConnectors>
```

Note

Recomendamos usar o prefixo masterslave: para as redes de agentes. O prefixo é idêntico à sintaxe mais explícita static:failover:()?randomize=false&maxReconnectAttempts=0.

Note

Essa XML configuração não permite espaços.

kahaDB

kahaDB é um filho do elemento do conjunto de filhos persistenceAdapter.


Atributos

concurrentStoreAndDispatchQueues

Especifica se é necessário usar armazenamento e despacho simultâneos para filas. Para obter mais informações, consulte [Desativar o armazenamento e a expedição simultâneos para filas com consumidores lentos](#).

Padrão: true

cleanupOnStop

 Compatível com
Apache ActiveMQ 15.16.x e versão superior

Quando desativada, a coleta de resíduos e a limpeza não ocorrem quando o agente é interrompido, o que agiliza o processo de desligamento. O aumento da velocidade é útil em casos com grandes bancos de dados ou bancos de dados do programador.


Padrão: true

journalDiskSyncIntervalo

Intervalo (ms) para quando executar uma sincronização de disco se `journalDiskSyncStrategy=periodic`. Para obter mais informações, consulte a [documentação do Apache ActiveMQ kahaDB](#).

Padrão: 1000

journalDiskSyncEstratégia

 Compatível com
Apache ActiveMQ 15.14.x e versão superior

Configura a política de sincronização de disco. Para obter mais informações, consulte a [documentação do Apache ActiveMQ kahaDB](#).

Padrão: `always`

Note

A [documentação do ActiveMQ](#) afirma que a perda de dados é limitada à duração de `journalDiskSyncInterval`, que tem um padrão de 1s. A perda de dados pode ser maior do que o intervalo, mas é difícil ser preciso. Tenha cuidado.

`preallocationStrategy`

Configura como o agente tentará pré-alocar os arquivos do diário quando um novo arquivo do diário for necessário. Para obter mais informações, consulte a [documentação do Apache ActiveMQ kahaDB](#).

Padrão: `sparse_file`

Exemplo de configuração

Example

```
<broker xmlns="http://activemq.apache.org/schema/core">
  <persistenceAdapter>
    <kahaDB preallocationStrategy="zeros"
concurrentStoreAndDispatchQueues="false" journalDiskSyncInterval="10000"
journalDiskSyncStrategy="periodic"/>
  </persistenceAdapter>
</broker>
```

`systemUsage`

`systemUsage` é um filho do elemento do conjunto de filhos `systemUsage`. Ele controla a quantidade máxima de espaço que o agente usará antes de desacelerar os produtores. Para obter mais informações, consulte [Controle do fluxo do produtor](#) na documentação do Apache ActiveMQ.

Elemento filho

memoryUsage

memoryUsage é um filho do elemento filho systemUsage. Ele gerencia o uso de memória. Use memoryUsage para acompanhar quanto de um elemento está sendo usado, para que você possa controlar o uso do conjunto de trabalho de forma produtiva. Para obter mais informações, consulte [o esquema](#) na documentação do Apache ActiveMQ.

Elemento filho

memoryUsage é um filho do elemento filho memoryUsage.

Atributo

percentOfJvmPilha

Número inteiro entre 0 (inclusive) e 70 (inclusive).

Padrão: 70

Atributos

sendFaillfNoSpace

Define se um método send() deverá falhar se não houver espaço livre. O valor padrão é false, o que bloqueia o método send() até haver espaço disponível. Para obter mais informações, consulte [o esquema](#) na documentação do Apache Active MQ.

Padrão: false

sendFaillfNoSpaceAfterTimeout

Padrão: null

Exemplo de configuração

Example

```
<broker xmlns="http://activemq.apache.org/schema/core">
    <systemUsage>
```

```
        <systemUsage sendFailIfNoSpace="true"
sendFailIfNoSpaceAfterTimeout="2000">
            <memoryUsage>
                <memoryUsage percentOfJvmHeap="60" />
            </memoryUsage>>
        </systemUsage>
    </systemUsage>
</broker>
</persistenceAdapter>
```

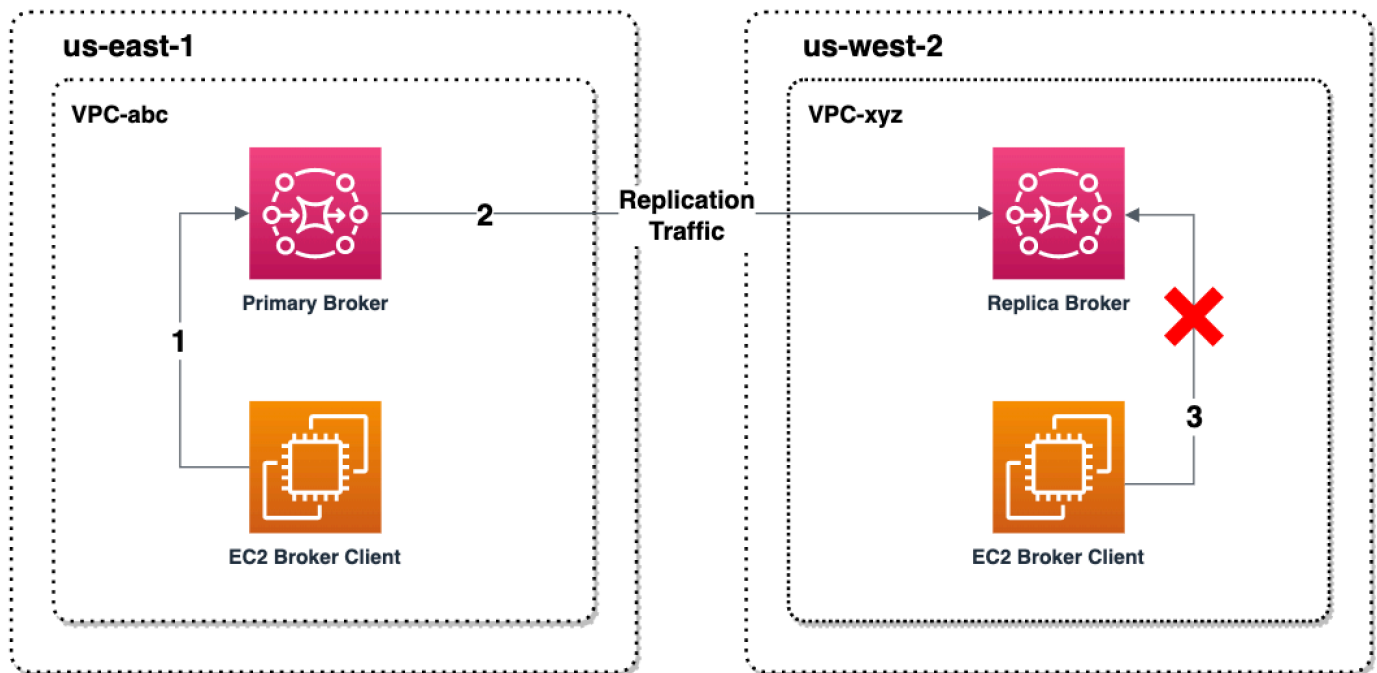
Replicação de dados entre regiões para o Amazon MQ for ActiveMQ

O Amazon MQ para ActiveMQ oferece um recurso de replicação de dados entre regiões (CRDR) que permite a replicação assíncrona de mensagens do agente principal em uma região primária para o agente de réplica em uma região de réplica. AWS Ao emitir uma solicitação de failover para o Amazon API MQ, o agente de réplica atual é promovido à função de agente principal, e o agente principal atual é rebaixado para a função de réplica.

Agentes primários e de réplica para replicação de dados entre regiões

Você pode criar agentes primários e de réplica para replicação assíncrona de dados do agente principal em uma região primária para o agente de réplica em uma AWS região de réplica. A região primária consiste em um par redundante de agentes ativo/em espera, denominado agente primário. A região secundária consiste em um par redundante de agentes ativo/em espera, denominado agente de réplica.

O diagrama a seguir ilustra um agente de réplica em uma região secundária recebendo dados replicados assíncronos do agente primário na região primária.



Os agentes primários e de réplica atuam como uma solução de recuperação de dados entre regiões. Se o agente primário na região primária falhar, você poderá promover o agente de réplica na região secundária para primário iniciando uma transição ou um failover. O antigo agente primário então se torna o agente de réplica, e o antigo agente de réplica é promovido a agente primário. Para ter instruções sobre como criar um agente primário e um agente de réplica, consulte [Criação de um agente de replicação de dados entre regiões do Amazon MQ](#).

Note

Disponível apenas para agentes ativo/em espera.

Criação de um agente de replicação de dados entre regiões do Amazon MQ

Com a replicação de dados entre regiões (CRDR), você pode alternar entre os agentes de mensagens do Amazon MQ para ActiveMQ em duas regiões, conforme necessário. AWS Você pode designar um agente existente como agente primário e criar uma réplica para esse agente, ou criar um agente primário e um agente de réplica juntos. Em seguida, você pode promover o agente de réplica para a função de agente principal usando a operação Amazon Promote API MQ. Para ter

mais informações sobre agentes primários e de réplica, consulte [Agentes primários e de réplica para replicação de dados entre regiões](#).

As instruções a seguir descrevem como criar e configurar um agente de réplica usando o Console de Gerenciamento do Amazon MQ.

Tópicos

- [Pré-requisitos](#)
- [Etapa 1 \(opcional\): Criar um agente primário](#)
- [Etapa 2: Criar uma réplica de um agente existente](#)

Pré-requisitos

Para usar o recurso de replicação de dados entre regiões, você deve analisar e cumprir os seguintes pré-requisitos:


- Versão: o atributo de replicação de dados entre regiões só está disponível para agentes do Amazon MQ para ActiveMQ nas versões 5.17.6 e posterior.
- Região: a replicação de dados entre regiões é aceita nas seguintes regiões: Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Oeste dos EUA (Norte da Califórnia).
- Tipo de instância: a replicação de dados entre regiões só está disponível para tamanhos de instância de agente `mq.m5.large` e posterior.
- Tipo de implantação: a replicação de dados entre regiões só está disponível para agentes ativos/em espera com implantação em várias zonas de disponibilidade.
- Status do agente: você só pode criar um agente de réplica para um agente primário com o status de agente `Running`.

Etapa 1 (opcional): Criar um agente primário

Criar um agente primário

1. Faça login no [console do Amazon MQ](#).
2. Na página Agentes do console do Amazon MQ, escolha Criar agentes.
3. Na página Select broker engine (Selecionar mecanismo de agente), selecione Apache ActiveMQ (Apache ActiveMQ).

4. Na página **Select deployment and storage** (Selecionar implantação e armazenamento), na seção **Deployment mode and storage type** (Modo de implantação e tipo de armazenamento), faça o seguinte:
 - Em Modo de implantação, escolha **Operador ativo/em espera de alta disponibilidade**. Um agente ativo/em espera é composto por dois agentes em duas zonas de disponibilidade diferentes, configuradas em um par redundante. Esses corretores se comunicam de forma síncrona com seu aplicativo e com a Amazon. EFS Para obter mais informações, consulte [Opções de implantação do Amazon MQ para agentes ActiveMQ](#).
5. Escolha **Próximo**.
6. Na página **Definir configurações**, faça o seguinte na seção **Detalhes**:
 - a. Digite o **Broker name** (Nome do agente).

 **Important**

Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nos nomes dos corretores. Os nomes dos corretores podem ser acessados por outros AWS serviços, incluindo CloudWatch registros. Nomes de agente não devem ser usados para dados privados ou sigilosos.

- b. Selecione o **Tipo de instância de agente** (por exemplo, `m5.large`). Para obter mais informações, consulte [Broker instance types](#).
7. Na seção **ActiveMQ Web Console access** (Acesso ao console da Web ActiveMQ), forneça um **Username** (Nome de usuário) e **Password** (Senha). As seguintes restrições se aplicam a nomes de usuário e senhas de agente:
 - Seu nome de usuário pode conter somente caracteres alfanuméricos, traços, pontos, sublinhados e tils (- . _ ~).
 - Sua senha deve ter pelo menos 12 caracteres, deve conter pelo menos 4 caracteres exclusivos e não deve conter vírgulas, dois pontos ou sinais de igual (,:=).

 **Important**

Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nos nomes de usuário da corretora. Os nomes de usuário dos corretores podem ser acessados por outros AWS serviços, incluindo CloudWatch

registros. Nomes de usuário do agente não devem ser usados para dados privados ou sigilosos.

A barra verde na parte superior da página confirma que o Amazon MQ está criando o agente de réplica na região de recuperação. Você também pode ver a CRDR função e o RPO status de seus corretores. Para desativar as colunas CRDR Função e RPO Status, escolha o ícone de engrenagem no canto superior direito da tabela Corretores. Em seguida, na página Preferências, desative CRDR Função ou RPO Status.

Etapa 2: Criar uma réplica de um agente existente

1. Na página Agentes do console do Amazon MQ, escolha Criar agente de réplica.
2. Na página Escolher corretor principal, selecione um corretor existente para usar como corretor CRDR principal. Em seguida, escolha Próximo.
3. Na página Configurar agente de réplica, use o menu suspenso para escolher a região da réplica.
4. Na seção Usuário do console ActiveMQ para agente de réplica, forneça um nome de usuário e uma senha para o usuário do console do agente de réplica. As seguintes restrições se aplicam a nomes de usuário e senhas de agente:
 - Seu nome de usuário pode conter somente caracteres alfanuméricos, traços, pontos, sublinhados e tils (- . _ ~).
 - Sua senha deve ter pelo menos 12 caracteres, deve conter pelo menos 4 caracteres exclusivos e não deve conter vírgulas, dois pontos ou sinais de igual (,:=).

Important

Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nos nomes de usuário da corretora. Os nomes de usuário dos corretores podem ser acessados por outros AWS serviços, incluindo CloudWatch registros. Nomes de usuário do agente não devem ser usados para dados privados ou sigilosos.

5. Na seção Usuário de replicação de dados para conectar o acesso entre agentes, forneça um nome de usuário e uma senha para o usuário que acessará o agente primário e o agente de réplica. As seguintes restrições se aplicam a nomes de usuário e senhas de agente:

- Seu nome de usuário pode conter somente caracteres alfanuméricos, traços, pontos, sublinhados e tils (- . _ ~).
- Sua senha deve ter pelo menos 12 caracteres, deve conter pelo menos 4 caracteres exclusivos e não deve conter vírgulas, dois pontos ou sinais de igual (,:=).

 Important

Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nos nomes de usuário da corretora. Os nomes de usuário dos corretores podem ser acessados por outros AWS serviços, incluindo CloudWatch registros. Nomes de usuário do agente não devem ser usados para dados privados ou sigilosos.

Defina todas as configurações adicionais. Em seguida, escolha Próximo.

6. Na página Analisar e criar, revise os detalhes do agente de réplica. Depois, escolha Criar operador de réplica.
7. Depois, reinicialize o agente primário. Isso também reinicializará o agente de réplica. Para ter instruções sobre como reiniciar seu agente, consulte [Rebooting a Broker](#).

Para ter mais informações sobre como definir configurações adicionais para seu agente do ActiveMQ, consulte [Começando: Criando e conectando-se a um corretor ActiveMQ](#).

Excluindo um agente de replicação de dados entre regiões do Amazon MQ

Para excluir um agente primário ou de réplica de replicação de dados entre regiões (CRDR), você deve primeiro desemparelhar e reinicializar os agentes. As instruções a seguir mostram como você pode desemparelhar e reinicializar os brokers usando o AWS Management Console.

1. Na página Corretores, selecione o CRDR corretor que você deseja desemparelhar e escolha Editar.
2. Na página Editar agente, na seção Replicação de dados, escolha Cancelar emparelhamento de agentes.
3. Digite “cancelar emparelhamento” na janela pop-up para confirmar sua escolha. Depois, escolha Cancelar emparelhamento de agentes.

4. Depois, reinicialize o agente primário não emparelhado. Isso também reinicializará o agente de réplica. Para ter instruções sobre como reiniciar seu agente, consulte [Rebooting a Broker](#). Depois que o agente primário for reinicializado, o emparelhamento dos dois agentes será cancelado e eles poderão ser excluídos individualmente. Para excluir seu agente, consulte [Deleting a broker](#).

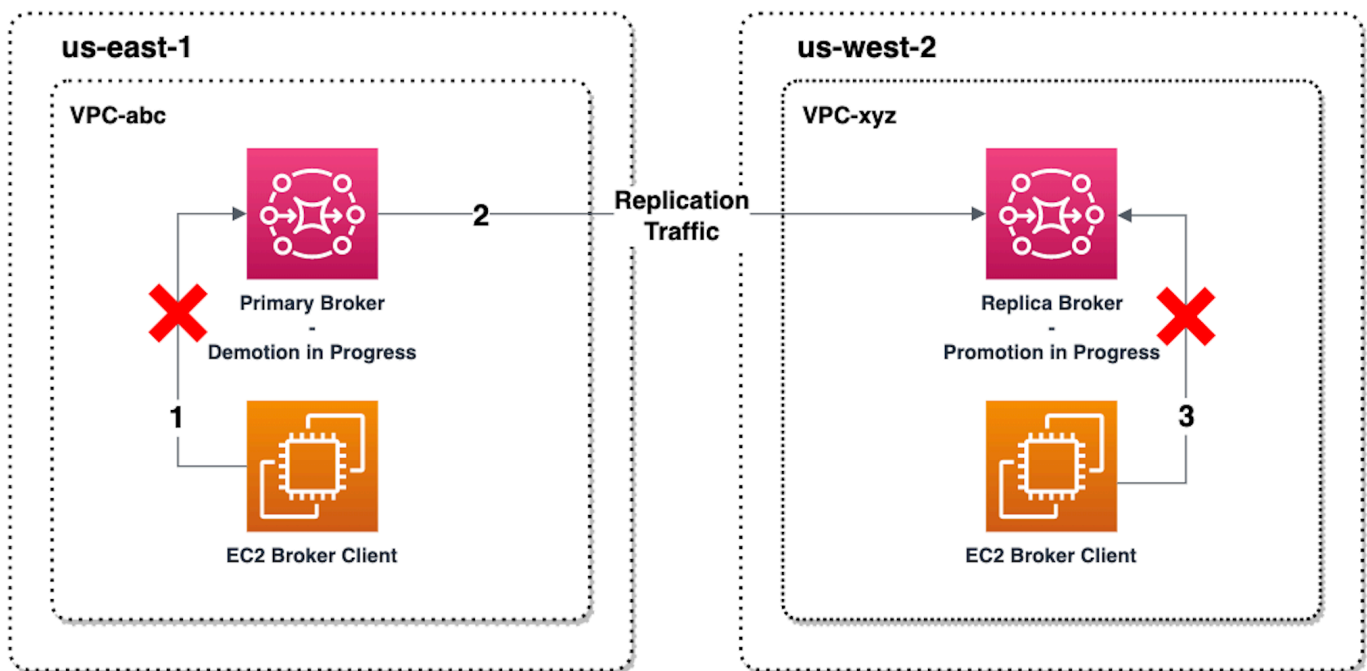
Iniciando a transição ou o failover para promover um agente de réplicas do Amazon MQ à função de agente principal

Você pode iniciar uma transição ou um failover quando quiser promover o agente de réplica à função de agente primário. Quando você promove o agente de réplica, o agente primário é rebaixado para a função de agente de réplica.

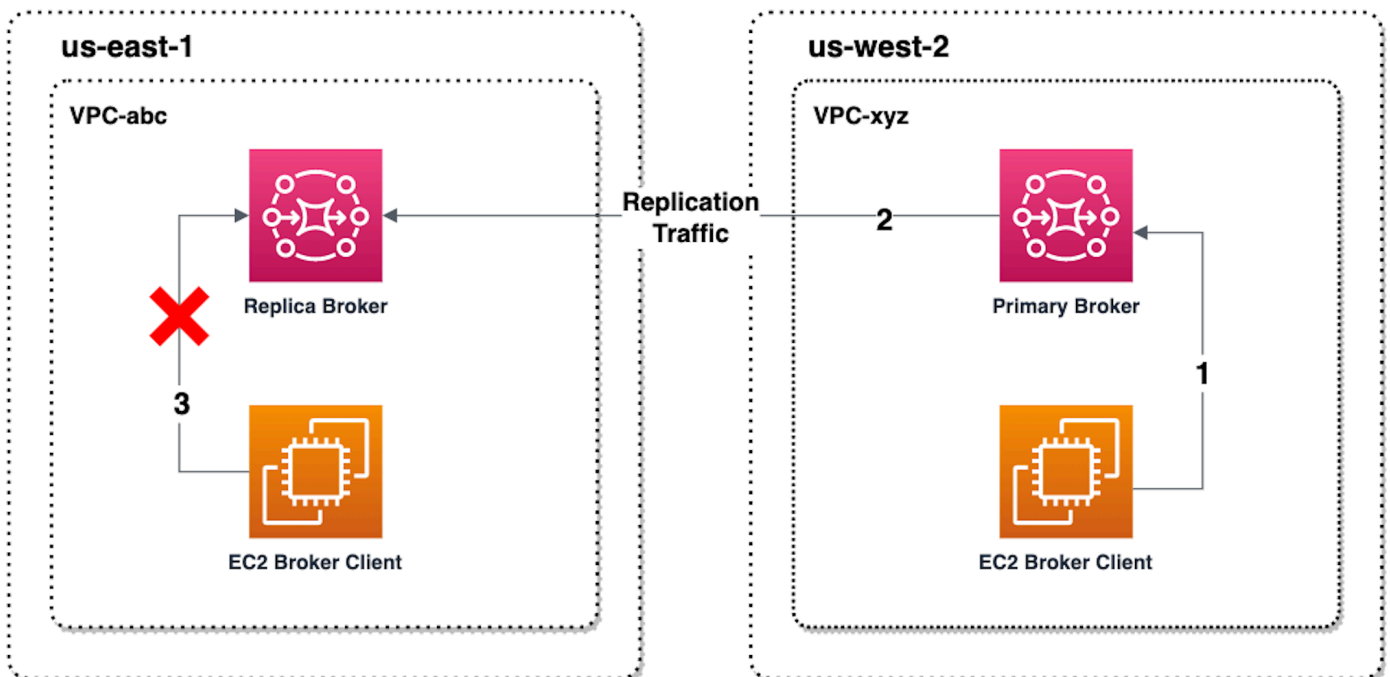
Uma transição prioriza a consistência em detrimento da disponibilidade. É garantido que os agentes tenham o mesmo estado quando essa operação de failover for concluída. Com uma transição, pode haver um período em que nenhum dos agentes esteja disponível para conexões com clientes e a consistência entre agentes seja estabelecida. Os dois agentes terão o mesmo estado no instante em que a réplica for promovida. O êxito da transição depende da integridade das duas regiões e da rede inter-regional.

Um failover prioriza a disponibilidade em detrimento da consistência. Não é garantido que os corretores tenham estados idênticos quando essa operação for concluída. Com um failover, é garantido que o agente de réplica fique imediatamente disponível para atender ao tráfego do cliente, sem esperar que os dados de replicação sejam sincronizados ou que o primário receba o sinal de desligamento. O failover não depende da integridade da região primária original nem da rede inter-regional para ter êxito.

O diagrama a seguir ilustra uma transição na qual nenhum dos agentes aceita conexões de clientes enquanto a fila de replicação está sendo drenada e os estados do agente são sincronizados. Nesse processo, o cliente da VPC corretora principal não consegue produzir mais alterações de estado enquanto a operação está em andamento, e a corretora principal está sendo rebaixada para uma réplica. Quando a fila de replicação é esgotada e os dois agentes atingem um estado idêntico, o cliente no agente de réplicas não consegue se conectar ao agente de réplicas até que a operação de failover VPC seja concluída e o agente de réplica seja promovido a principal.



O diagrama a seguir ilustra o status do agente após a conclusão do processo de transição. O agente de réplica original agora foi promovido à função de agente primário e está aceitando conexões de clientes. O cliente pode produzir e consumir dados do agente.



Promover o agente de réplica usando o console

Para promover o agente de réplica usando transição ou failover, siga estas etapas no console do Amazon MQ.

Note

Você não pode iniciar a transição nem o failover em um agente primário.

1. Mude para a região do seu agente de réplica. Na tabela Agentes, selecione o agente de réplica existente que você promoverá como primário.
2. Na página Detalhes do agente, faça o seguinte:
 1. Selecione Promover uma réplica.
 2. Na janela pop-up, escolha Transição ou Failover.
 3. Digite “confirmar” na caixa de texto para confirmar sua escolha.
 4. Selecione a opção Confirmar.

Depois de iniciar o failover, o status do agente muda para Failover em andamento. A barra de progresso azul na parte superior da página Agentes fica verde quando o failover é concluído.

Note

A configuração só é replicada no momento em que o agente replicado é criado. Nenhuma atualização posterior é replicada.

Métricas de replicação de dados entre regiões no Amazon CloudWatch

O atributo de replicação de dados entre regiões do Amazon MQ for ActiveMQ oferece métricas para manter a confiabilidade, a disponibilidade e a performance de seus agentes primários e de réplica. Durante o processo de replicação, um agente de réplica em uma região secundária recebe dados replicados de forma assíncrona do agente primário na região primária. Se o agente primário na região primária falhar, você poderá promover o agente de réplica na região secundária para primário iniciando uma transição ou um failover. Para ter instruções sobre como visualizar métricas no Amazon CloudWatch, consulte [Acessando CloudWatch métricas para o Amazon MQ](#).

Carimbos de data/hora da CRDR

Os carimbos de data/hora a seguir descrevem como as métricas encontradas no Amazon CloudWatch são calculadas. Há cinco carimbos de data/hora no processo de replicação de dados:

- Tempo de observação atual (TCO): o instante atual no tempo.
- Hora da criação (TC): o instante em que um evento foi criado na fila de replicação pelo agente primário. Disponível em agentes primários e de réplica.
- Hora da entrega (TD): o instante em que um evento foi entregue com êxito ao agente de réplicas. Disponível somente em agentes de réplica.
- Tempo de processamento (TP): o instante em que um evento foi processado com êxito pelo agente de réplica. Disponível somente em agentes de réplica.
- Tempo de confirmação (TA): o instante em que um evento foi reconhecido com êxito pelo agente principal. Disponível apenas em agentes primários.

Estime a performance de transição/failover com métricas do CRDR CloudWatch

O Amazon MQ habilita métricas para o seu agente por padrão. É possível visualizar as métricas do agente acessando o console do Amazon CloudWatch ou usando a API do CloudWatch. As métricas a seguir são úteis para entender a performance de replicação e de transição/failover de seus agentes de CRDR:

Métrica do Amazon MQ CloudWatch	Motivo do uso da CRDR
TotalReplicationLag	O tempo estimado entre TA e TC do último evento não confirmado no agente primário.
ReplicationLag	O tempo estimado entre TP e TC do último evento não confirmado no agente primário.
PrimaryWaitTime	O tempo estimado entre TCO e TC do último evento

Métrica do Amazon MQ CloudWatch	Motivo do uso da CRDR
	processado no agente primário.
ReplicaWaitTime	O tempo estimado entre TCO e TP do último evento processado no agente primário.
QueueSize	O número total de eventos não confirmados na fila de replicação no agente primário.

TotalReplicationLag e ReplicationLag descrevem o atraso na replicação entre os agentes primário e de réplica. As duas métricas também podem ser usadas para estimar o tempo até a conclusão da operação contínua de transição ou failover.

PrimaryWaitTime e ReplicaWaitTime podem ser usados para identificar quaisquer problemas contínuos com o processo de replicação. Se o valor da métrica estiver aumentando constantemente, isso poderá indicar que o processo de replicação está degradado ou pausado. A replicação lenta pode decorrer de problemas como particionamento de rede, inicialização de agentes e recuperação prolongada.

Tutoriais ActiveMQ

Os tutoriais a seguir mostram como você pode criar e se conectar aos agentes do ActiveMQ. Para usar o código de exemplo o ActiveMQ Java, será necessário instalar o [Kit de Desenvolvimento da Edição Padrão do Java](#) e fazer algumas alterações de configuração no código.

Tópicos

- [Criar e configurar uma rede de agentes Amazon MQ.](#)
- [Conectar uma aplicação Java ao agente do Amazon MQ](#)
- [Integração de agentes ActiveMQ com LDAP](#)
- [Criando um usuário do ActiveMQ broker](#)

- [Editar um usuário do ActiveMQ broker](#)
- [Excluir um usuário do ActiveMQ broker](#)
- [Exemplos práticos da utilização do Java Message Service \(JMS\) com o ActiveMQ](#)

Criar e configurar uma rede de agentes Amazon MQ.

A rede de agentes é composta por vários agentes ativos simultaneamente, [agentes de instância única](#) ou [agentes ativos/em espera](#). Você pode configurar redes de corretores em uma variedade de [topologias](#) (por exemplo, concentrador hub-and-spokes, árvore ou malha), dependendo das necessidades do seu aplicativo, como alta disponibilidade e escalabilidade. Por exemplo, uma rede [hub-and-spokes](#) (hub-e-raios) de agentes pode aumentar a resiliência, preservando mensagens se um agente não estiver acessível. Uma rede de agentes com uma topologia de [concentrador](#) pode coletar mensagens de um número maior de agentes que aceitam mensagens recebidas, e concentrá-las em agentes mais centrais, para lidar melhor com a carga de muitas mensagens recebidas. Neste tutorial, você aprende a criar uma rede de agentes de dois agentes com uma topologia de origem e de destino.

Para obter uma visão geral conceitual e informações detalhadas de configuração, consulte o seguinte:

- [Rede de corretores Amazon MQ](#)
- [Configurar sua rede de agentes corretamente](#)
- [networkConnector](#)
- [networkConnectionStartAssíncrono](#)
- [Redes de agentes](#) na documentação do ActiveMQ

Você pode usar o console do Amazon MQ para criar uma rede de agentes do Amazon MQ. Como você pode iniciar a criação dos dois agentes em paralelo, esse processo leva cerca de 15 minutos.

Tópicos

- [Pré-requisitos](#)
- [Etapa 1: Permitir tráfego entre agentes](#)
- [Etapa 2: Configurar os conectores de rede para o seu agente](#)
- [Próximos Passos](#)

Pré-requisitos

Para criar uma rede de agentes, você deve ter o seguinte:

- Dois ou mais agentes simultaneamente ativos (chamado MyBroker1 e MyBroker2 neste tutorial). Para obter mais informações sobre como criar agentes, consulte [Começando: Criando e conectando-se a um corretor ActiveMQ](#).
- Os dois corretores devem estar no mesmo lugar VPC ou em paresVPCs. Para obter mais informações sobreVPCs, consulte [O que é a AmazonVPC?](#) no Guia do VPC usuário da Amazon e [o que é VPC peering?](#) no Amazon VPC Peering Guide.

Important

Se você não tiver um padrãoVPC, uma sub-rede ou um grupo de segurança, deverá criá-los primeiro. Para obter mais informações, consulte o seguinte no Guia do VPC usuário da Amazon:

- [Criando um padrão VPC](#)
- [Criar uma sub-rede padrão](#)
- [Criar um grupo de segurança](#)

- Dois usuários com credenciais de login idênticas para ambos os agentes. Para obter mais informações sobre como criar usuários, consulte [Criando um usuário do ActiveMQ broker](#).

Note

Ao integrar a LDAP autenticação com uma rede de corretores, certifique-se de que o usuário exista tanto como corretor ActiveMQ quanto como usuário. LDAP

O exemplo a seguir usa dois [agentes de instância única](#). No entanto, você pode criar redes de agentes usando os [agentes ativos/em espera](#) ou uma combinação de modos de implantação de agente.

Etapa 1: Permitir tráfego entre agentes

Depois de criar seus agentes, é necessário permitir o tráfego entre eles.

1. No [console do Amazon MQ](#), na página MyBroker2, na seção Detalhes, em Segurança e rede, escolha o nome do seu grupo de segurança ou.



A página Grupos de Segurança do EC2 Painel é exibida.

2. Na lista de security group, escolha seu security group.
3. Na parte inferior da página, escolha Inbound (Entrada) e a seguir selecione Edit (Editar).
4. Na caixa de diálogo Editar regras de entrada, adicione uma regra para o OpenWire endpoint.
 - a. Escolha Add Rule.
 - b. Em Tipo, selecione Personalizado TCP.
 - c. Em Port Range, digite a OpenWire porta (61617).
 - d. Execute um destes procedimentos:
 - Se você deseja restringir o acesso a determinado endereço IP, em Source (Origem), deixe a opção Custom (Personalizar) selecionada e insira o endereço IP de MyBroker1, seguido por /32. (Isso converte o endereço IP em um CIDR registro válido). Para obter mais informações, consulte [Interfaces de rede elástica](#).

Tip

Para recuperar o endereço IP do MyBroker1, no [console do Amazon MQ](#), escolha o nome do agente e navegue até a seção Detalhes.

- Se todos os corretores forem privados e pertencerem aos mesmosVPC, em Source, deixe Personalizado selecionado e digite o ID do grupo de segurança que você está editando.

Note

Para agentes públicos, é necessário restringir o acesso usando endereços IP.

- e. Escolha Salvar.

Agora seu agente pode aceitar conexões de entrada.

Etapa 2: Configurar os conectores de rede para o seu agente

Depois de permitir o tráfego entre os agentes, você deve configurar os conectores de rede para um deles.

1. Edite a revisão da configuração para o agente `MyBroker1`.

- a. Na página `MyBroker1`, escolha `Editar`.
- b. Na página `Editar MyBroker 1`, na seção `Configuração`, escolha `Exibir`.

O tipo e a versão do mecanismo de agente que a configuração usa (por exemplo, Apache ActiveMQ 5.15.0) são exibidos.


- c. Na guia `Detalhes da configuração`, o número da revisão da configuração, a descrição e a configuração do broker em XML formato são exibidos.
- d. Escolha `Editar configuração`.
- e. Na parte inferior do arquivo de configuração, remova a seção `<networkConnectors>` e inclua as seguintes informações:
 - O nome para o conector de rede.
 - [O Console da Web ActiveMQ username](#) que é comum para ambos os agentes.
 - Ativa as conexões duplex.
 - Execute um destes procedimentos:
 - Se você estiver conectando o broker a um broker de instância única, use o `static` prefixo e o OpenWire endpoint uri para `MyBroker2` Por exemplo:

```
<networkConnectors>
  <networkConnector name="connector_1_to_2" userName="myCommonUser"
    duplex="true"
    uri="static:(ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
    east-2.amazonaws.com:61617)"/>
</networkConnectors>
```

- Se você estiver conectando a corretora a uma corretora ativa/em espera, use o `static +failover` transporte e o OpenWire endpoint uri para ambas as corretoras com os seguintes parâmetros de consulta. `?randomize=false&maxReconnectAttempts=0` Por exemplo:

```
<networkConnectors>
```

```
<networkConnector name="connector_1_to_2" userName="myCommonUser"
duplex="true"
uri="static:(failover:(ssl://
b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-east-2.amazonaws.com:61617,
ssl://b-9876l5k4-32ji-109h-8gfe-7d65c4b132a1-2.mq.us-
east-2.amazonaws.com:61617)?randomize=false&maxReconnectAttempts=0)"/>
</networkConnectors>
```

 Note

Não inclua as credenciais de login para o usuário do ActiveMQ.


- f. Escolha Salvar.
 - g. Na caixa de diálogo Salvar revisão, digite `Add network of brokers connector for MyBroker2`.
 - h. Escolha Salvar para salvar a nova revisão de configuração.
2. Edite `MyBroker1` para definir a última revisão de configuração para aplicar imediatamente.
 - a. Na página `MyBroker1`, escolha Editar.
 - b. Na página Editar `MyBroker 1`, na seção Configuração, escolha Programar modificações.
 - c. Na seção Programar modificações do agente, escolha para aplicar modificações imediatamente.
 - d. Selecione Apply (Aplicar).

`MyBroker1` é reinicializado e sua revisão de configuração será aplicada.

A rede de agentes é criada.

Próximos Passos

Depois de configurar a rede de agentes, você pode testá-la ao produzir e consumir mensagens.

 Important

Certifique-se de [habilitar conexões de entrada](#) de sua máquina local para o broker `MyBroker1` na porta 8162 (para o ActiveMQ Web Console) e na porta 61617 (para o endpoint). OpenWire

Também será necessário ajustar as configurações do grupo de segurança para permitir que o produtor e o consumidor se conectem à rede de agentes.

1. No [console do Amazon MQ](#), navegue até a seção Connections (Conexões) e anote o endpoint do Console da Web ActiveMQ para o agente MyBroker1.
2. Navegue até o Console da Web ActiveMQ para o agente MyBroker1.
3. Para verificar se a ponte de rede está conectada, escolha Rede.

Na seção Network Bridges, o nome e o endereço de MyBroker2 são listados nas colunas Remote Broker e Remote Address.

4. Em qualquer máquina que tem acesso ao agente do MyBroker2, crie um consumidor. Por exemplo:

```
activemq consumer --brokerUrl "ssl://  
b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com:61617" \  
--user commonUser \  
--password myPassword456 \  
--destination queue://MyQueue
```

O consumidor se conecta ao OpenWire endpoint MyBroker2 e começa a consumir mensagens da filaMyQueue.

5. Em qualquer máquina que tem acesso ao agente do MyBroker1, crie um produtor e envie algumas mensagens. Por exemplo:

```
activemq producer --brokerUrl "ssl://  
b-987615k4-32ji-109h-8gfe-7d65c4b132a1-1.mq.us-east-2.amazonaws.com:61617" \  
--user commonUser \  
--password myPassword456 \  
--destination queue://MyQueue \  
--persistent true \  
--messageSize 1000 \  
--messageCount 10000
```

O produtor se conecta ao OpenWire endpoint MyBroker1 e começa a produzir mensagens persistentes na filaMyQueue.

Conectar uma aplicação Java ao agente do Amazon MQ

Depois de criar um agente do Amazon MQ ActiveMQ, você pode conectar sua aplicação a ele. Os exemplos a seguir mostram como você pode usar o Java Message Service (JMS) para criar uma conexão com o broker, criar uma fila e enviar uma mensagem. Para obter um exemplo completo e funcional do Java, consulte [Working Java Example](#).

Você pode se conectar a agentes do ActiveMQ usando [vários clientes de ActiveMQ](#). Recomendamos usar o [Cliente ActiveMQ](#).

Tópicos

- [Pré-requisitos](#)
- [Para criar um produtor de mensagens e enviar uma mensagem](#)
- [Para criar um consumidor de mensagens e receber a mensagem](#)

Pré-requisitos

Ativar VPC atributos

Para garantir que seu corretor esteja acessível dentro de vocêVPC, você deve habilitar os `enableDnsSupport` VPC atributos `enableDnsHostnames` e. Para obter mais informações, consulte [DNSSupport VPC em seu](#) Guia do VPC usuário da Amazon.

Habilitar conexões de entrada

Em seguida, habilite as conexões de entrada para seu aplicativo.

1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, escolha o nome do seu corretor (por exemplo, MyBroker).
3. Sobre o **MyBroker** página, na seção Conexões, anote os endereços e portas do console web URL e dos protocolos de nível de fio do broker.
4. Na seção Details (Detalhes), em Security and network (Segurança e rede), escolha o nome do seu grupo de segurança ou



A página Grupos de Segurança do EC2 Painel é exibida.

5. Na lista de security group, escolha seu security group.
6. Na parte inferior da página, escolha Inbound (Entrada) e a seguir selecione Edit (Editar).

7. Na caixa de diálogo Editar regras de entrada, adicione uma regra para cada terminal URL ou endpoint que você deseja que seja acessível ao público (o exemplo a seguir mostra como fazer isso em um console web do broker).
 - a. Escolha Add Rule.
 - b. Em Tipo, selecione Personalizado TCP.
 - c. Para o Intervalo de Portas, digite a porta do console da Web (8162).
 - d. Para Source (Origem), deixe Custom (Personalizado) selecionado e, depois, digite o endereço IP do sistema ao qual deseja ser capaz de acessar o console da Web (por exemplo, 192.0.2.1).
 - e. Escolha Salvar.

Agora seu agente pode aceitar conexões de entrada.

Adicionar dependências de Java

Adicione os pacotes `activemq-client.jar` e `activemq-pool.jar` ao caminho da classe Java. O exemplo a seguir mostra essas dependências em um arquivo `pom.xml` do projeto Maven.

```
<dependencies>
  <dependency>
    <groupId>org.apache.activemq</groupId>
    <artifactId>activemq-client</artifactId>
    <version>5.15.16</version>
  </dependency>
  <dependency>
    <groupId>org.apache.activemq</groupId>
    <artifactId>activemq-pool</artifactId>
    <version>5.15.16</version>
  </dependency>
</dependencies>
```

Para obter mais informações sobre `activemq-client.jar`, consulte [Initial Configuration](#) (Configuração inicial) na documentação do Apache ActiveMQ.

Important

No código de exemplo a seguir, os produtores e consumidores são executados em um único thread. Para sistemas de produção (ou para testar o failover de instância do agente),

certifique-se de que seus produtores e consumidores sejam executados em hosts ou threads separados.

Para criar um produtor de mensagens e enviar uma mensagem

Use as instruções a seguir para criar um produtor de mensagens e receber uma mensagem.

1. Crie uma fábrica de conexões em JMS pool para o produtor de mensagens usando o endpoint do seu corretor e, em seguida, chame o `createConnection` método na fábrica.

Note

Para um agente ativo/em espera, o Amazon MQ fornece dois ActiveMQ Web ConsoleURLs, mas somente um está ativo por vez. URL Da mesma forma, o Amazon MQ fornece dois endpoints para cada protocolo de nível de conexão, mas apenas um endpoint está ativo em cada par de cada vez. Os sufixos -1 e -2 denotam um par redundante. Para obter mais informações, consulte [Opções de implantação do Amazon MQ para agentes ActiveMQ](#).

Para endpoints de protocolo de nível de conexão, você pode permitir que sua aplicação se conecte a qualquer endpoint usando o [Transporte de failover](#).

```
// Create a connection factory.
final ActiveMQConnectionFactory connectionFactory = new
    ActiveMQConnectionFactory(wireLevelEndpoint);

// Pass the sign-in credentials.
connectionFactory.setUsername(activeMqUsername);
connectionFactory.setPassword(activeMqPassword);

// Create a pooled connection factory.
final PooledConnectionFactory pooledConnectionFactory = new
    PooledConnectionFactory();
pooledConnectionFactory.setConnectionFactory(connectionFactory);
pooledConnectionFactory.setMaxConnections(10);

// Establish a connection for the producer.
final Connection producerConnection = pooledConnectionFactory.createConnection();
producerConnection.start();
```

```
// Close all connections in the pool.  
pooledConnectionFactory.clear();
```

Note

Os produtores de mensagens devem sempre usar a classe `PooledConnectionFactory`. Para obter mais informações, consulte [Sempre usar pooling de conexão](#).

2. Crie uma sessão, uma fila chamada `MyQueue` e um produtor de mensagens.

```
// Create a session.  
final Session producerSession = producerConnection.createSession(false,  
    Session.AUTO_ACKNOWLEDGE);  
  
// Create a queue named "MyQueue".  
final Destination producerDestination = producerSession.createQueue("MyQueue");  
  
// Create a producer from the session to the queue.  
final MessageProducer producer =  
    producerSession.createProducer(producerDestination);  
producer.setDeliveryMode(DeliveryMode.NON_PERSISTENT);
```

3. Crie a string da mensagem "Hello from Amazon MQ!" e, em seguida, envie a mensagem.

```
// Create a message.  
final String text = "Hello from Amazon MQ!";  
TextMessage producerMessage = producerSession.createTextMessage(text);  
  
// Send the message.  
producer.send(producerMessage);  
System.out.println("Message sent.");
```

4. Limpe o produtor.

```
producer.close();  
producerSession.close();  
producerConnection.close();
```

Para criar um consumidor de mensagens e receber a mensagem

Use as instruções a seguir para criar um produtor de mensagens e receber uma mensagem.

1. Crie uma fábrica de JMS conexões para o produtor de mensagens usando o endpoint do seu corretor e, em seguida, chame o `createConnection` método na fábrica.

```
// Create a connection factory.
final ActiveMQConnectionFactory connectionFactory = new
    ActiveMQConnectionFactory(wireLevelEndpoint);

// Pass the sign-in credentials.
connectionFactory.setUsername(activeMqUsername);
connectionFactory.setPassword(activeMqPassword);

// Establish a connection for the consumer.
final Connection consumerConnection = connectionFactory.createConnection();
consumerConnection.start();
```

Note

Os consumidores de mensagens nunca devem usar a classe `PooledConnectionFactory`. Para obter mais informações, consulte [Sempre usar pooling de conexão](#).

2. Crie uma sessão, uma fila chamada `MyQueue` e um consumidor de mensagens.

```
// Create a session.
final Session consumerSession = consumerConnection.createSession(false,
    Session.AUTO_ACKNOWLEDGE);

// Create a queue named "MyQueue".
final Destination consumerDestination = consumerSession.createQueue("MyQueue");

// Create a message consumer from the session to the queue.
final MessageConsumer consumer =
    consumerSession.createConsumer(consumerDestination);
```

3. Comece a aguardar mensagens e receba a mensagem quando ela chegar.

```
// Begin to wait for messages.
```

```
final Message consumerMessage = consumer.receive(1000);

// Receive the message when it arrives.
final TextMessage consumerTextMessage = (TextMessage) consumerMessage;
System.out.println("Message received: " + consumerTextMessage.getText());
```

Note

Ao contrário dos serviços de AWS mensagens (como a AmazonSQS), o consumidor está constantemente conectado à corretora.

4. Feche o consumidor, a sessão e a conexão.

```
consumer.close();
consumerSession.close();
consumerConnection.close();
```

Integração de agentes ActiveMQ com LDAP

Important


A integração LDAP não é compatível com agentes RabbitMQ.

Você pode acessar seus agentes do ActiveMQ usando os seguintes protocolos com TLS habilitado:

- [AMQP](#)
- [MQTT](#)
- MQTT pelo [WebSocket](#)
- [OpenWire](#)
- [STOMP](#)
- STOMP pelo WebSocket

O Amazon MQ oferece uma opção entre autenticação nativa do ActiveMQ e autenticação LDAP e autorização para gerenciar permissões de usuário. Para obter informações sobre restrições relacionadas a nomes de usuário e senhas do ActiveMQ, consulte [Usuários](#).

Para autorizar os usuários e grupos do ActiveMQ para trabalhar com filas e tópicos, você deve [editar a configuração do agente](#). O Amazon MQ usa o [Plugin de autenticação simples](#) do ActiveMQ para restringir a leitura e a gravação em destinos. Para obter mais informações e exemplos, consulte [Sempre configurar um mapa de autorização](#) e [authorizationEntry](#).

 Note

Atualmente, o Amazon MQ não é compatível com a autenticação de certificado de cliente.

Tópicos

- [Integrar LDAP com ActiveMQ](#)
- [Pré-requisitos](#)
- [Conceitos básicos do LDAP](#)
- [Como funciona a integração com LDAP](#)

Integrar LDAP com ActiveMQ

Você pode autenticar usuários do Amazon MQ por meio das credenciais armazenadas em seu servidor Lightweight Directory Access Protocol (LDAP). Você também pode adicionar, excluir e modificar usuários do Amazon MQ e atribuir permissões a tópicos e filas por meio dele. As operações de gerenciamento, como criação, atualização e exclusão de agentes, ainda exigem credenciais do IAM e não estão integradas ao LDAP.

Os clientes que desejam simplificar e centralizar sua autenticação e autorização do Agente Amazon MQ usando um servidor LDAP podem usar esse recurso. Manter todas as credenciais do usuário no servidor LDAP economiza tempo e esforço fornecendo um local central para armazenar e gerenciar essas credenciais.

O Amazon MQ é compatível com a LDAP usando o plugin Apache ActiveMQ JAAS. Qualquer servidor LDAP, como Microsoft Active Directory ou OpenLDAP que for suportado pelo plugin, também é compatível com o Amazon MQ. Para obter mais informações sobre o plugin, consulte a seção [Segurança](#) da documentação do ActiveMQ.

Além dos usuários, você pode especificar o acesso a tópicos e filas para um grupo específico ou um usuário por meio do servidor LDAP. Para fazer isso, crie entradas que representam tópicos e filas no servidor LDAP e, em seguida, atribua permissões a um usuário ou grupo LDAP específico. Em seguida, você pode configurar o broker para recuperar dados de autorização do servidor LDAP.

Pré-requisitos

Antes de adicionar compatibilidade com a LDAP a um agente Amazon MQ novo ou existente, você deve configurar uma conta de serviço. Essa conta de serviço é necessária para iniciar uma conexão com um servidor LDAP e deve ter as permissões corretas para fazer essa conexão. Esta conta de serviço configurará a autenticação LDAP para o seu agente. Quaisquer conexões sucessivas de cliente serão autenticadas através da mesma conexão.

Uma conta de serviço é uma conta no servidor LDAP que tem acesso para iniciar uma conexão. Isto é um requisito LDAP padrão e você deve fornecer as credenciais da conta de serviço apenas uma vez. Após a configuração da conexão, todas as conexões futuras do cliente são autenticadas por meio do servidor LDAP. Suas credenciais de conta de serviço são armazenadas de forma segura em um formulário criptografado, acessível somente para o Amazon MQ.

Para integrar com o ActiveMQ, é necessária uma Árvore de Informações de Diretório (DIT) específica no servidor LDAP. Para um exemplo `ldif` que mostra claramente esta estrutura, veja [Importe o seguinte arquivo LDIF para o servidor LDAP na Seção de Segurança da documentação do ActiveMQ.](#)

Conceitos básicos do LDAP

Para começar, navegue até o console do Amazon MQ e escolha Autorização e autenticação LDAP quando você cria uma nova Amazon MQ ou edita uma instância de agente existente.

Forneça as seguintes informações sobre a conta de serviço:

- Nome de domínio totalmente qualificado O local do servidor LDAP para o qual as solicitações de autenticação e autorização devem ser emitidas.

Note

O nome de domínio totalmente qualificado do servidor LDAP fornecido não deve incluir o protocolo ou o número da porta. O Amazon MQ substituirá o nome de domínio totalmente qualificado com o protocolo `ldaps` e anexará o número da porta `636`.

Por exemplo, se você fornecer o seguinte domínio totalmente qualificado: `example.com`, o Amazon MQ acessará seu servidor LDAP usando o seguinte URL: `ldaps://example.com:636`.

Para que o host do agente possa se comunicar com êxito com o servidor LDAP, o nome de domínio totalmente qualificado deve ser resolvido publicamente. Para manter o servidor

LDAP privado e seguro, restrinja o tráfego de entrada nas regras de entrada do servidor para permitir apenas o tráfego originado na VPC do agente.

- Nome de usuário da conta de serviço O nome distinto do usuário que será usado para executar a ligação inicial ao servidor LDAP.
- Senha da conta de serviço A senha do usuário que executa a vinculação inicial.

A imagem a seguir destaca onde fornecer esses detalhes.

Authentication and Authorization

Simple Authentication and Authorization
Authenticate and authorize users using the credentials stored in a broker.

LDAP Authentication and Authorization
Authenticate and authorize users using the credentials stored in an LDAP server.

Provide details for your organization's Active Directory or other LDAP server. [Info](#)

Fully qualified domain name

example.com

optional second server name

Service account username

Fully qualified name of the user that opens the connection to the directory server.

myserviceaccount

Service account password

The password for the service account provided above.

Maximum of 128 characters

Show

LDAP login configuration

Your server configuration to search and authenticate users.

User Base

Fully qualified name of the directory where you want to search for users.

ou=user, dc=example, dc=com

User Search Matching

The search criteria for the user object applied to the directory provided above.

(uid=0)

Role Base

Fully qualified name of the directory to search for a user's groups.

ou=user, dc=example, dc=com

Role Search Matching

The search criteria for the group object applied to the directory provided above.

(uid=0)

► Optional settings

Na Configuração de login LDAP, forneça as seguintes informações obrigatórias:

- Base de usuários O nome distinto do nó na DIT (árvore de informações de diretório) que será pesquisado para os usuários.
- Correspondência de pesquisa de usuários O filtro de pesquisa LDAP que será usado para localizar usuários na `userBase`. O nome de usuário do cliente é substituído no espaço reservado `{0}` no filtro de pesquisa. Para obter mais informações, consulte [Autenticação](#) e [Autorização](#).

- **Base de Funções** O nome distinto do nó na DIT que será pesquisado por funções. As funções podem ser configuradas como entradas de grupo LDAP explícitas em seu diretório. Uma entrada de função típica pode consistir em um atributo para o nome da função, como Nome comum (NC) e outro atributo, como `member`, com valores que representam os nomes distintos ou nomes de usuário dos usuários pertencentes ao grupo de funções. Por exemplo, dada a unidade organizacional, `group`, você pode fornecer o seguinte nome distinto: `ou=group,dc=example,dc=com`.
- **Correspondência de pesquisa de usuários** O filtro de pesquisa LDAP que será usado para localizar usuários na `roleBase`. O nome distinto do usuário resultante de comparado com `userSearchMatching` será substituído no espaço `{0}` reservado no filtro de pesquisa. O nome de usuário do cliente será substituído no lugar do `{1}` espaço reservado. Por exemplo, se as entradas de função em seu diretório incluírem um atributo chamado `member`, contendo os nomes de usuários para todos os usuários nessa função, você pode fornecer o seguinte filtro de pesquisa: `(member:=uid={1})`.

A imagem a seguir destaca onde especificar esses detalhes.

Authentication and Authorization

Simple Authentication and Authorization
Authenticate and authorize users using the credentials stored in a broker.

LDAP Authentication and Authorization
Authenticate and authorize users using the credentials stored in an LDAP server.

Provide details for your organization's Active Directory or other LDAP server. [Info](#)

Fully qualified domain name

example.com

optional second server name

Service account username

Fully qualified name of the user that opens the connection to the directory server.

myserviceaccount

Service account password

The password for the service account provided above.

Maximum of 128 characters

Show

LDAP login configuration

Your server configuration to search and authenticate users.

User Base

Fully qualified name of the directory where you want to search for users.

ou=user, dc=example, dc=com

User Search Matching

The search criteria for the user object applied to the directory provided above.

(uid=0)

Role Base

Fully qualified name of the directory to search for a user's groups.

ou=user, dc=example, dc=com

Role Search Matching

The search criteria for the group object applied to the directory provided above.

(uid=0)

► Optional settings

Nas Configurações opcionais, você pode fornecer as seguintes informações opcionais:

- **Nome da Função do Usuário** O nome do atributo LDAP na entrada do diretório do usuário para a associação a grupos do usuário. Em alguns casos, as funções de usuário podem ser identificadas pelo valor de um atributo na entrada do diretório do usuário. A opção `userRoleName` permite que você forneça o nome desse atributo. Por exemplo, vamos considerar a seguinte entrada de usuário:

```
dn: uid=jdoe,ou=user,dc=example,dc=com
objectClass: user
uid: jdoe
sn: jane
cn: Jane Doe
mail: j.doe@somecompany.com
memberOf: role1
userPassword: password
```

Para fornecer o `userRoleName` correto para o exemplo acima, você deve especificar o `memberOf` atributo. Se a autenticação for bem-sucedida, o usuário receberá a função `role1`.

- **Nome da Função** O atributo do nome do grupo em uma entrada de função cujo valor é o nome dessa função. Por exemplo, você pode especificar `cn` para o nome comum de uma entrada de grupo. Se a autenticação for bem-sucedida, o usuário receberá o valor do `cn` atributo para cada entrada de função da qual ele é membro.
- **Sub-árvore de pesquisa de usuários** Define o escopo da consulta de pesquisa do usuário LDAP. Se verdadeiro, o escopo é definido para pesquisar toda a sub-árvore sob o nó definido por `userBase`.
- **Sub-árvore de pesquisa de usuários** Define o escopo da consulta de pesquisa do usuário LDAP. Se verdadeiro, o escopo é definido para pesquisar toda a sub-árvore sob o nó definido por `roleBase`.

A imagem a seguir destaca onde especificar essas configurações opcionais.

Role Search Matching

The search criteria for the group object applied to the directory provided above.

```
(member:=uid={1})
```

▼ Optional settings**User Role Name**

Specifies the name of the LDAP attribute for the user group membership.

Role Name

Specifies the LDAP attribute that identifies the group name attribute in the object returned from the group membership query.

 User Search Subtree

This defines the directory search scope for the user. If set to true, scope is to search the entire sub-tree.

 Role Search Subtree

This defines the directory search scope for the role/group. If set to true, scope is to search the entire sub-tree.

Como funciona a integração com LDAP

Podemos pensar na integração em duas categorias principais: a estrutura de autenticação e a estrutura de autorização.

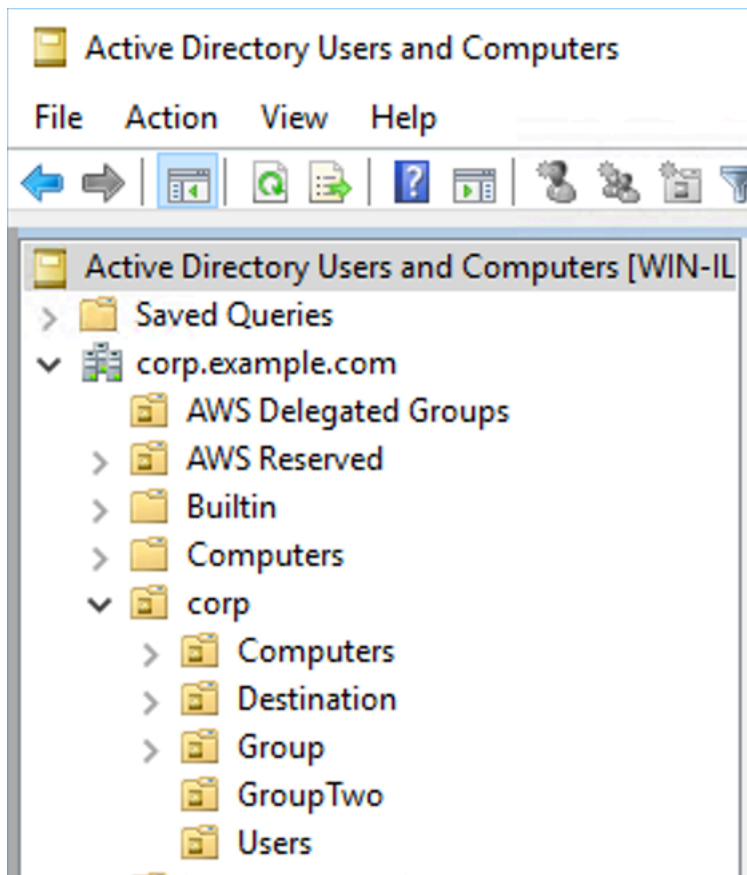
Autenticação

Para autenticação, as credenciais do cliente devem ser válidas. Essas credenciais são validadas em relação aos usuários na base de usuários no servidor LDAP.

A base de usuários fornecida ao agente ActiveMQ deve apontar para o nó na DIT onde os usuários são armazenados no servidor LDAP. Por exemplo, se você estiver usando o AWS Managed Microsoft AD e você tem os componentes de domínio corp, example e com, e dentro daqueles que você tem unidades organizacionais corp e Users, use o seguinte como base de usuários:

```
OU=Users,OU=corp,DC=corp,DC=example,DC=com
```

O agente do ActiveMQ procuraria usuários nesse local na DIT para autenticar solicitações de conexão do cliente para o broker.



Como o código-fonte ActiveMQ codifica o nome do atributo para os usuários como `uid`, você deve se certificar de que cada usuário tem esse atributo definido. Para simplificar, você pode usar o nome de usuário da conexão do usuário. Para obter mais informações, consulte o [ActiveMQ Código-fonte](#) e [Configurando mapeamentos de ID em Usuários e Computadores do Active Directory para Windows Server 2016 \(e versões subsequentes\)](#).

Para habilitar o acesso ao console do ActiveMQ para usuários específicos, verifique se eles pertencem ao grupo `amazonmq-console-admins`.

Autorização

Para autorização, as bases de pesquisa de permissões são especificadas na configuração do agente. A autorização é feita por destino (ou caractere coringa, destino definido) por meio do `cachedLdapAuthorizationMap` elemento encontrado no `activemq.xml` Arquivo de configuração. Para obter mais informações, consulte o [Módulo de autorização LDAP armazenado em cache](#).

Note

Para poder usar o elemento `cachedLDAPAuthorizationMap` no arquivo de configuração `activemq.xml` do seu agente, você deve escolher a opção LDAP Authentication and Authorization (Autorização e Autenticação LDAP) ao [criar uma configuração por meio do AWS Management Console](#), ou definir a propriedade `authenticationStrategy` como LDAP ao criar uma nova configuração usando a API do Amazon MQ.

Você deve fornecer os três atributos a seguir como parte do Elemento `cachedLDAPAuthorizationMap`:

- `queueSearchBase`
- `topicSearchBase`
- `tempSearchBase`

Important

Para evitar que informações confidenciais sejam colocadas diretamente no arquivo de configuração do agente, o Amazon MQ bloqueia que os seguintes atributos sejam usados no `cachedLdapAuthorizationMap`:

- `connectionURL`
- `connectionUsername`
- `connectionPassword`

Quando você cria um agente, o Amazon MQ substitui os valores que você fornece por meio do AWS Management Console, ou na propriedade `ldapServerMetadata` de sua solicitação de API para os atributos acima.

O seguinte exemplo demonstra o uso de deslocamentos `cachedLdapAuthorizationMap`.

```
<authorizationPlugin>
  <map>
    <cachedLDAPAuthorizationMap
```

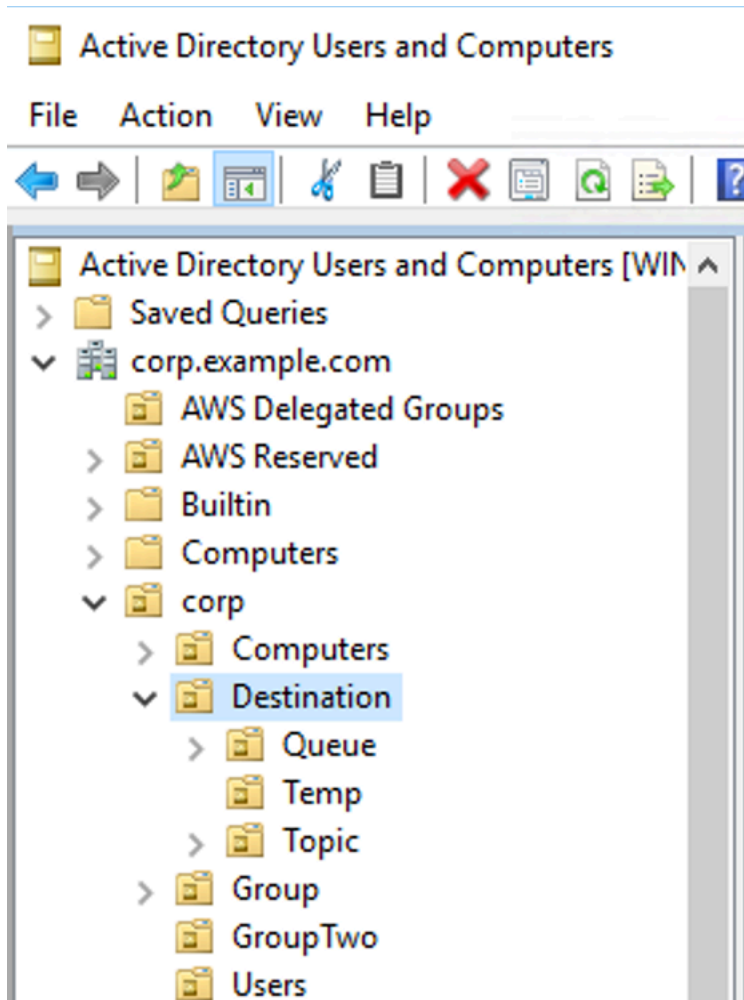


```
queueSearchBase="ou=Queue,ou=Destination,ou=corp,dc=corp,dc=example,dc=com"  
topicSearchBase="ou=Topic,ou=Destination,ou=corp,dc=corp,dc=example,dc=com"  
tempSearchBase="ou=Temp,ou=Destination,ou=corp,dc=corp,dc=example,dc=com"  
refreshInterval="300000"  
legacyGroupMapping="false"  
  />  
</map>  
</authorizationPlugin>
```

Esses valores identificam os locais dentro da DIT onde as permissões para cada tipo de destino são especificadas. Assim, para o exemplo acima com AWS Managed Microsoft AD, usando os mesmos componentes de domínio do corp, example e com, você especificaria uma unidade organizacional chamada destination para conter todos os tipos de destino. Dentro dessa UO, você criaria um para queues, um para topics, e um para tempdestinos.

Isso significaria que sua base de pesquisa de fila, que fornece informações de autorização para destinos da fila de tipo, teria o seguinte local em sua DIT:

```
OU=Queue,OU=Destination,OU=corp,DC=corp,DC=example,DC=com
```



Da mesma forma, as regras de permissões para tópicos e destinos temporários estariam localizadas no mesmo nível na DIT:

```
OU=Topic,OU=Destination,OU=corp,DC=corp,DC=example,DC=com
OU=Temp,OU=Destination,OU=corp,DC=corp,DC=example,DC=com
```

Dentro da UO para cada tipo de destino (fila, tópico, temporário), um coringa ou um nome de destino específico pode ser fornecido. Por exemplo, para fornecer uma regra de autorização para todas as filas que começam com o prefixo DEMO.EVENTS.\$., você pode criar a seguinte OU:

```
OU=DEMO.EVENTS.$,OU=Queue,OU=Destination,OU=corp,DC=corp,DC=example,DC=com
```

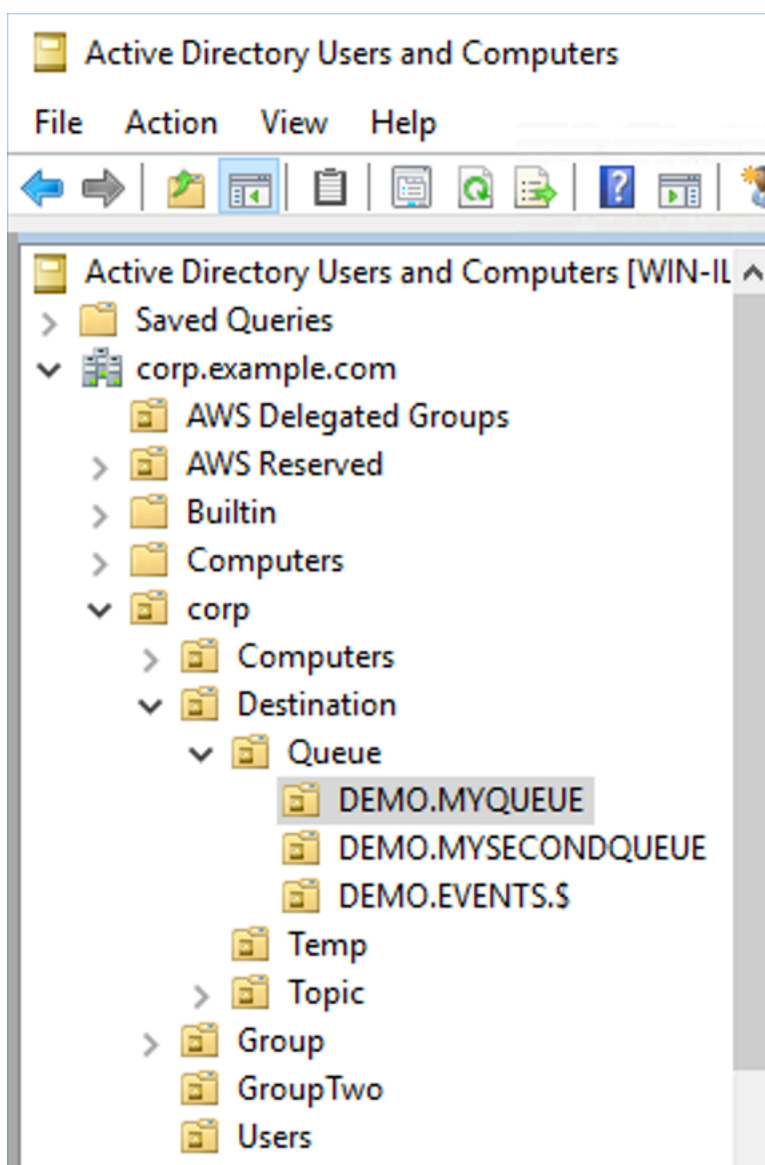
Note

A DEMO.EVENTS.\$ UO está dentro da Queue UO.

Para obter mais informações sobre coringas no ActiveMQ, consulte [Wildcards \(Coringas\)](#)

Para fornecer regras de autorização para filas específicas, como DEMO.MYQUEUE, especifique algo como o seguinte:

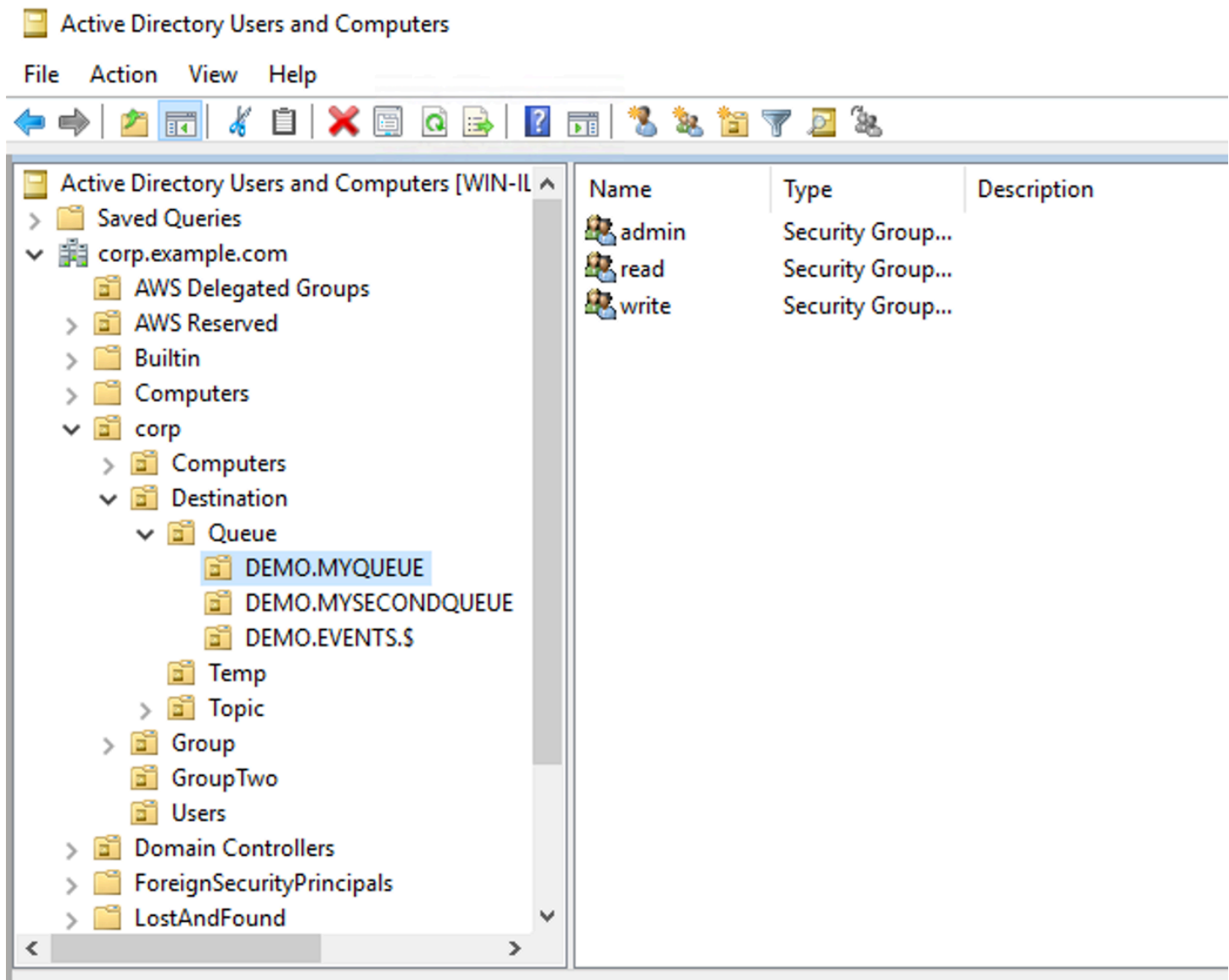
```
OU=DEMO.MYQUEUE,OU=Queue,OU=Destination,OU=corp,DC=corp,DC=example,DC=com
```



Security Groups (Grupos de segurança)

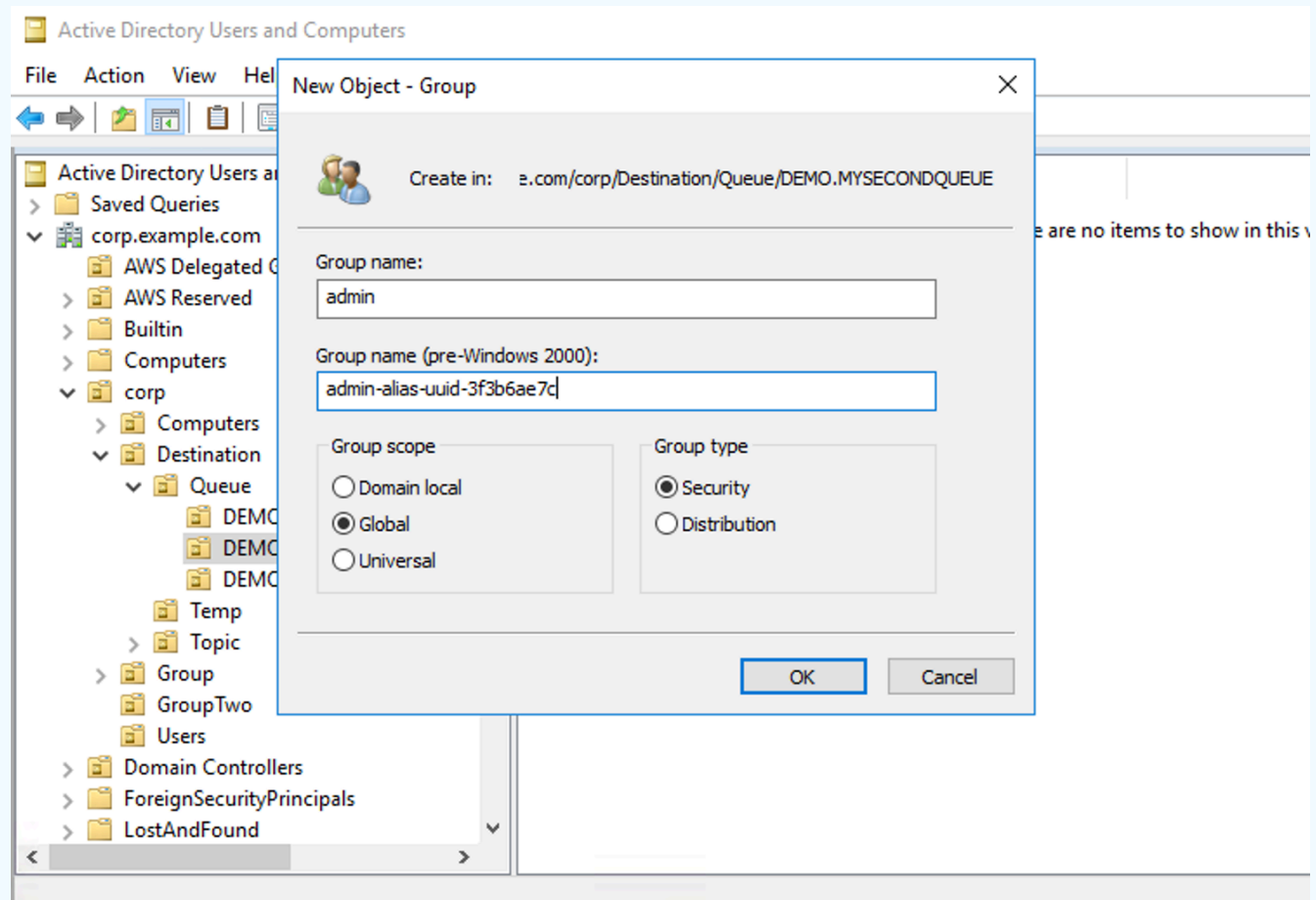
Dentro de cada UO que representa um destino ou um coringa, você deve criar três grupos de segurança. Tal como acontece com todas as permissões no ActiveMQ, estas são permissões de leitura/escrita/admin. Para obter mais informações sobre o que cada uma dessas permissões permite que um usuário faça, consulte [Segurança](#) na documentação do ActiveMQ.

Você deve nomear esses grupos de segurança `read`, `write`, e `admin`. Dentro de cada um desses grupos de segurança, você pode adicionar usuários ou grupos que terão permissão para executar as ações associadas. Você precisará desses grupos de segurança para cada conjunto de destinos coringa ou destino individual.



Note

Quando você cria o grupo de administração, surgirá um conflito com o nome do grupo. Esse conflito ocorre porque as regras anteriores ao Windows 2000 herdadas não permitem que grupos compartilhem o mesmo nome, mesmo que os grupos estejam em locais diferentes da DIT. O valor na caixa de texto pré-Windows 2000 não tem impacto na configuração, mas deve ser globalmente única. Para evitar esse conflito, você pode acrescentar um uuid sufixo para cada admin grupo.



Adicionar um usuário ao admin grupo de segurança para um destino específico permitirá que o usuário crie e exclua esse tópico. Adicionando-os ao read grupo de segurança permitirá que eles leiam a partir do destino e adicionando-os ao grupo write permitirá que eles escrevam no destino.

Além de adicionar usuários individuais às permissões do grupo de segurança, você também pode adicionar grupos inteiros. No entanto, como o ActiveMQ novamente codifica nomes de atributo para

grupos, você deve garantir que o grupo que deseja adicionar tem a classe de objeto `groupOfNames`, conforme mostrado no código-fonte do [ActiveMQ](#).

Para fazer isso, siga o mesmo processo que acontece com o `uid` para usuários. Consulte [Configurando mapeamentos de ID em Usuários e Computadores do Active Directory para Windows Server 2016 \(e versões subsequentes\)](#).

Criando um usuário do ActiveMQ broker

Um usuário do ActiveMQ é uma pessoa ou uma aplicação que pode acessar as filas e tópicos de um agente ActiveMQ. Você pode configurar usuários para que tenham permissões específicas. Por exemplo, é possível permitir que alguns usuários acessem o [Console da Web ActiveMQ](#).

Um grupo é um rótulo semântico. Você pode atribuir um grupo a um usuário e configurar permissões para grupos para enviar, receber e administrar filas e tópicos específicos.

Note

Não é possível configurar grupos independentemente dos usuários. Um rótulo de grupo é criado quando você adiciona pelo menos um usuário a ele e é excluído quando você remove todos os usuários dele.

Os exemplos a seguir mostram como criar, editar e excluir usuários de agente do Amazon MQ utilizando o AWS Management Console.

Criar um novo usuário do ActiveMQ broker

1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, escolha o nome do seu corretor (por exemplo, MyBroker) e escolha Exibir detalhes.

Sobre o **MyBroker** página, na seção Usuários, todos os usuários desta corretora são listados.

	Username	Console access	Groups	Pending modifications
<input type="radio"/>	paolo.santos	No	Devs	
<input type="radio"/>	jane.doe	Yes	Admins	

3. Selecione Criar usuário.
4. Na caixa de diálogo Create user (Criar usuário), digite um Username (Nome de usuário) e uma Password (Senha).
5. (Opcional) Digite os nomes dos grupos aos quais o usuário pertence, separados por vírgulas (por exemplo: Devs, Admins).
6. (Opcional) Para permitir que o usuário acesse o [Console da Web ActiveMQ](#), selecione Console da Web ActiveMQ.
7. Selecione Criar usuário.

 Important

Fazer alterações em um usuário não aplica as alterações ao usuário imediatamente. Para aplicar as alterações, você deve aguardar a próxima janela de manutenção ou [reiniciar o agente](#).

Editar um usuário do ActiveMQ broker

Para editar um usuário existente, faça o seguinte:

1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, escolha o nome do seu corretor (por exemplo, MyBroker) e escolha Exibir detalhes.

Sobre o **MyBroker** página, na seção Usuários, todos os usuários desta corretora são listados.

	Username ▼	Console access	Groups	Pending modifications
<input type="radio"/>	paolo.santos	No	Devs	
<input type="radio"/>	jane.doe	Yes	Admins	

3. Escolha suas credenciais de login e selecione Editar.

A caixa de diálogo Edit user (Editar usuário) será exibida.

4. (Opcional) Digite uma nova Password (Senha).
5. (Opcional) Adicione ou remova os nomes dos grupos aos quais o usuário pertence, separados por vírgulas (por exemplo: Managers, Admins).

- (Opcional) Para permitir que o usuário acesse o [Console da Web ActiveMQ](#), selecione Console da Web ActiveMQ.
- Para salvar as alterações do usuário, selecione Done (Concluído).

⚠ Important

Fazer alterações em um usuário não aplica as alterações ao usuário imediatamente. Para aplicar as alterações, você deve aguardar a próxima janela de manutenção ou [reiniciar o agente](#).

Excluir um usuário do ActiveMQ broker

Quando você não precisar mais de um usuário, poderá excluí-lo.

- Faça login no [console do Amazon MQ](#).
- Na lista de corretores, escolha o nome do seu corretor (por exemplo, MyBroker) e escolha Exibir detalhes.

Sobre o **MyBroker** página, na seção Usuários, todos os usuários desta corretora são listados.

	Username	Console access	Groups	Pending modifications
<input type="radio"/>	paolo.santos	No	Devs	
<input type="radio"/>	jane.doe	Yes	Admins	

- Selecione suas credenciais de login (por exemplo, **MyUser**) e, em seguida, escolha Excluir.
- Para confirmar a exclusão do usuário, em Excluir **MyUser**? caixa de diálogo, escolha Excluir.

⚠ Important

Fazer alterações em um usuário não aplica as alterações ao usuário imediatamente. Para aplicar as alterações, você deve aguardar a próxima janela de manutenção ou [reiniciar o agente](#).

Exemplos práticos da utilização do Java Message Service (JMS) com o ActiveMQ

Os exemplos a seguir mostram como você pode trabalhar com o ActiveMQ programaticamente:

- O código Java de OpenWire exemplo se conecta a um corretor, cria uma fila e envia e recebe uma mensagem. Para detalhamento e explicação, consulte [Connecting a Java application to your broker](#).
- O código Java de MQTT exemplo se conecta a um corretor, cria um tópico e publica e recebe uma mensagem.
- O código Java de WSS exemplo STOMP + se conecta a um corretor, cria uma fila e publica e recebe uma mensagem.

Pré-requisitos

Ativar VPC atributos

Para garantir que seu corretor esteja acessível dentro de vocêVPC, você deve habilitar os `enableDnsSupport` VPC atributos `enableDnsHostnames` e. Para obter mais informações, consulte [DNSSupport VPC em seu](#) Guia do VPC usuário da Amazon.

Habilitar conexões de entrada

Para trabalhar com o Amazon MQ de forma programática, você deve usar conexões de entrada.

1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, escolha o nome do seu corretor (por exemplo, MyBroker).
3. Sobre o **MyBroker** página, na seção Conexões, anote os endereços e portas do console web URL e dos protocolos de nível de fio do broker.
4. Na seção Details (Detalhes), em Security and network (Segurança e rede), escolha o nome do seu grupo de segurança ou



A página Grupos de Segurança do EC2 Painel é exibida.

5. Na lista de security group, escolha seu security group.
6. Na parte inferior da página, escolha Inbound (Entrada) e a seguir selecione Edit (Editar).

7. Na caixa de diálogo Editar regras de entrada, adicione uma regra para cada terminal URL ou endpoint que você deseja que seja acessível ao público (o exemplo a seguir mostra como fazer isso em um console web do broker).
 - a. Escolha Add Rule.
 - b. Em Tipo, selecione Personalizado TCP.
 - c. Para o Intervalo de Portas, digite a porta do console da Web (8162).
 - d. Para Source (Origem), deixe Custom (Personalizado) selecionado e, depois, digite o endereço IP do sistema ao qual deseja ser capaz de acessar o console da Web (por exemplo, 192.0.2.1).
 - e. Escolha Salvar.

Agora seu agente pode aceitar conexões de entrada.

Adicionar dependências de Java

OpenWire

Adicione os pacotes `activemq-client.jar` e `activemq-pool.jar` ao caminho da classe Java. O exemplo a seguir mostra essas dependências em um arquivo `pom.xml` do projeto Maven.

```
<dependencies>
  <dependency>
    <groupId>org.apache.activemq</groupId>
    <artifactId>activemq-client</artifactId>
    <version>5.15.16</version>
  </dependency>
  <dependency>
    <groupId>org.apache.activemq</groupId>
    <artifactId>activemq-pool</artifactId>
    <version>5.15.16</version>
  </dependency>
</dependencies>
```

Para obter mais informações sobre `activemq-client.jar`, consulte [Initial Configuration](#) (Configuração inicial) na documentação do Apache ActiveMQ.

MQTT

Adicione o pacote `org.eclipse.paho.client.mqttv3.jar` ao caminho da classe Java. O exemplo a seguir mostra essa dependência em um arquivo `pom.xml` do projeto Maven.

```
<dependencies>
    <dependency>
        <groupId>org.eclipse.paho</groupId>
        <artifactId>org.eclipse.paho.client.mqttv3</artifactId>
        <version>1.2.0</version>
    </dependency>
</dependencies>
```

Para obter mais informações sobre `org.eclipse.paho.client.mqttv3.jar`, consulte [Cliente Java Eclipse Paho](#).

STOMP+WSS

Adicione os seguintes pacotes ao caminho da classe Java:

- `spring-messaging.jar`
- `spring-websocket.jar`
- `javax.websocket-api.jar`
- `jetty-all.jar`
- `slf4j-simple.jar`
- `jackson-databind.jar`

O exemplo a seguir mostra essas dependências em um arquivo `pom.xml` do projeto Maven.

```
<dependencies>
    <dependency>
        <groupId>org.springframework</groupId>
        <artifactId>spring-messaging</artifactId>
        <version>5.0.5.RELEASE</version>
    </dependency>
    <dependency>
        <groupId>org.springframework</groupId>
        <artifactId>spring-websocket</artifactId>
        <version>5.0.5.RELEASE</version>
    </dependency>
```

```
<dependency>
  <groupId>javax.websocket</groupId>
  <artifactId>javax.websocket-api</artifactId>
  <version>1.1</version>
</dependency>
<dependency>
  <groupId>org.eclipse.jetty.aggregate</groupId>
  <artifactId>jetty-all</artifactId>
  <type>pom</type>
  <version>9.3.3.v20150827</version>
</dependency>
<dependency>
  <groupId>org.slf4j</groupId>
  <artifactId>slf4j-simple</artifactId>
  <version>1.6.6</version>
</dependency>
<dependency>
  <groupId>com.fasterxml.jackson.core</groupId>
  <artifactId>jackson-databind</artifactId>
  <version>2.5.0</version>
</dependency>
</dependencies>
```

Para obter mais informações, consulte [STOMP Support](#) na documentação do Spring Framework.

Um mazonMQExample .java

Important

No código de exemplo a seguir, os produtores e consumidores são executados em um único thread. Para sistemas de produção (ou para testar o failover de instância do agente), certifique-se de que seus produtores e consumidores sejam executados em hosts ou threads separados.

OpenWire

```
/*
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * Licensed under the Apache License, Version 2.0 (the "License").
```

```
* You may not use this file except in compliance with the License.
* A copy of the License is located at
*
* https://aws.amazon.com/apache2.0
*
* or in the "license" file accompanying this file. This file is distributed
* on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either
* express or implied. See the License for the specific language governing
* permissions and limitations under the License.
*
*/
```

```
import org.apache.activemq.ActiveMQConnectionFactory;
import org.apache.activemq.jms.pool.PooledConnectionFactory;

import javax.jms.*;

public class AmazonMQExample {

    // Specify the connection parameters.
    private final static String WIRE_LEVEL_ENDPOINT
        = "ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
east-2.amazonaws.com:61617";
    private final static String ACTIVE_MQ_USERNAME =
        "MyUsername123";
    private final static String ACTIVE_MQ_PASSWORD =
        "MyPassword456";

    public static void main(String[] args) throws JMSEException {
        final ActiveMQConnectionFactory connectionFactory =
            createActiveMQConnectionFactory();
        final PooledConnectionFactory pooledConnectionFactory =
            createPooledConnectionFactory(connectionFactory);

        sendMessage(pooledConnectionFactory);
        receiveMessage(connectionFactory);

        pooledConnectionFactory.stop();
    }

    private static void
    sendMessage(PooledConnectionFactory pooledConnectionFactory)
    throws JMSEException {
        // Establish a connection for the producer.
```

```
        final Connection producerConnection =
pooledConnectionFactory
            .createConnection();
        producerConnection.start();

        // Create a session.
        final Session producerSession = producerConnection
            .createSession(false, Session.AUTO_ACKNOWLEDGE);

        // Create a queue named "MyQueue".
        final Destination producerDestination = producerSession
            .createQueue("MyQueue");

        // Create a producer from the session to the queue.
        final MessageProducer producer = producerSession
            .createProducer(producerDestination);
        producer.setDeliveryMode(DeliveryMode.NON_PERSISTENT);

        // Create a message.
        final String text = "Hello from Amazon MQ!";
        final TextMessage producerMessage = producerSession
            .createTextMessage(text);

        // Send the message.
        producer.send(producerMessage);
        System.out.println("Message sent.");

        // Clean up the producer.
        producer.close();
        producerSession.close();
        producerConnection.close();
    }

    private static void
    receiveMessage(ActiveMQConnectionFactory connectionFactory)
    throws JMSEException {
        // Establish a connection for the consumer.
        // Note: Consumers should not use PooledConnectionFactory.
        final Connection consumerConnection =
connectionFactory.createConnection();
        consumerConnection.start();

        // Create a session.
        final Session consumerSession = consumerConnection
```

```
        .createSession(false, Session.AUTO_ACKNOWLEDGE);

// Create a queue named "MyQueue".
final Destination consumerDestination = consumerSession
    .createQueue("MyQueue");

// Create a message consumer from the session to the queue.
final MessageConsumer consumer = consumerSession
    .createConsumer(consumerDestination);

// Begin to wait for messages.
final Message consumerMessage = consumer.receive(1000);

// Receive the message when it arrives.
final TextMessage consumerTextMessage = (TextMessage)
consumerMessage;

    System.out.println("Message received: " +
consumerTextMessage.getText());

// Clean up the consumer.
consumer.close();
consumerSession.close();
consumerConnection.close();
}

private static PooledConnectionFactory
createPooledConnectionFactory(ActiveMQConnectionFactory
connectionFactory) {
// Create a pooled connection factory.
final PooledConnectionFactory pooledConnectionFactory =
    new PooledConnectionFactory();

pooledConnectionFactory.setConnectionFactory(connectionFactory);
pooledConnectionFactory.setMaxConnections(10);
return pooledConnectionFactory;
}

private static ActiveMQConnectionFactory
createActiveMQConnectionFactory() {
// Create a connection factory.
final ActiveMQConnectionFactory connectionFactory =
    new ActiveMQConnectionFactory(WIRE_LEVEL_ENDPOINT);

// Pass the sign-in credentials.
```

```
        connectionFactory.setUsername(ACTIVE_MQ_USERNAME);
        connectionFactory.setPassword(ACTIVE_MQ_PASSWORD);
        return connectionFactory;
    }
}
```

MQTT

```
/*
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * Licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License.
 * A copy of the License is located at
 *
 * https://aws.amazon.com/apache2.0
 *
 * or in the "license" file accompanying this file. This file is distributed
 * on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either
 * express or implied. See the License for the specific language governing
 * permissions and limitations under the License.
 */

import org.eclipse.paho.client.mqttv3.*;

public class AmazonMQExampleMqtt implements MqttCallback {

    // Specify the connection parameters.
    private final static String WIRE_LEVEL_ENDPOINT =
        "ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
east-2.amazonaws.com:8883";
    private final static String ACTIVE_MQ_USERNAME =
        "MyUsername123";
    private final static String ACTIVE_MQ_PASSWORD =
        "MyPassword456";

    public static void main(String[] args) throws Exception {
        new AmazonMQExampleMqtt().run();
    }

    private void run() throws MqttException, InterruptedException {
```



```
        // Specify the topic name and the message text.
        final String topic = "myTopic";
        final String text = "Hello from Amazon MQ!";

        // Create the MQTT client and specify the connection
options.
        final String clientId = "abc123";
        final MqttClient client = new
MqttClient(WIRE_LEVEL_ENDPOINT, clientId);
        final MqttConnectOptions connOpts = new
MqttConnectOptions();

        // Pass the sign-in credentials.
        connOpts.setUsername(ACTIVE_MQ_USERNAME);
        connOpts.setPassword(ACTIVE_MQ_PASSWORD.toCharArray());

        // Create a session and subscribe to a topic filter.
        client.connect(connOpts);
        client.setCallback(this);
        client.subscribe("+");

        // Create a message.
        final MqttMessage message = new
MqttMessage(text.getBytes());

        // Publish the message to a topic.
        client.publish(topic, message);
        System.out.println("Published message.");

        // Wait for the message to be received.
        Thread.sleep(3000L);

        // Clean up the connection.
        client.disconnect();
    }

    @Override
    public void connectionLost(Throwable cause) {
        System.out.println("Lost connection.");
    }

    @Override
    public void messageArrived(String topic, MqttMessage message)
throws MqttException {
```

```

        System.out.println("Received message from topic " + topic +
": " + message);
    }

    @Override
    public void deliveryComplete(IMqttDeliveryToken token) {
        System.out.println("Delivered message.");
    }
}

```

STOMP+WSS

```

/*
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * Licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License.
 * A copy of the License is located at
 *
 * https://aws.amazon.com/apache2.0
 *
 * or in the "license" file accompanying this file. This file is distributed
 * on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either
 * express or implied. See the License for the specific language governing
 * permissions and limitations under the License.
 */

import
org.springframework.messaging.converter.StringMessageConverter;
import org.springframework.messaging.simp.stomp.*;
import org.springframework.web.socket.WebSocketHttpHeaders;
import org.springframework.web.socket.client.WebSocketClient;
import
org.springframework.web.socket.client.standard.StandardWebSocketClient;
import
org.springframework.web.socket.messaging.WebSocketStompClient;

import java.lang.reflect.Type;

public class AmazonMQExampleStompWss {

    // Specify the connection parameters.

```

```
private final static String DESTINATION = "/queue";
private final static String WIRE_LEVEL_ENDPOINT =
    "wss://b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
east-2.amazonaws.com:61619";
private final static String ACTIVE_MQ_USERNAME =
    "MyUsername123";
private final static String ACTIVE_MQ_PASSWORD =
    "MyPassword456";

public static void main(String[] args) throws Exception {
    final AmazonMQExampleStompWss example = new
AmazonMQExampleStompWss();

    final StompSession stompSession = example.connect();
    System.out.println("Subscribed to a destination using
session.");

    example.subscribeToDestination(stompSession);

    System.out.println("Sent message to session.");
    example.sendMessage(stompSession);
    Thread.sleep(60000);
}

private StompSession connect() throws Exception {
    // Create a client.
    final WebSocketClient client = new
StandardWebSocketClient();
    final WebSocketStompClient stompClient = new
WebSocketStompClient(client);
    stompClient.setMessageConverter(new
StringMessageConverter());

    final WebSocketHttpHeaders headers = new
WebSocketHttpHeaders();

    // Create headers with authentication parameters.
    final StompHeaders head = new StompHeaders();
    head.add(StompHeaders.LOGIN, ACTIVE_MQ_USERNAME);
    head.add(StompHeaders.PASSCODE, ACTIVE_MQ_PASSWORD);

    final StompSessionHandler sessionHandler = new
MySessionHandler();

    // Create a connection.
```

```
        return stompClient.connect(WIRE_LEVEL_ENDPOINT, headers,
head,        sessionHandler).get();
    }

    private void subscribeToDestination(final StompSession
stompSession) {
        stompSession.subscribe(DESTINATION, new MyFrameHandler());
    }

    private void sendMessage(final StompSession stompSession) {
MQ!".getBytes());
        stompSession.send(DESTINATION, "Hello from Amazon
    }

    private static class MySessionHandler extends
StompSessionHandlerAdapter {
        public void afterConnected(final StompSession stompSession,
            final StompHeaders stompHeaders) {
            System.out.println("Connected to broker.");
        }
    }

    private static class MyFrameHandler implements StompFrameHandler
{
        public Type getPayloadType(final StompHeaders headers) {
            return String.class;
        }

        public void handleFrame(final StompHeaders stompHeaders,
            final Object message) {
            System.out.print("Received message from topic: " +
message);
        }
    }
}
```

Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ

O Apache ActiveMQ organiza números de versão de acordo com a especificação de versionamento semântico como X.Y.Z. Nas implementações do Amazon MQ para ActiveMQ, indica a versão principal, Y representa a versão secundária e X indica o número da versão do patch. Z O Amazon MQ considera que uma alteração de versão é principal se os números de versão principais mudarem. Por exemplo, a atualização da versão 5.17 para a 6.0 é considerada uma atualização importante da versão. Uma alteração de versão é considerada pequena se apenas o número da versão secundária ou do patch for alterado. Por exemplo, atualizando a partir da versão 5.17 a 5.18 é considerado um pequeno upgrade de versão.

O Amazon MQ para ActiveMQ recomenda que todos os corretores usem a última versão secundária compatível. Para obter instruções sobre como atualizar a versão do mecanismo de corretagem, consulte [Atualizar uma versão do mecanismo de corretora Amazon MQ](#).

Versões de motor suportadas no Amazon MQ para ActiveMQ

O calendário de suporte da versão Amazon MQ indica quando uma versão do broker Engine chegará ao fim do suporte. Quando uma versão chega ao fim do suporte, o Amazon MQ atualiza automaticamente todos os corretores dessa versão para a próxima versão compatível. Essa atualização ocorre durante as janelas de manutenção programada da sua corretora, dentro dos 45 dias após a end-of-support data.

O Amazon MQ avisa com pelo menos 90 dias de antecedência antes que uma versão chegue ao fim do suporte. Recomendamos atualizar seu corretor antes da end-of-support data para evitar interrupções. Além disso, você não pode criar novos corretores em versões programadas para o fim do suporte dentro de 30 dias da data de término do suporte.

Versão Apache ActiveMQ	Fim do suporte no Amazon MQ
ActiveMQ 5.18 (recomendado)	
ActiveMQ 5.17	
ActiveMQ 5.16	15 de novembro de 2024
ActiveMQ 5.15	16 de setembro de 2024

Ao criar um novo agente do Amazon MQ para ActiveMQ, você pode especificar qualquer versão do mecanismo do ActiveMQ compatível. Se você não especificar o número da versão do mecanismo ao criar um agente, o Amazon MQ automaticamente usará como padrão o número da versão mais recente do mecanismo.

Atualizações da versão do motor

Você pode atualizar manualmente seu corretor a qualquer momento para a próxima versão principal ou secundária compatível. Quando você ativa as [atualizações automáticas de versões secundárias](#), o Amazon MQ atualiza seu agente para a versão de patch mais recente suportada durante [a](#) janela de manutenção.

Para obter mais informações sobre como atualizar manualmente sua corretora, consulte [the section called “Atualizar a versão do mecanismo”](#).

Listando as versões compatíveis do mecanismo

Você pode listar todas as versões de mecanismos secundários e principais compatíveis usando o [describe-broker-instance-options](#) AWS CLI comando.

```
aws mq describe-broker-instance-options
```

Para filtrar os resultados por mecanismo e tipo de instância, use a opção `--engine-type` e `--host-instance-type`, conforme mostrado a seguir.

```
aws mq describe-broker-instance-options --engine-type engine-type --host-instance-type instance-type
```

Por exemplo, para filtrar os resultados do ActiveMQ `mq.m5.large` e do tipo de instância, substitua *engine-type* com `ACTIVEMQ` e *instance-type* com `commq.m5.large`.

Amazon MQ para tipos de armazenamento ActiveMQ

O Amazon MQ para ActiveMQ oferece suporte ao Amazon Elastic File System (EFS) e ao Amazon Elastic Block Store (EBS). Por padrão, os corretores ActiveMQ usam a Amazon EFS para armazenamento de corretores. Para aproveitar a alta durabilidade e a replicação em várias zonas de disponibilidade, use a AmazonEFS. Para aproveitar a baixa latência e a alta taxa de transferência, use a Amazon. EBS

⚠ Important

- Você pode usar a Amazon EBS somente com a família de tipos de instância do mq .m5 broker.
- Embora você possa alterar o tipo de instância de agente, você não pode alterar o tipo de armazenamento do agente depois de criar o agente.
- A Amazon EBS replica dados dentro de uma única zona de disponibilidade e não suporta o modo de implantação ativo/em espera do [ActiveMQ](#).

Diferenças entre tipos de armazenamento

A tabela a seguir fornece uma breve visão geral das diferenças entre os tipos de EBS armazenamento em memóriaEFS, Amazon e Amazon para agentes ActiveMQ.

Tipo de armazenamento	Persistência	Exemplo de caso de uso	Número máximo aproximado de mensagens enfileiradas por produtor, por segundo (mensagem de 1 KB)	Replicação
Na memória	Não persistente	<ul style="list-style-type: none"> • Cotações de ações • Atualizações de dados de localização • Dados alterados com frequência 	5.000	Nenhum
Amazon EBS	Persistente	<ul style="list-style-type: none"> • Grandes volumes de texto 	500	Várias cópias em uma única zona

Tipo de armazenamento	Persistência	Exemplo de caso de uso	Número máximo aproximado de mensagens enfileiradas por produtor, por segundo (mensagem de 1 KB)	Replicação
		<ul style="list-style-type: none"> Processamento de pedidos 		de disponibilidade (AZ)
Amazon EFS	Persistente	Transações financeiras	80	Várias cópias em várias AZs

O armazenamento de mensagens na memória fornece a latência mais baixa e a taxa de transferência mais alta. No entanto, as mensagens são perdidas durante a substituição da instância ou a reinicialização do agente.

EFSA Amazon foi projetada para ser altamente durável, replicada em vários componentes AZs para evitar a perda de dados resultante da falha de um único componente ou de um problema que afete a disponibilidade de uma AZ. A Amazon EBS é otimizada para taxa de transferência e replicada em vários servidores em uma única AZ.

Práticas recomendadas do Amazon MQ para ActiveMQ

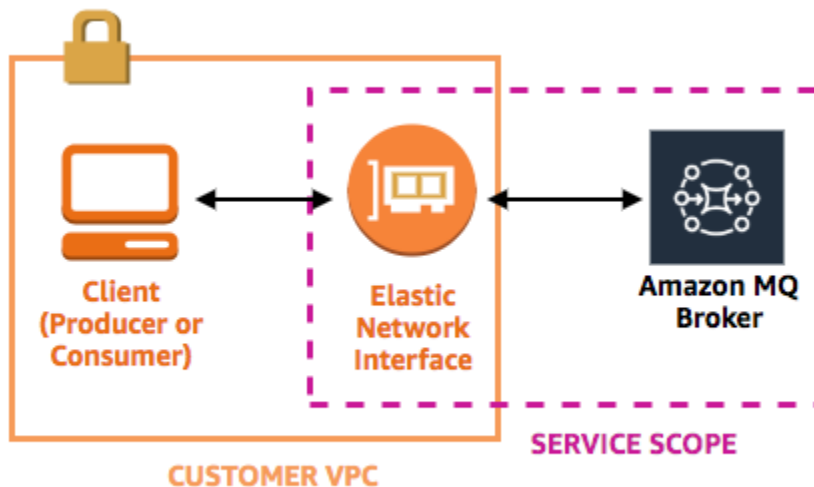
Use esta seção como referência para localizar rapidamente as recomendações para maximizar a performance e minimizar os custos de taxa de transferência para trabalhar com agentes do ActiveMQ no Amazon MQ.

Nunca modifique ou exclua a interface de rede elástica do Amazon MQ

[Quando você cria um agente Amazon MQ pela primeira vez, o Amazon MQ provisiona uma interface de rede elástica Virtual Private Cloud VPC \(\) em sua conta e, portanto, exige várias permissões. EC2](#) A interface de rede permite que seu cliente (produtor ou consumidor) se comunique com o agente do Amazon MQ. A interface de rede é considerada dentro do escopo do serviço do Amazon MQ, apesar de fazer parte da sua conta. VPC

⚠ Warning

Você não deve modificar ou excluir essa interface de rede. Modificar ou excluir a interface de rede pode causar uma perda permanente da conexão entre você VPC e seu corretor.



Sempre usar pooling de conexão

Em um cenário com um único produtor e um único consumidor (como o [Começando: Criando e conectando-se a um corretor ActiveMQ](#) tutorial), você pode usar uma única [ActiveMQConnectionFactory](#) classe para cada produtor e consumidor. Por exemplo:


```
// Create a connection factory.
final ActiveMQConnectionFactory connectionFactory = new
    ActiveMQConnectionFactory(wireLevelEndpoint);

// Pass the sign-in credentials.
connectionFactory.setUsername(activeMqUsername);
connectionFactory.setPassword(activeMqPassword);

// Establish a connection for the consumer.
final Connection consumerConnection = connectionFactory.createConnection();
consumerConnection.start();
```

No entanto, em cenários mais realistas com vários produtores e consumidores, pode ser dispendioso e ineficiente criar um grande número de conexões para vários produtores. Nesses cenários, você

deve agrupar solicitações de vários produtores usando a classe [PooledConnectionFactory](#). Por exemplo:

 Note

Os consumidores de mensagens nunca devem usar a classe `PooledConnectionFactory`.

```
// Create a connection factory.
final ActiveMQConnectionFactory connectionFactory = new
    ActiveMQConnectionFactory(wireLevelEndpoint);

// Pass the sign-in credentials.
connectionFactory.setUsername(activeMqUsername);
connectionFactory.setPassword(activeMqPassword);

// Create a pooled connection factory.
final PooledConnectionFactory pooledConnectionFactory = new PooledConnectionFactory();
pooledConnectionFactory.setConnectionFactory(connectionFactory);
pooledConnectionFactory.setMaxConnections(10);

// Establish a connection for the producer.
final Connection producerConnection = pooledConnectionFactory.createConnection();
producerConnection.start();
```

Sempre usar o transporte de failover para conectar-se a vários endpoints de operador

Se você precisar que a aplicação se conecte a vários endpoints do agente — por exemplo, ao usar um modo de implantação [ativo/em espera](#) ou ao [migrar de um agente de mensagens no local para o Amazon MQ](#) — use o [transporte de failover](#) para permitir que os consumidores se conectem aleatoriamente a um deles. Por exemplo:

```
failover:(ssl://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-
east-2.amazonaws.com:61617,ssl://b-987615k4-32ji-109h-8gfe-7d65c4b132a1-2.mq.us-
east-2.amazonaws.com:61617)?randomize=true
```

Evite usar seletores de mensagens

É possível usar [JMSseletores](#) para anexar filtros às assinaturas de tópicos (para encaminhar mensagens aos consumidores com base em seu conteúdo). No entanto, o uso de JMS seletores preenche o buffer de filtro do agente Amazon MQ, impedindo que ele filtre mensagens.

Em geral, evite permitir que os consumidores roteiem mensagens, pois, para um bom desacoplamento de consumidores e produtores, ambos devem ser temporários.

Preferir destinos virtuais a assinaturas duráveis

Uma [assinatura durável](#) pode ajudar a garantir que o consumidor receba todas as mensagens publicadas em um tópico, por exemplo, após a restauração de uma conexão perdida. No entanto, o uso de assinaturas duráveis também impede o uso de consumidores da concorrência e pode apresentar problemas de performance em escala. Considere o uso de [destinos virtuais](#), em vez disso.

Se estiver usando o Amazon VPC Peering, evite clientes ao IPs alcance CIDR **10.0.0.0/16**

Se você estiver configurando o Amazon VPC peering entre a infraestrutura local e seu agente Amazon MQ, você não deve configurar conexões de clientes dentro do alcance. IPs CIDR 10.0.0.0/16

Desativar o armazenamento e a expedição simultâneos para filas com consumidores lentos

Por padrão, o Amazon MQ é otimizado para filas com consumidores rápidos:

- Os consumidores são considerados rápidos se conseguem acompanhar a taxa de mensagens geradas pelos produtores.
- Os consumidores são considerados lentos se uma fila cria um acúmulo de mensagens não confirmadas, o que pode reduzir a taxa de transferência do produtor.

Para instruir o Amazon MQ para ser otimizado para filas com consumidores lentos, defina o atributo `concurrentStoreAndDispatchQueues` como `false`. Para obter uma configuração de exemplo, consulte [concurrentStoreAndDispatchQueues](#).

Selecionar o tipo de instância de agente correto para obter a melhor taxa de transferência

A taxa de transferência de mensagens de um [tipo de instância de agente](#) depende do caso de uso da aplicação e dos seguintes fatores:

- Uso do ActiveMQ no modo persistente
- Tamanho da mensagem
- O número de produtores e consumidores
- O número de destinos

Noções básicas sobre o relacionamento entre o tamanho, a latência e a taxa de transferência de mensagens

Dependendo do caso de uso, um tipo de instância de agente maior pode não necessariamente melhorar a taxa de transferência do sistema. Quando o ActiveMQ grava mensagens em um armazenamento durável, o tamanho de suas mensagens determina o fator limitante do sistema:

- Se as mensagens forem menores que 100 KB, a latência do armazenamento persistente será o fator limitante.
- Se as mensagens forem maiores que 100 KB, a taxa de transferência do armazenamento persistente será o fator limitante.

Ao usar o ActiveMQ no modo persistente, a gravação no armazenamento ocorrerá normalmente quando houver alguns consumidores ou quando os consumidores forem lentos. No modo não persistente, a gravação no armazenamento também ocorrerá com consumidores lentos se a memória do heap da instância de agente estiver cheia.

Para determinar o melhor tipo de instância de agente para a sua aplicação, recomendamos testar diferentes tipos de instância de operador. Para obter mais informações, consulte [Broker instance types](#) e também [Medindo a taxa de transferência do Amazon MQ usando JMS](#) o Benchmark.

Casos de uso de tipos de instância de agente maiores

Há três casos de uso comuns quando tipos de instância de agente maiores melhoram a taxa de transferência:

- **Modo não persistente:** quando sua aplicação é menos sensível à perda de mensagens durante o [failover de instância de agente](#) (por exemplo, ao transmitir placares de esportes), muitas vezes você pode usar o modo não persistente do ActiveMQ. Nesse modo, o ActiveMQ grava mensagens no armazenamento persistente somente se a memória do heap da instância de agente está cheia. Os sistemas que usam o modo não persistente podem se beneficiar da maior quantidade de memória e da rede cada CPU vez mais rápida disponível em tipos maiores de instâncias de broker.
- **Consumidores rápidos:** quando os consumidores ativos estão disponíveis e o sinalizador [concurrentStoreAndDispatchQueues](#) está habilitado, o ActiveMQ permite o fluxo das mensagens diretamente do produtor para o consumidor sem enviar mensagens ao armazenamento (mesmo em modo persistente). Se a sua aplicação pode consumir mensagens rapidamente (ou se você pode projetar seus consumidores para fazer isso), a aplicação pode se beneficiar de um tipo de instância de agente maior. Para permitir que seu aplicativo consuma mensagens com mais rapidez, adicione threads de consumidor às instâncias do aplicativo ou expanda as instâncias do aplicativo verticalmente ou horizontalmente.
- **Transações em lote:** quando você usa o modo persistente e envia várias mensagens por transação, você pode obter uma taxa de transferência de mensagens em geral mais alta usando tipos de instância de agente maiores. Para obter mais informações, consulte [Devo usar transações?](#) na documentação do ActiveMQ.

Escolha o tipo de armazenamento de agente correto para obter a melhor taxa de transferência

Para aproveitar a alta durabilidade e a replicação em várias zonas de disponibilidade, use a AmazonEFS. Para aproveitar a baixa latência e a alta taxa de transferência, use a Amazon. EBS Para obter mais informações, consulte [Storage](#).

Configurar sua rede de agentes corretamente

Quando você cria uma [rede de agentes](#), configure-a corretamente para seu aplicativo:

- **Ativar modo persistente:** Como (em relação a seus pares) cada instância de agente atua como um produtor ou um consumidor, redes de agentes não fornecem a replicação distribuída de mensagens. O primeiro agente que atua como um consumidor recebe uma mensagem e a mantém para armazenamento. Esse agente envia uma confirmação para o produtor e encaminha

a mensagem para o próximo agente. Quando o segundo agente reconhece a persistência da mensagem, o primeiro agente exclui a mensagem.

Se o modo persistente é desativado, o primeiro agente reconhece o produtor sem manter a mensagem para armazenamento. Para obter mais informações, consulte [Armazenamento de mensagem replicada](#) e [Qual é a diferença entre entrega persistente e não persistente?](#) na documentação do Apache ActiveMQ.

- Não desative mensagens de aviso para instâncias de agente: Para obter mais informações, consulte [Mensagens de aviso](#) na documentação do Apache ActiveMQ.
- Não use a descoberta do agente multicast: O Amazon MQ não é compatível com a descoberta do agente usando multicast. Para obter mais informações, consulte [Qual é a diferença entre a descoberta, multicast e zeroconf?](#) na documentação do Apache ActiveMQ.

Evite reinicializações lentas recuperando transações XA preparadas

O ActiveMQ oferece suporte a transações distribuídas (XA). Saber como o ActiveMQ processa transações XA pode ajudar a evitar tempos de recuperação mais lentos para reinicializações do agente e failovers no Amazon MQ.

Transações XA preparadas não resolvidas são reproduzidas novamente em cada reinicialização. Se elas permanecerem não resolvidas, o número de transações ficará cada vez maior com o tempo, aumentando significativamente o tempo necessário para inicializar o operador. Isso afeta o tempo de reinicialização e de failover. Você deve resolver essas transações com um `commit()` ou um, de `rollback()` para que não haja degradação de performance ao longo do tempo.

Para monitorar suas transações XA preparadas não resolvidas, você pode usar a `JournalFilesForFastRecovery` métrica no Amazon CloudWatch Logs. Se esse número estiver aumentando ou for consistentemente maior que 1, você deve recuperar suas transações não resolvidas com um código semelhante ao exemplo a seguir. Para obter mais informações, consulte [Cotas no Amazon MQ](#).

O código de exemplo a seguir aborda transações XA preparadas e as encerra com um `rollback()`.

```
import org.apache.activemq.ActiveMQXAConnectionFactory;

import javax.jms.XAConnection;
import javax.jms.XASession;
import javax.transaction.xa.XAResource;
```

```
import javax.transaction.xa.Xid;

public class RecoverXaTransactions {
    private static final ActiveMQXAConnectionFactory ACTIVE_MQ_CONNECTION_FACTORY;
    final static String WIRE_LEVEL_ENDPOINT =
        "tcp://localhost:61616";
    static {
        final String activeMqUsername = "MyUsername123";
        final String activeMqPassword = "MyPassword456";
        ACTIVE_MQ_CONNECTION_FACTORY = new
ActiveMQXAConnectionFactory(activeMqUsername, activeMqPassword, WIRE_LEVEL_ENDPOINT);
        ACTIVE_MQ_CONNECTION_FACTORY.setUserUsername(activeMqUsername);
        ACTIVE_MQ_CONNECTION_FACTORY.setPassword(activeMqPassword);
    }

    public static void main(String[] args) {
        try {
            final XAConnection connection =
ACTIVE_MQ_CONNECTION_FACTORY.createXAConnection();
            XASession xaSession = connection.createXASession();
            XAResource xaRes = xaSession.getXAResource();

            for (Xid id : xaRes.recover(XAResource.TMENDRSCAN)) {
                xaRes.rollback(id);
            }
            connection.close();

        } catch (Exception e) {
        }
    }
}
```

Em um cenário do mundo real, você pode verificar suas transações XA preparadas em relação ao Gerenciador de transações XA. Em seguida, você pode decidir se deseja tratar de cada transação preparada com um `rollback()` ou um `commit()`.

Usando o Amazon MQ para o RabbitMQ

O Amazon MQ facilita a criação de um agente de mensagem com os recursos de processamento e armazenamento que atendem às suas necessidades. Você pode criar, gerenciar e excluir corretores usando o AWS Management Console, Amazon REST API MQ ou o AWS Command Line Interface.

Esta seção descreve os elementos básicos de um agente de mensagens para os tipos de mecanismo ActiveMQ e RabbitMQ, lista os tipos de instâncias de agente de Amazon MQ disponíveis e seus status e fornece uma visão geral da arquitetura de agente e das opções de configuração.

Para saber mais sobre o Amazon MQ REST APIs, consulte a Referência do [Amazon REST API MQ](#).

Amazon MQ para corretores RabbitMQ

O que é um corretor Amazon MQ para RabbitMQ?

Um agente é um ambiente de agente de mensagens em execução no Amazon MQ. É o bloco de criação básico do Amazon MQ. A descrição combinada da classe (m5, t3) e do tamanho (large, micro) da instância do agente é um Tipo de instância de agente (por exemplo, mq.m5.large). Para obter mais informações, consulte [Broker instance types](#).

- Um agente de instância única é composto por um agente em uma zona de disponibilidade atrás de um Network Load Balancer NLB (). O agente se comunica com seu aplicativo e com um volume de armazenamento da Amazon. EBS
- A implantação de cluster é um agrupamento lógico de três nós do agente RabbitMQ por trás de um Balanceador de Carga da Rede, cada um compartilhando usuários, filas e um estado distribuído em várias Zonas de Disponibilidade (AZ).

Para obter mais informações, consulte [Opções de implantação do Amazon MQ para corretores RabbitMQ](#).

É possível habilitar as atualizações automáticas de versões secundárias para novas versões secundárias do mecanismo do agente à medida que novas versões do mecanismo RabbitMQ são lançadas. As atualizações automáticas ocorrem durante a janela de manutenção definida pelo dia da semana, a hora do dia (no formato de 24 horas) e o fuso horário (UTC por padrão).

Protocolos compatíveis

Você pode acessar seus corretores RabbitMQ usando [qualquer linguagem de programação compatível com o RabbitMQ](#) e habilitando os seguintes protocolos: TLS

- [AMQP\(0-9-1\)](#)

Portas listener

Os corretores RabbitMQ gerenciados pelo Amazon MQ oferecem suporte às seguintes portas de ouvinte para conectividade em nível de aplicativo viaamqps, bem como conexões de clientes usando o console web e o gerenciamento do RabbitMQ. API

- Porta do ouvinte 5671 - usada para conexões feitas por meio do seguro AMQPURL. Por exemplo, dado um corretor com ID de corretorb-c8352341-ec91-4a78-ad9c-a43f23d325bb, implantado na us-west-2 região, o seguinte é o completo do corretor amqpURL:b-c8352341-ec91-4a78-ad9c-a43f23d325bb.mq.us-west-2.amazonaws.com:5671.
- Portas de ouvinte 443 e 15671 - Ambas as portas de ouvinte podem ser usadas de forma intercambiável para acessar um corretor por meio do console web do RabbitMQ ou do gerenciamento. API

Atributos

Um agente RabbitMQ tem vários atributos:

- Um nome. Por exemplo, MyBroker.
- Um ID. Por exemplo, b-1234a5b6-78cd-901e-2fgh-3i45j6k17819.
- Um nome de recurso da Amazon (ARN). Por exemplo, arn:aws:mq:us-east-2:123456789012:broker:MyBroker:b-1234a5b6-78cd-901e-2fgh-3i45j6k17819.
- Um console web RabbitMQ. URL Por exemplo, https://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com.

Para obter mais informações, consulte o [Console da Web RabbitMQ](#) na documentação do RabbitMQ.

- Um AMQP endpoint seguro. Por exemplo, amqps://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-east-2.amazonaws.com.

Para obter uma lista completa dos atributos do agente, consulte o seguinte na Referência do Amazon MQ: REST API

- [RESTID da operação: Corretor](#)
- [RESTID da operação: Corretores](#)
- [RESTID da operação: Broker Reboot](#)

Amazon MQ para usuários do broker RabbitMQ

Cada conexão de cliente AMQP 0-9-1 tem um usuário associado que deve ser autenticado. Cada conexão de cliente também se destina a um host virtual (vhost) para o qual o usuário deve ter um conjunto de permissões. Um usuário pode ter permissão para configure (configurar), write (gravar) em, e read (ler) de filas e trocas em um vhost. As credenciais do usuário e o vhost de destino são especificadas no momento em que a conexão é estabelecida.

Quando você cria um agente do Amazon MQ para RabbitMQ pela primeira vez, o Amazon MQ usa as credenciais de login que você fornece para criar um usuário do RabbitMQ com a tag `administrator`. Em seguida, você pode adicionar e gerenciar usuários por meio do [gerenciamento](#) do RabbitMQ API ou do console web do RabbitMQ. Você também pode usar o console web do RabbitMQ ou o gerenciamento API para definir ou modificar as permissões e tags do usuário.

Note

[Os usuários do RabbitMQ não serão armazenados ou exibidos por meio dos usuários do Amazon MQ. API](#)

Important

O Amazon MQ para RabbitMQ não suporta o nome de usuário “convidado” e excluirá a conta de convidado padrão quando você criar um novo corretor. O Amazon MQ também excluirá periodicamente qualquer conta criada pelo cliente chamada “convidado”.

Para criar um novo usuário com o gerenciamento do RabbitMQAPI, use o seguinte API endpoint e corpo da solicitação. Substituir *username* e *password* com suas novas credenciais de login.

```
PUT /api/users/username HTTP/1.1
```

```
{"password":"password","tags":"administrator"}
```

Important

- Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nos nomes de usuário da corretora. Os nomes de usuário dos corretores podem ser acessados por outros AWS serviços, incluindo CloudWatch registros. Nomes de usuário do agente não devem ser usados para dados privados ou sigilosos.
- Se você esqueceu a senha de administrador definida ao criar o agente, não será possível redefinir as credenciais. Se você criou vários administradores, poderá fazer login usando outro usuário administrador e redefinir ou recriar as credenciais. Se tiver apenas um usuário administrador, você deverá excluir o agente e criar outro com novas credenciais. Recomendamos consumir ou fazer backup de mensagens antes de excluir o agente.

A chave `tags` é obrigatória e é uma lista de etiquetas separadas por vírgulas para o usuário. O Amazon MQ é compatível com as tags de usuário `administrator`, `management`, `monitoring` e `policymaker`.

Você pode definir permissões para um usuário individual usando o seguinte API endpoint e corpo de solicitação. Substituir `vhost` e `username` com suas informações. Para o vhost padrão `/`, use `%2F`.

```
PUT /api/permissions/vhost/username HTTP/1.1
```

```
{"configure":".*","write":".*","read":".*"}
```

Note

As chaves `configure`, `read` e `write` são obrigatórias.

Usando o valor de caractere curinga `.*`, esta operação concederá permissões de leitura, gravação e configuração para o usuário, em todas as filas no vhost especificado. [Para obter mais informações sobre o gerenciamento de usuários por meio do gerenciamento do RabbitMQAPI, consulte Gerenciamento do RabbitMQ. HTTP API](#)

Padrões de agentes do Amazon MQ for RabbitMQ

Quando você cria um Amazon MQ para agente RabbitMQ, o Amazon MQ aplica um conjunto padrão de políticas de agente e limites de vhost para otimizar a performance do seu agente. O Amazon MQ aplica limites de vhost somente ao vhost padrão (/). O Amazon MQ não aplicará políticas padrão a vhosts recém-criados. Recomendamos manter esses padrões para todos os agentes novos e existentes. No entanto, você pode modificar, substituir ou excluir esses padrões a qualquer momento.

O Amazon MQ cria políticas e limites com base no tipo de instância e no modo de implantação do agente que você escolhe ao criar seu agente. As políticas padrão são nomeadas de acordo com o modo de implantação, da seguinte maneira:

- Instância única — `AWS-DEFAULT-POLICY-SINGLE-INSTANCE`
- Implantação de cluster — `AWS-DEFAULT-POLICY-CLUSTER-MULTI-AZ`

Para os [agentes de instância única](#), o Amazon MQ define o valor de prioridade da política como 0. Para substituir o valor de prioridade padrão, você pode criar suas próprias políticas personalizadas com valores de prioridade mais altos. Para [implantações de cluster](#), o Amazon MQ define o valor de prioridade como 1 para padrões do agente. Para criar sua própria política personalizada para clusters, atribua um valor de prioridade maior que 1.

Note

Em implantações de cluster, as políticas de agente `ha-mode` e `ha-sync-mode` são necessárias para espelhamento clássico e alta disponibilidade (HA).

Se você exclui a política padrão `AWS-DEFAULT-POLICY-CLUSTER-MULTI-AZ`, o Amazon MQ usa a política `ha-all-AWS-OWNED-DO-NOT-DELETE` com um valor de prioridade 0. Isso garante que as políticas `ha-mode` e `ha-sync-mode` necessárias ainda estejam em vigor. Se você criar sua própria política personalizada, o Amazon MQ anexará automaticamente o `ha-mode` e `ha-sync-mode` nas suas definições de política.


Tópicos

- [Descrições de políticas e limites](#)
- [Valores padrão recomendados](#)


Descrições de políticas e limites

A lista a seguir descreve as políticas e limites padrão que o Amazon MQ aplica a um agente recém-criado. Os valores para `max-length`, `max-queues` e `max-connections` variam de acordo com o tipo de instância e o modo de implantação do seu agente. Esses valores estão listados na seção [Valores padrão recomendados](#).

- **queue-mode: lazy** (política) — Habilita filas lentas. Por padrão, as filas mantêm um cache na memória de mensagens, permitindo que o agente entregue mensagens aos consumidores o mais rápido possível. Isso pode fazer o agente ficar sem memória e acionar um alarme de alta memória. As filas lentas tentam mover as mensagens para o disco o mais cedo possível. Isso significa que menos mensagens são mantidas na memória em condições normais de operação. Usando filas lentas, o Amazon MQ para RabbitMQ pode ser compatível com sistemas de mensagens muito maiores e filas mais longas. Observe que, para determinados casos de uso, os agentes com filas lentas podem ter uma performance ligeiramente mais lenta. Isso ocorre porque as mensagens são movidas do disco para o agente, em vez de entregar mensagens de um cache na memória.

 Modos de implantação
Instância única, cluster

- **max-length: *number-of-messages*** (política) — Define um limite para o número de mensagens em uma fila. Em implantações de cluster, o limite impede a sincronização de fila pausada em casos como reinicializações de agente ou após uma janela de manutenção.

 Modos de implantação
Cluster

- **overflow: reject-publish** (política) — Impõe filas com uma política `max-length` para rejeitar novas mensagens depois do número de mensagens na fila atingir o valor `max-length`. Para garantir que as mensagens não sejam perdidas se uma fila estiver em um estado sobrecarregado, as aplicações dos clientes que publicam mensagens no agente devem implementar a [confirmação do editor](#). Para obter informações sobre como implementar a confirmação do editor, consulte [Confirmações do editor](#) no site do RabbitMQ.

 Modos de implantação

Cluster

- **max-queues:** *number-of-queues-per-vhost* (limite de vhost) — Define o limite para o número de filas em um agente. Similar à definição de política `max-length`, limitar o número de filas em implantações de cluster impede a sincronização de filas pausada após reinicializações de agente ou janelas de manutenção. Limitar as filas também evita o CPU uso excessivo da manutenção de filas.

 Modos de implantação


Instância única, cluster

- **max-connections:** *number-of-connections-per-vhost* (limite de vhost) — Define o limite para o número de conexões de cliente com o agente. Limitar o número de conexões de acordo com os valores recomendados impede o uso excessivo de memória pelo agente o que poderia resultar na sinalização de um alarme de alto uso de memória e na interrupção das operações.

 Modos de implantação

Instância única, cluster

Valores padrão recomendados

 Note

Os limites padrão `max-length` e `max-queue` são testados e avaliados com base em um tamanho médio de mensagem de 5 kB. Se as suas mensagens forem significativamente maiores do que 5 kB, você precisará ajustar e reduzir os limites `max-length` e `max-queue`.

A tabela a seguir lista os valores de limite padrão para um agente recém-criado. O Amazon MQ aplica esses valores de acordo com o tipo de instância e o modo de implantação do agente.


Tipo de instância	Modo de implantação	max-length	max-queues	max-connections
t3.micro	Instância única	N/D	500	500
m5.large	Instância única	N/D	20.000	4.000
	Cluster	8.000.000	4.000	15.000
m5.xlarge	Instância única	N/D	30.000	8.000
	Cluster	9.000.000	5.000	20.000
m5.2xlarge	Instância única	N/D	60.000	15.000
	Cluster	10,000,000	6.000	40.000
m5.4xlarge	Instância única	N/D	150.000	30.000
	Cluster	12.000.000	10.000	100.000

Amazon MQ para tipos de instância do broker RabbitMQ

Important

Não é possível fazer downgrade de um agente de um tipo de instância mq.m5 para um tipo de instância mq.t3.micro.

Tipo de instância	v CPU	Memória (GiB)	Performance de rede	Caso de uso
mq.t3.micro	2	1	Baixo	Avaliação

 Important
O tipo de instância

Tipo de instância	v CPU	Memória (GiB)	Performance de rede	Caso de uso
				mq.t3.micro não é compatível com a implantação de cluster .
mq.m5.large	2	8	Alta	Produção
mq.m5.xlarge	4	16	Alta	Produção
mq.m5.2xlarge	8	32	Alta	
mq.m5.4xlarge	16	64	Alta	

Diretrizes de dimensionamento do Amazon MQ para RabbitMQ

Você pode escolher o tipo de instância do broker que melhor oferece suporte ao seu aplicativo. Ao escolher um tipo de instância, é importante considerar os fatores que afetarão o desempenho do corretor:

- o número de clientes e filas
- o volume de mensagens enviadas
- mensagens mantidas na memória
- mensagens redundantes

Tipos menores de instância de broker (t3.micro) são recomendados somente para testar o desempenho do aplicativo. Recomendamos tipos de instância de broker maiores (m5.large e

superiores) para níveis de produção de clientes e filas, alta taxa de transferência, mensagens na memória e mensagens redundantes.

É importante testar seus corretores para determinar o tipo e o tamanho de instância apropriados para seus requisitos de mensagens de carga de trabalho. Use as diretrizes de dimensionamento a seguir para determinar o tipo de instância mais adequado para seu aplicativo.

Diretrizes de dimensionamento para implantação em uma única instância

A tabela a seguir mostra os valores-limite máximos para cada tipo de instância para agentes de instância única.

Tipo de instância	Conexões	Canais	Filas	Consumidores por canal	Pás
t3.micro	500	1.500	2.500	1.000	150
m5.large	5.000	15.000	30.000	1.000	250
m5.xlarge	10.000	30.000	60.000	1.000	500
m5.2xlarge	20.000	60.000	120.000	1.000	1.000
m5.4xlarge	40.000	120.000	240.000	1.000	2.000

Diretrizes de dimensionamento para implantação de clusters

A tabela a seguir mostra os valores-limite máximos para cada tipo de instância para agentes de cluster.

Tipo de instância	Conexões	Canais	Filas	Consumidores por canal	Pás
m5.large	15.000	45.000	10.000	1.000	150
m5.xlarge	30.000	90.000	15.000	1.000	300
m5.2xlarge	60.000	180.000	20.000	1.000	600

Tipo de instância	Conexões	Canais	Filas	Consumidores por canal	Pás
m5.4xlarge	120.000	360.000	30.000	1.000	1200

Os limites de conexão, canal e escavadeira são aplicados por nó. Os valores limite exatos para um agente de cluster podem ser menores do que o valor indicado, dependendo do número de nós disponíveis e de como o RabbitMQ distribui recursos entre os nós disponíveis.

Mensagens de erro

As mensagens de erro a seguir são retornadas quando os limites são excedidos. Todos os valores são baseados nos limites de m5.1large uma única instância.

Note

Os códigos de erro das mensagens a seguir podem mudar com base na biblioteca cliente que você está usando.

Conexão

```
ConnectionClosedByBroker 500 "NOT_ALLOWED - connection refused: node connection limit (500) is reached"
```

Channel (Canal)

```
ConnectionClosedByBroker 1500 "NOT_ALLOWED - number of channels opened on node 'rabbit@ip-10-0-23-173.us-west-2.compute.internal' has reached the maximum allowed limit of (15,000)"
```

Consumidor

```
ConnectionClosedByBroker: (530, 'NOT_ALLOWED - reached maximum (1,000) of consumers per channel')
```

Note

As mensagens de erro a seguir usam o API formato HTTP de gerenciamento.

Queue (Fila)

```
{"error": "bad_request", "reason": "cannot declare queue 'my_queue': queue limit in cluster (30,000) is reached"}
```

Pá

```
{"error": "bad_request", "reason": "Validation failed\n\ncomponent shovel is limited to 250 per node\n"}
```

Vhost

```
{"error": "bad_request", "reason": "cannot create vhost 'my_vhost': vhost limit of 4,000 is reached"}
```

Plug-ins para Amazon MQ para RabbitMQ

O Amazon MQ para RabbitMQ oferece suporte ao [plug-in de gerenciamento RabbitMQ, que alimenta o gerenciamento e o console web do RabbitMQ](#). API Você pode usar o console web e o gerenciamento API para criar e gerenciar usuários e políticas de corretores.

Além do plugin de gerenciamento, o Amazon MQ para RabbitMQ também é compatível com os seguintes plugins.

Tópicos

- [Plugin shovel](#)
- [Plugin de federação](#)
- [Plugin de troca de hash consistente](#)

Plugin shovel

Os agentes gerenciados pelo Amazon MQ são compatíveis com o [RabbitMQ shovel \(shovel RabbitMQ\)](#), permitindo que você mova mensagens de filas e trocas em uma instância de agente para outra. Você pode usar o shovel para conectar agentes de baixo acoplamento e distribuir mensagens longe dos nós com cargas de mensagens mais pesadas.

Os agentes RabbitMQ gerenciados pelo Amazon MQ são compatíveis com shovels dinâmicos. Shovels dinâmicos são configurados usando parâmetros de tempo de execução e podem ser

iniciados e interrompidos a qualquer momento programaticamente por uma conexão de cliente. Por exemplo, usando o gerenciamento do RabbitMQAPI, você pode criar uma PUT solicitação para o seguinte API endpoint para configurar uma escavadeira dinâmica. No exemplo, {vhost} pode ser substituído pelo nome do vhost do agente, e {name} pode ser substituído pelo nome do novo shovel dinâmico.

```
/api/parameters/shovel/{vhost}/{name}
```

No corpo da solicitação, você deve especificar uma fila ou uma troca, mas não ambos. Este exemplo abaixo configura uma pá dinâmica entre uma fila local especificada em `src-queue` e uma fila remota definida em `dest-queue`. Da mesma forma, você pode usar os parâmetros `src-exchange` e `dest-exchange` para configurar um shovel entre duas trocas.

```
{
  "value": {
    "src-protocol": "amqp091",
    "src-uri": "amqp://localhost",
    "src-queue": "source-queue-name",
    "dest-protocol": "amqp091",
    "dest-uri": "amqps://b-c8352341-ec91-4a78-ad9c-a43f23d325bb.mq.us-
west-2.amazonaws.com:5671",
    "dest-queue": "destination-queue-name"
  }
}
```

Important

Você não pode configurar shovels entre filas ou trocas se o destino do shovel for um agente privado. Você só pode configurar shovels entre filas ou trocas em agentes públicos, ou entre uma fonte em um agente privado e um destino em um agente público.

Para obter mais informações sobre como usar shovels dinâmicos, consulte [RabbitMQ dynamic shovel plugin \(Plugin de shovel dinâmico RabbitMQ\)](#).

Note

O Amazon MQ não é compatível com o uso de shovels estáticas.

Plugin de federação

O Amazon MQ é compatível com trocas e filas federadas. Com a federação, você pode replicar o fluxo de mensagens entre filas, trocas e consumidores em agentes separados. Filas e trocas federadas usam point-to-point links para se conectar a colegas em outras corretoras. Enquanto as trocas federadas, por padrão, roteiam mensagens uma vez, as filas federadas podem mover mensagens várias vezes conforme necessário pelos consumidores.

Você pode usar federação para permitir que um agente downstream consuma uma mensagem de uma troca ou de uma fila em um upstream. Você pode habilitar a federação em corretores downstream usando o console web do RabbitMQ ou o gerenciamento. API

Important

Não será possível configurar a federação se a fila ou troca de upstream estiver em um agente privado. Só será possível configurar a federação entre filas ou trocas em agentes públicos ou entre uma fila ou troca de upstream em um agente público e uma fila ou troca de downstream em um agente privado.

Por exemplo, usando o gerenciamentoAPI, você pode configurar a federação fazendo o seguinte.

- Configure um ou mais upstreams que definem conexões de federação com outros nós. Você pode definir conexões de federação usando o console web do RabbitMQ ou o gerenciamento. API Usando o gerenciamentoAPI, você pode criar uma POST solicitação `/api/parameters/federation-upstream/%2f/my-upstream` com o seguinte corpo de solicitação.

```
{"value":{"uri":"amqp://server-name","expires":3600000}}
```

- Configure uma política para permitir que suas filas ou trocas se tornem federadas. Você pode configurar políticas usando o console web do RabbitMQ ou o gerenciamento. API Usando o gerenciamentoAPI, você pode criar uma POST solicitação `/api/policies/%2f/federate-me` com o seguinte corpo de solicitação.

```
{"pattern":"^amq\\.","definition":{"federation-upstream-set":"all"},"apply-to":"exchanges"}
```

Note

O corpo da solicitação assume que as trocas no servidor são nomeadas começando com `amq`. Usar a expressão regular `^amq\.` vai garantir que a federação esteja habilitada para todas as trocas cujos nomes comecem com “`amq`”. As trocas no seu servidor RabbitMQ podem ser nomeadas de forma diferente.

Para obter mais informações sobre como configurar o plugin de federação, consulte [RabbitMQ federation plugin \(plugin de federação do RabbitMQ\)](#).

Plugin de troca de hash consistente

Por padrão, o Amazon MQ para RabbitMQ é compatível com o plugin tipo troca de Hash consistente. As trocas de hash consistentes fazem o roteamento de mensagens para filas com base em um valor de hash calculado a partir da routing key (chave de roteamento) de uma mensagem. Considerando uma chave de roteamento razoavelmente uniforme, as trocas de Hash consistentes podem distribuir mensagens entre filas de maneira razoavelmente uniforme.

Para filas vinculadas a uma troca de hash consistente, a chave de vinculação determina `number-as-a-string` o peso de vinculação de cada fila. As filas com um peso de vinculação maior receberão uma distribuição proporcionalmente maior de mensagens da troca de hash consistente à qual estão vinculadas. Em uma topologia de troca de hash consistente, os editores podem simplesmente publicar mensagens no Exchange, mas os consumidores devem ser explicitamente configurados para consumir mensagens de filas específicas.

Para obter mais informações sobre trocas de hash consistentes, consulte Tipo de [troca de hash consistente do RabbitMQ](#) no site. GitHub

Aplicação de políticas ao Amazon MQ para RabbitMQ

Você pode aplicar políticas e limites personalizados com os valores padrão recomendados pelo Amazon MQ. Se você excluiu as políticas e limites padrão recomendados e deseja recriá-los, ou se tiver criado vhosts adicionais e quiser aplicar as políticas e limites padrão aos novos vhosts, você pode usar as etapas a seguir.

⚠ Important

Para executar as etapas a seguir, é necessário ter um usuário do agente do Amazon MQ para RabbitMQ com permissões de administrador. Você pode usar o usuário administrador criado quando criou o agente pela primeira vez ou outro usuário que você possa ter criado posteriormente. A tabela a seguir fornece a etiqueta de usuário administrador necessária e as permissões como padrões de expressão regular (regex).

Etiquetas	Ler regex	Configurar regex	Escrever regex
administrator	.*	.*	.*

Para obter mais informações sobre criar usuários RabbitMQ e gerenciar etiquetas e permissões de usuário, consulte [Amazon MQ para usuários do broker RabbitMQ](#).

Para aplicar políticas padrão e limites de host virtual usando o console da Web RabbitMQ

1. Faça login no [console do Amazon MQ](#).
2. No painel de navegação à esquerda, escolha Agentes.
3. Na lista de agentes, escolha o nome do agente ao qual você deseja aplicar a nova política.
4. Na página de detalhes do broker, na seção Conexões, escolha o console web RabbitMQ. URL O console da Web do RabbitMQ é aberto em uma nova guia ou janela do navegador.
5. Faça login no console da Web do RabbitMQ com o nome de usuário e a senha do administrador do agente.
6. No console da Web do RabbitMQ, na parte superior da página, escolha Admin.
7. Na página Admin, no painel de navegação da direita, selecione Policies (Políticas).
8. Na página Policies (Políticas), você pode ver uma lista das User policies (Políticas de usuário) atuais do agente. Abaixo das User policies (Políticas de usuário), expanda Add/update a policy (Adicionar/atualizar uma política).
9. Para criar uma política de agente, em Add/update a policy (Adicionar/atualizar uma política), faça o seguinte:
 - a. Para o Virtual host (Host virtual), escolha o nome do vhost ao qual você deseja anexar as políticas da lista suspensa. Para escolher o vhost padrão, escolha /.

Note

Se você não tiver criado vhosts adicionais, a opção Virtual host (Host virtual) não aparecerá no console RabbitMQ, e as políticas serão aplicadas somente ao vhost padrão.

- b. Em Name (Nome), insira um nome para a sua política, por exemplo **policy-defaults**.
- c. Para Pattern (Padrão), insira o padrão de expressão regular **.*** para que a política corresponda a todas as filas no agente.
- d. Para Apply to (Aplicar em), escolha Exchanges and queues (Trocas e filas) na lista suspensa.
- e. Para Priority (Prioridade), insira um número inteiro maior que todas as outras políticas aplicadas ao vhost. Você pode aplicar exatamente um conjunto de definições de política a filas e trocas RabbitMQ a qualquer momento. O RabbitMQ escolhe a política correspondente com o valor de prioridade mais alto. Para obter mais informações sobre prioridades de política e como combinar políticas, consulte [Políticas](#) (Políticas) na Documentação do Servidor RabbitMQ.
- f. Para Definition (Definição), adicione os seguintes pares de chave-valor:
 - **queue-mode=lazy**. Selecione String (String) na lista suspensa.
 - **overflow=reject-publish**. Selecione String (String) na lista suspensa.

Note

Não se aplica aos agentes de instância única.

- **max-length=number-of-messages**. Substituir *number-of-messages* com o [valor recomendado do Amazon MQ](#) de acordo com o tamanho da instância e o modo de implantação do broker, por exemplo, **8000000** para um mq.m5.Large cluster. Selecione Number (Número) na lista suspensa.

Note

Não se aplica aos agentes de instância única.

- g. Escolha Add/update policy (Adicionar/atualizar política).

10. Confirme se a nova política aparece na lista de User policies (Políticas de usuário).

 Note

Para agentes de cluster, o Amazon MQ aplica automaticamente as definições de política `ha-mode: all` e `ha-sync-mode: automatic`.

11. No painel de navegação da direita, escolha Limits (Limites).

12. Na página Limites você poderá ver uma lista dos Virtual host limits (Limites de host virtual) atuais do agente. Abaixo dos Limites de host virtual, expanda Set/update a virtual host limit (Definir/atualizar um limite de host virtual).

13. Para criar um novo limite vhost, em Set/update a virtual host limit (Definir/atualizar um limite de host virtual), faça o seguinte:


- a. Para o Virtual host (Host virtual), escolha o nome do vhost ao qual você deseja anexar as políticas da lista suspensa. Para escolher o vhost padrão, escolha /.
- b. Para Limit (Limite), escolha máximo de conexões nas opções suspensas.
- c. Para Value (Valor), insira o [Amazon MQ recommended value \(Valor recomendado pelo Amazon MQ\)](#) de acordo com o tamanho da instância do agente e o modo de implantação, por exemplo, **15000** para um cluster `mq.m5.large`.
- d. Selecione Set/update limit (Definir/atualizar limite).
- e. Repita as etapas acima e, para Limit (Limite), escolha máximo de filas nas opções suspensas.

14. Confirme se os novos limites aparecem na lista de Virtual host limits (Limites de host virtual).

Para aplicar políticas padrão e limites de host virtual usando o gerenciamento do RabbitMQ API

1. Faça login no [console do Amazon MQ](#).
2. No painel de navegação à esquerda, escolha Agentes.
3. Na lista de agentes, escolha o nome do agente ao qual você deseja aplicar a nova política.
4. Na página do corretor, na seção Conexões, observe o console web do RabbitMQ. URL Esse é o endpoint do broker que você usa em uma HTTP solicitação.
5. Abra uma nova janela de terminal ou linha de comando de sua escolha.

- Para criar uma nova política de agente, insira o comando `curl` a seguir. Este comando assume uma fila no vhost / padrão, que é codificada como `%2F`. Para aplicar a política a outro vhost, substitua `%2F` pelo nome do vhost.

 Note


Substituir *username* e *password* com suas credenciais de login de administrador. Substituir *number-of-messages* com o [valor recomendado do Amazon MQ](#) de acordo com o tamanho da instância e o modo de implantação do broker. Substituir *policy-name* com um nome para sua apólice. Substituir *broker-endpoint* com o URL que você anotou anteriormente.

```
curl -i -u username:password -H "content-type:application/json" -XPUT \  
-d '{"pattern":".*", "priority":1, "definition":{"queue-mode":lazy, \  
  "overflow":"reject-publish", "max-length":"number-of-messages"}}' \  
broker-endpoint/api/policies/%2F/policy-name
```

- Para confirmar se a nova política foi adicionada às políticas de usuário do seu agente, insira o seguinte comando `curl` para listar todas as políticas de agente.

```
curl -i -u username:password broker-endpoint/api/policies
```

- Para criar um novo limites `max-connections` de host virtual, insira o seguinte comando `curl`. Este comando assume uma fila no vhost / padrão, que é codificada como `%2F`. Para aplicar a política a outro vhost, substitua `%2F` pelo nome do vhost.

 Note

Substituir *username* e *password* com suas credenciais de login de administrador. Substituir *max-connections* com o [valor recomendado do Amazon MQ](#) de acordo com o tamanho da instância e o modo de implantação do broker. Substitua o endpoint do broker pelo URL que você anotou anteriormente.

```
curl -i -u username:password -H "content-type:application/json" -XPUT \  
-d '{"value":"number-of-connections"}' \  

```

```
broker-endpoint/api/vhost-limits/%2F/max-connections
```

9. Para criar um novo limite de host virtual max-queues, repita a etapa anterior, mas modifique o comando curl conforme mostrado a seguir.

```
curl -i -u username:password -H "content-type:application/json" -XPUT \  
-d '{"value": "number-of-queues"}' \  
broker-endpoint/api/vhost-limits/%2F/max-queues
```

10. Para confirmar se os novos limites foram adicionados aos limites de host virtual do seu agente, insira o comando a seguir curl para listar todos os limites de host virtual do agente.

```
curl -i -u username:password broker-endpoint/api/vhost-limits
```

Opções de implantação do Amazon MQ para corretores RabbitMQ

Agentes RabbitMQ podem ser criados como agentes de instância única ou em uma implantação de cluster. Para ambos os modos de implantação, o Amazon MQ oferece alta durabilidade armazenando seus dados de forma redundante.

Você pode acessar seus corretores RabbitMQ usando [qualquer linguagem de programação compatível com o RabbitMQ](#) e habilitando os seguintes protocolos: TLS

- [AMQP\(0-9-1\)](#)

Tópicos

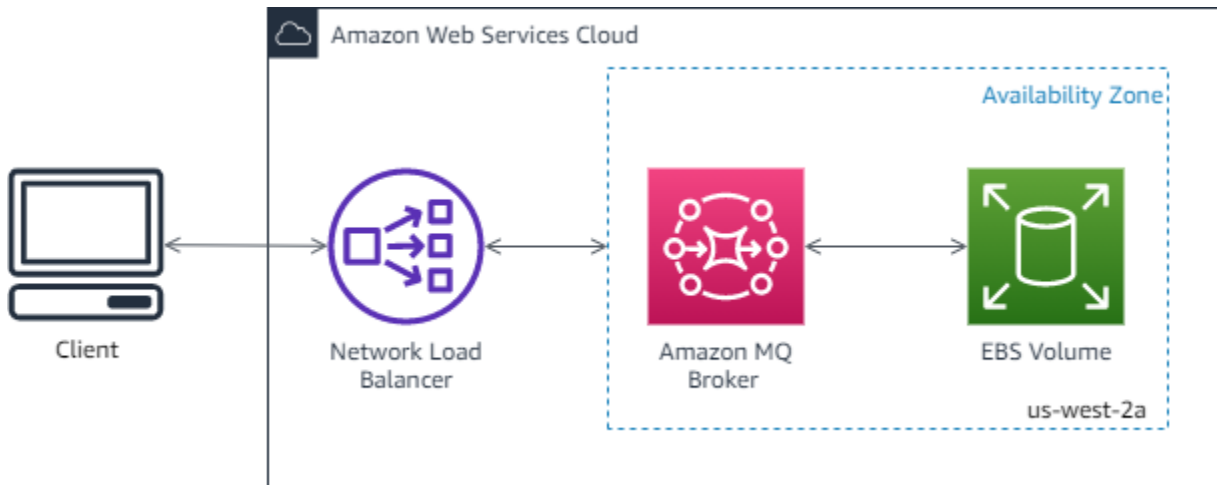
- [Opção 1: agente de instância única Amazon MQ para RabbitMQ](#)
- [Opção 2: Amazon MQ para implantação do cluster RabbitMQ](#)

Opção 1: agente de instância única Amazon MQ para RabbitMQ

Um agente de instância única é composto por um agente em uma zona de disponibilidade atrás de um Network Load NLB Balancer (). O corretor se comunica com seu aplicativo e com um volume de EBS armazenamento da Amazon. EBSA Amazon fornece armazenamento em nível de bloco otimizado para baixa latência e alta taxa de transferência.

O uso de um Network Load Balancer garante que seu endpoint do broker Amazon MQ for RabbitMQ permaneça inalterado se a instância do broker for substituída durante uma janela de manutenção ou devido a falhas subjacentes de hardware da Amazon. Um Balanceador de carga da rede permite que suas aplicações e usuários continuem a usar o mesmo endpoint para se conectar ao agente.

O diagrama a seguir ilustra um agente de instância única do Amazon MQ para RabbitMQ.



Opção 2: Amazon MQ para implantação do cluster RabbitMQ

A implantação de cluster é um agrupamento lógico de três nós do agente RabbitMQ por trás de um Balanceador de Carga da Rede, cada um compartilhando usuários, filas e um estado distribuído em várias Zonas de Disponibilidade (AZ).

Em uma implantação de cluster, o Amazon MQ gerencia automaticamente as políticas de agente para habilitar o espelhamento clássico em todos os nós, garantindo alta disponibilidade (HA). Cada fila espelhada consiste em um nó principal e um ou mais espelhos. Cada fila tem seu próprio nó principal. Todas as operações para uma determinada fila são aplicadas primeiro no nó principal da fila e depois propagadas para espelhos. O Amazon MQ cria uma política de sistema padrão que define o `ha-mode` para `all` e `ha-sync-mode` para `automatic`. Isso garante que os dados sejam replicados para todos os nós do cluster em diferentes zonas de disponibilidade para maior durabilidade.

Note

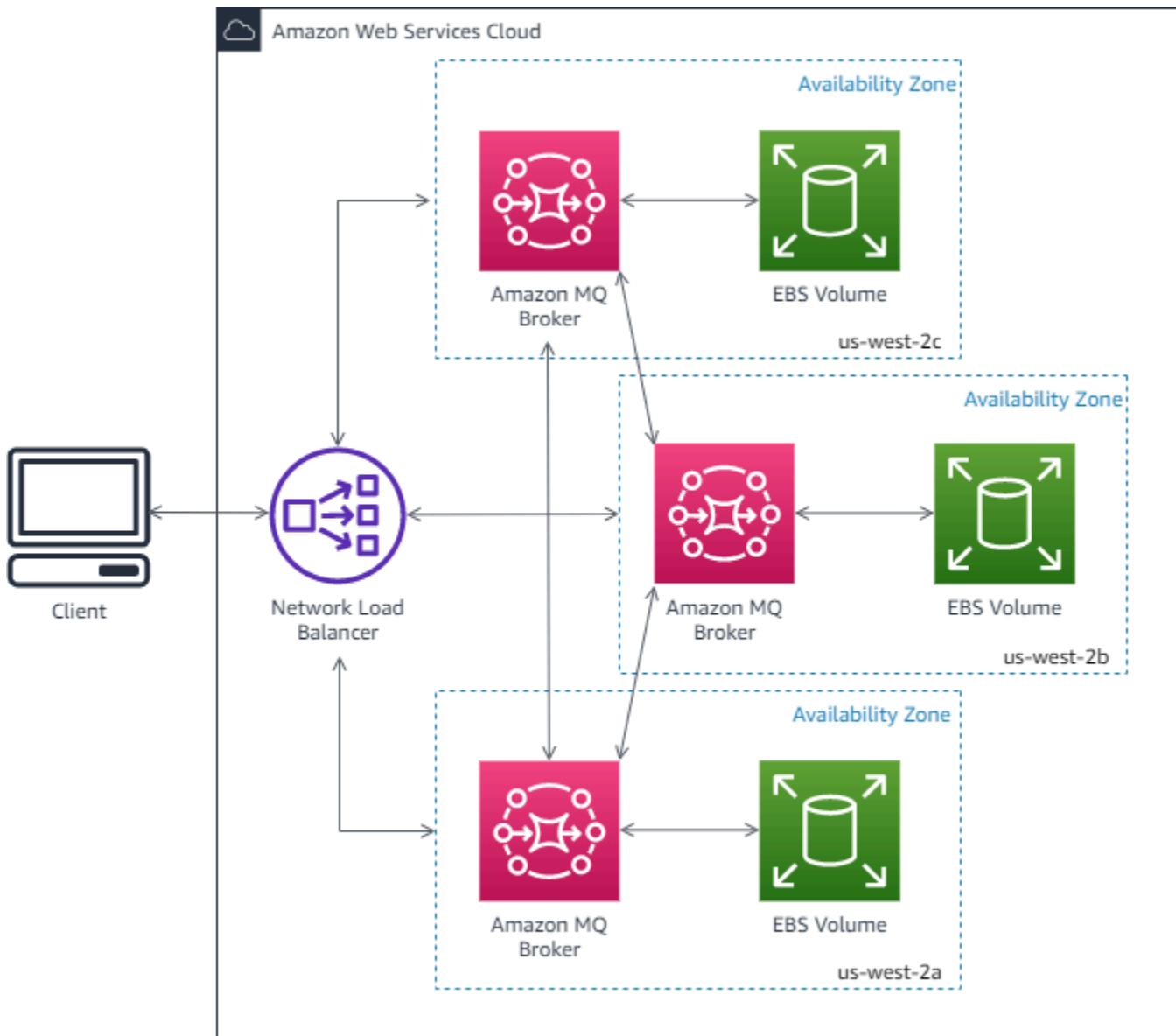
Durante uma janela de manutenção, toda a manutenção de um cluster é realizada em um nó de cada vez, mantendo pelo menos dois nós em execução o tempo todo. Cada vez que um nó é derrubado, as conexões de cliente para esse nó são cortadas e precisam ser

restabelecidas. Você deve garantir que seu código de cliente foi projetado para se reconectar automaticamente ao cluster. Para obter mais informações sobre a recuperação de conexões, consulte [the section called “Recuperação automática de falhas de rede”](#).

Como o Amazon MQ define `ha-sync-mode: automatic`, durante uma janela de manutenção, as filas serão sincronizadas quando cada nó voltar a ingressar no cluster. A sincronização de filas bloqueia todas as outras operações de fila. Você pode atenuar o impacto da sincronização de filas durante as janelas de manutenção mantendo as filas curtas.

A política padrão não deve ser excluída. Se você excluir essa política, o Amazon MQ a recriará automaticamente. O Amazon MQ também garantirá que as propriedades de HA sejam aplicadas a todas as outras políticas criadas em um agente em cluster. Se você adicionar uma política sem as propriedades de HA, o Amazon MQ as adicionará para você. Se você adicionar uma política com diferentes propriedades de alta disponibilidade, o Amazon MQ as substituirá. Para obter mais informações sobre o espelhamento clássico, consulte [filas espelhadas](#).

O diagrama a seguir ilustra a implantação de um agente de cluster RabbitMQ com três nós em três zonas de disponibilidade (AZ), cada uma com seu próprio EBS volume da Amazon e um estado compartilhado. EBSA Amazon fornece armazenamento em nível de bloco otimizado para baixa latência e alta taxa de transferência.



Configurações do agente do Amazon MQ para RabbitMQ

Uma configuração contém todas as definições do agente do RabbitMQ, no formato Cuttlefish. Você pode criar uma configuração antes de criar qualquer agente. Em seguida, você pode aplicar a configuração a um ou mais agentes.

Atributos

A configuração de um agente tem vários atributos, por exemplo:

- Um nome (MyConfiguration)

- Um ID (c-1234a5b6-78cd-901e-2fgh-3i45j6k17819)
- Um nome de recurso da Amazon (ARN) (arn:aws:mq:us-east-2:123456789012:configuration:c-1234a5b6-78cd-901e-2fgh-3i45j6k17819)

Para obter uma lista completa dos atributos de configuração, consulte o seguinte na Referência do Amazon MQ: REST API

- [RESTID da operação: Configuração](#)
- [RESTID da operação: configurações](#)

Para obter uma lista completa de atributos de revisão de configuração, consulte o seguinte:

- [RESTID da operação: revisão de configuração](#)
- [RESTID da operação: revisões de configuração](#)

Tópicos

- [Criação e aplicação de configurações do agente do RabbitMQ](#)
- [Editar uma revisão de configuração do Amazon MQ para RabbitMQ](#)
- [Políticas de configuração do RabbitMQ](#)

Criação e aplicação de configurações do agente do RabbitMQ

Uma configuração contém todas as definições do agente do RabbitMQ, no formato Cuttlefish. Você pode criar uma configuração antes de criar qualquer agente. Depois, você pode aplicar a configuração a um ou mais agentes

Os exemplos a seguir mostram como criar e aplicar uma configuração do agente do RabbitMQ utilizando o AWS Management Console.

Tópicos

- [Criar uma configuração](#)
- [Criar uma revisão de configuração](#)
- [Aplicar uma revisão de configuração ao operador](#)

Criar uma configuração

Para aplicar uma configuração ao seu broker, você deve primeiro criar a configuração.

1. Faça login no [console do Amazon MQ](#).
2. Do lado esquerdo, expanda o painel de navegação e selecione Configurations (Configurações).

Amazon MQ ×

Brokers

Configurations

3. Na página Configurations (Configurações), selecione Create configuration (Criar configuração).
4. Na página Create configuration, na seção Details, digite o Configuration name (por exemplo, MyConfiguration) e selecione uma versão do Broker engine.

Para saber mais sobre as versões do mecanismo do RabbitMQ compatíveis com o Amazon MQ para RabbitMQ, consulte [the section called “Gerenciamento de versão”](#).

5. Escolha Criar configuração.

Criar uma revisão de configuração

Depois de criar uma configuração, você deve editá-la usando uma revisão de configuração.

1. Na lista de configurações, escolha **MyConfiguration**.

Note

A primeira revisão de configuração será sempre criada para você quando o Amazon MQ criar a configuração.

Sobre o **MyConfiguration** página, o tipo e a versão do mecanismo do broker que sua nova revisão de configuração usa (por exemplo, RabbitMQ 3.xx.xx) são exibidos.

2. Na guia Detalhes da configuração, são exibidos o número de revisão da configuração, a descrição e a configuração do agente no formato Cuttlefish.

Note

Editar a configuração atual irá criar uma nova revisão da configuração.

3. Selecione Editar configuração e faça as alterações na configuração do Cuttlefish.
4. Escolha Salvar.

A caixa e diálogo Save revision (Salvar revisão) será exibida.

5. (Opcional) Tipo A description of the changes in this revision.
6. Escolha Salvar.

A nova revisão da configuração é salva.

Important

Fazer alterações em uma configuração não aplica as alterações ao agente imediatamente. Para aplicar as alterações, você deve aguardar a próxima janela de manutenção ou [reiniciar o agente](#).

No momento, não é possível excluir uma configuração.

Aplicar uma revisão de configuração ao operador

Depois de criar a revisão de configuração, você pode aplicar a revisão de configuração ao seu broker.

1. Do lado esquerdo, expanda o painel de navegação e selecione Brokers (Agentes).


Amazon MQ ×

Brokers

Configurations

2. Na lista de corretores, selecione seu corretor (por exemplo MyBroker) e escolha Editar.
3. Na edição **MyBroker** página, na seção Configuração, selecione uma Configuração e uma Revisão e, em seguida, escolha Programar Modificações.

4. Na seção **Schedule broker modifications** (Programar modificações no operador), escolha se deseja aplicar as modificações **During the next scheduled maintenance window** (Durante a próxima janela de manutenção programada) ou **Immediately** (Imediatamente).

 **Important**

O agente estará offline durante a reinicialização.


5. Selecione **Apply** (Aplicar).

Sua revisão de configuração será aplicada ao agente no horário especificado.

Editar uma revisão de configuração do Amazon MQ para RabbitMQ

As instruções a seguir descrevem como editar uma revisão de configuração para seu corretor.


1. Faça login no [console do Amazon MQ](#).
2. Na lista de corretores, selecione seu corretor (por exemplo MyBroker) e escolha **Editar**.
3. Sobre o **MyBroker** página, escolha **Editar**.
4. Na edição **MyBroker** página, na seção **Configuração**, selecione uma **Configuração** e uma **Revisão** e, em seguida, escolha **Editar**.

 **Note**

A menos que você selecione uma configuração ao criar um agente, a primeira revisão de configuração será sempre criada para você quando o Amazon MQ criar o agente.

Sobre o **MyBroker** página, o tipo e a versão do mecanismo do broker que a configuração usa (por exemplo, RabbitMQ 3.xx.xx) são exibidos.

5. Na guia **Detalhes da configuração**, são exibidos o número de revisão da configuração, a descrição e a configuração do agente no formato **Cuttlefish**.

 **Note**

Editar a configuração atual irá criar uma nova revisão da configuração.

6. Selecione Editar configuração e faça as alterações na configuração do Cuttlefish.
7. Escolha Salvar.

A caixa e diálogo Save revision (Salvar revisão) será exibida.

8. (Opcional) Tipo A description of the changes in this revision.
9. Escolha Salvar.

A nova revisão da configuração é salva.

Important

Fazer alterações em uma configuração não aplica as alterações ao agente imediatamente. Para aplicar as alterações, você deve aguardar a próxima janela de manutenção ou [reiniciar o agente](#).

No momento, não é possível excluir uma configuração.

Políticas de configuração do RabbitMQ

O Amazon MQ para RabbitMQ agora permite a criação e a aplicação de configurações ao agente do RabbitMQ. A política de operador padrão em cada host virtual tem as seguintes propriedades de HA recomendadas:

```
name: default_operator_policy_AWS_managed
pattern: .*
apply-to: all
priority: 0
definition: {
  ha-mode: all
  ha-sync-mode: automatic
}
```

Alterações nas políticas do operador por meio do AWS Management Console ou Gerenciamento não API estão disponíveis por padrão. Você pode ativar as alterações adicionando a seguinte linha à configuração do agente:

```
management.restrictions.operator_policy_changes.disabled=false
```

Se você fizer essa alteração, é altamente recomendável incluir as propriedades de HA em suas próprias políticas de operador. Para obter mais informações sobre como adicionar configurações ao agente, consulte [Creating and applying broker configurations](#).

Configurando cabeçalhos HTTP de segurança

A `secure.management.http.headers.enabled` configuração ativa os seguintes cabeçalhos de segurança não modificáveis HTTP:

- [X-Content-Type-Options: nosniff](#): impede que os navegadores realizem a detecção de conteúdo, algoritmos usados para deduzir o formato de arquivo dos sites.
- [X-Frame-Options: DENY](#): impede que outras pessoas incorporem o plug-in de gerenciamento em um quadro em seu próprio site para enganar outras pessoas
- [Strict-Transport-Security: max-age=47304000; includeSubDomains](#): obriga os navegadores a serem usados ao fazer conexões subsequentes HTTPS ao site e seus subdomínios por um longo período de tempo (1,5 anos).

Os corretores Amazon MQ para RabbitMQ criados nas versões 3.10 e superiores terão a configuração padrão. `secure.management.http.headers.enabled=true`
`true` Você pode ativar esses cabeçalhos HTTP de segurança configurando como `secure.management.http.headers.enabled=true`. `true` Se você deseja desativar esses cabeçalhos de HTTP segurança, `secure.management.http.headers.enabled=true` defina `false` como.

Filas de quórum para o RabbitMQ no Amazon MQ

Important

As filas de quórum só estão disponíveis para corretores no Amazon MQ para RabbitMQ versão 3.13 e superior.

As filas de quórum são um tipo de fila replicada composta por um líder (réplica primária) e seguidores (outras réplicas). Se o líder ficar indisponível, as filas de quórum usam o algoritmo de consenso [Raft](#) para eleger um novo nó líder pela maioria dos votos, e o líder anterior é rebaixado para um nó seguidor no mesmo cluster. Os seguidores restantes continuam se replicando como antes.

Como cada nó está em uma zona de disponibilidade diferente, se um nó estiver temporariamente indisponível, a entrega de mensagens continuará com a réplica líder recém-eleita em outra zona de disponibilidade.

As filas de quórum são úteis para lidar com mensagens suspeitas, que ocorrem quando uma mensagem falha e é enfileirada várias vezes.

Você não deve usar filas de quórum se você:

- usar filas transitórias
- têm longas filas de espera
- priorizar a baixa latência

Para declarar uma fila de quórum, defina o cabeçalho como. `x-queue-type quorum`

Tópicos

- [Migração de filas clássicas para filas de quórum no Amazon MQ para RabbitMQ](#)
- [Configurações de política para filas de quórum para Amazon MQ para RabbitMQ](#)
- [Melhores práticas para filas de quórum do Amazon MQ for RabbitMQ](#)

Migração de filas clássicas para filas de quórum no Amazon MQ para RabbitMQ

Você pode migrar suas filas espelhadas clássicas para filas de quórum nos corretores Amazon MQ na versão 3.13 ou superior criando um novo host virtual no mesmo cluster ou migrando no local.

Opção 1: migrar de filas espelhadas clássicas para filas de quórum com um novo host virtual

Você pode migrar suas filas espelhadas clássicas para filas de quórum nos corretores Amazon MQ na versão 3.13 ou superior criando um novo host virtual no mesmo cluster.

1. Em seu cluster existente, crie um novo host virtual (vhost) com o tipo de fila padrão como quorum.
2. Crie o a [Plugin de federação](#) partir do novo vhost URI apontando para o antigo usando filas espelhadas clássicas.

3. Usando `rabbitmqadmin`, exporte as definições do vhost antigo para um novo arquivo. Você deve fazer alterações no arquivo do esquema para que ele seja compatível com as filas de quórum. Para ver a lista completa das alterações que você precisa fazer no arquivo, consulte Como [mover definições](#) na documentação das filas de quórum do RabbitMQ. Depois de aplicar as alterações necessárias no arquivo, reimporte as definições para o novo vhost.
4. Crie uma nova política no novo vhost. Para obter recomendações sobre as configurações da política do Amazon MQ para filas de quórum, consulte. [Configurações de política para filas de quórum para Amazon MQ para RabbitMQ](#) Em seguida, inicie a Federação que você criou anteriormente do vhost antigo para o novo vhost.
5. Direcione consumidores e produtores para o novo vhost.
6. Configure o plug-in Shovel para mover as mensagens restantes. Quando a fila estiver vazia, exclua o Shovel.

Migração de filas espelhadas clássicas para filas de quórum em funcionamento

Você pode migrar suas filas espelhadas clássicas para filas de quórum nos corretores Amazon MQ na versão 3.13 ou superior migrando no local.

1. Pare os consumidores e produtores.
2. Crie uma nova fila de quórum temporária.
3. Configure o plug-in Shovel para mover qualquer mensagem da antiga fila espelhada clássica para a nova fila temporária de quórum. Depois que todas as mensagens forem movidas para a fila temporária de quórum, exclua o Shovel.
4. Exclua a fila espelhada clássica de origem. Em seguida, recrie uma fila de quórum com o mesmo nome e vínculos da fila espelhada clássica de origem.
5. Crie um novo Shovel para mover as mensagens da fila de quórum temporária para a nova fila de quórum.

Configurações de política para filas de quórum para Amazon MQ para RabbitMQ

Você pode adicionar configurações de políticas específicas às filas de quórum do seu agente RabbitMQ no Amazon MQ.

Ao criar uma política para filas de quórum, você deve fazer o seguinte:

- Remova todos os atributos da política que começam com `ha` `ha-mode` `ha-params`, como `ha-sync-mode` `ha-sync-batch-size` `ha-promote-on-shutdown` `ha-promote-on-failure` e.
- Remover `queue-mode`.
- Altere o estouro quando estiver definido como `reject-publish-dlx`

Important

O Amazon MQ para RabbitMQ aplica todos ou nenhum dos atributos em uma política. Você não pode criar uma política que se aplique tanto às filas espelhadas clássicas quanto às filas de quórum. Se você quiser que sua política se aplique somente às filas de quórum, defina como `--apply-to quorum_queues`. Se você estiver usando filas espelhadas clássicas e filas de quórum, deverá criar uma política separada com `--apply-to: bem classic_queues` como uma política de filas de quórum.

Você não precisa modificar `AWS-DEFAULT` as políticas porque elas adotam automaticamente o novo tipo de fila no parâmetro “se aplica a”. Para obter mais informações sobre as políticas padrão do Amazon MQ para RabbitMQ, consulte [RabbitMQ configuration policies](#)

Melhores práticas para filas de quórum do Amazon MQ for RabbitMQ

Recomendamos usar as seguintes práticas recomendadas para melhorar o desempenho ao trabalhar com filas de quórum.

Lidar com mensagens suspeitas definindo um limite de entrega

Mensagens suspeitas ocorrem quando uma mensagem falha e é reenviada várias vezes. Você pode definir um limite de entrega de mensagens usando o argumento `delivery-limit` de política para descartar mensagens que são reentregues várias vezes. Se uma mensagem for reentregue mais vezes do que o limite de entrega permitido, ela será descartada e excluída pelo RabbitMQ. Quando você define um limite de entrega, a mensagem é enfileirada perto do início da fila.

Prioridade de mensagens para filas de quórum

As filas de quórum não têm prioridade de mensagem. Se você precisar de prioridade de mensagem, deverá criar várias filas de quórum. Para obter mais informações sobre como priorizar mensagens com várias filas de quórum, consulte [Prioridade de mensagens na documentação do RabbitMQ](#).

Usando o fator de replicação padrão

O Amazon MQ para RabbitMQ usa como padrão um fator de replicação de três (3) nós para agentes de cluster que usam filas de quorum. Se você fizer alterações `ex-quorum-initial-group-size`, o Amazon MQ voltará a usar como padrão o fator de replicação de 3.

Solução de problemas RABBITMQ _ QUORUM _ QUEUES _ NOT _ SUPPORTED CURRENT _ ON _ _ VERSION

O Amazon MQ para RabbitMQ gerará o código de ação essencial necessário `RABBITMQ_QUORUM_QUEUES_NOT_SUPPORTED_ON_CURRENT_VERSION` quando você tentar criar filas de quórum em uma única instância ou agente de cluster usando a versão 3.12 e versões anteriores. Para obter mais informações sobre solução de problemas `RABBITMQ_QUORUM_QUEUES_NOT_SUPPORTED_ON_CURRENT_VERSION`, consulte [Alarme de filas de quórum do Amazon MQ para RabbitMQ](#).

Tutoriais do RabbitMQ

Os tutoriais a seguir mostram como é possível configurar e usar o RabbitMQ no Amazon MQ. Para saber mais sobre como trabalhar com bibliotecas de clientes compatíveis com várias linguagens de programação como Node.js, Python, .NET e muito mais, consulte [Tutoriais do RabbitMQ](#) no Guia de conceitos básicos do RabbitMQ.

Tópicos

- [Editar as preferências de agente](#)
- [Como usar Python Pika com o Amazon MQ para RabbitMQ](#)
- [Resolvendo a sincronização de fila pausada do RabbitMQ](#)

Editar as preferências de agente

Você pode editar suas preferências de agente, como habilitar ou desabilitar o CloudWatch Logs usando o AWS Management Console.

Editar opções do agente RabbitMQ

1. Faça login no [console do Amazon MQ](#).

2. Na lista de agentes, selecione seu agente (por exemplo, MyBroker (MeuAgente)) e, depois, escolha Edit (Editar).
3. Na página Edit **MyBroker**, na seção Especificações, selecione uma Broker engine version (Versão do mecanismo de agente) ou um Broker Instance type (Tipo de instâncias de agente).
4. Na seção CloudWatch Logs, clique no botão de alternância para habilitar ou desabilitar logs gerais. Nenhuma outra etapa é necessária.

Note

- Para agentes RabbitMQ, o Amazon MQ usa automaticamente uma função vinculada ao serviço (SLR) para publicar logs gerais no CloudWatch. Para obter mais informações, consulte [. the section called “Uso de funções vinculadas a serviço”](#)
- O Amazon MQ não é compatível com registros de auditoria para agentes RabbitMQ.

5. Na seção Maintenance (Manutenção), configure a programação de manutenção do agente:

Para atualizar o agente para novas versões à medida que são lançadas pela AWS, selecione Enable automatic minor version upgrades (Habilitar atualizações automáticas de versão secundária). Atualizações automáticas ocorrem durante a janela de manutenção definida pelo dia da semana, a hora do dia (no formato de 24 horas) e o fuso horário (UTC, por padrão).

6. Selecione Schedule modifications (Programar modificações).

Note

Se você selecionar somente Enable automatic minor version upgrades (Habilitar atualizações automáticas de versão secundária), o botão será alterado para Save (Salvar), pois não será necessária nenhuma reinicialização do agente.

Suas preferências serão aplicadas ao agente no horário especificado.

Como usar Python Pika com o Amazon MQ para RabbitMQ

O tutorial a seguir mostra como você pode configurar um cliente [Python Pika](#) com o TLS configurado para estabelecer conexão com o agente Amazon MQ para RabbitMQ. O Pika é uma implementação

Python do protocolo AMQP 0-9-1 para RabbitMQ. Este tutorial orienta você durante a instalação do Pika, declarando uma fila, configurando um publicador para enviar mensagens para a troca padrão do agente e configurar um consumidor para receber mensagens da fila.

Tópicos

- [Pré-requisitos](#)
- [Permissões](#)
- [Etapa um: criar um cliente Python Pika básico](#)
- [Etapa dois: criar um publicador e enviar uma mensagem](#)
- [Etapa três: criar um consumidor e receber uma mensagem](#)
- [Etapa quatro: \(opcional\) configurar um loop de eventos e consumir mensagens](#)
- [Próximas etapas](#)

Pré-requisitos

Para concluir as etapas neste tutorial, você precisa dos seguintes pré-requisitos:

- Um agente Amazon MQ para RabbitMQ. Para mais informações, consulte [Criar um agente Amazon MQ para RabbitMQ](#).
- O [Python 3](#) instalado para o seu sistema operacional.
- O [Pika](#) instalado usando o Python `pip`. Para instalar o Pika, abra uma nova janela de terminal e execute o seguinte.

```
$ python3 -m pip install pika
```

Permissões

Para este tutorial, você precisa de pelo menos um usuário do agente Amazon MQ para RabbitMQ com permissão para gravação em e leitura de um vhost. A tabela a seguir descreve as permissões mínimas necessárias como padrões de expressão regular (regex).

Tags	Configurar regex	Escrever regex	Ler regex
none		.*	.*

As permissões de usuário listadas fornecem apenas permissões de leitura e gravação para o usuário, sem conceder acesso ao plugin de gerenciamento para executar operações administrativas no agente. Você pode restringir ainda mais as permissões fornecendo padrões regexp que limitem o acesso do usuário às filas especificadas. Por exemplo, se você alterar o padrão regexp de leitura para `^[hello world].*`, o usuário só terá permissão de leitura para as filas que começam com `hello world`.

Para obter mais informações sobre criar usuários RabbitMQ e gerenciar etiquetas e permissões de usuário, consulte [Amazon MQ para usuários do broker RabbitMQ](#).

Etapa um: criar um cliente Python Pika básico

Para criar uma classe base de cliente Python Pika que define um construtor e fornece o contexto SSL necessário para a configuração TLS durante a interação com um agente Amazon MQ para RabbitMQ, faça o seguinte.

1. Abra uma nova janela de terminal, crie um novo diretório para seu projeto e acesse o diretório.

```
$ mkdir pika-tutorial
$ cd pika-tutorial
```

2. Crie um novo arquivo chamado `basicClient.py` contendo o seguinte código Python.

```
import ssl
import pika

class BasicPikaClient:

    def __init__(self, rabbitmq_broker_id, rabbitmq_user, rabbitmq_password,
region):

        # SSL Context for TLS configuration of Amazon MQ for RabbitMQ
        ssl_context = ssl.SSLContext(ssl.PROTOCOL_TLSv1_2)
        ssl_context.set_ciphers('ECDHE+AESGCM:!ECDSA')

        url = f"amqps://{rabbitmq_user}:
{rabbitmq_password}@{rabbitmq_broker_id}.mq.{region}.amazonaws.com:5671"
        parameters = pika.URLParameters(url)
        parameters.ssl_options = pika.SSLOptions(context=ssl_context)

        self.connection = pika.BlockingConnection(parameters)
```

```
self.channel = self.connection.channel()
```

Agora você pode definir classes adicionais para seu publicador e consumidor que herdam de `BasicPikaClient`.

Etapa dois: criar um publicador e enviar uma mensagem

Para criar um publicador que declara uma fila e envia uma única mensagem, faça o seguinte.

1. Copie o conteúdo da amostra de código a seguir e salve localmente como `publisher.py` no mesmo diretório que você criou na etapa anterior.

```
from basicClient import BasicPikaClient

class BasicMessageSender(BasicPikaClient):

    def declare_queue(self, queue_name):
        print(f"Trying to declare queue({queue_name})...")
        self.channel.queue_declare(queue=queue_name)

    def send_message(self, exchange, routing_key, body):
        channel = self.connection.channel()
        channel.basic_publish(exchange=exchange,
                              routing_key=routing_key,
                              body=body)
        print(f"Sent message. Exchange: {exchange}, Routing Key: {routing_key},
Body: {body}")

    def close(self):
        self.channel.close()
        self.connection.close()

if __name__ == "__main__":

    # Initialize Basic Message Sender which creates a connection
    # and channel for sending messages.
    basic_message_sender = BasicMessageSender(
        "<broker-id>",
        "<username>",
        "<password>",
        "<region>"
    )
```

```
# Declare a queue
basic_message_sender.declare_queue("hello world queue")

# Send a message to the queue.
basic_message_sender.send_message(exchange="", routing_key="hello world queue",
body=b'Hello World!')

# Close connections.
basic_message_sender.close()
```

A classe `BasicMessageSender` herda de `BasicPikaClient` e implementa métodos adicionais para declarar uma fila, enviar uma mensagem para a fila e fechar conexões. A amostra de código encaminha uma mensagem para a troca padrão, com uma chave de roteamento igual ao nome da fila.

2. Em `if __name__ == "__main__":`, substitua os parâmetros transmitidos para a declaração do construtor `BasicMessageSender` com as seguintes informações.
 - **<broker-id>** — O ID exclusivo que o Amazon MQ gera para o agente. Você pode analisar o ID do ARN do seu agente. Por exemplo, considerando o seguinte ARN, `arn:aws:mq:us-east-2:123456789012:broker:MyBroker:b-1234a5b6-78cd-901e-2fgh-3i45j6k17819`, o ID do agente seria `b-1234a5b6-78cd-901e-2fgh-3i45j6k17819`.
 - **<username>**: o nome de usuário de um usuário agente com permissões suficientes para gravação de mensagens no agente.
 - **<password>**: a senha de um usuário agente com permissões suficientes para gravação de mensagens no agente.
 - **<region>**: a região da AWS na qual você criou o agente do Amazon MQ para RabbitMQ. Por exemplo, `us-west-2`.
3. Execute o seguinte comando no mesmo diretório que você criou `publisher.py`.

```
$ python3 publisher.py
```

Se o código for executado com êxito, você verá o resultado a seguir na janela do seu terminal.

```
Trying to declare queue(hello world queue)...
Sent message. Exchange: , Routing Key: hello world queue, Body: b'Hello World!'
```

Etapa três: criar um consumidor e receber uma mensagem

Para criar um consumidor que recebe uma única mensagem da fila, faça o seguinte.

1. Copie o conteúdo da amostra de código a seguir e salve localmente como `consumer.py` no mesmo diretório.

```
from basicClient import BasicPikaClient

class BasicMessageReceiver(BasicPikaClient):

    def get_message(self, queue):
        method_frame, header_frame, body = self.channel.basic_get(queue)
        if method_frame:
            print(method_frame, header_frame, body)
            self.channel.basic_ack(method_frame.delivery_tag)
            return method_frame, header_frame, body
        else:
            print('No message returned')

    def close(self):
        self.channel.close()
        self.connection.close()

if __name__ == "__main__":

    # Create Basic Message Receiver which creates a connection
    # and channel for consuming messages.
    basic_message_receiver = BasicMessageReceiver(
        "<broker-id>",
        "<username>",
        "<password>",
        "<region>"
    )

    # Consume the message that was sent.
    basic_message_receiver.get_message("hello world queue")

    # Close connections.
    basic_message_receiver.close()
```

De modo semelhante ao publicador que você criou na etapa anterior, `BasicMessageReceiver` herda de `BasicPikaClient` e implementa métodos adicionais para receber uma única mensagem e fechar conexões.

2. Na declaração `if __name__ == "__main__":`, substitua os parâmetros transmitidos ao construtor `BasicMessageReceiver` com suas informações.
3. Execute o seguinte comando no diretório do projeto.

```
$ python3 consumer.py
```

Se o código for executado com êxito, você verá o corpo da mensagem e os cabeçalhos, incluindo a chave de roteamento, exibidos na janela do seu terminal.

```
<Basic.GetOk(['delivery_tag=1', 'exchange=', 'message_count=0',  
'redelivered=False', 'routing_key=hello world queue'])> <BasicProperties> b'Hello  
World!'
```

Etapa quatro: (opcional) configurar um loop de eventos e consumir mensagens

Para consumir várias mensagens de uma fila, use o método [basic_consume](#) do Pika e uma função de retorno de chamada conforme mostrado a seguir

1. Em `consumer.py`, adicione a definição de método a seguir à classe `BasicMessageReceiver`.

```
def consume_messages(self, queue):  
    def callback(ch, method, properties, body):  
        print(" [x] Received %r" % body)  
  
        self.channel.basic_consume(queue=queue, on_message_callback=callback,  
auto_ack=True)  
  
    print(' [*] Waiting for messages. To exit press CTRL+C')  
    self.channel.start_consuming()
```

2. Em `consumer.py`, sob `if __name__ == "__main__":`, invoque o método `consume_messages` definido por você na etapa anterior.

```
if __name__ == "__main__":

    # Create Basic Message Receiver which creates a connection and channel for
    # consuming messages.
    basic_message_receiver = BasicMessageReceiver(
        "<broker-id>",
        "<username>",
        "<password>",
        "<region>"
    )

    # Consume the message that was sent.
    # basic_message_receiver.get_message("hello world queue")

    # Consume multiple messages in an event loop.
    basic_message_receiver.consume_messages("hello world queue")

    # Close connections.
    basic_message_receiver.close()
```

3. Execute `consumer.py` novamente e, se bem-sucedidas, as mensagens na fila serão exibidas na janela do seu terminal.

```
[*] Waiting for messages. To exit press CTRL+C
[x] Received b'Hello World!'
[x] Received b'Hello World!'
...
```

Próximas etapas

- Para mais informações sobre outras bibliotecas suportadas de cliente do RabbitMQ, consulte [Documentação do cliente RabbitMQ](#) no site do RabbitMQ.

Resolvendo a sincronização de fila pausada do RabbitMQ

Em uma [implantação de cluster](#) do Amazon MQ para RabbitMQ, as mensagens publicadas em cada fila são replicadas em três nós de agente. Esta replicação, chamada de espelhamento, fornece alta disponibilidade (HA) para agentes RabbitMQ. As filas em uma implantação de cluster consistem em uma réplica principal em um nó e um ou mais espelhos. Cada operação aplicada a uma fila

espelhada, incluindo o enfileiramento de mensagens, é aplicada primeiro à fila principal e, em seguida, replicada em seus espelhos.

Por exemplo, considere uma fila espelhada replicada em três nós: o nó principal (`main`) e dois espelhos (`mirror-1` e `mirror-2`). Se todas as mensagens nessa fila espelhada forem propagadas com êxito para todos os espelhos, a fila será sincronizada. Se um nó (`mirror-1`) se tornar indisponível por um intervalo de tempo, a fila ainda estará operacional e poderá continuar a enfileirar mensagens. No entanto, para sincronizar a fila, as mensagens publicadas no `main` enquanto `mirror-1` estiver indisponível devem ser replicadas para `mirror-1`.

Para obter mais informações sobre o espelhamento, consulte [Filas Espelhadas Clássicas](#) no site RabbitMQ.

Manutenção e sincronização de filas

Durante as [janelas de manutenção](#), o Amazon MQ executa todos os trabalhos de manutenção um nó de cada vez para garantir que o agente permaneça operacional. Como resultado, as filas podem precisar sincronizar à medida que cada nó retoma a operação. Durante a sincronização, as mensagens que precisam ser replicadas em espelhos são carregadas na memória do volume correspondente do Amazon Elastic Block Store (Amazon EBS) para serem processadas em lotes. O processamento de mensagens em lotes permite que as filas sejam sincronizadas mais rapidamente.

Se as filas forem mantidas curtas e as mensagens forem pequenas, as filas serão sincronizadas com êxito e retomarão a operação conforme esperado. No entanto, se a quantidade de dados em um lote se aproximar do limite de memória do nó, o nó gera um alarme de memória alta, pausando a sincronização de fila. Você pode confirmar o uso da memória comparando as [métricas de nó do agente no CloudWatch](#) do `RabbitMemUsed` e `RabbitMqMemLimit`. A sincronização não pode ser concluída até que as mensagens sejam consumidas ou excluídas ou o número de mensagens no lote seja reduzido.

Note

Reduzir o tamanho do lote de sincronização de fila pode resultar em um número maior de transações de replicação.

Para resolver uma sincronização de fila pausada, siga as etapas deste tutorial, que demonstra a aplicação de uma política `ha-sync-batch-size` e reiniciar a sincronização de filas.

Tópicos

- [Pré-requisitos](#)
- [Etapa 1: Aplicar uma política `ha-sync-batch-size`](#)
- [Etapa 2: Reiniciar a sincronização de filas](#)
- [Próximas etapas](#)
- [Recursos relacionados](#)

Pré-requisitos

Para este tutorial, você deve ter um usuário do agente Amazon MQ para RabbitMQ com permissões de administrador. Você pode usar o usuário administrador criado quando criou o agente pela primeira vez ou outro usuário que você possa ter criado posteriormente. A tabela a seguir fornece a etiqueta de usuário administrador necessária e as permissões como padrões de expressão regular (regex).

Etiquetas	Ler regex	Configurar regex	Escrever regex
administrator	.*	.*	.*

Para obter mais informações sobre criar usuários RabbitMQ e gerenciar etiquetas e permissões de usuário, consulte [Amazon MQ para usuários do broker RabbitMQ](#).


Etapa 1: Aplicar uma política `ha-sync-batch-size`

Os procedimentos a seguir demonstram a adição de uma política que se aplica a todas as filas criadas no agente. Você pode usar o console da Web do RabbitMQ ou a API de gerenciamento do RabbitMQ. Para obter mais informações, consulte [Plugin Gerenciamento](#) no site do RabbitMQ.

Para aplicar uma política `ha-sync-batch-size` usando o console da Web RabbitMQ

1. Faça login no [console do Amazon MQ](#).
2. No painel de navegação à esquerda, escolha Agentes.
3. Na lista de agentes, escolha o nome do agente ao qual você deseja aplicar a nova política.
4. Na página do agente, na seção Conexões, escolha a URL RabbitMQ web console (Console da Web RabbitMQ). O console da Web do RabbitMQ é aberto em uma nova guia ou janela do navegador.

5. Faça login no console da Web do RabbitMQ com as credenciais de login de administrador do agente.
6. No console da Web do RabbitMQ, na parte superior da página, escolha Admin.
7. Na página Admin, no painel de navegação da direita, selecione Policies (Políticas).
8. Na página Policies (Políticas), você pode ver uma lista das User policies (Políticas de usuário) atuais do agente. Abaixo das User policies (Políticas de usuário), expanda Add/update a policy (Adicionar/atualizar uma política).

 Note

Por padrão, os clusters Amazon MQ para RabbitMQ são criados com uma política de agente inicial chamada `ha-all-AWS-OWNED-DO-NOT-DELETE`. O Amazon MQ gerencia essa política para garantir que cada fila no agente seja replicada para todos os três nós e que as filas sejam sincronizadas automaticamente.

9. Para criar uma política de agente, em Add/update a policy (Adicionar/atualizar uma política), faça o seguinte:
 - a. Em Nome, insira um nome para a sua política, por exemplo **batch-size-policy**.
 - b. Para Pattern (Padrão), insira o padrão de expressão regular `.*` para que a política corresponda a todas as filas no agente.
 - c. Para Apply to (Aplicar em), escolha Exchanges and queues (Trocacões e filas) na lista suspensa.
 - d. Para Priority (Prioridade), insira um número inteiro maior que todas as outras políticas aplicadas ao vhost. Você pode aplicar exatamente um conjunto de definições de política a filas e trocões RabbitMQ a qualquer momento. O RabbitMQ escolhe a política correspondente com o valor de prioridade mais alto. Para obter mais informações sobre prioridades de política e como combinar políticas, consulte [Policies](#) (Políticas) na Documentação do Servidor RabbitMQ.
 - e. Para Definition (Definição), adicione os seguintes pares de chave-valor:
 - **ha-sync-batch-size=100**. Selecione Number (Número) na lista suspensa.

Note

Talvez seja necessário ajustar e calibrar o valor de `ha-sync-batch-size` com base no número e tamanho das mensagens não sincronizadas nas filas.

- **ha-mode=all**. Selecione String (String) na lista suspensa.

Important

A definição `ha-mode` é necessária para todas as políticas relacionadas a HA. Omitir isso resulta em uma falha de validação.

- **ha-sync-mode=automatic**. Selecione String (String) na lista suspensa.

Note

A definição `ha-sync-mode` é necessária para todas as políticas personalizadas. Se isso for omitido, o Amazon MQ anexará automaticamente a definição.

f. Escolha Add/update policy (Adicionar/atualizar política).

10. Confirme se a nova política aparece na lista de User policies (Políticas de usuário).

Para aplicar uma política **ha-sync-batch-size** usando a API de gerenciamento RabbitMQ

1. Faça login no [console do Amazon MQ](#).
2. No painel de navegação à esquerda, escolha Agentes.
3. Na lista de agentes, escolha o nome do agente ao qual você deseja aplicar a nova política.
4. Na página do agente, na seção Connections (Conexões), anote a URL do RabbitMQ web console (Console da Web RabbitMQ). Este é o endpoint do agente que você usa em uma solicitação HTTP.
5. Abra uma nova janela de terminal ou linha de comando de sua escolha.
6. Para criar uma nova política de agente, insira o comando `curl` a seguir. Este comando assume uma fila no vhost / padrão, que é codificada como `%2F`.

Note

Substitua o *nome de usuário* e a *senha* pelas suas credenciais de login de administrador do agente. Talvez seja necessário ajustar e calibrar o valor de `ha-sync-batch-size` (*100*) com base no número e tamanho das mensagens não sincronizadas nas filas. Substitua o endpoint do agente com a URL que você anotou anteriormente.

```
curl -i -u username:password -H "content-type:application/json" -XPUT \  
-d '{"pattern":".*", "priority":1, "definition":{"ha-sync-batch-size":100, "ha-  
mode":"all", "ha-sync-mode":"automatic"}}' \  
https://b-589c045f-f81n-4ab0-a89c-co62e1c32ef8.mq.us-west-2.amazonaws.com/api/  
policies/%2Fbatch-size-policy
```

7. Para confirmar se a nova política foi adicionada às políticas de usuário do seu agente, insira o seguinte comando `curl` para listar todas as políticas de agente.

```
curl -i -u username:password https://b-589c045f-f81n-4ab0-a89c-co62e1c32ef8.mq.us-  
west-2.amazonaws.com/api/policies
```

Etapa 2: Reiniciar a sincronização de filas

Depois de aplicar uma nova política `ha-sync-batch-size` para seu agente, reinicie a sincronização de fila.

Para reiniciar a sincronização de filas usando o console da Web RabbitMQ

Note

Para abrir o console da Web RabbitMQ, consulte as instruções anteriores na Etapa 1 deste tutorial.

1. No console da Web do RabbitMQ, na parte superior da página, escolha Queues (Filas).
2. Na página Filas, em Todas as filas, localize sua fila pausada. Na coluna Recursos, sua fila deve listar o nome da nova política que você criou (por exemplo, `batch-size-policy`).

3. Para reiniciar o processo de sincronização com um tamanho de lote reduzido, escolha Restart sync (Reiniciar sincronização).

Note

Se a sincronização for interrompida e não for concluída com êxito, tente reduzir o valor `ha-sync-batch-size` e reiniciar a sincronização de fila novamente.

Próximas etapas

- Depois que a fila for sincronizada com êxito, você poderá monitorar a quantidade de memória que seus nós RabbitMQ usam visualizando a métrica `RabbitMQMemUsed` do Amazon CloudWatch. Você também pode visualizar a métrica `RabbitMQMemLimit` para monitorar o limite de memória de um nó. Para obter mais informações, consulte [Acessando CloudWatch métricas para o Amazon MQ](#) e [CloudWatch Métricas disponíveis para Amazon MQ para corretores RabbitMQ](#).
- Para evitar pausar a sincronização de filas, recomendamos manter as filas curtas e processar as mensagens. Para workloads com tamanhos de mensagem maiores, também recomendamos atualizar o tipo de instância do agente para um tamanho de instância maior com mais memória. Para obter mais informações sobre os tipos de instância do agente e as preferências de edição do agente, consulte [Amazon MQ para tipos de instância RabbitMQ](#) e [Editar as preferências de agente](#).
- Quando você cria um novo Amazon MQ para o agente RabbitMQ, o Amazon MQ aplica um conjunto de políticas padrão e limites de host virtual para otimizar a performance do agente. Se o seu agente não tiver as políticas e limites padrão recomendados, recomendamos criá-las você mesmo. Para obter mais informações sobre como criar políticas padrão e limites vhost, consulte [the section called “Padrões do agente”](#).

Recursos relacionados

- [UpdateBrokerInput](#): Use essa propriedade de agente para atualizar um tipo de instância de agente usando a API do Amazon MQ.
- [Parâmetros e Políticas](#) (Documentação do Servidor RabbitMQ): Saiba mais sobre os parâmetros e políticas do RabbitMQ no site do RabbitMQ.

- [API HTTP de gerenciamento do RabbitMQ](#) — Saiba mais sobre a API de gerenciamento do RabbitMQ.

Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ

O RabbitMQ organiza números de versão de acordo com a especificação de versionamento semântico como X.Y.Z. Nas implementações do Amazon MQ para RabbitMQ, X indica a versão principal, Y representa a versão secundária e indica o número da versão do patch. Z O Amazon MQ considera que uma alteração de versão é principal se os números de versão principais mudarem. Por exemplo, a atualização da versão 3.13 para a 4.0 é considerada uma atualização importante da versão. Uma alteração de versão é considerada pequena se apenas o número da versão secundária ou do patch for alterado. Por exemplo, atualizando a partir da versão 3.11.28 a 3.12.13 é considerado um pequeno upgrade de versão.

O Amazon MQ para RabbitMQ recomenda que todos os corretores usem a última versão secundária compatível. Para obter instruções sobre como atualizar a versão do mecanismo de corretagem, consulte [Atualizar uma versão do mecanismo de corretora Amazon MQ](#).

Important

[O Amazon MQ não oferece suporte a streams](#). Habilitar esse sinalizador de recurso e criar um stream resultará em perda de dados.

O Amazon MQ não oferece suporte ao uso de login estruturadoJSON, introduzido no RabbitMQ 3.9

Versões de mecanismo compatíveis no Amazon MQ para RabbitMQ

O calendário de suporte da versão Amazon MQ indica quando uma versão do broker Engine chegará ao fim do suporte. Quando uma versão chega ao fim do suporte, o Amazon MQ atualiza automaticamente todos os corretores dessa versão para a próxima versão compatível. Essa atualização ocorre durante as janelas de manutenção programada da sua corretora, dentro dos 45 dias após a end-of-support data.

O Amazon MQ avisa com pelo menos 90 dias de antecedência antes que uma versão chegue ao fim do suporte. Recomendamos atualizar seu corretor antes da end-of-support data para evitar interrupções. Além disso, você não pode criar novos corretores em versões programadas para o fim do suporte dentro de 30 dias da data de término do suporte.

Versão RabbitMQ	Fim do suporte no Amazon MQ
3.13 (recomendado)	
3.12	
3.11	
3.10	15 de outubro de 2024
3.9	16 de setembro de 2024

Ao criar um novo agente do Amazon MQ para RabbitMQ, você pode especificar qualquer versão compatível do mecanismo RabbitMQ. Se você não especificar o número da versão do mecanismo ao criar um agente, o Amazon MQ automaticamente usará como padrão o número da versão mais recente do mecanismo.

Atualizações da versão do motor

Você pode atualizar manualmente seu corretor a qualquer momento para a próxima versão principal ou secundária compatível. Quando você ativa as [atualizações automáticas de versões secundárias](#), o Amazon MQ atualiza seu agente para a versão de patch mais recente suportada durante [a](#) janela de manutenção.

Para obter mais informações sobre como atualizar manualmente sua corretora, consulte [the section called “Atualizar a versão do mecanismo”](#).

Para todos os corretores que usam a versão 3.13 e superior do mecanismo, o Amazon MQ gerencia as atualizações para a versão de patch mais recente suportada durante a janela de manutenção.

Important

O RabbitMQ só permite atualizações incrementais de versão (por exemplo, 3.9.x para 3.10.x). Você não pode pular versões secundárias ao atualizar (por exemplo: 3.8.x para 3.11.x).

Os agentes de instância única ficarão offline durante a reinicialização. Para agentes de cluster, as filas espelhadas devem ser sincronizadas durante a reinicialização. Com filas mais longas, o

processo de sincronização de filas pode demorar mais. Durante o processo de sincronização de filas, a fila não está disponível para consumidores e produtores. Quando o processo de sincronização de filas for concluído, o corretor ficará disponível novamente. Para minimizar o impacto, recomendamos a atualização durante um período de baixo tráfego. Para obter mais informações sobre as melhores práticas para atualizações de versão, consulte [Práticas recomendadas do Amazon MQ para RabbitMQ](#).

Listando as versões compatíveis do mecanismo

Você pode listar todas as versões de mecanismos secundários e principais compatíveis usando o [describe-broker-instance-options](#) AWS CLI comando.

```
aws mq describe-broker-instance-options
```

Para filtrar os resultados por mecanismo e tipo de instância, use a opção `--engine-type` e `--host-instance-type`, conforme mostrado a seguir.

```
aws mq describe-broker-instance-options --engine-type engine-type --host-instance-type instance-type
```

Por exemplo, para filtrar os resultados do RabbitMQ e do tipo de `mq.m5.large` instância, substitua *engine-type* com `RABBITMQ` e *instance-type* com `commq.m5.large`.

Práticas recomendadas do Amazon MQ para RabbitMQ

Use esta seção como referência para localizar rapidamente as recomendações para maximizar a performance e minimizar os custos de taxa de transferência para trabalhar com agentes do RabbitMQ no Amazon MQ.

Important

Atualmente, o Amazon MQ não oferece suporte a [streams](#) ou o uso de login estruturado, introduzido no RabbitMQ JSON 3.9.x.

⚠ Important

O Amazon MQ para RabbitMQ não suporta o nome de usuário “convidado” e excluirá a conta de convidado padrão quando você criar um novo corretor. O Amazon MQ também excluirá periodicamente qualquer conta criada pelo cliente chamada “convidado”.

Tópicos

- [Ativar atualizações automáticas de versões secundárias](#)
- [Usando recursos obsoletos](#)
- [Escolha o tipo correto de instância do broker para obter a melhor taxa de transferência](#)
- [Use vários canais](#)
- [Habilitar filas lazy](#)
- [Use mensagens persistentes e filas duráveis](#)
- [Mantenha as filas curtas](#)
- [Configurar reconhecimento e confirmação](#)
- [Configurar pré-busca](#)
- [Configurar o Celery](#)
- [Recuperação automática de falhas de rede](#)
- [Habilite o Classic Queue v2 para seu agente do RabbitMQ](#)

Ativar atualizações automáticas de versões secundárias

Usando a versão mais recente do broker, segurança, correções de bugs e melhorias de desempenho. Você pode ativar as atualizações automáticas de versões secundárias do Amazon MQ para gerenciar as atualizações para a versão mais recente do patch.

Usando recursos obsoletos

Se você estiver usando a versão 3.13 para o RabbitMQ no Amazon MQ, você verá um banner na interface de usuário do RabbitMQ Management que diz: `Deprecated features are being used`.

Isso ocorre porque o RabbitMQ no Amazon MQ usa os seguintes recursos que não são mais oferecidos no RabbitMQ ou são configurados automaticamente para o RabbitMQ no Amazon MQ:

- Espelhamento clássico de filas
- QoS global
- Filas transitórias não exclusivas

Este é um banner informativo para a versão 3.13 que não requer nenhuma ação. Seu corretor Amazon MQ continuará usando esses recursos.

Escolha o tipo correto de instância do broker para obter a melhor taxa de transferência

A taxa de transferência de mensagens de um tipo de instância do broker depende do caso de uso do seu aplicativo. Tipos menores de instâncias de corretor, como, só `t3.micro` devem ser usados para testar o desempenho do aplicativo. Usar essas microinstâncias antes de usar instâncias maiores na produção pode melhorar o desempenho do aplicativo e ajudar você a reduzir os custos de desenvolvimento. Em tipos de instância `m5.large` e superiores, você pode usar implantações de cluster para obter alta disponibilidade e durabilidade de mensagens. Tipos maiores de instâncias de broker podem lidar com níveis de produção de clientes e filas, alta taxa de transferência, mensagens na memória e mensagens redundantes. Para obter mais informações sobre como escolher o tipo de instância correto, consulte Diretrizes de dimensionamento.

Use vários canais

Para evitar a perda de conexão, use vários canais em uma única conexão. Os aplicativos devem evitar uma relação de conexão de 1:1 com o canal. Recomendamos usar uma conexão por processo e, em seguida, um canal por thread. Evite o uso excessivo do canal para evitar vazamentos no canal.

Habilitar filas lazy

Se você estiver trabalhando com filas muito longas que processam grandes volumes de mensagens, ativar filas preguiçosas pode melhorar o desempenho do corretor.

O comportamento padrão do RabbitMQ é armazenar mensagens em cache na memória e movê-las para o disco somente quando o agente precisar de mais memória disponível. Mover mensagens da memória para o disco leva tempo e interrompe o processamento das mensagens. As filas

preguiçosas aceleram significativamente o processo de memória para disco, armazenando mensagens em disco o mais rápido possível, resultando em menos mensagens armazenadas em cache na memória.

Você pode habilitar filas lentas definindo a propriedade `queue.declare` no momento da declaração ou configurando uma política por meio do console de gerenciamento RabbitMQ. O exemplo a seguir demonstra declarar uma fila lazy usando a biblioteca do cliente Java RabbitMQ.

```
Map<String, Object> args = new HashMap<String, Object>();
args.put("x-queue-mode", "lazy");
channel.queueDeclare("myqueue", false, false, false, args);
```

Todas as filas do Amazon MQ para RabbitMQ em 3.12.13 e versões posteriores se comportam como filas preguiçosas por padrão. Para fazer o upgrade para a versão mais recente do Amazon MQ para RabbitMQ, consulte [???](#)

Note

Ativar filas lazy pode aumentar as operações de E/S de disco.

Use mensagens persistentes e filas duráveis

Mensagens persistentes podem ajudar a evitar a perda de dados em situações em que um agente falha ou reinicia. Mensagens persistentes são gravadas no disco assim que chegam. Ao contrário das filas lazy, no entanto, as mensagens persistentes são armazenadas em cache tanto na memória quanto no disco, a menos que o agente necessite de mais memória. Nos casos em que mais memória é necessária, as mensagens são removidas da memória pelo mecanismo do agente RabbitMQ que gerencia o armazenamento de mensagens no disco, comumente chamado de camada de persistência.

Para habilitar a persistência de mensagens, você pode declarar suas filas como `durable` e definir o modo de entrega de mensagens como `persistent`. O exemplo a seguir demonstra declarar uma fila durável usando a [biblioteca do cliente Java RabbitMQ](#). Ao trabalhar com AMQP 0-9-1, você pode marcar mensagens como persistentes definindo o modo de entrega "2".

```
boolean durable = true;
channel.queueDeclare("my_queue", durable, false, false, null);
```

Depois de configurar sua fila como durável, você pode enviar uma mensagem persistente para a fila definindo `MessageProperties` como `PERSISTENT_TEXT_PLAIN`, da forma mostrada no exemplo a seguir.

```
import com.rabbitmq.client.MessageProperties;

channel.basicPublish("", "my_queue",
    MessageProperties.PERSISTENT_TEXT_PLAIN,
    message.getBytes());
```

Mantenha as filas curtas

Em implantações de cluster, filas com um grande número de mensagens podem levar à utilização excessiva de recursos. Quando um agente é utilizado em excesso, a reinicialização de um agente do Amazon MQ para RabbitMQ pode causar maior degradação da performance. Se reinicializados, os agentes usados em excesso podem deixar de responder no estado `REBOOT_IN_PROGRESS`.

Durante as [janelas de manutenção](#), o Amazon MQ executa todos os trabalhos de manutenção um nó de cada vez para garantir que o agente permaneça operacional. Como resultado, as filas podem precisar sincronizar à medida que cada nó retoma a operação. Durante a sincronização, as mensagens que precisam ser replicadas em espelhos são carregadas na memória a partir do volume correspondente do Amazon Elastic Block Store (AmazonEBS) para serem processadas em lotes. O processamento de mensagens em lotes permite que as filas sejam sincronizadas mais rapidamente.

Se as filas forem mantidas curtas e as mensagens forem pequenas, as filas serão sincronizadas com êxito e retomarão a operação conforme esperado. No entanto, se a quantidade de dados em um lote se aproximar do limite de memória do nó, o nó gera um alarme de memória alta, pausando a sincronização de fila. Você pode confirmar o uso da memória comparando as [métricas do nó `RabbitMemUsed` e do `RabbitMqMemLimit` broker em CloudWatch](#). A sincronização não pode ser concluída até que as mensagens sejam consumidas ou excluídas ou o número de mensagens no lote seja reduzido.

Se a sincronização de filas estiver pausada para uma implantação de cluster, recomendamos consumir ou excluir mensagens para diminuir o número de mensagens em filas. Quando a profundidade da fila for reduzida e a sincronização da fila for concluída, o status do agente mudará para `RUNNING`. Para resolver uma sincronização de fila pausada, você também pode aplicar uma política para [reduzir o tamanho do lote de sincronização de filas](#).

Você também pode definir a exclusão automática e TTL políticas para reduzir proativamente o uso de recursos, bem como reduzir ao mínimo o alcance NACKs dos consumidores. O enfileiramento de mensagens na corretora é CPU intensivo, portanto, um grande número de mensagens NACKs pode afetar o desempenho da corretora.

Configurar reconhecimento e confirmação

Quando uma aplicação do cliente envia confirmação de entrega e consumo de mensagens de volta para o agente, isso é conhecido como reconhecimento do consumidor. Da mesma forma, o processo de envio de confirmação para um editor é conhecido como confirmação do editor. O editor confirma que avisa seu aplicativo quando as mensagens foram armazenadas de forma confiável. Sem a confirmação do editor, seu corretor pode continuar aceitando mensagens mesmo quando está com pouca memória ou não consegue processá-las. Tanto o reconhecimento quanto a confirmação são essenciais para garantir a segurança dos dados ao trabalhar com agentes RabbitMQ.

A confirmação de entrega do consumidor geralmente é configurada na aplicação do cliente. Ao trabalhar com AMQP 0-9-1, a confirmação pode ser ativada configurando o `basic.consume` ou quando uma mensagem é buscada usando o método `basic.code`. AMQPOs clientes 0-9-1 também podem configurar as confirmações do editor enviando o método `confirm.select`

Normalmente, a confirmação de entrega está habilitada em um canal. Por exemplo, ao trabalhar com a biblioteca do cliente Java RabbitMQ, você pode usar o `Channel#basicAck` para configurar um reconhecimento positivo `basic.ack`, conforme mostrado no exemplo a seguir.

```
// this example assumes an existing channel instance

boolean autoAck = false;
channel.basicConsume(queueName, autoAck, "a-consumer-tag",
    new DefaultConsumer(channel) {
        @Override
        public void handleDelivery(String consumerTag,
            Envelope envelope,
            AMQP.BasicProperties properties,
            byte[] body)
            throws IOException
        {
            long deliveryTag = envelope.getDeliveryTag();
            // positively acknowledge a single delivery, the message will
            // be discarded
            channel.basicAck(deliveryTag, false);
        }
    }
);
```

```
    }  
});
```

Note

Mensagens não reconhecidas devem ser armazenadas em cache na memória. Você pode limitar o número de mensagens que um consumidor busca antecipadamente configurando [Pré-busca](#) para uma aplicação do cliente.

Configurar pré-busca

Você pode usar o valor de pré-busca RabbitMQ para otimizar como seus consumidores consomem mensagens. O RabbitMQ implementa o mecanismo de pré-busca de canais fornecido por AMQP 0-9-1 aplicando a contagem de pré-busca aos consumidores em vez dos canais. O valor de pré-busca é usado para especificar quantas mensagens estão sendo enviadas ao consumidor em um determinado momento. Por padrão, o RabbitMQ define um tamanho ilimitado de buffer para aplicações do cliente.

Há muitos fatores a serem considerados ao definir uma contagem de pré-busca para seus consumidores RabbitMQ. Primeiro, considere o ambiente e a configuração dos seus consumidores. Como os consumidores precisam manter todas as mensagens na memória enquanto estão sendo processadas, um alto valor de pré-busca pode ter um impacto negativo na performance de seus consumidores e, em alguns casos, pode resultar em um consumidor potencialmente travando tudo. Da mesma forma, o próprio agente RabbitMQ mantém todas as mensagens que envia armazenadas em cache na memória até receber reconhecimento do consumidor. Um valor de pré-busca alto pode fazer com que o servidor RabbitMQ fique sem memória rapidamente se a confirmação automática não estiver configurada para os consumidores e se os consumidores demorarem um tempo relativamente longo para processar mensagens.

Com as considerações acima em mente, recomendamos sempre definir um valor de pré-busca para evitar situações em que um agente RabbitMQ ou seus consumidores ficam sem memória devido a um grande número de mensagens não processadas ou não confirmadas. Se você precisar otimizar seus agentes para processar grandes volumes de mensagens, você pode testar seus agentes e consumidores usando uma gama de contagens de pré-busca para determinar o valor em que ponto a sobrecarga de rede se torna em grande parte insignificante em comparação com o tempo que um consumidor leva para processar mensagens.

Note

- Se as aplicações do seu cliente tiverem configurado para confirmar automaticamente a entrega de mensagens aos consumidores, a definição de um valor de pré-busca não terá efeito.
- Todas as mensagens pré-buscadas são removidas da fila.

O exemplo a seguir demonstra a configuração de um valor de pré-busca de 10 para um único consumidor usando a biblioteca do cliente Java RabbitMQ.

```
ConnectionFactory factory = new ConnectionFactory();

Connection connection = factory.newConnection();
Channel channel = connection.createChannel();

channel.basicQos(10, false);

QueueingConsumer consumer = new QueueingConsumer(channel);
channel.basicConsume("my_queue", false, consumer);
```

Note

Na biblioteca do cliente Java RabbitMQ, o valor padrão para `global` está definido como `false`, de modo que o exemplo acima pode ser escrito simplesmente como `channel.basicQos(10)`.

Configurar o Celery

O Python Celery envia muitas mensagens desnecessárias que podem dificultar a localização e o processamento das informações úteis. Para reduzir o ruído e facilitar o processamento, insira o comando a seguir:

```
celery -A app_name worker --without-heartbeat --without-gossip --without-mingle
```


Recuperação automática de falhas de rede

Recomendamos sempre habilitar a recuperação automática de rede para evitar tempo de inatividade significativo nos casos em que as conexões do cliente com os nós RabbitMQ falham. A biblioteca do cliente Java RabbitMQ é compatível com a recuperação automática de rede por padrão, começando com a versão 4.0.0.

A recuperação automática de conexão é acionada se uma exceção não processada for lançada no loop de E/S da conexão, se um tempo limite de operação de leitura de soquete for detectado ou se o servidor perder uma [pulsção](#).

Nos casos em que a conexão inicial entre um cliente e um nó RabbitMQ falha, a recuperação automática não será acionada. Recomendamos escrever o código da aplicação para levar em conta as falhas de conexão iniciais tentando a conexão novamente. O exemplo a seguir demonstra a repetição de falhas iniciais de rede usando a biblioteca de cliente Java RabbitMQ.

```
ConnectionFactory factory = new ConnectionFactory();
// enable automatic recovery if using RabbitMQ Java client library prior to version
4.0.0.
factory.setAutomaticRecoveryEnabled(true);
// configure various connection settings

try {
    Connection conn = factory.newConnection();
} catch (java.net.ConnectException e) {
    Thread.sleep(5000);
    // apply retry logic
}
```

Note

Se uma aplicação fecha uma conexão usando o método `Connection.Close`, a recuperação automática de rede não será ativada ou acionada.

Habilite o Classic Queue v2 para seu agente do RabbitMQ

Recomendamos ativar o Classic Queue v2 (CQv2) nas versões 3.10 e 3.11 do broker Engine para melhorias de desempenho, incluindo:

- Diminua o uso de memória
- Melhoria da entrega ao consumidor
- Aumento do throughput de workloads em que os consumidores acompanham os produtores

Todas as filas do Amazon MQ para RabbitMQ em 3.12.13 e versões posteriores são usadas por padrão. CQv2 Para fazer o upgrade para a versão mais recente do Amazon MQ para RabbitMQ, consulte. [???](#)

Migrando de para CQv1 CQv2

Para usarCQv2, você deve primeiro ativar o sinalizador de `classic_mirrored_queue_version` recurso. Para obter mais informações sobre sinalizadores de recursos, consulte [Como habilitar sinalizadores de recursos](#).

Para migrar de CQv1 paraCQv2, você deve criar uma nova política de fila ou editar uma política de fila existente com a definição da chave de `queue-version` política definida como. 2 Para obter mais informações sobre a aplicação de políticas, consulte [Aplicação de políticas ao Amazon MQ para RabbitMQ](#). Para obter mais informações sobre como habilitar CQv2 com uma política de filas, consulte [Filas clássicas na documentação](#) do RabbitMQ.

Recomendamos seguir nossas outras [práticas recomendadas de performance](#) antes de iniciar a migração.

Se você estiver usando uma política de filas, a exclusão da política de filas reduzirá as filas de volta para. CQv2 CQv1 Não recomendamos fazer o downgrade das CQv2 filas para CQv1 porque o RabbitMQ converterá a representação em disco da fila. Isso pode consumir muita memória e demorar muito para filas com alta profundidade.

Segurança no Amazon MQ

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de datacenters e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos [Programas de conformidade da AWS](#). Para saber mais sobre os programas de conformidade que se aplicam ao Amazon MQ, consulte [Serviços da AWS em escopo por programa de conformidade](#).
- Segurança da nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação te ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon MQ. Os tópicos a seguir mostram como configurar o Amazon MQ para atender aos seus objetivos de segurança e de conformidade. Saiba também como usar outros serviços da AWS que ajudam você a monitorar e proteger os recursos do Amazon MQ.

Tópicos

- [Proteção de dados no Amazon MQ](#)
- [Gerenciamento de identidade e acesso para o Amazon MQ](#)
- [Validação de conformidade para o Amazon MQ](#)
- [Resiliência no Amazon MQ](#)
- [Segurança da infraestrutura no Amazon MQ](#)
- [Práticas recomendadas de segurança para o Amazon MQ](#)

Proteção de dados no Amazon MQ

O [modelo de responsabilidade AWS compartilhada](#) de se aplica à proteção de dados no Amazon MQ. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte [Privacidade de dados FAQ](#). Para obter informações sobre proteção de dados na Europa, consulte o [Modelo de Responsabilidade AWS Compartilhada e GDPR](#) a postagem no blog AWS de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou uma API, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Amazon MQ ou outro Serviços da AWS usando o console,, API AWS CLI, ou. AWS SDKs Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de

diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Tanto para os corretores Amazon MQ para ActiveMQ quanto para Amazon MQ para corretores RabbitMQ, não use nenhuma informação de identificação pessoal () ou outras PII informações confidenciais ou sigilosas para nomes de corretores ou nomes de usuário ao criar recursos por meio do console web do agente ou do Amazon MQ. API Os nomes de corretores e nomes de usuário podem ser acessados por outros AWS serviços, incluindo CloudWatch registros. Nomes de usuário do agente não devem ser usados para dados privados ou sigilosos.

Criptografia

Os dados de usuário armazenados no Amazon MQ são criptografados em repouso. A criptografia do Amazon MQ em repouso fornece segurança aprimorada ao criptografar seus dados usando chaves de criptografia armazenadas no AWS Key Management Service (). KMS Esse serviço ajuda a reduzir a carga e a complexidade operacionais necessárias para proteger dados confidenciais. Com a criptografia de dados em repouso, você pode criar aplicativos confidenciais que atendem a requisitos de conformidade e regulamentação de criptografia.

Todas as conexões entre os agentes do Amazon MQ usam Transport layer Security (TLS) para fornecer criptografia em trânsito.

O Amazon MQ criptografa mensagens em repouso e em trânsito usando chaves de criptografia que gerencia e armazena com segurança. Para obter mais informações, consulte o [Guia do desenvolvedor do AWS Encryption SDK](#).

Criptografia em repouso

O Amazon MQ se integra com AWS Key Management Service (KMS) para oferecer criptografia transparente no lado do servidor. O Amazon MQ sempre criptografa seus dados em repouso.

Ao criar um agente Amazon MQ para ActiveMQ ou um agente Amazon MQ para RabbitMQ, você pode especificar o que AWS KMS key deseja que o Amazon MQ use para criptografar seus dados em repouso. Se você não especificar uma KMS chave, o Amazon MQ cria uma KMS chave AWS própria para você e a usa em seu nome. Atualmente, o Amazon MQ oferece suporte a chaves simétricas KMS. Para obter mais informações sobre KMS chaves, consulte [AWS KMS keys](#).

Ao criar um agente, você pode configurar o que o Amazon MQ utiliza para a sua chave de criptografia ao selecionar uma das seguintes ações.

- KMSChave de propriedade do Amazon MQ (padrão) — A chave pertence e é gerenciada pelo Amazon MQ e não está na sua conta.
- AWS KMSchave gerenciada — A KMS chave AWS gerenciada (aws/mq) é uma KMS chave em sua conta que é criada, gerenciada e usada em seu nome pelo Amazon MQ.
- Selecione a KMS chave gerenciada pelo cliente existente — As KMS chaves gerenciadas pelo cliente são criadas e gerenciadas por você em AWS Key Management Service (KMS).

Important

- A revogação de uma concessão não pode ser desfeita. Em vez disso, sugerimos excluir o agente se precisar revogar os direitos de acesso.
- Para corretores do Amazon MQ para ActiveMQ que usam o Amazon Elastic File System (EFS) para armazenar dados de mensagens, se você revogar a concessão que dá EFS permissão à Amazon para usar as KMS chaves em sua conta, isso não ocorrerá imediatamente.
- Para corretores Amazon MQ para RabbitMQ e Amazon MQ para ActiveMQ EBS que usam para armazenar dados de mensagens, se você desativar, agendar a exclusão ou revogar a concessão que dá EBS permissão à Amazon para usar KMS as chaves em sua conta, o Amazon MQ não poderá manter seu corretor e ele poderá mudar para um estado degradado.
- Se você desativou ou programou a exclusão da chave, poderá reativá-la ou cancelar a exclusão e manter o agente.
- A desativação de uma chave ou a revogação de uma concessão não ocorrerá imediatamente.

Ao criar um [único agente de instância](#) com uma KMS chave para o RabbitMQ, você verá dois CreateGrant eventos registrados. AWS CloudTrail O primeiro evento é o Amazon MQ criando uma concessão para a KMS chave. O segundo evento é EBS criar uma bolsa EBS para usar.

CreateGrant AWS CloudTrail entrada de registro: agente de instância única

mq_grant

```
{
```

```
"eventVersion": "1.08",
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AKIAIOSFODNN7EXAMPLE",
  "arn": "arn:aws:iam::111122223333:user/AmazonMqConsole",
  "accountId": "111122223333",
  "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AKIAIOSFODNN7EXAMPLE",
      "arn": "arn:aws:iam::111122223333:user/AmazonMqConsole",
      "accountId": "111122223333",
      "userName": "AmazonMqConsole"
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2023-02-23T18:59:10Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "mq.amazonaws.com"
},
"eventTime": "2018-06-28T22:23:46Z",
"eventSource": "amazonmq.amazonaws.com",
"eventName": "CreateGrant",
"awsRegion": "us-west-2",
"sourceIPAddress": "203.0.113.0",
"userAgent": "PostmanRuntime/7.1.5",
"requestParameters": {
  "granteePrincipal": "mq.amazonaws.com",
  "keyId": "arn:aws:kms:us-east-1:316438333700:key/bdbe42ae-f825-4e78-a8a1-828d411c4be2",
  "retiringPrincipal": "mq.amazonaws.com",
  "operations": [
    "CreateGrant",
    "Decrypt",
    "GenerateDataKeyWithoutPlaintext",
    "ReEncryptFrom",
    "ReEncryptTo",
    "DescribeKey"
  ]
},
"responseElements": {
```

```

    "grantId":
      "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
      "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",

      "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
      "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
      "readOnly": false,
      "resources": [
        {
          "accountId": "111122223333",
          "type": "AWS::KMS::Key",
          "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "sessionCredentialFromConsole": "true"
    }
  }

```

EBS grant creation

Você verá um evento para criação de EBS subsídios.

```

    {
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AWSService",
        "invokedBy": "mq.amazonaws.com"
      },
      "eventTime": "2023-02-23T19:09:40Z",
      "eventSource": "kms.amazonaws.com",
      "eventName": "CreateGrant",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "mq.amazonaws.com",
      "userAgent": "ExampleDesktop/1.0 (V1; OS)",
      "requestParameters": {
        "granteePrincipal": "mq.amazonaws.com",

```



```

    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "constraints": {
      "encryptionContextSubset": {
        "aws:ebs:id": "vol-0b670f00f7d5417c0"
      }
    },
    "operations": [
      "Decrypt"
    ],
    "retiringPrincipal": "ec2.us-east-1.amazonaws.com"
  },
  "responseElements": {
    "grantId":
"0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
  },
  "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventCategory": "Management"
}

```

Ao criar uma [implantação de cluster](#) com uma KMS chave para o RabbitMQ, você verá cinco CreateGrant eventos registrados. AWS CloudTrail Os dois primeiros eventos são criações de concessão para o Amazon MQ. Os próximos três eventos são subsídios criados EBS por for EBS to use.

CreateGrant AWS CloudTrail entrada de registro: implantação de cluster

mq_grant

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAIOSFODNN7EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/AmazonMqConsole",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/AmazonMqConsole",
        "accountId": "111122223333",
        "userName": "AmazonMqConsole"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-02-23T18:59:10Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "mq.amazonaws.com"
  },
  "eventTime": "2018-06-28T22:23:46Z",
  "eventSource": "amazonmq.amazonaws.com",
  "eventName": "CreateGrant",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "PostmanRuntime/7.1.5",
  "requestParameters": {
    "granteePrincipal": "mq.amazonaws.com",
    "keyId": "arn:aws:kms:us-east-1:316438333700:key/bdbe42ae-f825-4e78-a8a1-828d411c4be2",
    "retiringPrincipal": "mq.amazonaws.com",
    "operations": [
      "CreateGrant",
      "Encrypt",
      "Decrypt",

```

```

        "ReEncryptFrom",
        "ReEncryptTo",
        "GenerateDataKey",
        "GenerateDataKeyWithoutPlaintext",
        "DescribeKey"
    ]
},
"responseElements": {
    "grantId":
"0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",

    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}

```

mq_rabbit_grant

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/AmazonMqConsole",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",

```

```

    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/AmazonMqConsole",
        "accountId": "111122223333",
        "userName": "AmazonMqConsole"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-02-23T18:59:10Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "mq.amazonaws.com"
  },
  "eventTime": "2018-06-28T22:23:46Z",
  "eventSource": "amazonmq.amazonaws.com",
  "eventName": "CreateGrant",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "PostmanRuntime/7.1.5",
  "requestParameters": {
    "granteePrincipal": "mq.amazonaws.com",
    "retiringPrincipal": "mq.amazonaws.com",
    "operations": [
      "DescribeKey"
    ],
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
  },
  "responseElements": {
    "grantId":
"0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",

    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",

```

```

      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management",
  "sessionCredentialFromConsole": "true"
}

```

EBS grant creation

Você verá três eventos para criação de EBS subsídios.

```

      {
        "eventVersion": "1.08",
        "userIdentity": {
          "type": "AWSService",
          "invokedBy": "mq.amazonaws.com"
        },
        "eventTime": "2023-02-23T19:09:40Z",
        "eventSource": "kms.amazonaws.com",
        "eventName": "CreateGrant",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "mq.amazonaws.com",
        "userAgent": "ExampleDesktop/1.0 (V1; OS)",
        "requestParameters": {
          "granteePrincipal": "mq.amazonaws.com",
          "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
          "constraints": {
            "encryptionContextSubset": {
              "aws:ebs:id": "vol-0b670f00f7d5417c0"
            }
          },
          "operations": [
            "Decrypt"
          ],
          "retiringPrincipal": "ec2.us-east-1.amazonaws.com"
        },
        "responseElements": {

```

```

    "grantId":
      "0ab0ac0db000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
      "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
  }

```

Para obter mais informações sobre KMS chaves, consulte [AWS KMS keys](#) Guia do AWS Key Management Service desenvolvedor.

Criptografia em trânsito

Amazon MQ para ActiveMQ: O Amazon MQ para ActiveMQ exige uma forte Transport Layer Security (TLS) e criptografa os dados em trânsito entre os agentes da sua implantação do Amazon MQ. Todos os dados que passam entre os agentes do Amazon MQ são criptografados usando o forte Transport Layer Security (TLS). Isso se aplica a todos os protocolos disponíveis.

Amazon MQ para RabbitMQ: O Amazon MQ para RabbitMQ exige uma criptografia forte de Transport Layer Security (TLS) para todas as conexões de clientes. O tráfego de replicação do cluster do RabbitMQ transita apenas pelo seu corretor VPC e todo o tráfego de rede entre os AWS data centers é criptografado de forma transparente na camada física. Atualmente, os agentes em clusters do Amazon MQ para RabbitMQ não são compatíveis com a [criptografia entre nós](#) para replicação de clusters. Para saber mais data-in-transit, consulte [Criptografar dados em repouso e em trânsito](#).

Amazon MQ para protocolos do ActiveMQ

Você pode acessar seus corretores ActiveMQ usando os seguintes protocolos com habilitado: TLS

- [AMQP](#)
- [MQTT](#)
- MQTTterminado [WebSocket](#)
- [OpenWire](#)
- [STOMP](#)
- STOMPterminado WebSocket

Suítes de TLS criptografia compatíveis com o ActiveMQ

O ActiveMQ no Amazon MQ é compatível com os seguintes pacotes de criptografia:

- TLS_ _ ECDHE _ RSA WITH _ AES GCM _256_ _ SHA384
- TLS_ _ ECDHE _ RSA WITH _ AES CBC _256_ _ SHA384
- TLS_ _ ECDHE _ RSA WITH _ AES CBC _256_ _ SHA
- TLS_ _ DHE _ RSA WITH _ AES GCM _256_ _ SHA384
- TLS_ _ DHE _ RSA WITH _ AES CBC _256_ _ SHA256
- TLS_ _ DHE _ RSA WITH _ AES CBC _256_ _ SHA
- TLS_ _ RSA WITH _ AES GCM _256_ _ SHA384
- TLS_ _ RSA WITH _ AES CBC _256_ _ SHA256
- TLS_ _ RSA WITH _ AES CBC _256_ _ SHA
- TLS_ ECDHE _ _ RSA WITH _ AES GCM _128_ _ SHA256
- TLS_ ECDHE _ _ RSA WITH _ AES CBC _128_ _ SHA256
- TLS_ ECDHE _ _ RSA WITH _ AES CBC _128_ _ SHA
- TLS_ DHE _ _ RSA WITH _ AES GCM _128_ _ SHA256
- TLS_ DHE _ _ RSA WITH _ AES CBC _128_ _ SHA256
- TLS_ DHE _ _ RSA WITH _ AES CBC _128_ _ SHA
- TLS_ _ RSA WITH _ AES GCM _128_ _ SHA256
- TLS_ _ RSA WITH _ AES CBC _128_ _ SHA256
- TLS_ _ RSA WITH _ AES CBC _128_ _ SHA

Amazon MQ para protocolos RabbitMQ

Você pode acessar seus corretores RabbitMQ usando os seguintes protocolos com habilitado: TLS

- [AMQP\(0-9-1\)](#)

Suítes de TLS criptografia compatíveis com o RabbitMQ

O RabbitMQ no Amazon MQ é compatível com os seguintes pacotes de criptografia:

- TLS_ _ ECDHE _ RSA WITH _ AES GCM _256_ _ SHA384
- TLS_ ECDHE _ _ RSA WITH _ AES GCM _128_ _ SHA256

Gerenciamento de identidade e acesso para o Amazon MQ

AWS Identity and Access Management (IAM) é uma ferramenta Serviço da AWS que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do Amazon MQ. IAMé um Serviço da AWS que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciando acesso usando políticas](#)
- [Como o Amazon MQ funciona com IAM](#)
- [Exemplos de políticas baseadas em identidade do Amazon MQ](#)
- [Autorização e autenticação de API para o Amazon MQ](#)
- [AWS políticas gerenciadas para o Amazon MQ](#)
- [Uso de funções vinculadas ao serviço para o Amazon MQ](#)
- [Solução de problemas de identidade e acesso da Amazon MQ](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Amazon MQ.

Usuário do serviço: se você usar o serviço Amazon MQ para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que mais recursos do Amazon MQ forem usados para realizar o trabalho, talvez sejam necessárias permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não puder acessar um recurso no Amazon MQ, consulte [Solução de problemas de identidade e acesso da Amazon MQ](#).

Administrador do serviço: se você for o responsável pelos recursos do Amazon MQ em sua empresa, você provavelmente terá acesso total ao Amazon MQ. Cabe a você determinar quais funcionalidades e recursos do Amazon MQ os usuários do seu serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar IAM o Amazon MQ, consulte. [Como o Amazon MQ funciona com IAM](#)

IAM administrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Amazon MQ. Para ver exemplos de políticas baseadas em identidade do Amazon MQ que você pode usar, consulte. IAM [Exemplos de políticas baseadas em identidade do Amazon MQ](#)

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como IAM usuário ou assumindo uma IAM função. Usuário raiz da conta da AWS

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte [Como fazer login Conta da AWS no](#) Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as

solicitações. Para obter mais informações sobre como usar o método recomendado para você mesmo assinar solicitações, consulte [Assinar AWS API solicitações](#) no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação multifator](#) no Guia AWS IAM Identity Center do usuário e [Uso da autenticação multifator \(MFA\) AWS no Guia do IAMusuário](#).

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do IAM usuário.

Usuários e grupos

Um [IAMusuário](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte [Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo](#) no Guia do IAMusuário.

Um [IAMgrupo](#) é uma identidade que especifica uma coleção de IAM usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Quando criar um IAM usuário \(em vez de uma função\)](#) no Guia do IAM usuário.

IAMfunções

Uma [IAMfunção](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console [trocando de funções](#). Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte [Usando IAM funções](#) no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte [Criação de uma função para um provedor de identidade terceirizado](#) no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Manual do Usuário do AWS IAM Identity Center .
- **Permissões temporárias IAM de IAM usuário** — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- **Acesso entre contas** — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte [Acesso a recursos entre contas IAM no Guia](#) do IAM usuário.
- **Acesso entre serviços** — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
 - **Sessões de acesso direto (FAS)** — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para

fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte [Encaminhar sessões de acesso](#).

- Função de serviço — Uma função de serviço é uma [IAMfunção](#) que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamente IAM. Para obter mais informações, consulte [Criação de uma função para delegar permissões a uma Serviço da AWS](#) no Guia do IAM usuário.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte [Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon](#) no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte [Quando criar uma IAM função \(em vez de um usuário\)](#) no Guia do IAM usuário.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte [Visão geral das JSON políticas](#) no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criação de IAM políticas no Guia](#) do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte [Escolha entre políticas gerenciadas e políticas em linha no Guia](#) do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a [visão geral da lista de controle de acesso \(ACL\)](#) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- **Limites de permissões** — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAM usuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para IAM entidades](#) no Guia IAM do usuário.
- **Políticas de controle de serviço (SCPs)** — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte [Políticas de controle de serviços](#) no Guia AWS Organizations do Usuário.
- **Políticas de sessão:** são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do

usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia IAM do usuário.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte [Lógica de avaliação](#) de políticas no Guia IAM do usuário.

Como o Amazon MQ funciona com IAM

Antes de usar IAM para gerenciar o acesso ao Amazon MQ, você deve entender quais IAM recursos estão disponíveis para uso com o Amazon MQ. Para obter uma visão de alto nível de como o Amazon MQ e AWS outros serviços funcionam IAM com, [AWS consulte Serviços que funcionam IAM](#) com no Guia IAMdo usuário.

O Amazon MQ usa IAM para criar, atualizar e excluir operações, mas a autenticação nativa do ActiveMQ para corretores. Para obter mais informações, consulte [Integração de agentes ActiveMQ com LDAP](#).

Tópicos

- [Políticas baseadas em identidade do Amazon MQ](#)
- [Políticas baseadas em recursos do Amazon MQ](#)
- [Autorização baseada em etiquetas do Amazon MQ](#)
- [Funções do Amazon MQ IAM](#)

Políticas baseadas em identidade do Amazon MQ

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. O Amazon MQ é compatível com ações, chaves de condição e recursos específicos. Para saber mais sobre todos os elementos que você usa em uma JSON política, consulte [Referência IAM JSON de elementos de política](#) no Guia do IAM usuário.

Ações

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente com permissão que não têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de política no Amazon MQ usam o seguinte prefixo antes da ação: `mq:`. Por exemplo, para conceder permissão a alguém para executar uma instância do Amazon MQ com a operação do Amazon `CreateBroker` API MQ, você inclui `mq:CreateBroker` a ação na política dessa pessoa. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Amazon MQ define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

```
"Action": [  
    "mq:action1",  
    "mq:action2"
```

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

```
"Action": "mq:Describe*"
```

Para ver uma lista de ações do Amazon MQ, consulte [Ações definidas pelo Amazon MQ](#) no IAM Guia do usuário.

Recursos

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada,

especifique um recurso usando seu [Amazon Resource Name \(ARN\)](#). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

No Amazon MQ, os principais AWS recursos são um agente de mensagens do Amazon MQ e sua configuração. Cada agente e configuração do Amazon MQ tem Amazon Resource Names (ARNs) exclusivos associados a eles, conforme mostrado na tabela a seguir.

Tipos de recursos	ARN	Chaves de condição
brokers	arn:aws:mq:us-east-1:123456789012:broker:\${brokerName}:\${brokerId}	aws:ResourceTag/\${TagKey}
configurations	arn:\${Partition}:mq:\${Region}:\${Account}:configuration:\${configuration-id}	aws:ResourceTag/\${TagKey}

Para obter mais informações sobre o formato de ARNs, consulte [Amazon Resource Names \(ARNs\) e AWS Service Namespaces](#).

Por exemplo, para especificar o corretor nomeado MyBroker com brokerId b-1234a5b6-78cd-901e-2fgh-3i45j6k17819 em sua declaração, use o seguinte ARN:

```
"Resource": "arn:aws:mq:us-east-1:123456789012:broker:MyBroker:b-1234a5b6-78cd-901e-2fgh-3i45j6k17819"
```

Para especificar todos os agentes e configurações que pertencem a uma conta específica, use o caractere curinga (*):

```
"Resource": "arn:aws:mq:us-east-1:123456789012:*"
```

Algumas ações do Amazon MQ, como as de criação de recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

```
"Resource": "*" 
```

A API ação `CreateTags` requer um intermediário e uma configuração. Para especificar vários recursos em uma única instrução, separe-os ARNs com vírgulas.

```
"Resource": [
  "resource1",
  "resource2" ]
```

Para ver uma lista dos tipos de recursos do Amazon MQ e seus ARNs, consulte [Recursos definidos pelo Amazon MQ](#) no IAM Guia do usuário. Para saber com quais ações você pode especificar cada recurso, consulte [Ações definidas pelo Amazon MQ](#). ARN

Chaves de condição

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma OR operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte [elementos de IAM política: variáveis e tags](#) no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia IAM do usuário.

O Amazon MQ não define nenhuma chave de condição específica ao serviço, mas é compatível com o uso de algumas chaves de condição globais. Para ver uma lista das chaves de condição do Amazon MQ, consulte a tabela abaixo ou [as chaves de condição do Amazon MQ](#) no IAM Guia do usuário. Para saber com quais ações e recursos você pode usar a chave de condição, consulte [Ações definidas pelo Amazon MQ](#).

Chaves de condição	Descrição	Tipo
foi: RequestTag / \$ { } TagKey	Filtra ações com base nas tags transmitidas na solicitação.	String
foi: ResourceTag /\$ { } TagKey	Filtra as ações com base nas tags associadas ao recurso.	String
leis: TagKeys	Filtra ações com base nas chaves de tag transmitidas na solicitação.	String

Exemplos

Para visualizar exemplos de políticas baseadas em identidade do Amazon MQ, consulte [Exemplos de políticas baseadas em identidade do Amazon MQ](#).

Políticas baseadas em recursos do Amazon MQ

Atualmente, o Amazon MQ não oferece suporte à IAM autenticação usando permissões ou políticas baseadas em recursos.

Autorização baseada em etiquetas do Amazon MQ

É possível anexar etiquetas aos recursos do Amazon MQ ou informar etiquetas em uma solicitação para o Amazon MQ. Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `mq:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

O Amazon MQ é compatível com políticas baseadas em etiquetas. Por exemplo, você pode negar acesso a todos os recursos do Amazon MQ que incluem uma etiqueta com a chave `environment` e o valor `production`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "mq:DeleteBroker",
        "mq:RebootBroker",
        "mq>DeleteTags"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/environment": "production"
        }
      }
    }
  ]
}
```

Esta política vai Deny a capacidade de excluir ou reiniciar um agente do Amazon MQ que inclui a etiqueta `environment/production`.

Para obter mais informações sobre marcação, consulte:

- [Adicionar tags aos recursos do Amazon MQ](#)
- [Controlando o acesso usando IAM tags](#)

Funções do Amazon MQ IAM

Uma [IAMfunção](#) é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usar credenciais temporárias com o Amazon MQ

Você pode usar credenciais temporárias para entrar com a federação, assumir uma IAM função ou assumir uma função entre contas. Você obtém credenciais de segurança temporárias ligando para AWS STS API operações como [AssumeRole](#) ou [GetFederationToken](#).

A Amazon MQ é compatível com o uso de credenciais temporárias.

Perfis de serviço

Esse atributo permite que um serviço assuma um [perfil de serviço](#) em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. As funções de serviço aparecem na sua IAM conta e são de propriedade da conta. Isso significa que um IAM administrador pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

O Amazon MQ é compatível com as funções de serviço.

Exemplos de políticas baseadas em identidade do Amazon MQ

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Amazon MQ. Eles também não podem executar tarefas usando o AWS Management Console, a AWS CLI ou uma API da AWS. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte [Criar políticas na guia JSON](#) no Manual do usuário do IAM.

Tópicos

- [Práticas recomendadas de políticas](#)
- [Usar o console do Amazon MQ](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Amazon MQ em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para

obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um Serviço da AWS específico, como o AWS CloudFormation. Para obter mais informações, consulte [Elementos de política JSON do IAM: Condition](#) no Manual do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do usuário do IAM.
- Require multi-factor authentication (MFA) (Exigir autenticação multifator (MFA)): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

Usar o console do Amazon MQ

Para acessar o console da Amazon MQ, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir listar e visualizar detalhes sobre os recursos do Amazon MQ em sua conta AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou funções do IAM) com essa política.

Para garantir que essas entidades ainda possam usar o console do Amazon MQ, anexe também a seguinte política gerenciada AWS às entidades. Para obter mais informações, consulte [Adição de permissões a um usuário](#) no Manual do usuário do IAM:

```
AmazonMQReadOnlyAccess
```

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",

```

```
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

Autorização e autenticação de API para o Amazon MQ

O Amazon MQ usa a assinatura de solicitações padrão AWS para autenticação da API. Para obter mais informações, consulte [Assinatura de solicitações da AWSAPI da](#) no Referência geral da AWS.

Note

Atualmente, o Amazon MQ não é compatível com a autenticação IAM que usam permissões baseadas em recursos ou políticas baseadas em recursos.

Para autorizar os usuários AWS a trabalhar com agentes, configurações e usuários, você deve editar as permissões da política do IAM.

Tópicos

- [Permissões de IAM necessárias para criar um agente Amazon MQ](#)
- [Referência de permissões da API REST do Amazon MQ](#)
- [Permissões no nível do recurso suportadas para ações de API do Amazon MQ](#)

Permissões de IAM necessárias para criar um agente Amazon MQ

Para criar um agente, você deve usar a política do IAM `AmazonMQFullAccess` ou incluir as permissões do EC2 a seguir em sua política do IAM.

A seguinte política personalizada é composta de duas declarações (uma condicional) que concedem permissões para manipular os recursos que o Amazon MQ exige para criar um agente do ActiveMQ.

Important

- A ação `ec2:CreateNetworkInterface` é necessária para permitir que o Amazon MQ crie uma interface de rede elástica (ENI) em sua conta em seu nome.

- A ação do `ec2:CreateNetworkInterfacePermission` autoriza o Amazon MQ a anexar a ENI para um agente do ActiveMQ.
- A chave de condição `ec2:AuthorizedService` garante que as permissões de ENI possam ser concedidas apenas para contas de serviço do Amazon MQ.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "mq:*",
      "ec2:CreateNetworkInterface",
      "ec2>DeleteNetworkInterface",
      "ec2:DetachNetworkInterface",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }, {
    "Action": [
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:DescribeNetworkInterfacePermissions"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ec2:AuthorizedService": "mq.amazonaws.com"
      }
    }
  }
]}
```

Para obter mais informações, consulte [Etapa 2: criar um usuário e obter suas AWS credenciais e Nunca modifique ou exclua a interface de rede elástica do Amazon MQ.](#)

Referência de permissões da API REST do Amazon MQ

A tabela a seguir relaciona as APIs REST do Amazon MQ e as permissões correspondentes do IAM.

APIs REST e permissões necessárias do Amazon MQ

APIs REST do Amazon MQ	Permissões obrigatórias
CreateBroker	mq:CreateBroker
CreateConfiguration	mq:CreateConfiguration
CreateTags	mq:CreateTags
CreateUser	mq:CreateUser
DeleteBroker	mq>DeleteBroker
DeleteUser	mq>DeleteUser
DescribeBroker	mq:DescribeBroker
DescribeConfiguration	mq:DescribeConfiguration
DescribeConfigurationRevision	mq:DescribeConfigurationRevision
DescribeUser	mq:DescribeUser
ListBrokers	mq:ListBrokers
ListConfigurationRevisions	mq:ListConfigurationRevisions
ListConfigurations	mq:ListConfigurations
ListTags	mq:ListTags
ListUsers	mq:ListUsers
RebootBroker	mq:RebootBroker
UpdateBroker	mq:UpdateBroker
UpdateConfiguration	mq:UpdateConfiguration

APIs REST do Amazon MQ	Permissões obrigatórias
UpdateUser	mq:UpdateUser

Permissões no nível do recurso suportadas para ações de API do Amazon MQ

O termo permissões no nível do recurso se refere à capacidade de especificar em quais recursos os usuários têm permissão para realizar ações. O Amazon MQ é compatível parcialmente com as permissões no nível do recurso. Para determinadas ações do Amazon MQ, você pode controlar quando os usuários têm permissão para usar essas ações com base em condições que precisam ser concluídas, ou em recursos específicos que os usuários têm permissão para usar.

A tabela a seguir descreve as ações de API do Amazon MQ que são compatíveis no momento com as permissões no nível do recurso, bem como os recursos compatíveis, os ARNs de recurso e as chaves de condição para cada ação.

Important

Caso uma ação de API do Amazon MQ não esteja listada nessa tabela, isso significa que ela não é compatível com as permissões no nível do recurso. Se uma ação da API do Amazon MQ não for compatível com as permissões em nível de recurso, você poderá conceder aos usuários permissão para usar a ação, mas precisará especificar um curinga * para o elemento do recurso da declaração de política.

Ação API	Tipos de recursos (*necessários)
CreateConfiguration	configurações*
CreateTags	agentes , configurações
CreateUser	operadores*
DeleteBroker	operadores*
DeleteUser	operadores*
DescribeBroker	operadores*

Ação API	Tipos de recursos (*necessários)
DescribeConfiguration	configurações*
DescribeConfigurationRevision	configurações*
DescribeUser	operadores*
ListConfigurationRevisions	configurações*
ListConfigurationRevisions	configurações*
ListTags	agentes , configurações
ListUsers	operadores*
RebootBroker	operadores*
UpdateBroker	operadores*
UpdateConfiguration	configurações*
UpdateUser	operadores*

AWS políticas gerenciadas para o Amazon MQ

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo [políticas gerenciadas pelo cliente da](#) específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades

principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova Serviço da AWS é lançada ou novas API operações são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte [políticas AWS gerenciadas](#) no Guia IAM do usuário.

AWS política gerenciada: A mazonMQService RolePolicy

Você não pode se vincular `AmazonMQServiceRolePolicy` às suas IAM entidades. Essa política é anexada a uma função vinculada ao serviço que permite que o Amazon MQ realize ações em seu nome. Para obter mais informações sobre essa política de permissão e as ações que ela permite que o Amazon MQ execute, consulte [the section called “Permissões de função vinculada ao serviço para o Amazon MQ”](#).

Atualizações do Amazon MQ para AWS políticas gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Amazon MQ desde que esse serviço começou a monitorar essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o RSS feed na página de [histórico de documentos](#) do Amazon MQ.

Alteração	Descrição	Data
O Amazon MQ passou a monitorar as alterações	O Amazon MQ começou a monitorar as alterações em suas políticas AWS gerenciadas.	5 de maio de 2021

Uso de funções vinculadas ao serviço para o Amazon MQ

O Amazon MQ usa [funções vinculadas ao serviço](#) do AWS Identity and Access Management IAM. A função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao Amazon MQ. As funções vinculadas a serviços são predefinidas pelo Amazon MQ e incluem todas as permissões que o serviço requer para chamar outros produtos da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do Amazon MQ porque você não precisa adicionar as permissões necessárias manualmente. O Amazon MQ define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Amazon MQ pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus recursos do Amazon MQ, pois você não pode remover por engano as permissões para acessar os recursos.

Para mais informações sobre outros serviços que são compatíveis com funções vinculadas a serviços, consulte [Serviços da AWS que funcionam com o IAM](#) e procure por serviços que contêm Sim na coluna Função vinculada ao serviço. Escolha um Sim com um link para exibir a documentação da função vinculada a serviço desse serviço.

Permissões de função vinculada ao serviço para o Amazon MQ

O Amazon MQ usa a função vinculada ao serviço chamada `AWSServiceRoleForAmazonMQ` — O Amazon MQ usa essa função vinculada ao serviço para chamar os serviços AWS em seu nome.

A função vinculada ao serviço `AWSServiceRoleForAmazonMQ` confia nos seguintes serviços para assumir a função:

- `mq.amazonaws.com`

O Amazon MQ usa a política de permissão [AmazonMQServiceRolePolicy](#), que é anexada à função vinculada ao serviço `AWSServiceRoleForAmazonMQ`, para concluir as seguintes ações nos recursos especificados:

- Ação: `ec2:CreateVpcEndpoint` no recurso `vpc`.
- Ação: `ec2:CreateVpcEndpoint` no recurso `subnet`.
- Ação: `ec2:CreateVpcEndpoint` no recurso `security-group`.
- Ação: `ec2:CreateVpcEndpoint` no recurso `vpc-endpoint`.
- Ação: `ec2:DescribeVpcEndpoints` no recurso `vpc`.
- Ação: `ec2:DescribeVpcEndpoints` no recurso `subnet`.

- Ação: `ec2:CreateTags` no recurso `vpc-endpoint`.
- Ação: `logs:PutLogEvents` no recurso `log-group`.
- Ação: `logs:DescribeLogStreams` no recurso `log-group`.
- Ação: `logs:DescribeLogGroups` no recurso `log-group`.
- Ação: `CreateLogStream` no recurso `log-group`.
- Ação: `CreateLogGroup` no recurso `log-group`.

Quando você cria um Amazon MQ para agente RabbitMQ, a política de permissão `AmazonMQServiceRolePolicy` do Amazon MQ realize as seguintes tarefas em seu nome.

- Cria um endpoint da Amazon VPC para o agente usando o Amazon VPC, a sub-rede e o grupo de segurança que você fornece. Você pode usar o endpoint criado para que seu agente se conecte ao agente por meio do console de gerenciamento RabbitMQ, da API de gerenciamento ou de forma programática.
- Crie grupos de logs e publique logs do agente no Amazon CloudWatch Logs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource": [
```

```

        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateVpcEndpoint"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/AMQManaged": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateVpcEndpoint"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2>DeleteVpcEndpoints"
    ],
    "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition": {
        "StringEquals": {
            "ec2:ResourceTag/AMQManaged": "true"
        }
    }
},
{

```



```
    "Effect": "Allow",
    "Action": [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
    ]
}
]
```

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte [Permissões de função vinculada ao serviço](#) no Guia do usuário do IAM.

Criação de uma função vinculada ao serviço para Amazon MQ

Você não precisa criar manualmente uma função vinculada a serviço. Ao criar um agente da pela primeira vez, o Amazon MQ cria uma função vinculada ao serviço para chamar o AWS em seu nome. Todos os agentes subsequentes que você criar usarão a mesma função e nenhuma nova função será criada.

Important

Essa função vinculada ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os recursos compatíveis com essa função. Para saber mais, consulte [Uma nova função apareceu na minha conta do IAM](#).

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta.

Você também pode usar o console do IAM para criar uma função vinculada ao serviço com o caso de uso do Amazon MQ. Na AWS CLI ou na API do AWS, crie uma função vinculada ao serviço com o nome de serviço `mq.amazonaws.com`. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Manual do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Edição de uma função vinculada ao serviço do Amazon MQ

O Amazon MQ não permite que você edite a função vinculada ao serviço `AWSServiceRoleForAmazonMQ`. No entanto, você poderá editar a descrição da função usando o IAM. Para obter mais informações, consulte [Editar uma função vinculada a serviço](#) no Guia do usuário do IAM.

Exclusão de uma função vinculada ao serviço do Amazon MQ

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

Note

Se o serviço do Amazon MQ estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos do Amazon MQ usados por `AWSServiceRoleForAmazonMQ`

- Exclua seus agentes do Amazon MQ usando o AWS Management Console, Amazon MQ CLI ou Amazon MQ API. Para obter mais informações sobre como excluir um agente, consulte [???](#).

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, AWS CLI ou a API AWS para excluir a função vinculada a serviço `AWSServiceRoleForAmazonMQ`. Para obter mais informações, consulte [Excluir uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Regiões compatíveis com as funções vinculadas a serviços do Amazon MQ

O Amazon MQ é compatível com as funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte [Regiões e endpoints do AWS](#).

Nome da região	Identidade da região	Compatível com o Amazon MQ
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Sim
US West (N. Califórnia)	us-west-1	Sim
Oeste dos EUA (Oregon)	us-west-2	Sim
Asia Pacific (Mumbai)	ap-south-1	Sim
Asia Pacific (Osaka)	ap-northeast-3	Sim
Ásia-Pacífico (Seul)	ap-northeast-2	Sim
Ásia-Pacífico (Singapura)	ap-southeast-1	Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	Sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	Sim
Canada (Central)	ca-central-1	Sim
Europa (Frankfurt)	eu-central-1	Sim
Europa (Irlanda)	eu-west-1	Sim
Europe (London)	eu-west-2	Sim
Europe (Paris)	eu-west-3	Sim
América do Sul (São Paulo)	sa-east-1	Sim
AWS GovCloud (US)	us-gov-west-1	Não

Solução de problemas de identidade e acesso da Amazon MQ

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Amazon MQ e IAM

Tópicos

- [Não tenho autorização para executar uma ação na Amazon MQ](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Amazon MQ](#)

Não tenho autorização para executar uma ação na Amazon MQ

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o mateojackson usuário tenta usar o console para ver detalhes sobre um *widget* mas não tem mq: *GetWidget* permissões.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
mq: GetWidget on resource: my-example-widget
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso *my-example-widget* usando a ação mq: *GetWidget*.

Não estou autorizado a realizar iam: PassRole

Se receber uma mensagem de erro informando que você não tem autorização para executar a ação iam:PassRole, suas políticas devem ser atualizadas para permitir a transmissão de um perfil ao Amazon MQ.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um IAM usuário chamado marymajor tenta usar o console para realizar uma ação no Amazon MQ. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Amazon MQ

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon MQ é compatível com esses recursos, consulte [Como o Amazon MQ funciona com IAM](#).
- Para saber como fornecer acesso aos seus recursos em todas as Contas da AWS que você possui, consulte [Fornecer acesso a um IAM usuário em outra Conta da AWS de sua propriedade](#) no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte [Fornecer Contas da AWS acesso a terceiros](#) no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte [Fornecendo acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do IAM usuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a [recursos entre contas IAM no Guia](#) do IAM usuário.

Validação de conformidade para o Amazon MQ


Audidores terceirizados avaliam a segurança e a conformidade do Amazon MQ como parte de AWS vários programas de conformidade. Isso inclui SOC, PCIHIPAA, e outros.

Para saber se um Serviço da AWS está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#).

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Guias de início rápido sobre segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- [Arquitetura para HIPAA segurança e conformidade na Amazon Web Services](#) — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos qualificados.

 Note

Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a [Referência de serviços HIPAA elegíveis](#).

- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização ()). ISO
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#) — Isso Serviço da AWS fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso Serviço da AWS detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de

conformidade, por exemplo PCIDSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- [AWS Audit Manager](#)— Isso Serviço da AWS ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no Amazon MQ

A infraestrutura global da AWS é criada com base em Regiões e Zonas de Disponibilidade AWS da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas a redes altamente redundantes com baixa latência e altas taxas de transferência. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte [Infraestrutura global da AWS](#).

Segurança da infraestrutura no Amazon MQ

Como serviço gerenciado, é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte [AWS Cloud Security](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção](#) de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa API chamadas AWS publicadas para acessar pela rede. Os clientes devem oferecer suporte para:

- Segurança da camada de transporte (TLS). Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Suítes de criptografia com sigilo direto perfeito (), como (Ephemeral PFS Diffie-Hellman) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Práticas recomendadas de segurança para o Amazon MQ

Os padrões de design a seguir podem melhorar a segurança de seu agente do Amazon MQ.

Tópicos

- [Preferir agentes sem acessibilidade pública](#)
- [Sempre configurar um mapa de autorização](#)
- [Bloquear protocolos desnecessários com os grupos de segurança da VPC](#)

Para obter mais informações sobre como o Amazon MQ criptografa seus dados, bem como uma lista de protocolos compatíveis, consulte [Proteção de dados](#).

Preferir agentes sem acessibilidade pública

Agentes criados sem acessibilidade pública não podem ser acessados de fora de sua [VPC](#). Isso reduz significativamente a vulnerabilidade do agente a ataques do tipo Distributed Denial of Service (DDoS) da Internet pública. Para obter mais informações, consulte [Acessando o console web do Amazon MQ broker sem acessibilidade pública](#) neste guia e [Como se preparar para ataques DDoS reduzindo sua superfície de ataque](#) no Blog de Segurança da AWS.

Sempre configurar um mapa de autorização

Como o ActiveMQ não tem um mapa de autorização configurado por padrão, qualquer usuário autenticado pode executar qualquer ação no agente. Portanto, uma prática recomendada é restringir as permissões por grupo. Para obter mais informações, consulte [authorizationEntry](#).

Important

Se você especificar um mapa de autorização que não inclua o `activemq-webconsole`, você não poderá usar o Console da Web do ActiveMQ porque o grupo não estará autorizado a enviar mensagens ou receber mensagens do agente do Amazon MQ.

Bloquear protocolos desnecessários com os grupos de segurança da VPC

Para melhorar a segurança, você deve restringir as conexões de portas e protocolos desnecessários configurando adequadamente o grupo de segurança do Amazon VPC. Por exemplo, para restringir o acesso à maioria dos protocolos enquanto concede acesso ao OpenWire e ao console da Web, você poderia conceder acesso somente às portas 61617 e 8162. Isso limita sua exposição, bloqueando protocolos que não estão sendo usados, ao mesmo tempo em que permite que o OpenWire e o console da Web funcionem normalmente.

Permita somente as portas de protocolos que estão sendo usados.

- AMQP: 5671
- MQTT: 8883
- OpenWire: 61617
- STOMP: 61614
- WebSocket: 61619

Para obter mais informações, consulte:

- [Definir configurações adicionais do agente Amazon MQ](#)
- [Grupos de segurança para sua VPC](#)
- [Security group padrão para sua VPC](#)
- [Como trabalhar com security groups](#)

Monitoramento e registro em agentes do Amazon MQ

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de suas AWS soluções. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha multiponto, caso ocorra. AWS fornece várias ferramentas para monitorar seus recursos do Amazon MQ e responder a possíveis incidentes:

Você pode usar CloudWatch para visualizar e analisar métricas para seu corretor Amazon MQ. Você pode visualizar e analisar as métricas do seu corretor no CloudWatch console AWS CLI, no ou no CloudWatch AWS CLI. CloudWatch as métricas do Amazon MQ são automaticamente pesquisadas pela corretora e, em seguida, enviadas para CloudWatch cada minuto. Para corretores ActiveMQ CloudWatch, monitora somente os primeiros 1000 destinos. Para os corretores RabbitMQ, CloudWatch monitora apenas os primeiros 500 destinos, ordenados por número de consumidores.

Para obter uma lista completa das métricas do Amazon MQ, consulte [CloudWatch Métricas disponíveis Amazon MQ para corretores ActiveMQ](#).

Para obter informações sobre como criar um CloudWatch alarme para uma métrica, consulte [Criar ou editar um CloudWatch alarme](#) no Guia CloudWatch do usuário da Amazon.

Acessando CloudWatch métricas para o Amazon MQ

Você pode acessar CloudWatch as métricas usando o AWS Management Console AWS CLI, API e.

Talvez você queira acessar CloudWatch as métricas sem usar AWS Management Console o.

Para acessar as métricas do Amazon MQ usando o AWS CLI, use o [get-metric-statistics](#) comando. Para obter mais informações, consulte [Obter estatísticas de uma métrica](#) no Guia CloudWatch do usuário da Amazon.

Para acessar as métricas do Amazon MQ usando o CloudWatch API, use a [GetMetricStatistics](#) ação. Para obter mais informações, consulte [Obter estatísticas de uma métrica](#) no Guia CloudWatch do usuário da Amazon.

Acessando CloudWatch métricas usando o AWS Management Console

O exemplo a seguir mostra como acessar CloudWatch as métricas do Amazon MQ usando AWS Management Console. Se você já estiver conectado ao console do Amazon MQ, na página de detalhes do agente, escolha Ações, Visualizar métricas. CloudWatch

1. Faça login no [CloudWatchconsole](#).
2. No painel de navegação, selecione Métricas.
3. Selecione o namespace de métrica do AmazonMQ.
4. Selecione uma das seguintes dimensões de métricas:
 - Broker Metrics (Métricas do agente)
 - Métricas de fila por operador
 - Métricas de tópico por operador

Neste exemplo, está selecionado Broker Metrics (Métricas do operador).

5. Agora você pode examinar as métricas do Amazon MQ:
 - Para classificar a métrica, use o cabeçalho da coluna.
 - Para criar o gráfico de uma métrica, marque a caixa de seleção ao lado da métrica.
 - Para filtrar por métrica, selecione o nome da métrica e, em seguida, escolha Adicionar à pesquisa.

CloudWatch Métricas disponíveis Amazon MQ para corretores ActiveMQ

Métricas do Amazon MQ para ActiveMQ

Métrica	Unidade	Descrição
AmqpMaximumConnections	Contagem	O número máximo de clientes que você pode conectar à sua corretora usando AMQP. Para

Métrica	Unidade	Descrição
		obter mais informações sobre cotas de conexão, consulte Quotas in Amazon MQ .
BurstBalance	Percentual	A porcentagem de créditos intermitentes restantes no EBS volume da Amazon usado para manter os dados de mensagens de corretores com produtividade otimizada. Se esse saldo chegar a zero, o EBS volume IOPS fornecido pela Amazon diminuirá até que o Burst Balance seja reabastecido. Para obter mais informações sobre como os Burst Balances funcionam na AmazonEBS, consulte: Créditos de E/S e Burst Performance .

Métrica	Unidade	Descrição
CpuCreditBalance	Créditos (v CPU -minutos)	<p>⚠ Important</p> <p>Essa métrica está disponível somente para os tipos de instância de agente <code>mq.t2.micro</code>. CPUs métricas de crédito estão disponíveis somente em intervalos de cinco minutos.</p> <p>O número de CPU créditos ganhos que uma instância acumulou desde que foi lançada ou iniciada (incluindo o número de créditos de lançamento). O saldo de crédito está disponível para a instância da corretora gastar em aumentos além da utilização básica CPU.</p> <p>Os créditos são acumulados no saldo de créditos após terem sido ganhos e são removidos do saldo de créditos após serem gastos. O saldo de créditos tem um limite máximo. Depois que o limite é atingido, todos os créditos ganhos mais</p>


Métrica	Unidade	Descrição
		recentemente são descartados.
CpuUtilization	Percentual	A porcentagem de unidades de EC2 computação alocadas da Amazon que o corretor usa atualmente.
CurrentConnectionsCount	Contagem	O número atual de conexões ativas no agente atual.
EstablishedConnectionsCount	Contagem	O número total de conexões, ativas e inativas, que foram estabelecidas com o operador.
HeapUsage	Percentual	A porcentagem do limite de memória do JVM ActiveMQ que o broker usa atualmente.
InactiveDurableTopicSubscribersCount	Contagem	O número de inscritos inativos no tópico durável, até um máximo de 2000.
JobSchedulerStorePercentUsage	Percentual	A porcentagem de espaço em disco usada pelo armazenamento do agendador de tarefas.
JournalFilesForFastRecovery	Contagem	O número de arquivos de diário que serão reproduzidos novamente após um desligamento normal.
JournalFilesForFullRecovery	Contagem	O número de arquivos de diário que serão reproduzidos novamente após um desligamento inesperado.

Métrica	Unidade	Descrição
MqttMaximumConnections	Contagem	O número máximo de clientes que você pode conectar à sua corretora usando MQTT. Para obter mais informações sobre cotas de conexão, consulte Quotas in Amazon MQ .
NetworkConnectorConnectionCount	Contagem	O número de nós conectados ao corretor em uma rede de corretores usando NetworkConnector.
NetworkIn	Bytes	O volume de tráfego de entrada para o operador.
NetworkOut	Bytes	O volume de tráfego de saída para o operador.
OpenTransactionCount	Contagem	O número total de transações em andamento.
OpenwireMaximumConnections	Contagem	O número máximo de clientes que você pode conectar à sua corretora usando OpenWire. Para obter mais informações sobre cotas de conexão, consulte Quotas in Amazon MQ .
StompMaximumConnections	Contagem	O número máximo de clientes que você pode conectar à sua corretora usando STOMP. Para obter mais informações sobre cotas de conexão, consulte Quotas in Amazon MQ .

Métrica	Unidade	Descrição
StorePercentUsage	Percentual	A porcentagem usada pelo limite de armazenamento. Se ela chegar a 100, o agente recusará mensagens.
TempPercentUsage	Percentual	A porcentagem de armazenamento temporário o disponível usada por mensagens não persistentes.
TotalConsumerCount	Contagem	O número de consumidores de mensagens inscritos em destinos no agente atual.
TotalMessageCount	Contagem	O número de mensagens armazenadas no operador.
TotalProducerCount	Contagem	O número de produtores de mensagens ativos em destinos no agente atual.
VolumeReadOps	Contagem	O número de operações de leitura realizadas no EBS volume da Amazon.
VolumeWriteOps	Contagem	O número de operações de gravação realizadas no EBS volume da Amazon.
WsMaximumConnections	Contagem	O número máximo de clientes que você pode conectar à sua corretora usando WebSocket . Para obter mais informações sobre cotas de conexão, consulte Quotas in Amazon MQ .

Dimensões para métricas do agente ActiveMQ

Dimensão	Descrição
Broker	O nome do agente

 **Note**

Um agente de instância única tem o sufixo -1. Um agente ativo/em espera para alta disponibilidade tem os sufixos -1 e -2 para seu par redundante.

Métricas de destino do ActiveMQ (fila e tópico)

Important

As métricas a seguir incluem contagens por minuto para o período da CloudWatch pesquisa.

- EnqueueCount
- ExpiredCount
- DequeueCount
- DispatchCount
- InFlightCount

Por exemplo, em um [CloudWatch período](#) de cinco minutos, EnqueueCount tem cinco valores de contagem, cada um para uma parte de um minuto do período. As estatísticas Minimum e Maximum fornecem o valor mais baixo e mais alto por minuto durante o período especificado.

Métrica	Unidade	Descrição
ConsumerCount	Contagem	O número de consumidores que se inscreveram para o destino.
EnqueueCount	Contagem	O número de mensagens enviadas ao destino por minuto.
EnqueueTime	Tempo (milissegundos)	A end-to-end latência desde o momento em que uma mensagem chega a uma corretora até ser entregue ao consumidor. <div data-bbox="1068 871 1510 1862"><p>Note</p><p>EnqueueTime não mede a end-to-end latência desde o momento em que uma mensagem é enviada por um produtor até chegar ao corretor, nem a latência de quando uma mensagem é recebida por um corretor até ser confirmada pelo corretor. Em vez disso, EnqueueTime é o número de milissegundos a partir do momento em que uma mensagem é recebida pelo agente</p></div>

Métrica	Unidade	Descrição
		até ser entregue com sucesso a um consumidor.
ExpiredCount	Contagem	O número de mensagens que não puderam ser entregues porque expiraram, por minuto.
DispatchCount	Contagem	O número de mensagens enviadas a consumidores por minuto.
DequeueCount	Contagem	O número de mensagens confirmadas por consumidores por minuto.
InFlightCount	Contagem	O número de mensagens enviadas para os consumidores que não foram reconhecidos.
ReceiveCount	Contagem	O número de mensagens que foram recebidas do agente remoto por um conector de rede duplex.
MemoryUsage	Percentual	A porcentagem do limite de memória que o destino usa atualmente.
ProducerCount	Contagem	O número de produtores para o destino.

Métrica	Unidade	Descrição
QueueSize	Contagem	O número de mensagens na fila. <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; background-color: #fff0f0;">⚠ Important Esta métrica aplica-se apenas às filas.</div>
TotalEnqueueCount	Contagem	O número total de mensagens que foram enviadas para o agente.
TotalDequeueCount	Contagem	O número total de mensagens que foram consumidas pelos clientes.

Note

As métricas `TotalEnqueueCount` e `TotalDequeueCount` incluem mensagens para tópicos de aviso. Para obter mais informações sobre mensagens de tópico de aviso, consulte a [documentação do ActiveMQ](#).

Dimensões para métricas de destino do ActiveMQ (fila e tópico)


Dimensão	Descrição
Broker	O nome do operador. <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; background-color: #e6f2ff;">Note Um agente de instância única tem o sufixo <code>-1</code>. Um agente ativo/em espera</div>

Dimensão	Descrição
	para alta disponibilidade tem os sufixos -1 e -2 para seu par redundante.
Topic ou Queue	O nome do tópico ou da fila.
NetworkConnector	O nome do conector de rede.

CloudWatch Métricas disponíveis para Amazon MQ para corretores RabbitMQ

Métricas do agente RabbitMQ

Métrica	Unidade	Descrição
ExchangeCount	Contagem	O número total de trocas configuradas com o agente.
QueueCount	Contagem	O número total de filas configuradas com o agente.
ConnectionCount	Contagem	O número total de conexões estabelecidas com o agente.
ChannelCount	Contagem	O número total de canais estabelecidas com o agente.
ConsumerCount	Contagem	O número total de consumidores conectados com o agente.
MessageCount	Contagem	O número de mensagens nas filas.

Métrica	Unidade	Descrição
		<p> Note</p> <p>O número produzido é a soma total de mensagens prontas e não reconhecidas no agente.</p>
MessageReadyCount	Contagem	O número total de mensagens prontas nas filas.
MessageUnacknowledgedCount	Contagem	O número total de mensagens não reconhecidas nas filas.
PublishRate	Contagem	<p>A taxa na qual as mensagens são publicadas para o agente.</p> <p>O número produzido representa o número de mensagens por segundo no momento da amostragem.</p>
ConfirmRate	Contagem	<p>A taxa com a qual o servidor RabbitMQ está confirmando mensagens publicadas. Você pode comparar essa métrica com PublishRate para entender melhor a performance do seu agente.</p> <p>O número produzido representa o número de mensagens por segundo no momento da amostragem.</p>

Métrica	Unidade	Descrição
AckRate	Contagem	<p>A taxa em que as mensagens estão sendo reconhecidas pelos consumidores.</p> <p>O número produzido represent a o número de mensagens por segundo no momento da amostragem.</p>
SystemCpuUtilization	Percentual	A porcentagem de unidades de EC2 computação alocadas da Amazon que o corretor usa atualmente. Para implantações de cluster, esse valor representa o agregado dos três valores métricos correspondentes dos três nós RabbitMQ.
RabbitMQMemLimit	Bytes	O RAM limite para um corretor RabbitMQ. Para implantações de cluster, esse valor representa o agregado dos três valores métricos correspondentes dos três nós RabbitMQ.
RabbitMQMemUsed	Bytes	O volume RAM usado por um corretor RabbitMQ. Para implantações de cluster, esse valor representa o agregado dos três valores métricos correspondentes dos três nós RabbitMQ.

Métrica	Unidade	Descrição
RabbitMQDiskFreeLimit	Bytes	O limite de disco para um agente RabbitMQ. Para implantações de cluster, esse valor representa o agregado dos três valores métricos correspondentes dos três nós RabbitMQ. Esta métrica é diferente por tamanho de instância. Para obter mais informações sobre os tipos de instância do Amazon MQ, consulte the section called “Amazon MQ para tipos de instância RabbitMQ” .
RabbitMQDiskFree	Bytes	O volume total de espaço livre em disco disponível em um agente RabbitMQ. Quando o uso do disco ultrapassa seu limite, o cluster bloqueará todas as conexões do produtor. Para implantações de cluster, esse valor representa o agregado dos três valores métricos correspondentes dos três nós RabbitMQ.
RabbitMQFdUsed	Contagem	Número de descritores de arquivos usados. Para implantações de cluster, esse valor representa o agregado dos três valores métricos correspondentes dos três nós RabbitMQ.

Métrica	Unidade	Descrição
RabbitMQIOReadAverageTime	Contagem	O tempo médio (em milissegundos) para o RabbitMQ realizar uma operação de leitura. O valor é proporcional ao tamanho da mensagem.
RabbitMQIOWriteAverageTime	Contagem	O tempo médio (em milissegundos) para o RabbitMQ realizar uma operação de gravação. O valor é proporcional ao tamanho da mensagem.

Dimensões para métricas de agente RabbitMQ


Dimensão	Descrição
Broker	O nome do operador.

Métricas do nó RabbitMQ

Métrica	Unidade	Descrição
SystemCpuUtilization	Percentual	A porcentagem de unidades de EC2 computação alocadas da Amazon que o corretor usa atualmente.
RabbitMQMemLimit	Bytes	O RAM limite para um nó RabbitMQ.
RabbitMQMemUsed	Bytes	O volume RAM usado por um nó RabbitMQ. Quando o uso da memória ultrapassa

Métrica	Unidade	Descrição
		o limite, o cluster bloqueará todas as conexões do produtor.
RabbitMQDiskFreeLimit	Bytes	O limite de disco para um nó RabbitMQ. Esta métrica é diferente por tamanho de instância. Para obter mais informações sobre os tipos de instância do Amazon MQ, consulte the section called “Amazon MQ para tipos de instância RabbitMQ” .
RabbitMQDiskFree	Bytes	O volume total de espaço livre em disco disponível em um nó RabbitMQ. Quando o uso do disco ultrapassa seu limite, o cluster bloqueará todas as conexões do produtor.
RabbitMQFdUsed	Contagem	Número de descritores de arquivos usados.

Dimensões para métricas de nó RabbitMQ

Dimensão	Descrição
Node	<p>Nome do nó.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Um nome de nó consiste em duas partes: um prefixo (normalmente <code>rabbit</code>) e um nome de host. Por</p> </div>

Dimensão	Descrição
	<p>exemplo, <code>rabbit@ip-10-0-0-230.us-west-2.compute.internal</code> é um nome de nó com o prefixo <code>rabbit</code> e o nome do host <code>ip-10-0-0-230.us-west-2.compute.internal</code>.</p>
Broker	O nome do operador.

Métricas de fila RabbitMQ

Métrica	Unidade	Descrição
ConsumerCount	Contagem	O número de consumidores que se inscreveram para a fila.
MessageReadyCount	Contagem	O número de mensagens que estão atualmente disponíveis para serem entregues.
MessageUnacknowledgedCount	Contagem	O número de mensagens para as quais o servidor está aguardando confirmação.
MessageCount	Contagem	O número total de <code>MessageReadyCount</code> e <code>MessageUnacknowledgedCount</code> (também conhecida como profundidade de fila).

Dimensões para métricas de fila RabbitMQ

Note

O Amazon MQ para RabbitMQ não publicará métricas para hosts virtuais e filas com nomes contendo espaços em branco, guias ou outros caracteres que não sejam caracteres ASCII. Para obter mais informações sobre nomes de dimensões, consulte [Dimension](#) na Amazon CloudWatch API Reference.

Dimensão	Descrição
Queue	O nome da fila do .
VirtualHost	O nome do host virtual.
Broker	O nome do operador.

Configurar logs do Amazon MQ for RabbitMQ

Quando você ativa o CloudWatch registro em log para seus corretores RabbitMQ, o Amazon MQ usa uma função vinculada ao serviço para publicar registros gerais. CloudWatch Se nenhuma função vinculada ao serviço do Amazon MQ existir quando você criar um agente pela primeira vez, o Amazon MQ criará um agente automaticamente. Todos os corretores subsequentes do RabbitMQ usarão a mesma função vinculada ao serviço para publicar registros. CloudWatch

Para obter mais informações sobre funções vinculadas a serviços, consulte [Usando funções vinculadas a serviços no Guia do usuário](#).AWS Identity and Access Management Para obter mais informações sobre o Amazon MQ usa as funções vinculadas ao serviço, consulte [the section called “Uso de funções vinculadas a serviço”](#).

Registrando chamadas do Amazon MQ usando API AWS CloudTrail

O Amazon MQ é integrado com AWS CloudTrail, um serviço que fornece um registro das chamadas do Amazon MQ que um usuário, AWS função ou serviço faz. CloudTrail captura API chamadas

relacionadas aos agentes e configurações do Amazon MQ como eventos, incluindo chamadas do console do Amazon MQ e chamadas de código do Amazon MQ. APIs Para obter mais informações sobre CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

Note

CloudTrail não registra API chamadas relacionadas às operações do ActiveMQ (por exemplo, envio e recebimento de mensagens) ou ao ActiveMQ Web Console. Para registrar informações relacionadas às operações do ActiveMQ, você pode configurar o [Amazon MQ para publicar registros gerais e de auditoria no Amazon](#) Logs. CloudWatch

Usando as informações CloudTrail coletadas, você pode identificar uma solicitação específica para um Amazon API MQ, o endereço IP do solicitante, a identidade do solicitante, a data e a hora da solicitação e assim por diante. Se você configurar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3. Se você não configurar uma trilha, poderá ver os eventos mais recentes no histórico de eventos no CloudTrail console. Para mais informações, consulte [Visão geral da criação de uma trilha](#) no [Guia do usuário do AWS CloudTrail](#).

Informações sobre o Amazon MQ em CloudTrail

Quando você cria sua AWS conta, CloudTrail está habilitado. Quando ocorre uma atividade de evento compatível do Amazon MQ, ela é registrada em um CloudTrail evento com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e fazer download de eventos recentes para a sua conta da AWS . Para obter mais informações, consulte [Visualizar eventos com histórico de CloudTrail eventos](#) no Guia AWS CloudTrail do usuário.


Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Você pode criar uma trilha para manter um registro contínuo dos eventos em sua AWS conta. Por padrão, quando você cria uma trilha usando o AWS Management Console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as AWS regiões e entrega arquivos de log para o bucket especificado do Amazon S3. Você também pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS CloudTrail :

- [CloudTrail Serviços e integrações compatíveis](#)
- [Configurando as SNS notificações da Amazon para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#)


- [Recebendo arquivos de CloudTrail log de várias contas](#)

O Amazon MQ suporta o registro dos parâmetros de solicitação e das respostas para o seguinte APIs como eventos em arquivos de CloudTrail log:

- [CreateConfiguration](#)
- [DeleteBroker](#)
- [DeleteUser](#)
- [RebootBroker](#)
- [UpdateBroker](#)

 Note

RebootBroker os arquivos de log são registrados quando você reinicia o broker. Durante a janela de manutenção, o serviço é reinicializado automaticamente e os arquivos de RebootBroker log não são registrados.

 Important

Para os GET métodos a seguir APIs, os parâmetros da solicitação são registrados, mas as respostas são editadas:

- [DescribeBroker](#)
- [DescribeConfiguration](#)
- [DescribeConfigurationRevision](#)
- [DescribeUser](#)
- [ListBrokers](#)
- [ListConfigurationRevisions](#)
- [ListConfigurations](#)
- [ListUsers](#)

Para o seguinte APIs, os parâmetros de password solicitação data e estão ocultos por asteriscos ()***:

- [CreateBroker](#) (POST)
- [CreateUser](#) (POST)
- [UpdateConfiguration](#) (PUT)
- [UpdateUser](#) (PUT)

Cada evento ou entrada de log contém informações sobre o solicitante. As informações ajudam a identificar:

- A solicitação foi feita com credenciais de usuário raiz ou do ?
- A solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado?
- A solicitação foi feita por outro AWS serviço?

Para obter mais informações, consulte [CloudTrail userIdentity Element](#) no Guia AWS CloudTrail do usuário.

Exemplo de entrada do arquivo de log do Amazon MQ

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para o bucket especificado do Amazon S3. CloudTrail os arquivos de log contém uma ou mais entradas de log.

Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a solicitação para um Amazon MQAPI, o endereço IP do solicitante, a identidade do solicitante, a data e a hora da solicitação e assim por diante.

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma [CreateBroker](#)APIchamada.

Note

Como os arquivos de CloudTrail log não são um rastreamento de pilha ordenado do públicoAPIs, eles não listam as informações em nenhuma ordem específica.

```
{  
  "eventVersion": "1.06",
```

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AKIAIOSFODNN7EXAMPLE",
  "arn": "arn:aws:iam::111122223333:user/AmazonMqConsole",
  "accountId": "111122223333",
  "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
  "userName": "AmazonMqConsole"
},
"eventTime": "2018-06-28T22:23:46Z",
"eventSource": "amazonmq.amazonaws.com",
"eventName": "CreateBroker",
"awsRegion": "us-west-2",
"sourceIPAddress": "203.0.113.0",
"userAgent": "PostmanRuntime/7.1.5",
"requestParameters": {
  "engineVersion": "5.15.9",
  "deploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
  "maintenanceWindowStartTime": {
    "dayOfWeek": "THURSDAY",
    "timeOfDay": "22:45",
    "timeZone": "America/Los_Angeles"
  },
  "engineType": "ActiveMQ",
  "hostInstanceType": "mq.m5.large",
  "users": [
    {
      "username": "MyUsername123",
      "password": "****",
      "consoleAccess": true,
      "groups": [
        "admins",
        "support"
      ]
    },
    {
      "username": "MyUsername456",
      "password": "****",
      "groups": [
        "admins"
      ]
    }
  ],
  "creatorRequestId": "1",
  "publiclyAccessible": true,
```



```
    "securityGroups": [
      "sg-a1b234cd"
    ],
    "brokerName": "MyBroker",
    "autoMinorVersionUpgrade": false,
    "subnetIds": [
      "subnet-12a3b45c",
      "subnet-67d8e90f"
    ]
  },
  "responseElements": {
    "brokerId": "b-1234a5b6-78cd-901e-2fgh-3i45j6k17819",
    "brokerArn": "arn:aws:mq:us-east-2:123456789012:broker:MyBroker:b-1234a5b6-78cd-901e-2fgh-3i45j6k17819"
  },
  "requestID": "a1b2c345-6d78-90e1-f2g3-4hi56jk7l890",
  "eventID": "a12bcd3e-fg45-67h8-ij90-12k34d5l16mn",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

Configurar logs do Amazon MQ for ActiveMQ

Para permitir que o Amazon MQ publique registros no CloudWatch Logs, você deve [adicionar uma permissão ao seu usuário do Amazon MQ](#) e [também configurar uma política baseada em recursos para o Amazon MQ](#) antes de criar ou reiniciar o agente.

Note

Quando você ativa os registros e publica mensagens do console web ActiveMQ, o conteúdo da mensagem é enviado e exibido CloudWatch nos registros.

A seguir, descrevemos as etapas para configurar CloudWatch registros para seus corretores ActiveMQ.

Tópicos

- [Entendendo a estrutura do registro em CloudWatch Logs](#)
- [Adicionar a permissão CreateLogGroup ao seu usuário do Amazon MQ](#)

- [Configure uma política baseada em recursos para o Amazon MQ](#)
- [Prevenção contra o ataque do “substituto confuso” em todos os serviços](#)

Entendendo a estrutura do registro em CloudWatch Logs

Você pode habilitar o registro geral e de auditoria ao [configurar definições avançadas do agente](#) na criação ou edição de um agente.

O registro geral ativa o nível de INFO registro padrão (o DEBUG registro não é suportado) e publica `activemq.log` em um grupo de registros em sua CloudWatch conta. O grupo de logs tem um formato semelhante ao seguinte:

```
/aws/amazonmq/broker/b-1234a5b6-78cd-901e-2fgh-3i45j6k17819/general
```

O [registro de auditoria](#) permite o registro de ações de gerenciamento realizadas usando JMX ou usando o ActiveMQ Web Console e `audit.log` as publica em um grupo de registros em sua conta. CloudWatch O grupo de logs tem um formato semelhante ao seguinte:

```
/aws/amazonmq/broker/b-1234a5b6-78cd-901e-2fgh-3i45j6k17819/audit
```

Dependendo se você tem um [agente de instância única](#) ou um [agente ativo/em espera](#), o Amazon MQ cria uma ou duas transmissões de log dentro de cada grupo de logs. Os fluxos de log têm um formato semelhante ao seguinte:

```
activemq-b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.log  
activemq-b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-2.log
```

Os sufixos `-1` e `-2` denotam instâncias individuais do agente. Para obter mais informações, consulte Como [trabalhar com grupos de registros e fluxos de registros](#) no [Guia do usuário do Amazon CloudWatch Logs](#).

Adicionar a permissão **CreateLogGroup** ao seu usuário do Amazon MQ

Para permitir que o Amazon MQ crie um grupo de CloudWatch logs de registros, você deve garantir que o usuário que cria ou reinicializa o agente tenha a permissão. `logs:CreateLogGroup`

⚠ Important

Se você não adicionar a permissão `CreateLogGroup` ao seu usuário do Amazon MQ antes que ele crie ou reinicialize o agente, o Amazon MQ não criará o grupo de logs.

A [política IAM baseada no](#) exemplo a seguir concede permissão `logs:CreateLogGroup` aos usuários aos quais essa política está anexada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
        }
    ]
}
```

ℹ Note

Aqui, o termo usuário se refere a Usuários e não a Usuários do Amazon MQ, que são criados quando um novo agente é configurado. Para obter mais informações sobre a configuração de usuários e IAM políticas, consulte a seção [Visão geral do gerenciamento de identidades](#) do Guia do IAM usuário.

Para obter mais informações, consulte [CreateLogGroup](#) a Amazon CloudWatch Logs API Reference.

Configure uma política baseada em recursos para o Amazon MQ

⚠ Important

Se você não configurar uma política baseada em recursos para o Amazon MQ, o agente não poderá publicar os registros no Logs. CloudWatch

Para permitir que o Amazon MQ publique registros em seu grupo de CloudWatch registros de registros, configure uma política baseada em recursos para dar ao Amazon MQ acesso às seguintes ações de registros: CloudWatch API

- [CreateLogStream](#)— Cria um fluxo de CloudWatch registros para o grupo de registros especificado.
- [PutLogEvents](#)— Entrega eventos para o fluxo de registro de CloudWatch registros especificado.

A seguinte política baseada em recursos concede permissão para `logs:CreateLogStream` e `logs:PutLogEvents` para. AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": { "Service": "mq.amazonaws.com" },
            "Action": [ "logs:CreateLogStream",
"logs:PutLogEvents" ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/
amazonmq/*"
        }
    ]
}
```

Essa política baseada em recursos deve ser configurada usando o, AWS CLI conforme mostrado no comando a seguir. No exemplo, substitua *us-east-1* com suas próprias informações.

```
aws --region us-east-1 logs put-resource-policy --policy-name AmazonMQ-logs \
    --policy-document "{\"Version\": \"2012-10-17\", \"Statement\":
[ { \"Effect\": \"Allow\", \"Principal\": { \"Service\": \"mq.amazonaws.com\" },
    \"Action\": [\"logs:CreateLogStream\", \"logs:PutLogEvents\"],
    \"Resource\": \"arn:aws:logs:*:*:log-group:/aws/amazonmq/*\" } ]}"
```

Note

Como esse exemplo usa o `/aws/amazonmq/` prefixo, você precisa configurar a política baseada em recursos somente uma vez por AWS conta, por região.

Prevenção contra o ataque do “substituto confuso” em todos os serviços

“Confused deputy” é um problema de segurança no qual uma entidade sem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar em um problema confuso de delegado. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com diretores de serviços que receberam acesso aos recursos em sua conta.

Recomendamos usar as [aws:SourceArn](#) chaves de contexto de condição [aws:SourceAccount](#) global em sua política baseada em recursos do Amazon MQ para limitar o acesso aos CloudWatch registros a um ou mais corretores específicos.

Note

Se você utilizar ambas as chaves de contexto de condição global, o valor `aws:SourceAccount` e a conta `aws:SourceArn` no valor deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

O exemplo a seguir demonstra uma política baseada em recursos que limita o acesso aos CloudWatch registros a um único agente do Amazon MQ.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "mq.amazonaws.com"
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/amazonmq/*",
            "Condition": {
                "StringEquals": {
```

```

        "aws:SourceAccount": "123456789012",
        "aws:SourceArn": "arn:aws:mq:us-
east-2:123456789012:broker:MyBroker:b-1234a5b6-78cd-901e-2fgh-3i45j6k17819"
    }
}
]
}

```

Você também pode configurar sua política baseada em recursos para limitar o acesso aos CloudWatch registros a todos os corretores em uma conta, conforme mostrado a seguir.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "mq.amazonaws.com"
                ]
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/amazonmq/
*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn":
"arn:aws:mq:*:123456789012:broker:*"
                },
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                }
            }
        }
    ]
}

```

Para obter mais informações sobre o problema de segurança de representante confuso, consulte [O problema do representante confuso](#), no Guia do usuário.

Solução de problemas na configuração de CloudWatch registros com o Amazon MQ

Em alguns casos, CloudWatch os registros nem sempre se comportam conforme o esperado. Esta seção fornece uma visão geral dos problemas comuns e mostra como resolvê-los.

Grupos de registros não aparecem em CloudWatch

[Adicione a permissão `CreateLogGroup` ao seu usuário do Amazon MQ](#) e reinicialize o agente. Isso permite que o Amazon MQ crie o grupo de logs.

Os fluxos de registros não aparecem nos grupos de CloudWatch registros

[Configure uma política baseada em recursos para o Amazon MQ](#). Isso permite que seu agente publique seus logs.

Cotas no Amazon MQ

Este tópico lista os limites dentro do Amazon MQ. Muitos dos limites a seguir podem ser alterados para AWS contas específicas. Para solicitar o aumento de um limite, consulte [Cotas de serviço da AWS](#) na Referência geral da Amazon Web Services. Os limites atualizados não estarão visíveis mesmo após a aplicação do aumento do limite. Para obter mais informações sobre como visualizar os limites atuais de conexão na Amazon CloudWatch, consulte [Monitoramento de agentes do Amazon MQ usando](#) a Amazon. CloudWatch



Tópicos

- [Operadores](#)
- [Configurações](#)
- [Usuários](#)
- [Armazenamento de dados](#)
- [APILimitação](#)

Operadores

A tabela a seguir lista as cotas relacionadas aos agente do Amazon MQ.

Limite	Descrição
Nome do agente	<ul style="list-style-type: none">• Deve ser exclusivo em sua AWS conta.• Deve ter entre 1 e 50 caracteres.• Deve conter somente caracteres especificados no conjunto de caracteres ASCII imprimíveis.• Pode conter somente caracteres alfanuméricos, traços, pontos, sublinhados e tils (- . _ ~).

Limite	Descrição
Número de agentes, por região	50
Conexões de nível de fio por protocolo para agente menor	<div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> Important Não se aplica aos agentes do RabbitMQ.</p> </div> <p>300 para agentes de tipo de instância <code>mq.*.micro</code> .</p>
Conexões de nível de fio por protocolo para agente maior	<div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> Important Não se aplica aos agentes do RabbitMQ.</p> </div> <p>2 mil para agentes de tipo de instância <code>mq.*.*large</code> .</p>
Grupos de segurança por agente	5
Destinos do ActiveMQ (filas e tópicos) monitorados em CloudWatch	CloudWatch monitora somente os primeiros 1000 destinos.
Destinos (filas) do RabbitMQ monitorados em CloudWatch	CloudWatch monitora apenas os primeiros 500 destinos, ordenados por número de consumido res.
Etiquetas por agente	50

Configurações

A tabela a seguir lista as cotas relacionadas às configurações do Amazon MQ.

⚠ Important

Não se aplica aos agentes do RabbitMQ.

Limite	Descrição
Nome da configuração	<ul style="list-style-type: none"> • Deve ter entre 1 e 150 caracteres. • Deve conter somente caracteres especificados no conjunto de caracteres ASCII imprimíveis. • Pode conter somente caracteres alfanuméricos, traços, pontos, sublinhados e tils (- . _ ~).
Revisões por configuração	300

Usuários

A tabela a seguir lista as cotas relacionadas aos usuários do Amazon MQ ActiveMQ.

⚠ Important

Não se aplica aos agentes do RabbitMQ.




Limite	Descrição
Nome de usuário	<ul style="list-style-type: none"> • Deve ter entre 1 e 100 caracteres. • Deve conter somente caracteres especificados no conjunto de caracteres ASCII imprimíveis.

Limite	Descrição
	<ul style="list-style-type: none"> • Pode conter somente caracteres alfanuméricos, traços, pontos, sublinhados e tils (- . _ ~). • Não deve conter vírgulas (,).
Senha	<ul style="list-style-type: none"> • Deve ter entre 12 e 250 caracteres. • Deve conter somente caracteres especificados no conjunto de caracteres ASCII imprimíveis. • Deve conter pelo menos 4 caracteres únicos. • Não deve conter vírgulas (,).
Usuários por agente (autenticação simples)	250
Grupos por usuário (autenticação simples)	20

Armazenamento de dados

A tabela a seguir lista as cotas relacionadas ao armazenamento de dados do Amazon MQ.

Limite	Descrição
Capacidade de armazenamento por agente	20 GB para agentes de tipo de instância mq.*.micro. Para obter mais informações sobre os tipos de instância do Amazon MQ, consulte Broker instance types .
Capacidade de armazenamento por agente	200 GB para agentes de tipo de instância mq.*.*large. Para obter mais informações

Limite	Descrição
<p>Limite de uso do agendador de trabalhos por corretor apoiado pela Amazon EBS</p>	<p>es sobre os tipos de instância do Amazon MQ, consulte Broker instance types.</p> <div data-bbox="829 367 1507 590" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Important Não se aplica aos agentes do RabbitMQ.</p> </div> <p>50 GB. Para obter mais informações sobre o uso do agendador de tarefas, consulte JobSchedulerUsage a documentação do Apache ActiveMQ. API</p>
<p>Capacidade de armazenamento temporário por intermediário menor.</p>	<div data-bbox="829 913 1507 1136" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Important Não se aplica aos agentes do RabbitMQ.</p> </div> <p>5 GB para agentes de tipo de instância <code>mq.*.micro</code> .</p>
<p>Capacidade de armazenamento temporário por intermediário maior.</p>	<div data-bbox="829 1358 1507 1581" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Important Não se aplica aos agentes do RabbitMQ.</p> </div> <p>50 GB para agentes de tipo de instância <code>mq.*.*large</code> .</p>

API Limitação

As seguintes cotas de limitação são agregadas por AWS conta, em todo o Amazon MQ, para manter a largura de banda do serviço. APIs Para obter mais informações sobre o Amazon MQ APIs, consulte a Referência do [Amazon REST API MQ](#).

Important

Essas cotas não se aplicam às mensagens do agente Amazon MQ para ActiveMQ ou Amazon MQ para RabbitMQ. APIs Por exemplo, o Amazon MQ não limita o envio nem o recebimento de mensagens.

API limite de explosão	API limite de taxa
100	15

Solução de problemas do Amazon MQ

Esta seção descreve problemas comuns que você pode encontrar ao usar os agentes do Amazon MQ e as etapas que você pode implementar para resolvê-los.

Solução de problemas: Amazon MQ geral

Use as informações desta seção para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com agentes do Amazon MQ, como problemas de conexão com seu o agente e reinicializações do agente.


Sumário

- [Não consigo me conectar ao console da Web ou endpoints do agente.](#)
- [Meu corretor está funcionando e eu posso verificar a conectividade usando telnet, mas meus clientes não conseguem se conectar e estão retornando SSL exceções.](#)
- [Criei um agente, mas a criação falhou.](#)
- [Meu agente reiniciou e não sei por quê.](#)

Não consigo me conectar ao console da Web ou endpoints do agente.

Se você estiver enfrentando problemas para se conectar ao seu agente usando o console da Web ou endpoints em nível de fio, recomendamos as etapas a seguir.

1. Confira se você está tentando se conectar ao seu agente por trás de um firewall. Pode ser necessário configurar o firewall para permitir o acesso ao agente.
2. Verifique se você está tentando se conectar ao seu corretor usando um [FIPS](#) endpoint. O Amazon MQ só oferece suporte a FIPS endpoints ao usar API operações, e não para conexões em nível de fio com a própria instância do broker.
3. Confira se a Acessibilidade pública para o seu agente está definida como Yes (Sim). Se estiver definido como Não, verifique as regras da [Lista de Controle de Acesso \(ACL\)](#) da rede da sua sub-rede. Se você criou uma rede personalizada ACLs, talvez seja necessário alterar ACL as regras da rede para fornecer acesso ao seu corretor. Para obter mais informações sobre a VPC rede da Amazon, consulte [Habilitando o acesso à Internet](#) no Guia VPC do usuário da Amazon
4. Confira as regras do Grupo de Segurança do seu agente. Confira se você está permitindo conexões com as seguintes portas:

 Note

As portas a seguir são agrupadas de acordo com os tipos de mecanismo, pois o Amazon MQ para ActiveMQ e o Amazon MQ para RabbitMQ usam portas diferentes para conexões.


Amazon MQ para ActiveMQ

- Console da Web — Porta 8162
- OpenWire — Porto 61617
- AMQP— Porto 5671
- STOMP— Porto 61614
- MQTT— Porto 8883
- WSS— Porto 61619

Amazon MQ para RabbitMQ

- Console e gerenciamento da Web API — Porta 443 e 15671
- AMQP— Porto 5671

5. Execute os seguintes testes de conectividade de rede para o tipo de mecanismo do agente.

 Note

Para corretores sem acessibilidade pública, execute os testes em uma EC2 instância da Amazon dentro da VPC mesma Amazon do seu agente Amazon MQ e avalie as respostas.

Amazon MQ for ActiveMQ

Para testar o seu Amazon MQ quanto à conectividade de rede do agente ActiveMQ

1. Abra uma nova janela de terminal ou de linha de comando.
2. Execute o `nslookup` comando a seguir para consultar o DNS registro do seu corretor. Para implantações [ativas/em espera](#), teste os endpoints ativos e em espera. Os endpoints

ativos/em espera são identificados com um sufixo, -1 ou -2 adicionados ao ID exclusivo do agente. Substitua o endpoint com as suas informações.

```
$ nslookup b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-west-2.amazonaws.com
```

Se a consulta for bem-sucedida, você verá um resultado semelhante a este.

```
Non-authoritative answer:
Server: dns-resolver-corp-sfo-1.sfo.corp.amazon.com
Address: 172.10.123.456

Name: ec2-12-345-123-45.us-west-2.compute.amazonaws.com
Address: 12.345.123.45
Aliases: b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-west-2.amazonaws.com
```

O endereço IP resolvido deve corresponder aos endereços IP fornecidos no console do Amazon MQ. Isso indica que o nome de domínio está sendo resolvido corretamente no DNS servidor e você pode passar para a próxima etapa.

3. Execute o seguinte comando `telnet` para testar o caminho de rede para o seu agente. Substitua o endpoint com as suas informações. Substituir *port* com o número 8162 da porta do console web ou outras portas de nível de fio para testar protocolos adicionais conforme necessário.

Note

Para implantações ativas/em espera, você receberá uma mensagem de erro `Connect failed` caso execute `telnet` com o endpoint em espera. Isso é esperado, pois a própria instância em espera está em execução, mas o processo ActiveMQ não está em execução e não tem acesso ao volume de armazenamento Amazon da corretora. EFS Execute o comando para ambos os endpoints -1 e -2 para garantir que você teste as instâncias ativas e em espera.

```
$ telnet b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-west-2.amazonaws.com port
```

Para a instância ativa, você verá um resultado semelhante ao seguinte.


```
Connected to b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-  
west-2.amazonaws.com.  
Escape character is '^]'.
```

4. Faça uma das coisas a seguir.

- Se o comando `telnet` tiver êxito, confira a métrica [EstablishedConnectionsCount](#) e confirme que o agente não tenha atingido o limite máximo de [conexões com fio](#). Você também pode confirmar se o limite foi atingido revisando os logs `General` do agente. Se essa métrica for maior que zero, há pelo menos um cliente conectado ao agente no momento. Se a métrica não mostrar nenhuma conexão, execute o teste de caminho `telnet` novamente e aguarde pelo menos um minuto antes de desconectar, pois as métricas do agente são publicadas a cada minuto.
- Se o comando `telnet` falhar, confira o status da [interface de rede elástica](#) do agente e confirme se o status é `in-use`. [Crie um registro de VPC fluxo da Amazon](#) para a interface de rede de cada instância e analise os registros de fluxo gerados. Procure os endereços IP do agente quando você executou o comando `telnet` e confirme se os pacotes de conexão estão `ACCEPTED`, incluindo um pacote de devolução. Para obter mais informações e ver um exemplo de registro de fluxo, consulte [Exemplos de registros de log de fluxo](#) no Amazon VPC Developer Guide.

5. Execute o seguinte comando `curl` para conferir a conectividade com o console da Web de administração do ActiveMQ.

```
$ curl https://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-  
west-2.amazonaws.com:8162/index.html
```

Se o comando for bem-sucedido, a saída deverá ser um HTML documento semelhante ao seguinte.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://  
www.w3.org/TR/html4/loose.dtd">  
<html>  
  <head>  
    <meta http-equiv="Content-Type" content="text/html;  
charset=iso-8859-1" />  
    <title>Apache ActiveMQ</title>  
    ...
```

Amazon MQ for RabbitMQ

Para testar o seu Amazon MQ quanto à conectividade de rede do agente RabbitMQ

1. Abra uma nova janela de terminal ou de linha de comando.
2. Execute o `nslookup` comando a seguir para consultar o DNS registro do seu corretor. Substitua o endpoint com as suas informações.

```
$ nslookup b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-west-2.amazonaws.com
```

Se a consulta for bem-sucedida, você verá um resultado semelhante a este.

```
Non-authoritative answer:
Server: dns-resolver-corp-sfo-1.sfo.corp.amazon.com
Address: 172.10.123.456

Name: rabbit-broker-1c23e456ca78-b9000123b4ebbab5.elb.us-
west-2.amazonaws.com
Addresses: 52.12.345.678
           52.23.234.56
           41.234.567.890
           54.123.45.678
Aliases: b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-west-2.amazonaws.com
```

3. Execute o seguinte comando `telnet` para testar o caminho de rede para o seu agente. Substitua o endpoint com as suas informações. Você pode substituir *port* com porta 443 para o console web e 5671 para testar a conexão em nível de fioAMQP.

```
$ telnet b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
west-2.amazonaws.com port
```

Se o comando for bem-sucedido, você verá um resultado semelhante a este.

```
Connected to b-1234a5b6-78cd-901e-2fgh-3i45j6k178l9-1.mq.us-
west-2.amazonaws.com.
Escape character is '^]'.
```

Note

A conexão telnet será fechada automaticamente após alguns segundos.

4. Faça uma das coisas a seguir.
 - Se o comando `telnet` for bem-sucedido, confira a métrica [ConnectionCount](#) e confirme que o agente não atingiu o valor definido na política padrão [max-connections](#). Você também pode confirmar se o limite foi atingido revisando o grupo de logs do agente `Connection.log`. Se essa métrica for maior que zero, há pelo menos um cliente conectado ao agente no momento. Se a métrica não mostrar nenhuma conexão, execute o teste de caminho `telnet` novamente. Talvez seja necessário repetir esse processo se a conexão for fechada antes que seu agente publique novas métricas de conexão para CloudWatch. As métricas são publicadas a cada minuto.
 - Para agentes não acessíveis publicamente, se o comando `telnet` falhar, verifique o status das [interfaces de rede elástica](#) do agente e confirme se o status é `in-use`. [Crie um registro de VPC fluxo da Amazon](#) para cada interface de rede e revise os registros de fluxo gerados. Procure os endereços IP privados do agente quando o comando `telnet` foi evocado e confirme se os pacotes de conexão estão `ACCEPTED`, incluindo um pacote de devolução. Para obter mais informações e ver um exemplo de registro de fluxo, consulte [Exemplos de registros de log de fluxo](#) no Amazon VPC Developer Guide.

Note

Esta etapa não se aplica a agentes do Amazon MQ para RabbitMQ com acessibilidade pública.

5. Execute o seguinte comando `curl` para conferir a conectividade com o console da Web de administração do RabbitMQ.

```
$ curl https://b-1234a5b6-78cd-901e-2fgh-3i45j6k17819-1.mq.us-west-2.amazonaws.com:443/index.html
```

Se o comando for bem-sucedido, a saída deverá ser um HTML documento semelhante ao seguinte.

```
<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>RabbitMQ Management</title>
    ...
```

Meu corretor está funcionando e eu posso verificar a conectividade usando **telnet**, mas meus clientes não conseguem se conectar e estão retornando SSL exceções.

Seu certificado de endpoint do agente pode ter sido atualizado durante a [janela de manutenção](#) do agente. Os certificados de agente do Amazon MQ são alternados periodicamente para garantir a disponibilidade contínua e a segurança dos agentes.

Recomendamos o uso da autoridade de certificação (CA) raiz da Amazon no [Amazon Trust Services](#) para autenticar no armazenamento de confiança de seus clientes. Todos os certificados do agente do Amazon MQ são assinados com essa CA raiz. Ao usar uma CA raiz da Amazon, você não precisará mais baixar o novo certificado de agente do Amazon MQ sempre que um certificado for atualizado no agente.

Criei um agente, mas a criação falhou.

Se o seu agente estiver em um status `CREATION_FAILED`, faça o seguinte.

- Verifique suas IAM permissões. Para criar um agente, você deve usar a IAM política AWS gerenciada `AmazonMQFullAccess` ou ter o conjunto correto de EC2 permissões da Amazon em sua IAM política personalizada. Para saber mais sobre as EC2 permissões necessárias da Amazon, consulte [IAMPermissões necessárias para criar um agente Amazon MQ](#).
- Verifique se a sub-rede que você está escolhendo para seu corretor está em uma Amazon Virtual Private Cloud compartilhada (VPC). Para criar um agente Amazon MQ em uma Amazon compartilhadaVPC, você deve criá-lo na conta proprietária da Amazon. VPC

Meu agente reiniciou e não sei por quê.

Se o seu agente foi reiniciado automaticamente, pode ter sido por um dos motivos a seguir.

- Seu agente pode ter sido reiniciado devido a uma janela de manutenção semanal agendada. Periodicamente, o Amazon MQ realiza a manutenção do hardware, do sistema operacional ou do software do mecanismo de um agente de mensagens. A duração da manutenção varia, mas pode durar até duas horas, dependendo das operações agendadas para o agente de mensagens. Os agentes podem reiniciar a qualquer momento durante a janela de manutenção de duas horas. Para obter mais informações sobre janelas de manutenção do agente, consulte [the section called “Agendamento da manutenção do corretor”](#).
- O tipo de instância do seu agente pode não ser adequado ao workload da sua aplicação. Por exemplo, executar um workload de produção em um `mq.t2.micro` pode resultar na falta de recursos do agente. A alta CPU utilização ou o alto uso da memória da corretora podem fazer com que uma corretora reinicie inesperadamente. Para ver quanta CPU memória está sendo utilizada por seu corretor, use as seguintes CloudWatch métricas para seu tipo de mecanismo.
 - Amazon MQ para ActiveMQ — Verifique a porcentagem de unidades de EC2 computação `CpuUtilization` da Amazon alocadas que o agente usa atualmente. `HeapUsage` Verifique a porcentagem do limite de memória do JVM ActiveMQ que o broker usa atualmente.
 - Amazon MQ para RabbitMQ — Verifique `SystemCpuUtilization` a porcentagem de unidades EC2 computacionais alocadas da Amazon que o agente usa atualmente. `RabbitMQMemUsed` Verifique o volume RAM usado em Bytes e divida `RabbitMQMemLimit` pela porcentagem de memória usada pelo nó RabbitMQ.

Para obter mais informações sobre tipos de instância de agente e como escolher o tipo de instância correto para seu workload, consulte [Broker instance types](#).

Solução de problemas do Amazon MQ para ActiveMQ

Use as informações desta seção para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Amazon MQ para agentes ActiveMQ.

Sumário

- [Não consigo ver os registros gerais ou de auditoria do meu corretor no CloudWatch Logs, embora eu tenha ativado o registro.](#)

- [Após a reinicialização do agente ou da janela de manutenção, não consigo me conectar ao meu agente, embora o status seja RUNNING. Por quê?](#)
- [Vejo alguns dos meus clientes se conectando ao agente, enquanto outros não conseguem se conectar.](#)
- [Estou vendo a exceção org.apache.jasper.JasperException: An exception occurred processing JSP page no console do ActiveMQ ao executar operações.](#)

Não consigo ver os registros gerais ou de auditoria do meu corretor no CloudWatch Logs, embora eu tenha ativado o registro.

Se você não conseguir visualizar os registros do seu corretor em CloudWatch Logs, faça o seguinte.

1. Confira se o usuário que cria ou reinicializa o agente tem a permissão `logs:CreateLogGroup`. Se você não adicionar a permissão `CreateLogGroup` a um usuário antes que este crie ou reinicialize o agente, o Amazon MQ não criará o grupo de logs.
2. Verifique se você configurou uma política baseada em recursos para permitir que o Amazon MQ publique registros no Logs. CloudWatch Para permitir que o Amazon MQ publique registros em seu grupo de CloudWatch registros de registros, configure uma política baseada em recursos para dar ao Amazon MQ acesso às seguintes ações de registros: CloudWatch API
 - [CreateLogStream](#)— Cria um fluxo de CloudWatch registros para o grupo de registros especificado.
 - [PutLogEvents](#)— Entrega eventos para o fluxo de registro de CloudWatch registros especificado.

[Para obter mais informações sobre como configurar o Amazon MQ para que o ActiveMQ publique logs em Logs, consulte Configurando registros CloudWatch .](#)

Após a reinicialização do agente ou da janela de manutenção, não consigo me conectar ao meu agente, embora o status seja **RUNNING**. Por quê?

Você pode estar enfrentando problemas de conexão após a reinicialização de um agente, após a conclusão de uma janela de manutenção programada ou em um evento de falha, em que a instância em espera é ativada. Em ambos os casos, os problemas de conexão após a reinicialização da corretora provavelmente são causados por um número anormalmente grande de mensagens persistentes no volume de EBS armazenamento da Amazon ou da EFS Amazon de sua corretora.

Durante uma reinicialização, o Amazon MQ move mensagens persistentes do armazenamento para a memória do agente. Para confirmar esse diagnóstico, você pode monitorar as seguintes métricas CloudWatch para seu agente Amazon MQ for ActiveMQ:

- **StoragePercentUsage** — Grandes porcentagens em ou perto de 100% podem fazer com que o agente recuse conexões.
- **JournalFilesForFullRecovery** — Indica o número de arquivos do diário que serão reproduzidos após desligamento e reinicialização não planejados. Um valor crescente, ou consistentemente maior que um, indica transações não resolvidas que podem causar problemas de conexão após a reinicialização.
- **OpenTransactionCount** — Um número maior que zero após uma reinicialização indica que o agente tentará armazenar mensagens consumidas anteriormente, causando assim problemas de conexão.

Para resolver esse problema, recomendamos resolver suas transações XA com `rollback()` ou `commit()`. Para obter mais informações e ver um exemplo de código para resolver transações XA usando `rollback()`, consulte [Recuperar Transações XA](#).

Vejo alguns dos meus clientes se conectando ao agente, enquanto outros não conseguem se conectar.

Se o seu agente está no status RUNNING e alguns clientes são capazes de se conectar ao agente com sucesso, enquanto outros não conseguem fazê-lo, você pode ter chegado ao limite de [Conexões em nível de fio](#) para o agente. Para verificar se você atingiu o limite de conexões em nível de fio, faça o seguinte:

- Verifique os registros gerais do broker do seu agente Amazon MQ for ActiveMQ em Logs. CloudWatch Se o limite tiver sido atingido, você verá Reached Maximum Connections nos logs do agente. Para obter mais informações sobre CloudWatch os registros do Amazon MQ para corretores ActiveMQ, consulte. [the section called “Entendendo a estrutura do registro em CloudWatch Logs”](#)

Quando o limite de conexões em nível de fio for atingido, o agente recusará ativamente novas conexões de entrada. Para resolver esse problema, recomendamos atualizar o tipo de instância do seu agente. Para obter mais informações sobre como escolher o melhor tipo de instância para seu workload, consulte [Broker instance types](#).

Se você confirmou que o número de conexões em nível de fio é menor que o limite de conexão do agente, o problema pode estar relacionado à reinicialização de clientes. Verifique, nos logs do agente, entradas numerosas e frequentes de `... Inactive for longer than 600000 ms - removing ...`. A entrada de log indica reinicialização de clientes ou problemas de conectividade. Esse efeito é mais evidente quando os clientes se conectam ao broker por meio de um Network Load Balancer (NLB) com clientes que frequentemente se desconectam e se reconectam ao broker. Isso geralmente é observado em clientes baseados em contêiner.

Para obter mais detalhes, verifique seus logs no lado do cliente. O agente limpará TCP as conexões inativas após 600.000 ms e liberará o soquete de conexão.

Estou vendo a exceção `org.apache.jasper.JasperException: An exception occurred processing JSP page` no console do ActiveMQ ao executar operações.

Se você estiver usando autenticação simples e configurando `AuthorizationPlugin` para autorização de filas e tópicos, certifique-se de usar o `AuthorizationEntries` elemento em seu arquivo de XML configuração e permitir que o `activemq-webconsole` grupo tenha permissão para todas as filas e tópicos. Isso garante que o console da Web do ActiveMQ possa se comunicar com o agente do ActiveMQ.

O exemplo `AuthorizationEntry` a seguir concede permissões de leitura e gravação para todas as filas e tópicos para o grupo `activemq-webconsole`.

```
<authorizationEntries>
  <authorizationEntry admin="activemq-webconsole,admins,users" topic="">
    read="activemq-webconsole,admins,users" write="activemq-webconsole,admins,users" />
  <authorizationEntry admin="activemq-webconsole,admins,users" queue="">
    read="activemq-webconsole,admins,users" write="activemq-webconsole,admins,users" />
</authorizationEntries>
```

Da mesma forma, ao integrar seu corretorLDAP, certifique-se de conceder permissão para o `amazonmq-console-admins` grupo. Para obter mais informações sobre LDAP integração, consulte [the section called “Como funciona a integração com LDAP”](#).

Solução de problemas: Amazon MQ para RabbitMQ

Use as informações desta seção para ajudar a diagnosticar e resolver problemas comuns que você pode encontrar ao trabalhar com o Amazon MQ para agentes RabbitMQ.

Sumário

- [Não consigo ver as métricas das minhas filas ou dos meus hosts virtuais em CloudWatch.](#)
- [Como faço para habilitar plugins no Amazon MQ para RabbitMQ?](#)
- [Não consigo alterar a VPC configuração da Amazon para o corretor.](#)

Não consigo ver as métricas das minhas filas ou dos meus hosts virtuais em CloudWatch.

Se você não conseguir visualizar as métricas de suas filas ou hosts virtuais em CloudWatch, verifique se os nomes da fila ou do host virtual contêm espaços em branco, guias ou outros nomes que não sejam caracteres. ASCII

O Amazon MQ não pode publicar métricas para hosts virtuais e filas com nomes contendo espaços em branco, guias ou outros caracteres que não sejam caracteres. ASCII

Para obter mais informações sobre nomes de dimensões, consulte [Dimension](#) na Amazon CloudWatch API Reference.

Como faço para habilitar plugins no Amazon MQ para RabbitMQ?

Atualmente, o Amazon MQ para RabbitMQ é compatível apenas com o plugin de gerenciamento, shovel, federação, troca de hash consistente do RabbitMQ, que estão habilitados por padrão. Para obter mais informações sobre como usar plugins compatíveis, consulte o [the section called “Plugins”](#).

Não consigo alterar a VPC configuração da Amazon para o corretor.

O Amazon MQ não oferece suporte à alteração da VPC configuração da Amazon após a criação do seu agente. Observe que você precisará criar uma nova corretora com a nova VPC configuração da Amazon e atualizar a conexão do cliente URL com a nova conexão de corretoraURL.

Amazon MQ for RabbitMQ: Alarme de alta memória

O RabbitMQ emitirá um alarme de alta memória quando o uso de memória do corretor, identificado pela CloudWatch métrica `RabbitMQMemUsed`, exceder o limite de memória identificado por `RabbitMQMemLimit` `RabbitMQMemLimit` definido pelo Amazon MQ e foi ajustado especificamente considerando a memória disponível para cada tipo de instância de host.

Um agente do Amazon MQ for RabbitMQ que tiver gerado um alarme de alta memória bloqueará todos os clientes que estiverem publicando mensagens. Devido ao alto uso de memória, seu agente pode ter também outros problemas que complicam o diagnóstico e a resolução do alarme.

Agentes de instância única incapazes de concluir a inicialização devido ao alto uso de memória podem entrar em um loop de reinicialização, durante o qual as interações com o agente são limitadas. Em implantações de cluster, filas podem apresentar sincronização pausada de mensagens entre réplicas em diferentes nós. Sincronizações de filas pausadas impedem o consumo de mensagens dessas filas e devem ser abordadas separadamente ao resolver o alarme de alta memória.

O Amazon MQ não reiniciará um agente com um alarme de memória alta e retornará uma exceção para [RebootBroker](#) APIs operações, desde que o agente continue disparando o alarme.

Use as informações nesta seção para ajudar a diagnosticar e resolver alarmes de alta memória do RabbitMQ gerados pelo seu agente.

Note

Pode levar várias horas para que o ALARM status RABBITMQ _ MEMORY _ desapareça após você realizar as ações necessárias.

Note

Não é possível fazer downgrade de um agente de um tipo de instância mq . m5 . para um tipo de instância mq . t3 . micro. Se quiser fazer downgrade, você deverá excluir o agente e criar outro.

Tópicos

- [Diagnosticar alarme de alta memória com o console da Web do RabbitMQ](#)
- [Diagnosticar o alarme de alta memória usando métricas do Amazon MQ](#)
- [Solucionar o alarme de alta memória](#)
- [Reduzir o número de conexões e canais](#)
- [Solucionar sincronizações de filas pausadas em implantações de cluster](#)
- [Solucionar loops de reinicialização em agentes de instância única](#)

- [Evitar alarmes de alta memória](#)

Diagnosticar alarme de alta memória com o console da Web do RabbitMQ

O console da Web do RabbitMQ pode gerar e exibir informações detalhadas de uso de memória para cada nó. Para encontrar essas informações, faça o seguinte:

1. Faça login AWS Management Console e abra o console web RabbitMQ do seu corretor.
2. No console do RabbitMQ, na página Overview (Visão geral), escolha o nome de um nó na lista Nodes (Nós).
3. Na página de detalhes do nó, escolha Memory details (Detalhes da memória) para expandir a seção e visualizar as informações de uso de memória do nó.

As informações de uso de memória fornecidas pelo RabbitMQ no console da Web podem ajudar você a determinar quais recursos podem estar consumindo muita memória e contribuindo para o alarme de alta memória. Para obter mais informações sobre os detalhes de uso da memória disponíveis no console da Web do RabbitMQ, consulte o tópico de [Considerações sobre o uso da memória](#) no site de documentação do RabbitMQ Server.

Diagnosticar o alarme de alta memória usando métricas do Amazon MQ

O Amazon MQ habilita métricas para o seu agente por padrão. Você pode [visualizar as métricas do seu corretor](#) acessando o CloudWatch console ou usando CloudWatch API o. As seguintes métricas são úteis ao diagnosticar o alarme de alta memória do RabbitMQ.

Métrica do Amazon MQ CloudWatch	Motivo do alto uso de memória
MessageCount	Mensagens são armazenadas na memória até que sejam consumidas ou descartadas. Uma alta contagem de mensagens pode indicar o excesso de uso de recursos e pode resultar em um alarme de alta memória.

Métrica do Amazon MQ CloudWatch	Motivo do alto uso de memória	
QueueCount	Filas são armazenadas na memória, e um grande número de filas pode resultar em um alarme de alta memória.	
ConnectionCount	Conexões de clientes usam memória, e muitas conexões simultâneas podem resultar em um alarme de alta memória.	
ChannelCount	De maneira semelhante a conexões, canais estabelecidos usando cada conexão também são armazenados na memória do nó, e um alto número de canais pode resultar em um alarme de alta memória.	
ConsumerCount	Para cada consumidor conectado ao agente, um número definido de mensagens é carregado do armazenamento na memória antes de ser entregue ao consumidor. Um alto número de conexões de consumidor pode causar alto uso de memória e resultar em um alarme de alta memória.	

Métrica do Amazon MQ CloudWatch	Motivo do alto uso de memória	
PublishRate	A publicação de mensagens utiliza a memória do agente. Se a taxa na qual as mensagens são publicadas no agente for muito alta e ultrapassar significativamente a taxa na qual o agente entrega mensagens aos consumidores, o agente poderá gerar um alarme de alta memória.	

Solucionar o alarme de alta memória

Para cada colaborador identificado, convém seguir este conjunto de ações para atenuar e resolver o alarme de alta memória do agente.

Motivo do alto uso de memória	Recomendação do Amazon MQ	
O número de mensagens nas filas é alto demais.	<p>Faça o seguinte:</p> <ul style="list-style-type: none"> • Consuma as mensagens publicadas nas filas. • Limpe mensagens das filas. • Exclua as filas do seu agente. 	
O número de filas configuradas no agente é alto demais.	Reduza o número dessas filas.	
O número de conexões estabelecidas no agente é alto demais.	Reduza o número dessas conexões. Para obter mais informações, consulte the	

Motivo do alto uso de memória	Recomendação do Amazon MQ	
	section called “Reduzir o número de conexões e canais” .	
O número de canais estabelecidos no agente é alto demais.	Reduza o número desses canais. Para obter mais informações, consulte the section called “Reduzir o número de conexões e canais” .	
O número de consumidores conectados ao agente é alto demais.	Reduza o número de consumidores conectados ao agente.	
A taxa de publicação de mensagens é alta demais.	Reduza a taxa na qual os publicadores enviam mensagens ao agente.	
A taxa de tentativa de conexão dos clientes é alta demais.	Reduza a frequência na qual os clientes tentam se conectar ao agente para publicar ou consumir mensagens ou configure o agente.	

Reduzir o número de conexões e canais

As conexões com o seu agente do Amazon MQ for RabbitMQ podem ser encerradas por suas aplicações cliente ou manualmente com o uso do console da Web do RabbitMQ. Para encerrar uma conexão usando o console da Web do RabbitMQ, faça o seguinte.

1. Faça login AWS Management Console e abra o console web RabbitMQ do seu corretor.
2. No console do RabbitMQ, escolha a guia Connections (Conexões).

3. Na página Connections (Conexões), em All connections (Todas as conexões), escolha na lista o nome da conexão que você deseja encerrar.
4. Na página de detalhes da conexão, escolha Close this connection (Encerrar esta conexão) para expandir a seção e depois escolha Force Close (Forçar encerramento). Como opção, você pode substituir o texto padrão do campo Reason (Motivo) pela sua própria descrição. O Amazon MQ for RabbitMQ retornará o motivo especificado ao cliente quando você encerrar a conexão.
5. Escolha OK na caixa de diálogo para confirmar e encerrar a conexão.

Quando você encerrar uma conexão, todos os canais associados à conexão encerrada também serão encerrados.

Note

Suas aplicações cliente podem ser configuradas para restabelecer automaticamente as conexões com o agentes depois que estas são encerradas. Nesse caso, encerrar conexões pelo console da Web do agente não será suficiente para reduzir a contagem de conexões ou canais.

Para corretores sem acesso público, você pode bloquear temporariamente as conexões negando o tráfego de entrada na porta de protocolo de mensagem apropriada, por exemplo, porta 5671 para conexões. AMQP É possível bloquear a porta no grupo de segurança que você forneceu ao Amazon MQ ao criar o agente. Para obter mais informações sobre como modificar seu grupo de segurança, consulte [Adicionar regras a um grupo de segurança](#) no Guia do VPC usuário da Amazon.

Solucionar sincronizações de filas pausadas em implantações de cluster

Ao solucionar alarmes de alta memória do RabbitMQ, você pode constatar que as mensagens em uma ou várias filas não podem ser consumidas. Essas filas podem estar no processo de sincronização de mensagens entre nós, durante o qual as respectivas filas ficam indisponíveis para publicação e consumo. As sincronizações de filas podem ficar pausadas devido ao alarme de alta memória e até mesmo contribuir para o alarme de memória.

Para saber mais sobre como interromper e repetir sincronizações de filas pausadas, consulte [the section called “Resolvendo a sincronização de fila pausada”](#).

Solucionar loops de reinicialização em agentes de instância única

Um agente de instância única do Amazon MQ for RabbitMQ que gera um alarme de alta memória corre o risco de se tornar indisponível se for reiniciado e não tiver memória suficiente para a inicialização. Isso pode fazer com que o RabbitMQ entre em um loop de reinicialização e evite interações adicionais com o agente até que o problema seja resolvido. Se o seu agente estiver em um loop de reinicialização, não será possível aplicar as ações recomendadas do Amazon MQ descritas anteriormente nesta seção para resolver o alarme de alta memória.

Para recuperar o agente, recomendamos fazer upgrade para um tipo de instância maior com mais memória. Ao contrário de implantações de cluster, você pode fazer upgrade de um agente de instância única enquanto ele está enfrentando um alarme de alta memória, pois não há sincronizações de filas a serem executadas entre nós durante uma reinicialização.

Evitar alarmes de alta memória

Para cada fator contribuinte identificado, recomendamos o seguinte conjunto de ações para evitar e reduzir a ocorrência de alarmes de alta memória do RabbitMQ.

Motivo do alto uso de memória	Recomendação do Amazon MQ
O número de mensagens nas filas é alto demais.	Faça o seguinte: <ul style="list-style-type: none"> Habilite filas lazy. Defina ou reduza o limite de profundidade de filas.
O número de filas configura das no agente é alto demais.	Defina ou reduza o limite de contagem de filas .
O número de conexões estabelecidas no agente é alto demais.	Defina ou reduza o limite de contagem de conexões .
O número de canais estabelecidos no agente é alto demais.	Defina um número máximo de canais por conexão em aplicações cliente.

Motivo do alto uso de memória	Recomendação do Amazon MQ
O número de consumidores conectados ao agente é alto demais.	Defina um pequeno limite de pré-busca de consumidores.
A taxa de tentativa de conexão dos clientes é alta demais.	Use conexões de maior duração para reduzir o número e a frequência de tentativas de conexão.

Depois que o alarme de alta memória do agente for resolvido, você poderá fazer upgrade do tipo de instância do host para uma instância com recursos adicionais. Para obter informações sobre como atualizar o tipo de instância do seu corretor, consulte [UpdateBrokerInputa](#) Referência do Amazon MQ REST API.

Para obter uma listagem completa dos tipos de instância de agentes, consulte [the section called “Amazon MQ para tipos de instância RabbitMQ”](#).

Amazon MQ para RabbitMQ: chave inválida AWS Key Management Service

O Amazon MQ para RabbitMQ gerará um código `INVALID_KMS_KEY` de ação crítica necessária quando um agente criado com um cliente gerenciado AWS KMS key(CMK) detectar que a chave () está desativada AWS Key Management Service . KMS Um corretor RabbitMQ verifica CMK periodicamente se a KMS chave está habilitada e se o corretor tem todas as concessões necessárias. Se o RabbitMQ não puder verificar se a chave está habilitada, o broker será colocado em quarentena e o RabbitMQ retornará `INVALID_KMS_KEY`.

Sem uma KMS chave ativa, o corretor não tem permissões básicas para KMS chaves gerenciadas pelo cliente. O agente não pode realizar operações criptográficas usando sua chave até que você reative-a e o agente reinicie. Um corretor RabbitMQ com uma KMS chave desativada é colocado em quarentena para evitar a deterioração. Depois que o RabbitMQ determinar que a KMS chave está ativa novamente, seu corretor é removido da quarentena. O Amazon MQ não reinicia um agente com uma KMS chave desativada e retorna uma exceção para `RebootBroker` API as operações, desde que o agente continue com uma chave KMS inválida.

Diagnosticando e abordando INVALID __ KMS KEY

Para diagnosticar e endereçar o código necessário da KEY ação INVALID KMS __, você deve usar a interface de linha de AWS comando (CLI) e o AWS Key Management Service console.

Para reativar sua chave KMS

1. Chame o `DescribeBroker` método para recuperá-lo `kmsKeyId` para seu CMK corretor.
2. Faça login no AWS Key Management Service console.
3. Na página Chaves gerenciadas pelo cliente, localize a ID da KMS chave do corretor problemático e verifique se o status está Ativado.
4. Se sua KMS chave tiver sido desativada, reative a chave escolhendo Ações principais e, em seguida, escolha Ativar. Depois que a chave for reativada, você deverá esperar que o RabbitMQ remova o agente da quarentena.

Para verificar se as concessões necessárias ainda estão associadas à KMS chave do corretor, chame o `ListGrant` método para verificar se `mq_rabbit_grant` e `mq_grant` estão presentes. Se a KMS concessão ou a chave tiver sido excluída, você deverá excluir o corretor e criar um novo com todas as concessões necessárias. Para ver as etapas de exclusão de um agente, consulte [Excluir um agente](#).

Para evitar o código necessário de ação KEY crítica INVALID KMS __, não exclua ou desative manualmente uma KMS chave ou CMK concessão. Se você quiser excluir a chave, exclua primeiro o agente.

Amazon MQ para ActiveMQ: alarme de interface de rede elástica excluído

O Amazon MQ para ActiveMQ emitirá um DELETED alarme `BROKER __ ENI __` quando você excluir a Elastic Network Interface (ENI) de um broker. ENI [Quando você cria um agente Amazon MQ pela primeira vez, o Amazon MQ provisiona uma interface de rede elástica Virtual Private Cloud VPC em sua conta e, portanto, exige várias permissões. EC2](#)

Você não deve modificar ou excluir essa interface de rede. Modificar ou excluir a interface de rede pode causar uma perda permanente da conexão entre você VPC e seu corretor. Se você quiser excluir a interface de rede, exclua primeiro o agente.

Amazon MQ para ActiveMQ: alarme de falta de memória do agente

O Amazon MQ for ActiveMQ emitirá um OOM alarme BROKER _ quando o agente passar por um loop de reinicialização devido à capacidade de memória insuficiente. Quando um agente está em um ciclo de reinicialização, também chamado de ciclo de rejeição, o agente inicia repetidas tentativas de recuperação em um curto espaço de tempo. Agentes que não conseguem concluir a inicialização devido à capacidade de memória insuficiente podem entrar em um ciclo de reinicialização, no qual as interações com o agente ficam limitadas.

O Amazon MQ habilita métricas para o seu agente por padrão. Você pode visualizar as métricas do seu corretor acessando o CloudWatch console da Amazon ou usando CloudWatch API o. As métricas a seguir são úteis ao diagnosticar o alarme BROKER OOM ActiveMQ _:

Métrica do Amazon MQ CloudWatch	Motivo do alto uso de memória
TotalMessageCount	Mensagens são armazenadas na memória até que sejam consumidas ou descartadas. Uma alta contagem de mensagens pode indicar o excesso de uso de recursos e pode resultar em um alarme de alta memória.
HeapUsage	A porcentagem do limite de memória do JVM ActiveMQ que o broker usa atualmente. Uma porcentagem maior indica que o corretor está usando recursos significativos e pode causar um OOM alarme.
ConnectionCount	Conexões de clientes usam memória, e muitas conexões simultâneas podem resultar

Métrica do Amazon MQ CloudWatch	Motivo do alto uso de memória	
	em um alarme de alta memória.	
CpuUtilization	A porcentagem de unidades EC2 computacionais alocadas que o broker usa atualmente.	
TotalConsumerCount	Para cada consumidor conectado ao agente, um número definido de mensagens é carregado do armazenamento na memória antes de ser entregue ao consumidor. Um alto número de conexões de consumidor pode causar alto uso de memória e resultar em um alarme de alta memória.	

Para evitar loops de reinicialização e evitar o OOM alarme BROKER __, certifique-se de que as mensagens sejam consumidas rapidamente. É possível fazer isso escolhendo o tipo de instância de agente mais eficaz e limpando a [fila de mensagens não entregues](#) para descartar mensagens não entregues ou expiradas. É possível saber mais sobre como garantir um desempenho eficaz em [Práticas recomendadas do Amazon MQ para ActiveMQ](#).

Amazon MQ para RabbitMQ: alarme de limite de disco

O alarme de limite de disco é uma indicação de que o volume de disco usado por um nó do RabbitMQ diminuiu devido ao alto número de mensagens não consumidas enquanto novas mensagens foram adicionadas. O RabbitMQ emitirá um alarme de limite de disco quando o espaço livre em disco do corretor, identificado pela CloudWatch métrica da AmazonRabbitMQDiskFree, atingir o limite de disco, identificado por RabbitMQDiskFreeLimit RabbitMQDiskFreeLimité definido pelo Amazon MQ e foi definido considerando o espaço em disco disponível para cada tipo de instância do broker.

Um agente do Amazon MQ for RabbitMQ que tiver gerado um alarme de limite de disco ficará indisponível para novas mensagens que estiverem sendo publicadas. Ao executar o RabbitMQ em um cluster, o alarme de disco abrange todo o cluster. Se um nó ficar abaixo do limite, todos os outros nós bloquearão as mensagens recebidas. Devido à falta de espaço em disco, o agente pode ter também outros problemas que complicam o diagnóstico e a resolução do alarme.

O Amazon MQ não reiniciará um agente que esteja passando por um alarme de disco e retornará uma exceção para `RebootBroker` API as operações, desde que o agente continue disparando o alarme.

Note

Não é possível fazer downgrade de um agente de um tipo de instância `mq.m5` para um tipo de instância `mq.t3.micro`. Se quiser fazer downgrade, você deverá excluir o agente e criar outro.

Diagnostico e solução do alarme de limite de disco

O Amazon MQ habilita métricas para o seu agente por padrão. Você pode [visualizar as métricas do seu corretor](#) acessando o CloudWatch console da Amazon ou usando CloudWatch API o.

`MessageCount` é uma métrica útil ao diagnosticar o alarme de limite de disco do RabbitMQ.

Mensagens são armazenadas na memória até que sejam consumidas ou descartadas. Uma alta contagem de mensagens indica o uso em excesso de armazenamento em disco e pode levar a um alarme de disco.

Para diagnosticar o alarme de limite de disco, use o Console de Gerenciamento do Amazon MQ para:

- Consuma as mensagens publicadas nas filas.
- Limpe mensagens das filas.
- Exclua as filas do seu agente.

Note

Pode levar várias horas para que o `ALARM status RABBITMQ _ DISK _` desapareça após você realizar as ações necessárias.

Para evitar que o alarme de limite de disco seja gerado novamente, é possível fazer upgrade do [tipo de instância](#) do host para uma instância com recursos adicionais. Para obter informações sobre como atualizar o tipo de instância do seu corretor, consulte `UpdateBrokerInput` a Referência do Amazon MQ RESTAPI.

Alarme de filas de quórum do Amazon MQ para RabbitMQ

As filas de quórum são suportadas somente no Amazon MQ para as versões 3.13 e superiores do RabbitMQ. O Amazon MQ para RabbitMQ gerará o código de ação essencial necessário `RABBITMQ_QUORUM_QUEUES_NOT_SUPPORTED_ON_CURRENT_VERSION` quando você tentar criar filas de quórum em uma única instância ou agente de cluster usando a versão 3.12 e versões anteriores.

Para diagnosticar e solucionar o

`RABBITMQ_QUORUM_QUEUES_NOT_SUPPORTED_ON_CURRENT_VERSION` alarme, você pode ver sua lista de filas de quórum no painel de gerenciamento do RabbitMQ:

- Se você não precisar reter mensagens, poderá excluir as filas de quórum, atualizar seu agente para a versão 3.13 ou superior e recriar as filas de quórum após atualizar o agente.
- Se precisar reter mensagens, você deverá criar um novo agente na versão 3.13 e superior e, em seguida, criar filas de quórum no novo agente. Depois de criar o novo broker e as filas de quorum, você pode migrar mensagens do broker antigo para o novo broker usando o plug-in Shovel ou Federation. Em seguida, exclua o corretor antigo.

Para evitar um `RABBITMQ_QUORUM_QUEUES_NOT_SUPPORTED_ON_CURRENT_VERSION`, atualize seu corretor para a versão 3.13 ou superior antes de criar filas de quorum nesse corretor.

Recursos relacionados

Recursos do Amazon MQ

A tabela a seguir lista recursos úteis para trabalhar com o Amazon MQ .

Recurso	Descrição
Referência da API REST do Amazon MQ	Descrições de recursos REST, solicitações de exemplo, métodos HTTP, esquemas, parâmetros e erros que o serviço retorna.
Amazon MQ na AWS CLIReferência de comandos	Descrições dos comandos da AWS CLI que você pode usar para trabalhar com agentes de mensagem.
Amazon MQ no AWS CloudFormation Manual do Usuário	<p>O recurso AWS::Amazon MQ::Broker permite criar agentes do Amazon MQ, adicionar alterações de configuração ou modificar usuários para o agente especificado, retornar informações sobre o agente especificado e excluir o agente especificado.</p> <p>O recurso AWS::Amazon MQ::Configuration permite que você crie configurações do Amazon MQ, adicione alterações de configuração ou modifique usuários e retorne informações sobre a configuração especificada.</p>
Regiões e endpoints	Informações sobre regiões e endpoints do Amazon MQ
Página do produto	A principal página da Web para obter informações sobre o Amazon MQ.

Recurso	Descrição
Fórum de discussão	Um fórum comunitário para que os desenvolvedores discutam questões técnicas relacionadas ao Amazon MQ.
AWS Informações sobre o Premium Support	A principal página da Web para obter informações sobre o AWS Premium Support, um canal de suporte de resposta rápida e com atendimento individual, para ajudá-lo a desenvolver e executar aplicações nos serviços de infraestrutura da AWS

Recursos do Amazon MQ para ActiveMQ

A tabela a seguir lista os recursos úteis para trabalhar com o Apache ActiveMQ.

Recurso	Descrição
Guia de conceitos básicos do Apache ActiveMQ	A documentação oficial do Apache ActiveMQ.
ActiveMQ em ação	Um guia para o Apache ActiveMQ que abrange a anatomia das mensagens JMS, conectores, persistência de mensagem, autenticação e autorização.
Clientes interlinguagem	Uma lista de linguagens de programação e bibliotecas Apache ActiveMQ correspondentes. Consulte também Cliente ActiveMQ e Cliente QpidJMS .

Recursos do Amazon MQ para RabbitMQ

A tabela a seguir lista os recursos úteis para trabalhar com o RabbitMQ.

Recurso	Descrição
O Guia de conceitos básicos do RabbitMQ:	A documentação oficial do RabbitMQ.
Ferramentas de desenvolvedor e bibliotecas de cliente RabbitMQ	Um guia para as bibliotecas clientes oficialmente compatíveis e ferramentas de desenvolvedor para trabalhar com RabbitMQ usando uma variedade de linguagens e plataformas de programação.
Melhores práticas do RabbitMQ	O guia do CloudAMQP sobre práticas recomendadas e recomendações para trabalhar com o RabbitMQ.

Notas de lançamento do Amazon MQ

A tabela a seguir relaciona as versões e as melhorias de recursos do Amazon MQ.

Data	Atualização da documentação
25 de julho de 2024	<p>O Amazon MQ agora oferece suporte ao ActiveMQ 5.18, uma nova versão secundária do mecanismo. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Página de lançamento do ActiveMQ 5.18• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Atualizando uma versão do mecanismo de agente do Amazon MQ• Usando arquivos de XML configuração do Spring
22 de julho de 2024	<p>O Amazon MQ agora oferece suporte a filas de quórum somente em corretores que usam a versão 3.13 e superior. As filas de quórum são um tipo de FIFO fila replicada que usa o algoritmo de consenso Raft para manter a consistência dos dados. As filas de quórum fornecem tratamento fraudulento de mensagens, o que pode ajudá-lo a gerenciar mensagens não processadas.</p> <p>Para começar a usar as filas de quórum, consulte. Filas de quórum para o RabbitMQ no Amazon MQ</p>
2 de julho de 2024	<p>O Amazon MQ para RabbitMQ agora oferece suporte ao RabbitMQ 3.13, uma versão secundária. Para todos os corretores que usam a versão 3.13 e superior do mecanismo, o Amazon MQ gerencia as atualizações para a versão de patch mais recente suportada durante a janela de manutenção. Para obter mais informações, consulte Atualizando uma versão do mecanismo de agente do Amazon MQ.</p> <p>Diretrizes de dimensionamento do Amazon MQ para RabbitMQ foram atualizados para incluir novos limites para filas, consumidores por canal e escavadeiras para corretores que usam a versão 3.13 do motor.</p>

Data	Atualização da documentação
	<p>Para obter mais informações sobre as correções e os recursos desta versão, consulte as notas de lançamento do RabbitMQ 3.13 no repositório do servidor RabbitMQ. GitHub</p> <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>
10 de junho de 2024	<p>O Amazon MQ agora está disponível na região Oeste do Canadá (Calgary) . Para obter informações sobre as regiões disponíveis, consulte Regiões e endpoints da AWS na Guia de Referência geral da AWS .</p>
10 de maio de 2024	<p>O calendário de suporte da versão Amazon MQ indica quando uma versão do broker Engine chega ao fim do suporte. Quando uma versão do mecanismo chega ao fim do suporte, o Amazon MQ atualiza automaticamente todos os corretores da versão para a próxima versão secundária compatível. O Amazon MQ avisa com pelo menos 90 dias de antecedência antes que uma versão do motor chegue ao fim do suporte.</p> <p>Para ver o calendário de suporte da versão e o fim do suporte, consulte o seguinte:</p> <ul style="list-style-type: none">• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ <p>Você também pode ativar atualizações automáticas de versões secundárias para que seu corretor atualize para a próxima versão do patch durante uma janela de manutenção. Para ter mais informações, consulte Atualizando uma versão do mecanismo de agente do Amazon MQ</p>

Data	Atualização da documentação
9 de maio de 2024	<p>O Amazon MQ para RabbitMQ agora oferece suporte ao RabbitMQ 3.12, uma versão secundária. Todos os corretores em 3.12.13 e superiores usam Classic Queues versão 2 (CQv2), e todas as filas em 3.12.13 e superiores se comportam como filas preguiçosas.</p> <p>Recomendamos que os corretores nas versões anteriores à 3.12.13 habilitem CQv2 e lazy queues ou atualizem para a versão mais recente do Amazon MQ para RabbitMQ.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.12 no repositório do servidor RabbitMQ. GitHub• Habilite o Classic Queue v2 para seu agente do RabbitMQ• Habilitar filas lazy <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>
4 de março de 2024	<p>O Amazon MQ para RabbitMQ agora oferece suporte ao RabbitMQ 3.11.28.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.11.28 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>

Data	Atualização da documentação
19 de janeiro de 2024	<p>O Amazon MQ para RabbitMQ não suporta o nome de usuário “convidado” e excluirá a conta de convidado padrão quando você criar um novo corretor. O Amazon MQ também excluirá periodicamente qualquer conta criada pelo cliente chamada “convidado”.</p>
15 de dezembro de 2023	<p>O Amazon MQ agora está disponível na região de Israel (Tel Aviv). Para obter informações sobre as regiões disponíveis, consulte Regiões e endpoints da AWS na Guia de Referência geral da AWS .</p>
11 de dezembro de 2023	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ 3.10.25.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.10.25 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>
26 de outubro de 2023	<p>O Amazon MQ lançou as versões secundárias mais recentes do ActiveMQ 5.15.16, 5.16.7, 5.17.6 com uma atualização importante. Descontinuamos as versões secundárias mais antigas do ActiveMQ e atualizaremos todos os agentes em todas as versões de 5.15 a 5.15.16 ou de 5.16 a 5.16.7 e de 5.17 a 5.17.6.</p> <p>Para receber mais informações sobre como atualizar o agente do ActiveMQ, consulte Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ.</p>

Data	Atualização da documentação
27 de setembro de 2023	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ 3.11.20.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.11.20 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>
27 de julho de 2023	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ 3.11.16.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.11.16 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>
27 de julho de 2023	<p>O Amazon MQ para RabbitMQ agora permite a criação e a aplicação de configurações ao agente do RabbitMQ.</p> <p>Para obter mais informações sobre como adicionar configurações ao agente, consulte RabbitMQ Broker Configurations.</p> <p>Para obter mais informações sobre esse atributo, consulte:</p> <ul style="list-style-type: none">• Políticas do operador• Mudanças nas políticas do operador

Data	Atualização da documentação
23 de junho de 2023	<p>O Amazon MQ agora é compatível com o ActiveMQ 5.17.3, uma nova versão secundária do mecanismo. Esta versão oferece suporte ao novo recurso de replicação de dados entre regiões (CRDR) do Amazon MQ.</p> <p>Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Para começar CRDR, consulte Replicação de dados entre regiões para o Amazon MQ for ActiveMQ o Guia do desenvolvedor.• Página da versão do ActiveMQ 5.17.3• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Atualizando uma versão do mecanismo de agente do Amazon MQ• Usando arquivos de XML configuração do Spring
21 de junho de 2023	<p>O Amazon MQ para ActiveMQ agora oferece um recurso de replicação de dados entre regiões (CRDR) que permite a replicação assíncrona de mensagens do agente principal em uma região primária para o agente de réplica em uma região de réplica. AWS Se o agente primário na região primária falhar, você poderá promover o agente de réplica na região secundária para primário iniciando uma transição ou um failover.</p> <p>Para começar CRDR, consulte Replicação de dados entre regiões para o Amazon MQ for ActiveMQ o Guia do desenvolvedor.</p>
18 de maio de 2023	<p>O Amazon MQ já está disponível nas seguintes regiões:</p> <ul style="list-style-type: none">• Ásia-Pacífico (Melbourne)• Ásia-Pacífico (Hyderabad)• Europa (Espanha)• Europa (Zurique) <p>Para obter informações sobre as regiões disponíveis, consulte Regiões e endpoints da AWS na Guia de Referência geral da AWS .</p>

Data	Atualização da documentação
14 de abril de 2023	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.9.27.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.9.27 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>
14 de abril de 2023	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.10.20.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.10.20 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>


Data	Atualização da documentação
31 de março de 2023	<p>O Amazon MQ para RabbitMQ desativou o RabbitMQ versão de mecanismo 3.10.17.</p> <p>A equipe do Amazon MQ para RabbitMQ e os mantenedores de código aberto do RabbitMQ identificaram um problema com o console de gerenciamento do RabbitMQ na versão 3.10.17. O Amazon MQ retirou essa versão. Para mitigar os impactos desse problema, crie outros agentes com a versão 3.10.20 enquanto trabalhamos para oferecer suporte a uma nova versão de patch do RabbitMQ. Recomendamos ativar a opção de atualização automática da versão secundária para obter automaticamente as últimas correções de erros, atualizações de segurança e aprimoramentos de desempenho.</p> <p>Para obter mais informações sobre as versões disponíveis do Amazon MQ para RabbitMQ, consulte Versões de mecanismo do Amazon MQ para RabbitMQ.</p>
1 de março de 2023	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.10.17.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.10.17 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>

Data	Atualização da documentação
21 de fevereiro de 2023	<p>O Amazon MQ para RabbitMQ agora se integra com AWS Key Management Service (KMS) para oferecer criptografia no lado do servidor. Agora você pode selecionar seu próprio cliente CMK gerenciado ou usar uma KMS chave AWS gerenciada em sua AWS KMS conta. Para obter mais informações, consulte Criptografia em repouso.</p> <p>O Amazon MQ oferece suporte ao uso de AWS KMS chaves das seguintes formas.</p> <ul style="list-style-type: none">• KMSChave de propriedade do Amazon MQ (padrão) — A chave pertence e é gerenciada pelo Amazon MQ e não está na sua conta.• AWS KMSChave gerenciada — A KMS chave AWS gerenciada (aws/mq) é uma KMS chave em sua conta que é criada, gerenciada e usada em seu nome pelo Amazon MQ.• Selecione a KMS chave gerenciada pelo cliente existente — As KMS chaves gerenciadas pelo cliente são criadas e gerenciadas por você em AWS Key Management Service (KMS).
13 de janeiro de 2023	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.8.34.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.8.34 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>

Data	Atualização da documentação
15 de dezembro de 2022	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.9.24.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.9.24 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>
13 de dezembro de 2022	<p>O Amazon MQ agora está disponível na região Oriente Médio (UAE). Para obter informações sobre as regiões disponíveis, consulte Regiões e endpoints da AWS na Guia de Referência geral da AWS .</p>
14 de novembro de 2022	<p>O Amazon MQ para RabbitMQ agora é compatível com a versão 3.10, uma versão principal do mecanismo. Agora você pode habilitar as filas clássicas versão 2 (CQv2) em suas filas do RabbitMQ. Não é possível fazer atualizações diretas da versão 3.8 para a 3.10. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.10.10• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>

Data	Atualização da documentação
9 de novembro de 2022	<p>O Amazon MQ agora é compatível com o ActiveMQ 5.17.2, uma nova versão secundária do mecanismo. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Página da versão do ActiveMQ 5.17.2• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Atualizando uma versão do mecanismo de agente do Amazon MQ• Usando arquivos de XML configuração do Spring
17 de agosto de 2022	<p>O Amazon MQ agora é compatível com o ActiveMQ 5.17.1, uma nova versão principal do mecanismo. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Página da versão do ActiveMQ 5.17.1• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Atualizando uma versão do mecanismo de agente do Amazon MQ• Usando arquivos de XML configuração do Spring
14 de julho de 2022	<p>O Amazon MQ agora é compatível com o ActiveMQ 5.16.5, uma versão secundária do mecanismo. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Página da versão do ActiveMQ 5.16.5• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Usando arquivos de XML configuração do Spring• Atualizando uma versão do mecanismo de agente do Amazon MQ
4 de maio de 2022	<p>O Amazon MQ contém linguagem inclusiva para o elemento <code>networkConnector</code> na configuração do agente.</p> <ul style="list-style-type: none">• Criar e configurar uma rede de agentes do Amazon MQ

Data	Atualização da documentação
25 de abril de 2022	<p>Amazon MQ Esta versão adiciona o estado do <code>CRITICAL_ACTION_REQUIRED</code> corretor e a <code>ActionRequired</code> API propriedade. <code>CRITICAL_ACTION_REQUIRED</code> informa quando seu corretor está degradado. <code>ActionRequired</code> fornece um código que você pode usar para encontrar instruções no Guia do Desenvolvedor sobre como resolver o problema.</p> <ul style="list-style-type: none">• Solução de problemas• ActionRequired documentação na Referência do Amazon MQ API.
20 de abril de 2022	<p>O Amazon MQ agora é compatível com o ActiveMQ 5.16.4, uma nova versão secundária do mecanismo. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Página da versão do ActiveMQ 5.16.4• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Usando arquivos de XML configuração do Spring• Atualizando uma versão do mecanismo de agente do Amazon MQ
1º de março de 2022	<p>O Amazon MQ agora está disponível na região Ásia-Pacífico (Jacarta). Para obter informações sobre as regiões disponíveis, consulte Regiões e endpoints da AWS na Guia de Referência geral da AWS .</p>
25 de fevereiro de 2022	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.8.27.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.8.27 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>

Data	Atualização da documentação
16 de fevereiro de 2022	<p>O Amazon MQ agora está disponível na Região da África (Cidade do Cabo). Para obter informações sobre as regiões disponíveis, consulte Regiões e endpoints da AWS na Guia de Referência geral da AWS .</p>
14 de fevereiro de 2022	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.9.13. Atualizações da versão secundária automáticas não podem ser usadas para atualizar do Rabbit 3.8 para 3.9. Para isso, atualize manualmente seu agente.</p> <p>Para obter mais informações sobre os novos recursos introduzidos no RabbitMQ 3.9, consulte a página de notas de lançamento da versão 3.9.0 no site. GitHub</p> <div data-bbox="402 800 1507 1016"><p> Note</p><p>Atualmente, o Amazon MQ não oferece suporte a streams ou o uso de login estruturadoJSON, introduzido no RabbitMQ 3.9.</p></div> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.9.13 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>


Data	Atualização da documentação
07 de fevereiro de 2022	<p>O Amazon MQ for RabbitMQ apresenta novas métricas de agente, permitindo que você monitore a utilização média de recursos em todos os três nós em uma implantação de cluster.</p> <p>Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• the section called “Métricas para RabbitMQ”
18 de janeiro de 2022	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.8.26.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.8.26 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>
13 de janeiro de 2022	<p>O Amazon MQ introduz o código de status RABBITMQ_MEMORY_ALARM para informar você quando seu agente gerou um alarme de alta memória e se encontra em estado não íntegro. O Amazon MQ fornece informações detalhadas e recomendações para ajudar você a diagnosticar, solucionar e evitar alarmes de alta memória. Para obter mais informações, consulte:</p> <ul style="list-style-type: none">• the section called “RABBITMQ_MEMORY_ALARM”

Data	Atualização da documentação
6 de janeiro de 2022	<p>Quando você configura o CloudWatch Logs for Amazon MQ para agentes do ActiveMQ, o Amazon MQ suporta o uso das chaves de contexto de condição global aws:SourceAccount e aws:SourceArn das chaves de contexto em políticas baseadas IAM em recursos para evitar o problema confuso do deputado. Para obter mais informações, consulte:</p> <ul style="list-style-type: none">• the section called “Prevenção contra o ataque do “substituto confuso” em todos os serviços”
20 de dezembro de 2021	<p>O Amazon MQ for ActiveMQ introduz um conjunto de novas métricas, permitindo que você monitore o número máximo de conexões que pode fazer com seu agente usando diferentes protocolos de transporte com suporte, bem como uma nova métrica adicional que permite monitorar o número de nós conectados ao seu agente em uma rede de agentes. Para obter mais informações, consulte:</p> <ul style="list-style-type: none">• the section called “Métricas do ActiveMQ”
16 de novembro de 2021	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.8.23.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.8.23 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ.</p>

Data	Atualização da documentação
12 de outubro de 2021	<p>O Amazon MQ agora é compatível com o ActiveMQ 5.16.3, uma nova versão secundária do mecanismo. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Página da versão do ActiveMQ 5.16.3• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Atualizando uma versão do mecanismo de agente do Amazon MQ• Usando arquivos de XML configuração do Spring
8 de setembro de 2021	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.8.22.</p> <p>Esta versão inclui uma correção para um problema com filas usando por mensagem TTL (tempo de vida), identificado na versão anteriormente suportada, RabbitMQ 3.8.17. Recomendamos atualizar seus agentes existentes para a versão 3.8.22.</p> <p>Para obter mais informações sobre as correções e recursos nesta versão, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.8.22 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ <p>Para obter mais informações sobre as versões compatíveis do Amazon MQ for RabbitMQ e atualizações de agentes, consulte Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ</p>
25 de agosto de 2021	<p>O Amazon MQ para RabbitMQ desativou temporariamente a versão 3.8.17 do mecanismo RabbitMQ devido a um problema identificado com filas usando <code>por mensagem ()</code>. <code>time-to-live TTL</code> Recomendamos usar a versão 3.8.11.</p>

Data	Atualização da documentação
29 de julho de 2021	<p>O Amazon MQ para RabbitMQ agora é compatível com o RabbitMQ versão 3.8.17. Para obter mais informações sobre as correções e recursos contidos nesta atualização, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.8.17 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ• Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ
16 de julho de 2021	<p>Agora você pode ajustar a janela de manutenção de um agente do Amazon MQ usando o AWS Management Console AWS CLI, ou o Amazon MQ. API Para saber mais sobre as janelas de manutenção do agente, consulte o seguinte.</p> <ul style="list-style-type: none">• Programando a janela de manutenção para um agente Amazon MQ
6 de julho de 2021	<p>O Amazon MQ para RabbitMQ oferece compatibilidade com o tipo de troca Consistent Hash. As trocas de hash consistentes fazem o roteamento de mensagens para filas com base em um valor de hash calculado a partir da routing key (chave de roteamento) de uma mensagem. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Plugin de troca de hash consistente• Tipo de troca de hash consistente do RabbitMQ no repositório do RabbitMQ GitHub
7 de junho de 2021	<p>O Amazon MQ agora é compatível com o ActiveMQ 5.16.2, uma nova versão principal do mecanismo. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Página da versão do ActiveMQ 5.16.2• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Atualizando uma versão do mecanismo de agente do Amazon MQ• Usando arquivos de XML configuração do Spring

Data	Atualização da documentação
26 de maio de 2021	O Amazon MQ para RabbitMQ agora está disponível nas regiões China (Pequim) e China (Ningxia). Para obter informações sobre regiões disponíveis, consulte AWS Regiões e endpoints .
18 de maio de 2021	<p>O Amazon MQ para RabbitMQ implementa os padrões do agente.</p> <p>Quando você cria um agente pela primeira vez, o Amazon MQ cria um conjunto de políticas de agente e limites de vhost com base no tipo de instância e no modo de implantação escolhidos, a fim de otimizar a performance do agente. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Padrões de agentes do Amazon MQ for RabbitMQ
5 de maio de 2021	<p>O Amazon MQ agora é compatível com o ActiveMQ 5.15.15. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Página da versão do ActiveMQ 5.15.15• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Usando arquivos de XML configuração do Spring
5 de maio de 2021	<p>O Amazon MQ começou a monitorar as alterações nas políticas AWS gerenciadas. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• the section called “AWS políticas gerenciadas”
14 de abril de 2021	O Amazon MQ agora está disponível nas regiões China (Pequim) e China (Ningxia). Para obter informações sobre regiões disponíveis, consulte AWS Regiões e endpoints .


Data	Atualização da documentação
7 de abril de 2021	<p>O Amazon MQ agora é compatível com o RabbitMQ 3.8.11. Para obter mais informações sobre as correções e recursos contidos nesta atualização, consulte:</p> <ul style="list-style-type: none">• Notas de lançamento do RabbitMQ 3.8.11 no repositório do servidor RabbitMQ GitHub• Log de alterações do RabbitMQ• Gerenciando o Amazon MQ para versões do mecanismo RabbitMQ
1.º de abril de 2021	<p>O Amazon MQ agora está disponível na região Ásia-Pacífico (Osaka). Para obter mais informações sobre as regiões e os endpoints disponíveis consulte Regiões e endpoints do Amazon MQ.</p>
21 de dezembro de 2020	<p>O Amazon MQ agora é compatível com o ActiveMQ 5.15.14. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Notas de lançamento do ActiveMQ 5.15.14• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Usando arquivos de XML configuração do Spring• <div data-bbox="431 1115 1508 1430" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Devido a um problema conhecido do Apache ActiveMQ nesta versão, o novo botão Pausar Fila no console da Web ActiveMQ não pode ser usado com o Amazon MQ para agentes ActiveMQ. Para obter mais informações sobre esse problema, consulte AMQ-8104.</p></div>

Data	Atualização da documentação
4 de novembro de 2020	<p>O Amazon MQ agora é compatível com o RabbitMQ, o popular agente de mensagens de código aberto. Isso permite que você migre seus agentes de mensagens existentes do RabbitMQ AWS sem precisar reescrever o código.</p> <p>O Amazon MQ para RabbitMQ gerencia agentes de mensagens individuais e em cluster e lida com tarefas como provisionamento da infraestrutura, configuração do agente e atualização do software.</p> <ul style="list-style-type: none">• O Amazon MQ é compatível com o RabbitMQ 3.8.6. Para obter mais informações sobre as versões de engine compatíveis, consulte the section called “Gerenciamento de versão”.• O AWS Nível gratuito inclui até 750 horas de uma única instância de <code>agentmq.t3.micro</code> e até 20GB de armazenamento por mês durante um ano. Para obter mais informações sobre os tipos de instâncias compatíveis, consulte Broker instance types.• Com o Amazon MQ para RabbitMQ, você pode acessar seus corretores usando AMQP 0-9-1 e com qualquer linguagem suportada pelas bibliotecas de cliente do RabbitMQ. Para obter mais informações sobre protocolos e portas compatíveis, consulte the section called “Amazon MQ para protocolos RabbitMQ”.• O Amazon MQ para RabbitMQ está disponível em todas as regiões em que o Amazon MQ está disponível no momento. Para saber mais sobre todas as regiões disponíveis, consulte a AWS Tabela de região. <p>Para começar a usar o Amazon MQ, criar um agente e conectar um aplicativo JVM baseado ao seu agente RabbitMQ, consulte Começando: Criando e conectando-se a um corretor RabbitMQ</p>
22 de outubro de 2020	<p>O Amazon MQ é compatível com o ActiveMQ 5.15.13. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Notas de lançamento do ActiveMQ 5.15.13• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Usando arquivos de XML configuração do Spring

Data	Atualização da documentação
30 de setembro de 2020	O Amazon MQ agora está disponível na Região da Europa (Milão). Para obter mais informações sobre as regiões e os endpoints disponíveis consulte Regiões e endpoints do Amazon MQ .
27 de julho de 2020	Você pode autenticar usuários do Amazon MQ usando as credenciais armazenadas no seu Active Directory ou em outro servidor. LDAP Você também pode adicionar, excluir e modificar usuários do Amazon MQ e atribuir permissões a tópicos e filas. Para obter mais informações, consulte Integrar LDAP com ActiveMQ .
17 de julho de 2020	O Amazon MQ agora é compatível com o tipo de instância <code>mq.t3.micro</code> . Para obter mais informações, consulte Broker instance types .
30 de junho de 2020	O Amazon MQ é compatível com o ActiveMQ 5.15.12. Para obter mais informações, consulte as informações a seguir: <ul style="list-style-type: none">• Notas de lançamento do ActiveMQ 5.15.12• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Usando arquivos de XML configuração do Spring

Data	Atualização da documentação
30 de abril de 2020	<p>O Amazon MQ é compatível com um novo elemento da coleção filho, <code>systemUsage</code>, no elemento <code>broker</code>. Para obter mais informações, consulte systemUsage.</p> <p>O Amazon MQ também é compatível com três novos atributos no <code>kahaDB</code> elemento filho.</p> <ul style="list-style-type: none">• <code>journalDiskSyncInterval</code> — intervalo (ms) para quando executar uma sincronização de disco se <code>journalDiskSyncStrategy=periodic</code>.• <code>journalDiskSyncStrategy</code> — configura a política de sincronização de disco.• <code>preallocationStrategy</code> — configura como o agente tentará pré-alocar os arquivos do diário quando um novo arquivo do diário for necessário. <p>Para obter mais informações, consulte Atributos.</p>
3 de março de 2020	<p>O Amazon MQ oferece suporte a duas novas métricas CloudWatch</p> <ul style="list-style-type: none">• <code>TempPercentUsage</code> — a porcentagem de armazenamento temporário disponível usada por mensagens não persistentes.• <code>JobSchedulerStorePercentUsage</code> — A porcentagem de espaço em disco usada pelo armazenamento do programador de trabalhos. <p>Para obter mais informações, consulte Monitoring and logging Amazon MQ brokers.</p>
4 de fevereiro de 2020	<p>O Amazon MQ está disponível nas regiões Ásia-Pacífico (Hong Kong) e Oriente Médio (Bahrein) Para obter informações sobre regiões disponíveis, consulte AWS Regiões e endpoints.</p>

Data	Atualização da documentação
22 de janeiro de 2020	<p>O Amazon MQ é compatível com o ActiveMQ 5.15.10. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Notas de lançamento do ActiveMQ 5.15.10• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Usando arquivos de XML configuração do Spring
19 de dezembro de 2019	<p>O Amazon MQ está disponível nas regiões Europa (Estocolmo) e América do Sul (São Paulo) Para obter informações sobre regiões disponíveis, consulte AWS Regiões e endpoints.</p>

Data	Atualização da documentação
16 de dezembro de 2019	<p>O Amazon MQ oferece suporte à criação de corretores com taxa de transferência otimizada usando o Amazon Elastic Block Store (EBS) — em vez do Amazon Elastic File System (Amazon) padrão — para armazenamento de corretores. Para aproveitar a alta durabilidade e a replicação em várias zonas de disponibilidade, use a AmazonEFS. Para aproveitar a baixa latência e a alta taxa de transferência, use a Amazon. EBS</p> <div data-bbox="402 541 1507 1087" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; background-color: #fff9f9;"> <p> Important</p> <ul style="list-style-type: none"> • Você pode usar a Amazon EBS somente com a família de tipos de instância do mq.m5 broker. • Embora você possa alterar o tipo de instância de agente, você não pode alterar o tipo de armazenamento do agente depois de criar o agente. • A Amazon EBS replica dados dentro de uma única zona de disponibilidade e não suporta o modo de implantação ativo/em espera do ActiveMQ. </div> <p>Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none"> • Storage • Escolha o tipo de armazenamento de agente correto para obter a melhor taxa de transferência • A <code>storageType</code> propriedade do broker-instance-operations recurso na Referência do Amazon MQ REST API • As métricas <code>BurstBalance</code>, <code>VolumeReadOps</code> e <code>VolumeWriteOps</code> na seção Monitoring and logging Amazon MQ brokers.
18 de outubro de 2019	<p>Duas CloudWatch métricas da Amazon estão disponíveis: <code>TotalEnqueueCount</code> e <code>TotalDequeueCount</code>. Para obter mais informações, consulte Monitoring and logging Amazon MQ brokers</p>

Data	Atualização da documentação
11 de outubro de 2019	<p>O Amazon MQ agora oferece suporte a endpoints em conformidade com o Padrão Federal de Processamento de Informações 140-2 (FIPS) nas regiões comerciais dos EUA.</p> <p>Para obter mais informações, consulte:</p> <ul style="list-style-type: none">• Padrão Federal de Processamento de Informações (FIPS) 140-2• Regiões e endpoints do Amazon MQ
30 de setembro de 2019	<p>Agora o Amazon MQ inclui a capacidade de escalar os agentes alterando o tipo de instância do host. Para obter mais informações, consulte a propriedade de <code>hostInstanceType</code> de UpdateBrokerInput e a propriedade <code>pendingHostInstanceType</code> de DescribeBrokerOutput.</p>
30 de agosto de 2019	<p>Agora é possível atualizar os grupos de segurança associados a um agente, tanto no console quanto no UpdateBrokerInput.</p>
22 de julho de 2019	<p>O Amazon MQ se integra com AWS Key Management Service (KMS) para oferecer criptografia no lado do servidor. Agora você pode selecionar seu próprio cliente CMK gerenciado ou usar uma KMS chave AWS gerenciada em sua AWS KMS conta. Para obter mais informações, consulte Criptografia em repouso.</p> <p>O Amazon MQ oferece suporte ao uso de AWS KMS chaves das seguintes formas.</p> <ul style="list-style-type: none">• AWS KMSchave própria — A chave é de propriedade do Amazon MQ e não está na sua conta.• AWS KMSchave gerenciada — A KMS chave AWS gerenciada (<code>aws/mq</code>) é uma KMS chave na sua conta que é criada, gerenciada e usada em seu nome pelo Amazon MQ.• Selecione o cliente existente gerenciado CMK — CMKs Os gerenciados pelo cliente são criados e gerenciados por você em AWS Key Management Service (KMS).

Data	Atualização da documentação
19 de junho de 2019	<p>O Amazon MQ está disponível nas regiões Europa (Paris) e Ásia-Pacífico (Mumbai). Para obter informações sobre regiões disponíveis, consulte AWS Regiões e endpoints.</p>
12 de junho de 2019	<p>O Amazon MQ está disponível na região Canadá (Central). Para obter informações sobre regiões disponíveis, consulte AWS Regiões e endpoints.</p>
3 de junho de 2019	<p>Duas novas CloudWatch métricas da Amazon estão disponíveis: <code>EstablishedConnectionsCount</code> e <code>InactiveDurableSubscribers</code>. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Monitoring and logging Amazon MQ brokers• Monitoring and logging Amazon MQ brokers
10 de maio de 2019	<p>O armazenamento de dados para novos tipos de instância <code>mq.t2.micro</code> é limitado a 20 GB. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• the section called “Armazenamento de dados”• Broker instance types
29 de abril de 2019	<p>Agora você pode usar políticas baseadas em tags e permissões no nível de recursos. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Como o Amazon MQ funciona com IAM• Permissões no nível do recurso suportadas para ações de API do Amazon MQ
16 de abril de 2019	<p>Agora você pode recuperar informações sobre o mecanismo do corretor e as opções de instância do corretor usando o REST API. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Opções de instâncias de agente• Tipos de mecanismo de agente



Data	Atualização da documentação
8 de abril de 2019	<p>O Amazon MQ é compatível com o ActiveMQ 5.15.9. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Notas de lançamento do ActiveMQ 5.15.9• Gerenciar as versões do mecanismo do Amazon MQ para ActiveMQ• Usando arquivos de XML configuração do Spring
4 de março de 2019	<p>A documentação para configurar o failover dinâmico e o rebalanceamento de clientes para uma rede de agentes foi aprimorada. Habilite o failover dinâmico configurando as opções de configuração do <code>transportConnectors</code> com <code>networkConnectors</code>. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Failover dinâmico com conectores de transporte• Rede de corretores Amazon MQ• Amazon MQ Broker Configuration Parameters
27 de fevereiro de 2019	<p>O Amazon MQ está disponível na região Europa (Londres), além das seguintes regiões:</p> <ul style="list-style-type: none">• Ásia-Pacífico (Singapura)• Leste dos EUA (Ohio)• Leste dos EUA (N. da Virgínia)• Oeste dos EUA (N. da Califórnia)• Oeste dos EUA (Oregon)• Ásia-Pacífico (Tóquio)• Ásia-Pacífico (Seul)• Ásia-Pacífico (Sydney)• Europa (Frankfurt)• Europa (Irlanda)
24 de janeiro de 2019	<p>Agora, a configuração padrão inclui uma política para eliminar destinos inativos.</p>



Data	Atualização da documentação
17 de janeiro de 2019	Agora os tipos de instância <code>mq.t2.micro</code> do Amazon MQ são compatíveis somente com 100 conexões por protocolo de nível de conexão. Para obter mais informações, consulte Quotas in Amazon MQ .
19 de dezembro de 2018	<p>Você pode configurar uma série de agentes do Amazon MQ em uma rede de agentes. Para obter mais informações, consulte as seções a seguir:</p> <ul style="list-style-type: none"> • Rede de corretores Amazon MQ • Creating and Configuring a Network of Brokers • Configurar sua rede de agentes corretamente • networkConnector • networkConnectionStartAssíncrono
11 de dezembro de 2018	<p>O Amazon MQ é compatível com o ActiveMQ 5.15.8, 5.15.6 e 5.15.0.</p> <ul style="list-style-type: none"> • Bugs resolvidos e melhorias no ActiveMQ: <ul style="list-style-type: none"> • Notas de lançamento do ActiveMQ 5.15.8 • Notas de lançamento do ActiveMQ 5.15.7
5 de dezembro de 2018	AWS oferece suporte à marcação de recursos para ajudar a monitorar sua alocação de custos. É possível etiquetar recursos ao criá-los ou visualizando os detalhes do recurso. Para obter mais informações, consulte Etiquetar recursos .
19 de novembro de 2018	AWS expandiu seu programa de SOC conformidade para incluir o Amazon MQ como um serviço SOCcompatível .
15 de outubro de 2018	<ul style="list-style-type: none"> • O número máximo de grupos por usuário é 20. Para obter mais informações, consulte Usuários. • O número máximo de conexões por agente, por protocolos de nível de conexão é 1.000. Para obter mais informações, consulte Operadores.
2 de outubro de 2018	AWS expandiu seu programa de HIPAA conformidade para incluir o Amazon MQ como um serviço HIPAAqualificado .

Data	Atualização da documentação
27 de setembro de 2018	<p>O Amazon MQ é compatível com ActiveMQ 5.15.6, além do 5.15.0. Para obter mais informações, consulte as informações a seguir.</p> <ul style="list-style-type: none">• Começando: Criando e conectando-se a um corretor ActiveMQ• Bugs resolvidos e melhorias na documentação do ActiveMQ:<ul style="list-style-type: none">• Notas de lançamento do ActiveMQ 5.15.6• Notas de lançamento do ActiveMQ 5.15.5• Notas de lançamento do ActiveMQ 5.15.4• Notas de lançamento do ActiveMQ 5.15.3• Notas de lançamento do ActiveMQ 5.15.2• Notas de lançamento do ActiveMQ 5.15.1• Cliente ActiveMQ 5.15.6
31 de agosto de 2018	<ul style="list-style-type: none">• As seguintes métricas estão disponíveis:<ul style="list-style-type: none">• <code>CurrentConnectionsCount</code>• <code>TotalConsumerCount</code>• <code>TotalProducerCount</code> <p>Para obter mais informações, consulte a seção Monitoring and logging Amazon MQ brokers.</p> <ul style="list-style-type: none">• O endereço IP do agente é exibido na página Detalhes. <div data-bbox="431 1325 1508 1545" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;"><p> Note</p><p>Para agentes com acessibilidade pública desabilitada, o endereço IP interno é exibido.</p></div>

Data	Atualização da documentação
30 de agosto de 2018	<p>O Amazon MQ está disponível na região Ásia-Pacífico (Singapura), além das seguintes regiões:</p> <ul style="list-style-type: none">• Leste dos EUA (Ohio)• Leste dos EUA (N. da Virgínia)• Oeste dos EUA (N. da Califórnia)• Oeste dos EUA (Oregon)• Ásia-Pacífico (Tóquio)• Ásia-Pacífico (Seul)• Ásia-Pacífico (Sydney)• Europa (Frankfurt)• Europa (Irlanda)
30 de julho de 2018	<p>Você pode configurar o Amazon MQ para publicar registros gerais e de auditoria no Amazon CloudWatch Logs. Para obter mais informações, consulte Monitoring and logging Amazon MQ brokers.</p>
25 de julho de 2018	<p>O Amazon MQ está disponível nas regiões Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Seul), além das seguintes regiões:</p> <ul style="list-style-type: none">• Leste dos EUA (Ohio)• Leste dos EUA (N. da Virgínia)• Oeste dos EUA (N. da Califórnia)• Oeste dos EUA (Oregon)• Ásia-Pacífico (Sydney)• Europa (Frankfurt)• Europa (Irlanda)
19 de julho de 2018	<p>Você pode usar AWS CloudTrail para registrar chamadas do Amazon MQAPI. Para obter mais informações, consulte Logging Amazon MQ API calls using CloudTrail.</p>

Data	Atualização da documentação
29 de junho de 2018	<p>Além de <code>mq.t2.micro</code> e <code>mq.m4.large</code>, os seguintes tipos de instância de agente estão disponíveis para workloads normais de desenvolvimento, teste e produção que exigem uma alta taxa de transferência:</p> <ul style="list-style-type: none">• <code>mq.m5.large</code>• <code>mq.m5.xlarge</code>• <code>mq.m5.2xlarge</code>• <code>mq.m5.4xlarge</code> <p>Para obter mais informações, consulte Broker instance types.</p>
27 de junho de 2018	<p>O Amazon MQ está disponível na região Oeste dos EUA (Norte da Califórnia), além das seguintes regiões:</p> <ul style="list-style-type: none">• Leste dos EUA (Ohio)• Leste dos EUA (N. da Virgínia)• Oeste dos EUA (Oregon)• Ásia-Pacífico (Sydney)• Europa (Frankfurt)• Europa (Irlanda)

Data	Atualização da documentação
14 de junho de 2018	<ul style="list-style-type: none"> • Você pode usar o AWS::Amazon MQ::Broker AWS CloudFormation recurso para realizar as seguintes ações: <ul style="list-style-type: none"> • Criar um agente. • Adicionar alterações de configuração ou modificar usuários para o agente. • Retornar informações sobre o agente especificado. • Excluir o agente especificado. <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>Quando você altera qualquer propriedade do tipo de propriedade Amazon MQ Broker ConfigurationId ou Amazon MQ Broker User, o broker é reiniciado imediatamente.</p> </div> <ul style="list-style-type: none"> • Você pode usar o AWS::Amazon MQ::Configuration AWS CloudFormation recurso para realizar as seguintes ações: <ul style="list-style-type: none"> • Criar uma configuração. • Atualizar a configuração especificada. • Retornar informações sobre a configuração especificada. <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>Você pode usar AWS CloudFormation para modificar, mas não excluir, uma configuração do Amazon MQ.</p> </div>
7 de junho de 2018	O console do Amazon MQ é compatível com alemão, português do Brasil, espanhol, italiano e chinês tradicional.
17 de maio de 2018	O limite do número de usuários por agente é de 250. Para obter mais informações, consulte Usuários .
13 de março de 2018	A criação de um agente leva cerca de 15 minutos. Para obter mais informações, consulte Concluir a criação do agente .

Data	Atualização da documentação
1º de março de 2018	<ul style="list-style-type: none">• Você pode configurar o armazenamento e a expedição simultâneos para o Apache KahaDB usando o atributo concurrentStoreAndDispatchQueues .• A CpuCreditBalance CloudWatch métrica > está disponível para o tipo de instância do mq.t2.micro broker.
10 de janeiro de 2018	<p>As alterações a seguir afetam o console do Amazon MQ:</p> <ul style="list-style-type: none">• Na lista de agentes, a coluna Creation (Criação) é oculta por padrão. Para personalizar o tamanho da página e as colunas, selecione  .• Sobre o MyBroker página, na seção Conexões, escolhendo o nome do seu grupo de segurança ou  abrindo o EC2 console (em vez do VPC console). O EC2 console permite uma configuração mais intuitiva das regras de entrada e saída. Para obter mais informações, consulte a seção Habilitar conexões de entrada atualizada.
9 de janeiro de 2018	<ul style="list-style-type: none">• A permissão para REST a ID de operação UpdateBroker está listada corretamente como mq:UpdateBroker no IAM console.• A mq:DescribeEngine permissão incorreta é removida do console. IAM

Data	Atualização da documentação
28 de novembro de 2017	<p>Esta é a versão inicial do Amazon MQ e do Guia do Desenvolvedor do Amazon MQ.</p> <ul style="list-style-type: none">• O Amazon MQ está disponível nas seguintes regiões:<ul style="list-style-type: none">• Leste dos EUA (Ohio)• Leste dos EUA (N. da Virgínia)• Oeste dos EUA (Oregon)• Ásia-Pacífico (Sydney)• Europa (Frankfurt)• Europa (Irlanda) <p>O uso do tipo de <code>mq.t2.micro</code> instância está sujeito a CPUcréditos e desempenho básico, com a capacidade de ultrapassar o nível básico (para obter mais informações, consulte a métrica). CpuCreditBalance Se a sua aplicação exigir performance fixa, considere usar um tipo de instância <code>mq.m5.large</code> .</p> <ul style="list-style-type: none">• Você pode criar agentes <code>mq.m4.large</code> e <code>mq.t2.micro</code> . <p>O uso do tipo de <code>mq.t2.micro</code> instância está sujeito a CPUcréditos e desempenho básico, com a capacidade de ultrapassar o nível básico (para obter mais informações, consulte a métrica). CpuCreditBalance Se a sua aplicação exigir performance fixa, considere usar um tipo de instância <code>mq.m5.large</code> .</p> <ul style="list-style-type: none">• Você pode usar o mecanismo de agente ActiveMQ 5.15.0.• Você também pode criar e gerenciar corretores de forma programática usando o Amazon MQ e RESTAPI AWS SDKs• Você pode acessar seus corretores usando qualquer linguagem de programação compatível com o ActiveMQ e TLS habilitando explicitamente os seguintes protocolos:<ul style="list-style-type: none">• AMQP• MQTT• MQTTterminado WebSocket• OpenWire

Data	Atualização da documentação
	<ul style="list-style-type: none">• STOMP• STOMPterminado WebSocket• Você pode se conectar a agentes do ActiveMQ usando vários clientes de ActiveMQ. Recomendamos usar o Cliente ActiveMQ. Para obter mais informações, consulte Connecting a Java application to your broker.• Seu agente pode enviar e receber mensagens de qualquer tamanho.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.