Qpid Dispatch Router (QDR) Access Policy

Table of Contents

Introduction

Qpid Dispatch Router (QDR) access policy (Policy) is an optional authorization mechanism enforcing

- Per-router total and per-application user connection limits.
- Per-user, per-application resource limits.

Connection Limits

Policy enforces a total connection limit.

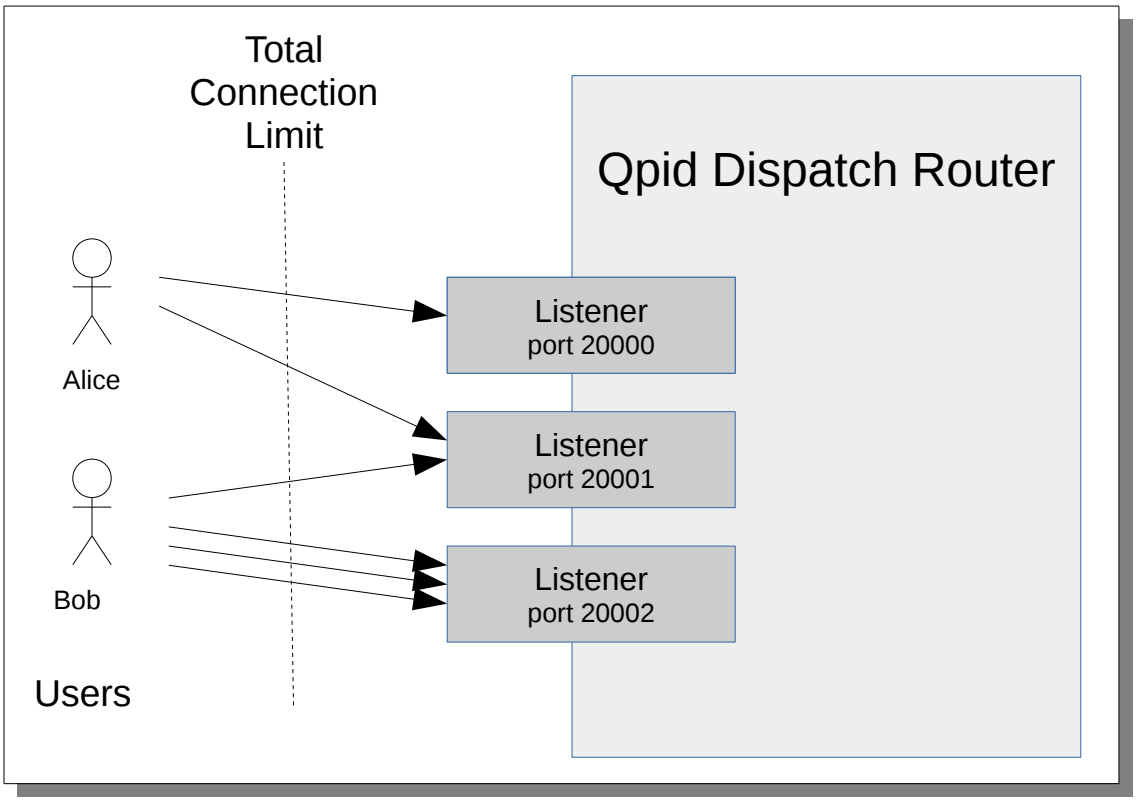

Figure 1 – Policy Total Connection Limit

The Total Connection Limit enforces a maximum number of user connections to the QDR service connectors. This limit protects against file descriptor resource exhaustion.

Policy enforces per-application connection limits.

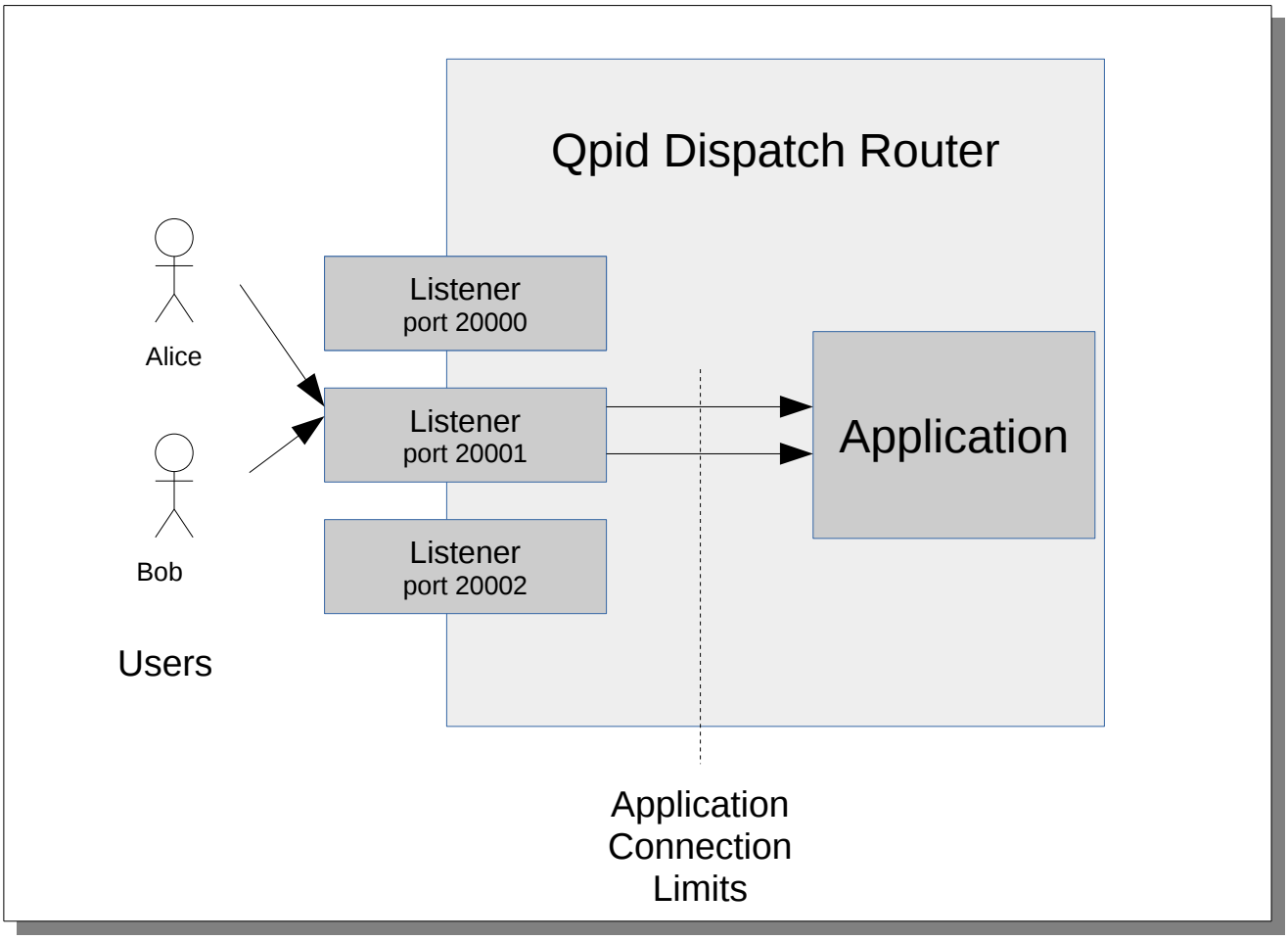

Figure 2 – Policy Application Connection Limits

The Application Connection Limits enforce a maximum number of user connections that the QDR will allow to a given application. Several limits may be specified.

Application Connection Limit	**Enforces**
maximumConnections	The total number of connections allowed regardless of source.
maximumConnectionsPerUser	The total number of connections allowed for a given authenticated user regardless of which remote host the user is connecting from.
maximumConnectionsPerHost	The total number of connections allowed from a remote host regardless of which user is originating the connection.

Table 1 – Policy Application Connection Limits

Resource Limits

If an authenticated user is allowed to connect to an application then the connection is subject to further restrictions.

Application Resource Limit	Enforces
maxFrameSize	Largest frame that may be sent on this connection. (AMQP Open, max-frame-size)
maxMessageSize	Largest message size supported by links created on this connection. (AMQP Attach, max-message-size)
maxSessionWindow	Largest incoming and outgoing window for sessions created on this connection. (AMQP Begin, incoming-window, outgoing-window)
maxSessions	Maximum number of sessions that may be created on this connection. (AMQP Open, channel-max)
maxSenders	Maximum number of sending links that may be created on this connection.
maxReceivers	Maximum number of receiving links that may be created on this connection.
allowDynamicSrc	This connection is allowed to use the dynamic link source feature.
allowAnonymousSender	This connection is allowed to use the Anonymous Sender feature.
sources	List of Source addresses allowed when creating receiving links.
targets	List of Target addresses allowed when creating sending links.

Table 2 – Policy Application Resource Limits

Policy Enforcement

Total Connection Limit

The total connection limit is enforced at a low level in QDR when a TCP socket is being opened. The same limit value applies to all user connections from any remote host. If the total connection limit is reached then the socket is simply closed.

Note that the total connection limit applies only to incoming user network connections. The limit does not apply to outbound connections created by QDR nor to inter-router connections.

Application Resource Limits

Application resource limits are applied later in the AMQP protocol processing starting with the reception of an AMQP Open performative. The following illustration shows an incoming connection.

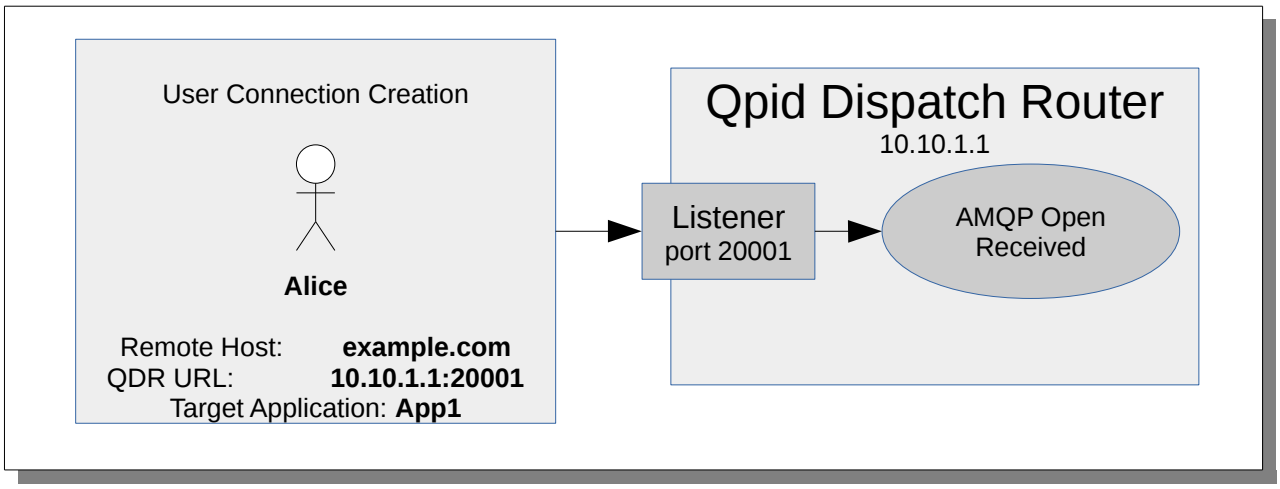

Figure 3 – User Connection Creation

In this example remote user ***Alice*** on system example.com (***93.184.216.34***) opens a connection to the Qpid Dispatch Router at URL 10.10.1.1:20001. The hostname field of the AMQP Open, in this case ***App1***, identifies the application targeted by this connection. When QDR receives the AMQP Open the following information is known:

Open Received	**Value Source**	**Value**
Remote Host	TCP socket peer	**93.184.216.34**
Authenticated User	SASL user name	**Alice**
QDR Application	AMQP Open hostname field	**App1**

Table 3 – AMQP Open Received information known by QDR

Application Resource Limits are enforced in two stages. First the connection must be approved. If the connection is disapproved then QDR closes the AMQP connection. If approved then QDR looks up the resource policy for the connection. When that is discovered then the connection may proceed using the associated Application Resource Limits.

Connection Approval

With no Policy in place QDR simply forwards client AMQP Open requests to the router network.

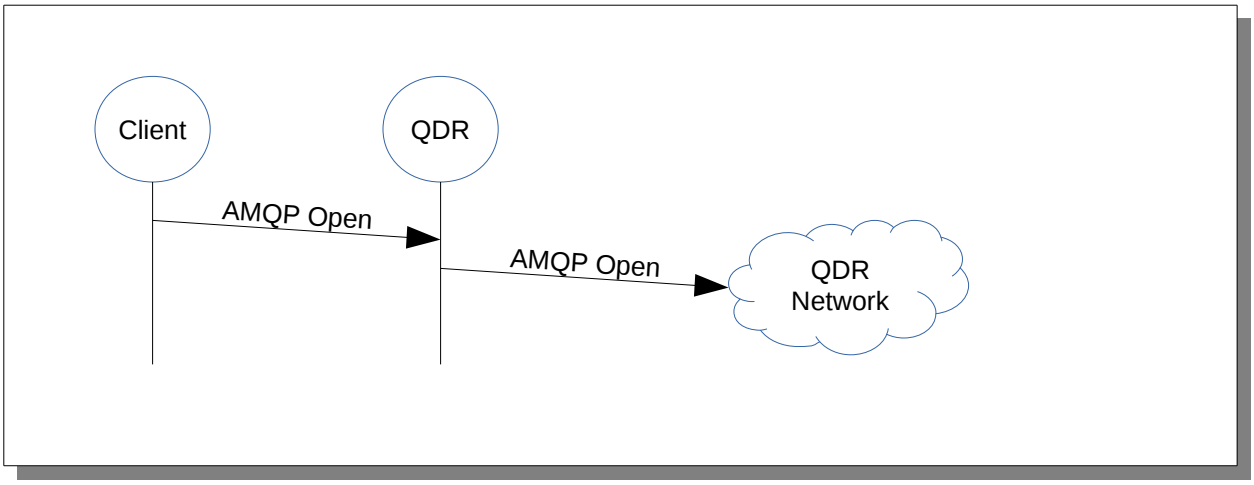

Figure 4 – AMQP Open Forwarding with No Policy Approval

With Policy enforcement QDR intercepts the AMQP Open and queries Policy for approval.

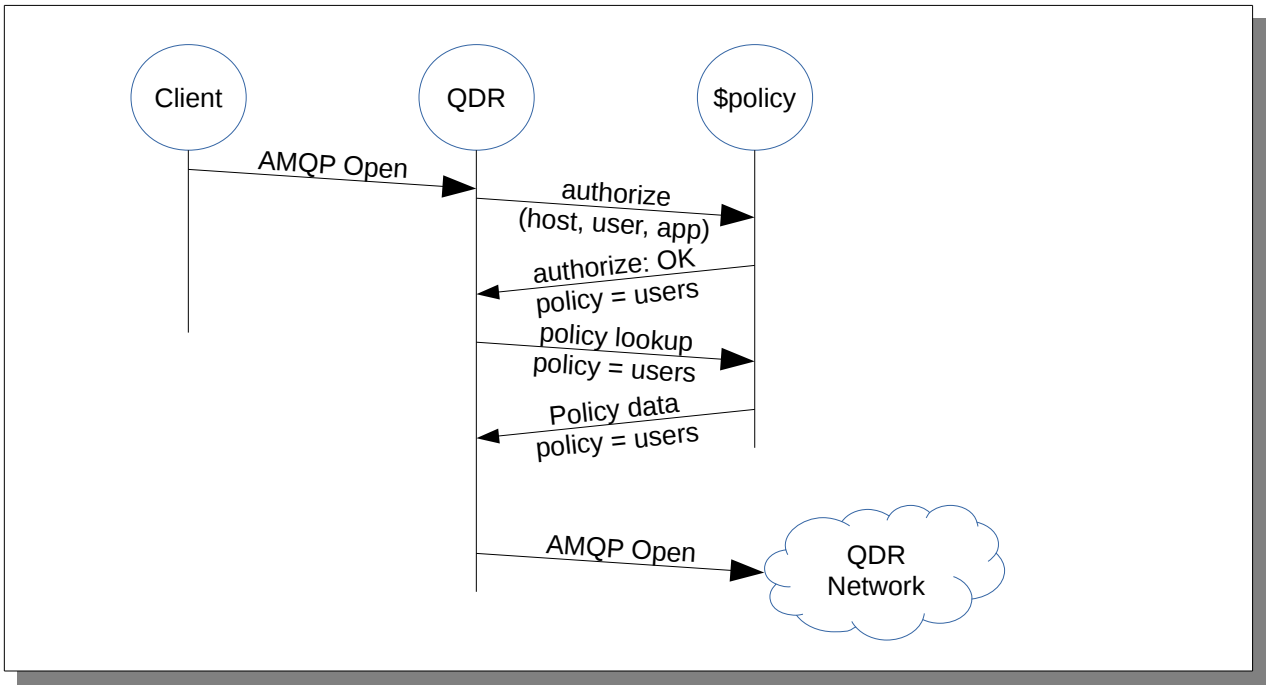

Figure 5 – AMQP Open Forwarding with Policy Approval

Approval may come from

- Local Policy service.

  Using local policy the approval is done locally.

- Remote Policy service.

With the remote service, TBD but probably a connection to ***$policy***.

QDR will cache both steps of the policy lookup.

Policy cache key	**Cached policy data**
Host, user, application	Resource Limit Policy name
Resource Limit Policy name	Resource Limits

Table 4 – QDR Policy caches

Resource Limits

Policy enforcement maintains a cache of named Resource Limit policy values (see Table 2 above). QDR uses the cached values for completing the connection.

Resource limits are applied at various points in the AMQP connection life cycle:

- AMQP Open
- AMQP Begin
- AMQP Attach