Pivotal

Table of Contents

RabbitMQ for Pivotal Cloud Foundry® Documentation

RabbitMQ is a fast and dependable open-source message server that supports a wide range of use cases including reliable integration, content based routing and global data delivery, and high volume monitoring and data ingestion.

Emerging as the de facto standard for cloud messaging, RabbitMQ is used for efficient communication between servers, applications and devices, and creates lasting value by enabling rapid development of modern decentralized application and data architectures that can scale with your business needs. The Pivotal Cloud Foundry® ⓦ (PCF) installer enables cloud operators to deploy a RabbitMQ service ⓦ in PCF. You can deploy the service as a single node or a cluster.

Product snapshot

Current RabbitMQ for PCF Details

> **Version**: 1.5.28
> **Release Date**: 27th April 2017
> **Software component version**: RabbitMQ OSS 3.5.8
> **Compatible Ops Manager Version(s)**: 1.7.x, 1.6.x, 1.5.x, 1.4.x
> **Compatible Elastic Runtime Version(s)**: 1.7.x, 1.6.x, 1.5.x, 1.4.x
> **vSphere support?** Yes
> **AWS support?** Yes
> **OpenStack support?** Yes
> **IPsec support?** No

Upgrading to the Latest Version

Consider the following compatibility information before upgrading RabbitMQ for Pivotal Cloud Foundry®.

> Ⓦ **Note**: Customers looking to upgrade to v1.6.19 should not install this version (1.5.28), but should upgrade directly from their existing version

> Ⓦ **Note**: Before you upgrade to Ops Manager 1.4.x, you must first upgrade RabbitMQ for PCF to at least 1.3.4. This allows RabbitMQ for PCF upgrades after you install Ops Manager 1.4.x.

> Ⓦ **Note**: Only version 1.5.9 and above are certified to work in new installations of Ops Manager 1.7.x.

For more information, refer to the full Product Compatibility Matrix ⓦ.

Ops Manager Version	Supported Upgrades from Imported RabbitMQ Installation
1.6.x, 1.5.x and 1.4.x	• From 1.4.0 through to 1.5.28
1.7.x	• From 1.5.9 through to 1.5.28

Features

- Provision an instance of the RabbitMQ service, which corresponds to a unique RabbitMQ vhost (virtual host)
- Bind applications to an instance of the plan, providing unique credentials for each binding
- Management dashboard access to PCF Operators and application developers
- Deployment across multiple availability zones, with nodes striped across the AZs automatically
- Enable SSL (Secure Sockets Layer) for the AMQP, MQTT, STOMP protocols
- 2 node RabbitMQ cluster in a default deployment
- HAProxy load balancer across all nodes to balance connections
- Plugin configuration can be easily changed at any time and the cluster redeployed and updated
- The cluster topology can be changed and easily scaled out

- Default configurable policy applied to all new instances to mirror queues on two nodes
- Automated upgrades of RabbitMQ for major, minor and patch releases.

Install via Pivotal Ops Manager

To install RabbitMQ for PCF, follow the procedure for installing Pivotal Ops Manager tiles:

1. Download the product file from Pivotal Network ⊠.

2. Upload the product file to your Ops Manager installation.

3. Click **Add** next to the uploaded product description in the Ops Manager `Available Products` view to add this product to your staging area.

4. Click the newly added tile to review any configurable options.

5. Click **Apply Changes** to install the service.

This product requires Ops Manager version 1.4.0 or greater.

Using RabbitMQ in your application

RabbitMQ is shown in the services marketplace, either in the Apps Manager or through `cf marketplace` on the CLI.

Application developers can create an instance of the application with `cf create-service p-rabbitmq standard <your name>` . For this service an instance equals a **Vhost** on the RabbitMQ cluster.

Creating a binding gives the user permissions to access this Vhost and associated management dashboard.

Current Limitations

Limitations with the current RabbitMQ for PCF product include:

- Availability Zone configuration **cannot** be changed once deployed.

We hope to address all of these limitations in future releases.

Known Issues

- In versions `1.4.1` and `1.4.2` , the `manage` button for your RabbitMQ instance in Apps Manager will not automatically log you into the RabbitMQ Dashboard. You need to press `logout` and then login with your `username` and `password` which can be obtained from inspecting the environment variables for your instance.
- In versions `1.5.0` and `1.5.1` , when performing a fresh installation or upgrade, if the Elastic Runtime system and application domains are different then the `Broker Registrar` errand will fail. To resolve this disable the errand and redeploy, then register the broker manually using the system domain route `pivotal-rabbitmq-broker.system.domain` . For more information on registering brokers see the CloudFoundry documentation ⊠.
- In the `1.5.0, 1.5.1, 1.5.2, 1.5.3` releases, when performing a fresh installation or upgrade, if you have the rabbitmq_jsonrpc_channel or rabbitmq_jsonrpc_channel_examples plugins selected then the RabbitMQ nodes will fail to start. The plugins are no longer distributed with RabbitMQ and plugin validation was introduced in RabbitMQ `3.5.7` , causing the nodes to fail to start. To resolve this issue you should install/upgrade to version `1.5.4` or above of the tile.
- In the `1.4.x` and `1.5.x` tiles it not possible to install the RabbitMQ tile in multiAZ with multi-subnet networks.
- It is not possible to upgrade directly from the latest v.1.5.x patch version to the latest v1.6.x patch version. You can only upgrade to a tile which has a higher stemcell version than the one which you have installed.

Please provide any bugs, feature requests, or questions to the Pivotal Cloud Foundry® Feedback list.

Pivotal

Deploying the RabbitMQ Service

Default Deployment

Deploying RabbitMQ for Pivotal Cloud Foundry® ⓜ (PCF) through Ops Manager will deploy a RabbitMQ cluster of **2 nodes** by default.

The deployment includes a single load balancer `haproxy` which spreads connections on all of the default ports, for all of the shipped plugins across all of the machines within the cluster.

The deployment will occur in a single availability zone (AZ).
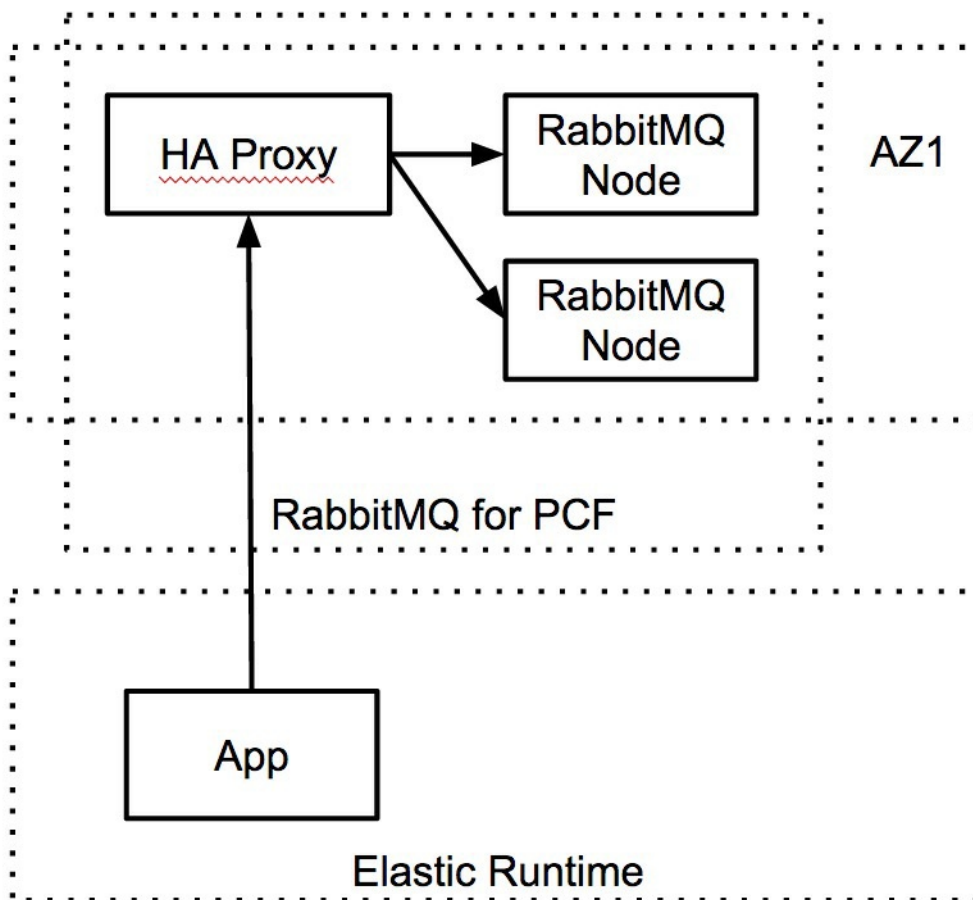
Considerations for this deployment

- Provides HA for RabbitMQ nodes to avoid data loss

- HAProxy is a single point of failure (SPOF)

- The entire deployment is in a single AZ, which does not protect against external failures from failures in hardware, networking, etc.

Recommended Deployment

We recommend that RabbitMQ is deployed across at least two availability zones.

The HAProxy job instance count should also be increased to match the number of AZs to ensure there is a HAProxy located in each AZ. This removes the HAProxy SPOF and provides further redundancy.
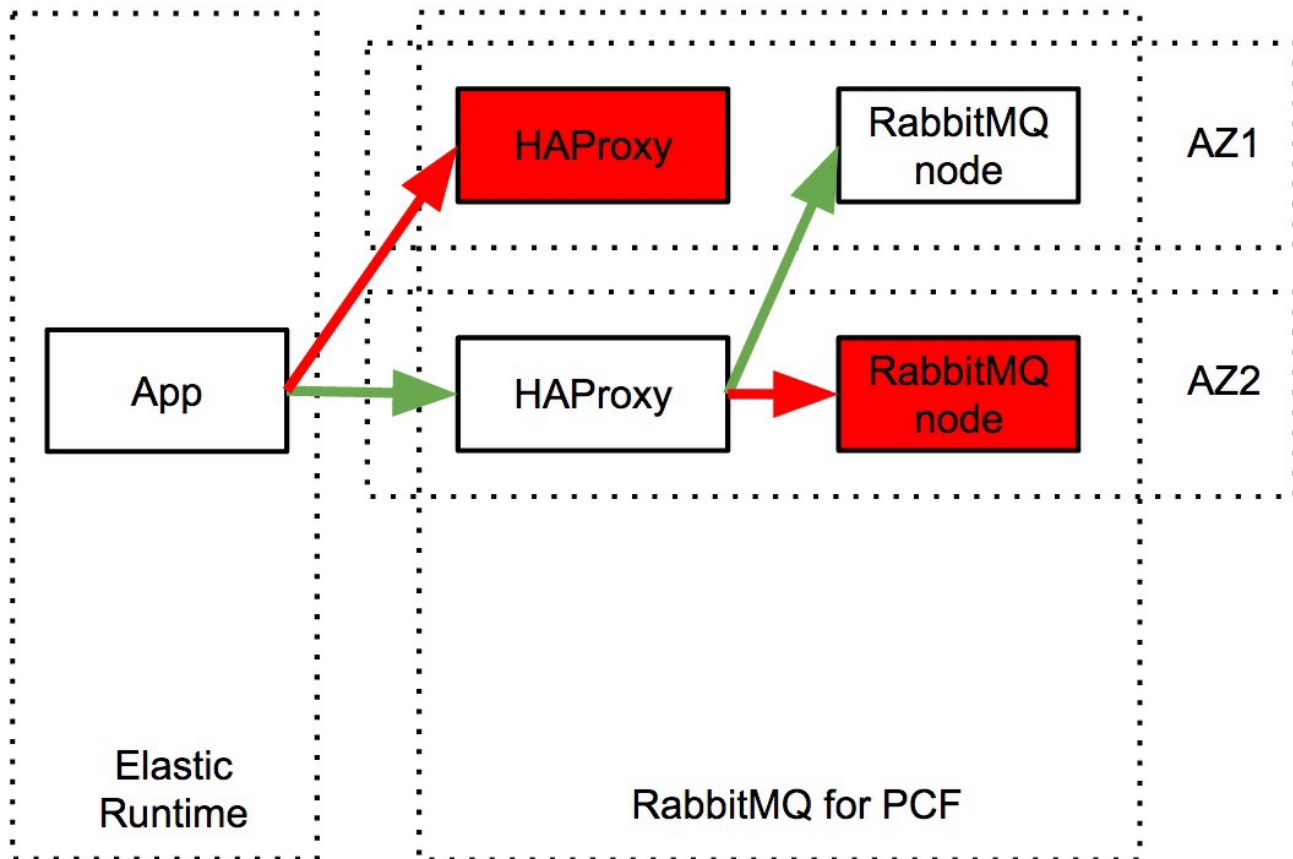
In the above diagram, you can see that you can now suffer the failure of a single HAProxy and single RabbitMQ node and still keep your cluster online and applications connected.

Upgrading to this deployment from a single AZ deployment

It is **not** possible to upgrade to this setup from the default deployment across a single AZ.

This is because the AZ setup cannot be changed once the tile has being deployed for the first time, this is to protect against data loss when moving jobs between AZs.

Upgrading to this deployment from a multi AZ deployment

If you have deployed the tile across two AZs, but with a single HAProxy instance you can migrate to this setup as follows:

1. Deploy an additional HAProxy instance through Ops Manager

2. New or re-bound applications to the RabbitMQ service will see the IPs of both HAProxys immediately

3. Existing bound applications will continue to work, but only using the previously deployed HAProxy IP Address. They can be re-bound as required at your discretion.

## Considerations for this deployment

- Requires IaaS configuration for availability zones ahead of deploying the RabbitMQ tile
- Application developers will be handed the IPs of each deployed HAProxy in their environment variables

Advanced Deployment

This deployment builds upon the above recommended deployment, so follows the same upgrade paths.

This allows you to replace the use of HAProxy with your own external load balancer.

You may choose to do this to remove any knowledge of the topology of the RabbitMQ setup from application developers.
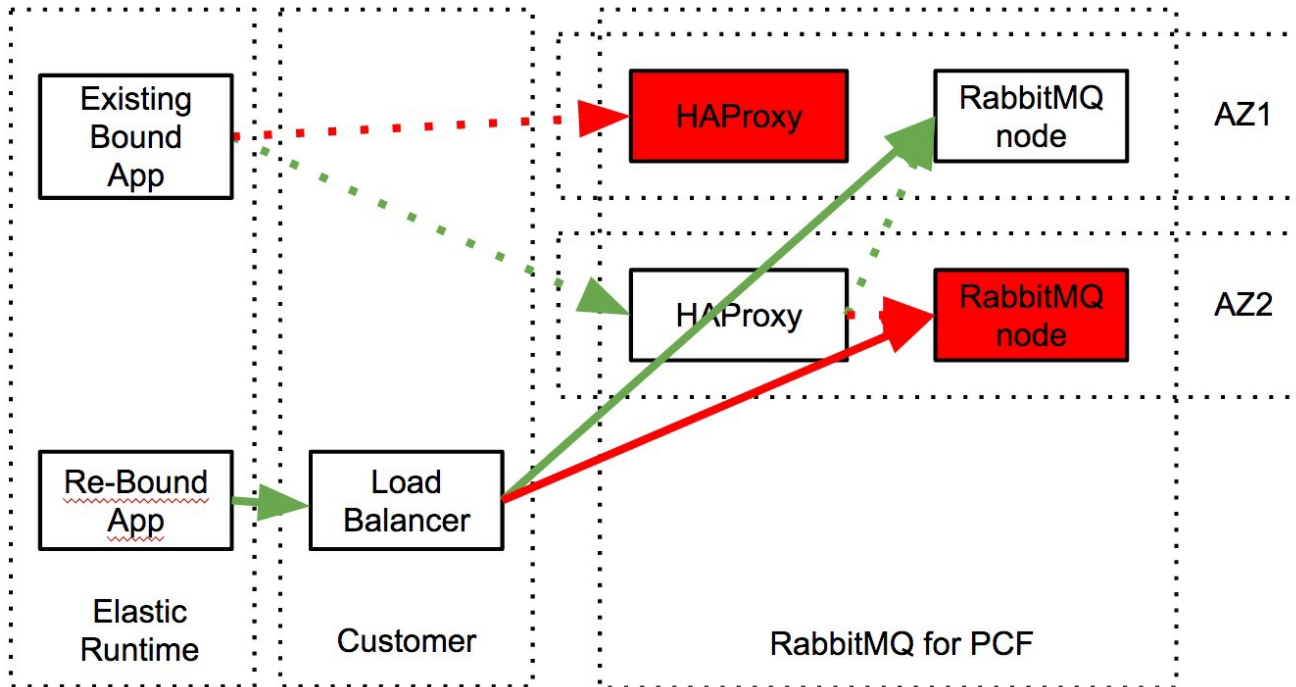
Advantages

- Application developers do not need to handle multiple IPs for the HAProxy jobs in their applications

Disadvantages

- The load balancer needs to be configured with the IPs of the RabbitMQ Nodes. These will only be known once the deployment has finished. The IPs should remain the same during subsequent deployments but there is a risk they can change.

Upgrading to this deployment from the recommended deployment

It is possible to first deploy with multiple HAProxy jobs, as per the recommended deployment and decided to later use your own external load balancer.

This can be achieved without downtime to your applications.

This can be achieved as follows:

1. Configure your external load balancer to point to the RabbitMQ Node IPs

2. Configure the DNS name or IP address for the external load balancer (ELB) on the RabbitMQ tile in Ops Manager

3. Deploy the changes

4. Any new instances of the RabbitMQ service **or** any re-bound connections will use the DNS name or IP address of the ELB in their `VCAP_SERVICES`

5. Any existing instances will continue to use the HAProxy IP addresses in their `VCAP_SERVICES`

6. Phase the re-binding of existing applications to have their environment variables updated

7. Once all applications are updated

8. Reduce the instance count of the `HAProxy` job in Ops Manager to 0

9. Deploy the changes

1.5

This approach works as any existing bound applications have their `VCAP_SERVICES` information cached in the cloud controller and are only updated by a re-bind request.

Downgrading from this deployment to the recommended deployment

If you are currently using an external load balancer, then you can move back to using HAProxys instead.

You can achieve this by following the above steps in reverse order and re-instating the HAProxy jobs.

RabbitMQ for Pivotal Cloud Foundry®

Upgrades

This product enables a seamless upgrade experience between versions of the product that is deployed through Ops Manager.

The upgrade paths are detailed here ⊠ for each released version.

To upgrade the product:

- The Operator should download the latest version of the product from Pivotal Network ⊠
- Upload the new .pivotal file to Ops Manager
- Upload the stemcell associated with the update (*if required*)
- Update any new mandatory configuration parameters (*if required*)
- Press "Apply changes" and the rest of the process is automated

It is necessary to increase the number of HAProxy instances from the default of one to two, before an upgrade is initiated to enable a zero downtime upgrade. During a typical upgrade deployment, nodes are upgraded one at a time in the cluster providing a zero downtime deployment. Applications may experience a disconnected session, if the application attempts to reconnect it will be directed to another working node automatically.

Only when upgrading between specific versions of Erlang or RabbitMQ is an outage required on the cluster. This will be clearly stated on the release notes for that version, should this be required.

The length of the downtime depends on whether there is a stemcell update to replace the operating system image or whether the existing VM can simply have the RabbitMQ software updated. Stemcell updates incur additional downtime while the IaaS creates the new VM while updates without a stemcell update are faster.

Ops Manager ensures the instances are updated with the new packages and any configuration changes are applied automatically.

Upgrading to a newer version of the product does not cause any loss of data or configuration. This is explicitly tested for during our build and test process for a new release of the product. (In future releases of the product the default number of HAProxy instances will be increased to two).

Release policy

When a new version of RabbitMQ is released we aim to release a new version of the product containing this soon after.

Where there is a new version of RabbitMQ or another dependent software component such as the stemcell released due to a critical CVE, Pivotal's goal is to release a new version of the product within 48 hours.

Configuring the RabbitMQ Service

Configuration

On the RabbitMQ for Pivotal Cloud Foundry® ⊠ (PCF) tile in Ops Manager, you can configure the following items:

Management dashboard

You must choose an admin username and password for RabbitMQ.

This will grant you full admin access to RabbitMQ via the Management UI.

RabbitMQ cluster configuration.

RabbitMQ admin user credentials *

admin

•••••

Plugins

You can choose which plugins you wish to enable.

You must leave the management plugin enabled otherwise nothing will work.

RabbitMQ plugins *

- ☐ rabbitmq_amqp1_0
- ☐ rabbitmq_auth_backend_ldap
- ☐ rabbitmq_auth_mechanism_ssl
- ☐ rabbitmq_consistent_hash_exchange
- ☐ rabbitmq_federation
- ☐ rabbitmq_federation_management
- ☐ rabbitmq_jsonrpc_channel
- ☐ rabbitmq_jsonrpc_channel_examples
- ☑ rabbitmq_management
- ☐ rabbitmq_management_visualiser
- ☐ rabbitmq_mqtt
- ☐ rabbitmq_shovel
- ☐ rabbitmq_shovel_management
- ☐ rabbitmq_stomp
- ☐ rabbitmq_tracing
- ☐ rabbitmq_web_stomp
- ☐ rabbitmq_web_stomp_examples

Click here for more information about RabbitMQ plugins ⊠

HAProxy ports

You can choose which ports HAProxy should load balance to the RabbitMQ nodes.

RabbitMQ cluster HAproxy ports *

15672, 5672, 5671, 1883, 8883, 61613, 61614

By default all the default ports of all the available plugins will be load-balanced.

However, if you install extra protocol plugins, or provide a custom configuration which changes the ports that RabbitMQ listens on then you must update the list of load-balanced ports.

Note that you must always leave the management plugin listening on port 15672 and load balance that port.

If you change the topology of your RabbitMQ cluster, the HAProxy is automatically reconfigured during the deployment.

Port to protocol mappings

15672 = Management dashboard

5672 = Rabbit

5671 = Rabbit ssl

1883 = MQTT

8883 = MQTT SSL

61613 = STOMP

61614 = STOMP SSL

15674 = Web STOMP

SSL

You can provide SSL certificates and keys for use by the RabbitMQ cluster.

RabbitMQ server private key

RabbitMQ server certificate

RabbitMQ server CA certificate

Note SSL is simultaneously provided on the AMQPS port (5671) and the management port (15672).

If you provide SSL keys and certificates, you are disabling non-SSL support.

No other plugins are automatically configured for use with SSL.

Note SSL settings are applied equally across all machines in the cluster.

Click here for more information about SSL support ⊠

Pivotal

Erlang Cookie

You can provide an Erlang cookie to be used by the cluster if you wish. This can be useful if you want to connect directly to the RabbitMQ cluster such as with `rabbitmqctl` or to connect other machines running Erlang.

Erlang cookie used by RabbitMQ nodes and rabbitmqctl

RabbitMQ Config

You can provide a full `rabbitmq.config` file, if you wish.

RabbitMQ configuration

This file is then provided to all the nodes in the cluster.

Click here for more information about the RabbitMQ configuration file ⊠

TLS Support

TLS v1.0 is disabled by default, due to insecurities.

RabbitMQ TLS 1.0 Support
☐ TLS 1.0 (required for JDK 6.0)

You can enable it again by ticking the checkbox.

TLS v1.1 and 1.2 are enabled by default and cannot be turned on or off.

External load balancer

External load balancer DNS name

You can configure a DNS name or IP address of an external load balancer to be returned in the binding credentials (`VCAP_SERVICES`) to application developers.

Assigned IPs

It is not supported to change the IP addresses which have been assigned to the RabbitMQ deployments. Doing so will cause the deployment to fail. For example it is not supported to change the subnet into which the RabbitMQ cluster was originally provisioned.

Default policies for the RabbitMQ Service

Policy

An example policy is configured in Ops Manager but not enabled.

You should configure the policy to suit your own deployment. The example in the "Policy for new instances" textarea is given as guidance of how to format the configuration.

The following rules apply:

- The policy is only applied to new instances
- Any existing instances will not have the policy applied
- The policy can be updated in Ops Manager and this will only be applied to any new instances created there after
- The policy can only be deleted manually from the RabbitMQ nodes

Viewing or changing the policy

In Ops Manager on the RabbitMQ tile, there is a left hand menu item called `Policy`

The policy must be valid JSON and it should use valid RabbitMQ policy criteria. This is not validated during the deployment, so any errors could either cause the deployment to fail or policies to not be applied correctly.

For more information, view RabbitMQ Policies ⊻.

RabbitMQ Dashboard

You can view the policy on the RabbitMQ Dashboard. The URL can be obtained from your `VCAP_SERVICES` for application developers.

The policy is applied to all queues, with a rank of 50 so it can be overriden by defining your own policy with a higher rank.

You can see any new queues created have the policy automatically applied.

Queues

All queues

Filter: [   ] ☐ Regex (?)

Overview			Messages			Message rates			+/-
Name	**Features**	**State**	**Ready**	**Unacked**	**Total**	**incoming**	**deliver / get**	**ack**	
test	D operator_set_policy	■ running	0	0	0				

       1.5

Pivotal

Clustering and Network Partitions

The RabbitMQ tile uses the `pause_minority` option for handling cluster partitions by default. This ensures data integrity by pausing the partition of the cluster in the minority, and resumes it with the data from the majority partition. You must maintain more than two nodes. If there is a partition when you only have two nodes, both nodes immediately pause.

You can also choose the `autoheal` option in the **RabbitMQ Policy** tab. In this mode, if a partition occurs, RabbitMQ automatically decides on a winning partition, and restarts all nodes that are not in the winning partition. This option allows you to continue to receive connections to both parts of partitions.

Detecting a Network Partition

When a network partition occurs, a log message is written to the RabbitMQ node log:

```
=ERROR REPORT==== 15-Oct-2012::18:02:30 ===
Mnesia(rabbit@da3be74c053640fe92c6a39e2d7a5e46): ** ERROR ** mnesia_event got
    {inconsistent_database, running_partitioned_network, rabbit@21b6557b73f343201277dbf290ae8b79}
```

You can also run the `rabbitmqctl cluster_status` command on any of the RabbitMQ nodes to see the network partition. To run `rabbitmqctl cluster_status`, do the following:

1. `$ sudo su -`

2. `$ cd /var/vcap/packages`

3. `$ export ERL_DIR=$PWD/erlang/bin/`

4. `$ cd rabbitmq-server/bin/`

5. `$ ./rabbitmqctl cluster_status`

   ```
   [...
   {partitions,
       [{rabbit@da3be74c053640fe92c6a39e2d7a5e46,
           [rabbit@21b6557b73f343201277dbf290ae8b79]}]}]
   ```

Recovering

Because the RabbitMQ tile uses the `pause_minority` option, minority nodes recover automatically after the partition is resolved. After a node recovers, it resumes accessing the queue along with data from the queues on the other nodes. However, if your queues use `ha-mode: all`, they only synchronize fully after consuming all the messages created while the node was down. This is similar to how messages synchronize when you create a new queue.

Manually Synchronizing after a Partition

After a network partition, a queue on a minority node synchronizes after consuming all the messages created while it was down. You can also run the `sync_queue` command to synchronize a queue manually. To run `sync_queue`, do the following on each node:

1. `$ sudo su -`

2. `$ cd /var/vcap/packages`

3. `$ export ERL_DIR=$PWD/erlang/bin/`

4. `$ cd rabbitmq-server/bin/`

5. `$ ./rabbitmqctl list_queues`

6. `$ ./rabbitmqctl sync_queue name`

Managing the RabbitMQ Service

RabbitMQ Management Dashboard

Admin User

To gain access to the management dashboard as the `admin` user, visit http://pivotal-rabbitmq.your.cf.installation.com ⌧

The username and password is the username and password you provided in the RabbitMQ configuration in Ops Manager, which is also shown in the Credentials tab.

Application Developer

Users of Cloud Foundry who create instances via the Apps Manager, or the `cf` CLI also get access to the Management UI. This is done using credentials that provide access only to their particular **vhost**.

The appropriate URL is accessible via the Manage button within the Apps Manager.

SERVICES — Add Service

SERVICE INSTANCE	SERVICE PLAN	BOUND APPS
rabbit Manage | Documentation | Support | Delete	RabbitMQ for Pivotal CF Production	0

Or it is also injected into the `VCAP_SERVICES` environment variable provided to apps running on Cloud Foundry. This can also be found via the CLI using `cf env <your app name>`.

```
→ ~ cf env lab-rat
Getting env variables for app lab-rat in org development / space development as me...
OK

System-Provided:
{
 "VCAP_SERVICES": {
  "p-rabbitmq": [
   {
    "credentials": {
     "dashboard_url": "http://pivotal-rabbitmq.crystal.pepsi.cf-app.com/#/login/fd87c5d4-ca55-41f3-ba8a-cf0b0711f052/243bvlaa8c5m5dka1701b207ff",
```

Logging

A TCP Syslog endpoint can be configured in Ops Manager. Logs are currently only forwarded for the RabbitMQ cluster.

RabbitMQ CLI

If you wish to run commands such as `rabbitmqctl` then you have two options:

SSH into one of the machines running the rabbitmq-server. IPs can be found from the Status tab and access credentials from the Credentials tab within the RabbitMQ component of the installer. From there you need to bring RabbitMQ and Erlang into your environment and from there you can use `rabbitmqctl`:

```
bash-4.1# export PATH=$PATH:/var/vcap/packages/rabbitmq-server/bin
bash-4.1# export PATH=$PATH:/var/vcap/packages/erlang/bin
bash-4.1# rabbitmqctl cluster_status
Cluster status of node rabbit@node0 ...
[{nodes,[{disc,[rabbit@node0,rabbit@node1,rabbit@node2,rabbit@node3]}]},
 {running_nodes,[rabbit@node3,rabbit@node2,rabbit@node1,rabbit@node0]},
 {partitions,[]}]
...done.
```

Alternatively, install RabbitMQ and Erlang on a machine of your choice. Be sure to match versions of both to the cluster: the Management UI shows both the version of RabbitMQ and Erlang.

Then set your `~/.erlang.cookie` to match the cookie used in the cluster (you may have supplied this as part of the installation; see above).

You'll need to set up your `/etc/hosts` file to match the RabbitMQ nodes.

HAProxy Statistics

The HAProxy statistics page can be viewed at the IP address for the HAProxy node.

This page is only accessible via the internal IP address, so access will be required to your PCF network.

Identify the IP address of the HAProxy from the `Status` page in Ops Manager for the RabbitMQ tile

Here, this is 10.0.0.55

Identify the credentials for the HAProxy job, from the Credentials page in Ops Manager.

Visit http://10.0.0.55 and input the username & password to view the dashboard.

If you have got multiple HAProxys then there will be separate dashboards on each IP.

RabbitMQ Entries in the VCAP_SERVICES Environment Variable

Applications running in Cloud Foundry gain access to the bound service instances via an environment variable credentials hash called `VCAP_SERVICES` . An example hash is show below:

```
{
  "p-rabbitmq": [{
    "label": "p-rabbitmq",
    "name": "my-rabbit-service-instance",
    "plan": "standard",
    "tags": ["rabbitmq", "messaging", "message-queue", "amqp", "pivotal"],
    "credentials": {
      "dashboard_url": "http://pivotal-rabbitmq.your.pcf.com/#/login/b5d0ad14-4352-48e8-8982-d5b1d257029f/tavk86pnnns1ddiqpsdtbchurn",
      "username": "b5d0ad14-4352-48e8-8982-d5b1d257029f",
      "vhost": "62e5ab21-7b38-44ac-b139-6aa97af01cd7",
      "password": "tavk86pnnns1ddiqpsdtbchurn",
      "ssl": false,
      "hostname": "10.0.0.41",
      "hostnames": [
        "10.0.0.41",
        "10.0.0.51"],
      "uri": "amqp://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.41/62e5ab21-7b38-44ac-b139-6aa97af01cd7",
      "uris": [
        "amqp://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.41/62e5ab21-7b38-44ac-b139-6aa97af01cd7",
        "amqp://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.51/62e5ab21-7b38-44ac-b139-6aa97af01cd7"],
      "http_api_uri": "http://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.41:15672/api",
      "http_api_uris": [
        "http://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.41:15672/api",
        "http://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.51:15672/api"],
      "protocols": {
        "amqp": {
          "password": "tavk86pnnns1ddiqpsdtbchurn",
          "port": 5672,
          "ssl": false,
          "username": "b5d0ad14-4352-48e8-8982-d5b1d257029f",
          "vhost": "62e5ab21-7b38-44ac-b139-6aa97af01cd7",
          "host": "10.0.0.41",
          "hosts": [
            "10.0.0.41",
            "10.0.0.51"],
          "uri": "amqp://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.41:5672/62e5ab21-7b38-44ac-b139-6aa97af01cd7",
          "uris": [
            "amqp://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.41:5672/62e5ab21-7b38-44ac-b139-6aa97af01cd7",
            "amqp://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.51:5672/62e5ab21-7b38-44ac-b139-6aa97af01cd7"]},
        "management": {
          "username": "b5d0ad14-4352-48e8-8982-d5b1d257029f",
          "password": "tavk86pnnns1ddiqpsdtbchurn",
          "path": "/api",
          "port": 15672,
          "ssl": false,
          "host": "10.0.0.41",
          "hosts": [
            "10.0.0.41",
            "10.0.0.51"],
          "uri": "http://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.41:15672/api",
          "uris": [
            "http://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.41:15672/api",
            "http://b5d0ad14-4352-48e8-8982-d5b1d257029f:tavk86pnnns1ddiqpsdtbchurn@10.0.0.51:15672/api"]}}}}]}
```

You can search for your service by its `name` , given when creating the service instance, or dynamically via the `tags` or `label` properties. The `credentials` property can be used as follows:

- The top level properties `uri` , `uris` , `vhost` , `username` , `password` , `hostname` and `hostnames` provide access to the AMQP 0.9.1 protocol.
- A more flexible approach is provided by the `credentials.protocols` property, which has a key per enabled protocol. The possible keys are `amqp` , `management` , `mqtt` , and `stomp` . If SSL is enabled, then the keys will be `amqp+ssl` , `management+ssl` , `mqtt+ssl` , and `stomp+ssl` respectively.
- The values associated with each of these keys gives access credentials specific to each protocol. In all cases, URIs are provided, along with the individual components.

Connecting to a Highly Available RabbitMQ Cluster

The latest version of RabbitMQ tile 1.5.*, allows for a highly available cluster through multiple HAProxy nodes. The `hostnames` , `uris` and `hosts` properties have been added and should be used in preference over the equivalent singular properties. The singular properties are maintained for backwards

compatibility and will always contain the first value from the equivalent plural property. The singular properties will eventually be deprecated.

For example with two HAProxy jobs deployed the following properties will be present:

```
"hostname": "10.0.0.41",
"hostnames": [
    "10.0.0.41",
    "10.0.0.51"]
```

Changing Enabled Plugins and Protocols

Note: Removing or adding plugins/protocols may cause apps bound with RabbitMQ to break.

If you adjust the plugins and protocols enabled for RabbitMQ, you may need to force all app's `VCAP_SERVICES` environment variable to be regenerated. Adding / removing the following plugins require bound applications to be restaged:

- rabbitmq_management,

- rabbitmq_stomp,

- rabbitmq_mqtt

- rabbitmq_amqp1_0

In common with all services in Pivotal Cloud Foundry® ⊠ (PCF), the `VCAP_SERVICES` environment variable for an application is only modified when the application is bound to a service instance. Users will need to `cf unbind-service` , `cf bind-service` and `cf restage` their app in this scenario.

RabbitMQ® for PCF Release Notes

Pivotal recommends that you upgrade to the latest version of your current minor line, and then upgrade to the latest available version of the new minor line. For example, if you're on an older v1.7.x version, upgrade to the latest v1.7.x version before upgrading to the latest v1.8.x version.

For product versions and upgrade paths, see the Product Compatibility Matrix ⊠.

v1.7.x

For v1.7.x versions of RabbitMQ for PCF, see the release notes ⊠ in the v1.7 version of this documentation.

v1.6.x

For v1.6.x versions of RabbitMQ for PCF, see the release notes ⊠ in the v1.6 version of this documentation.

v1.5.x

Pivotal released v1.5.0 in December 2015, and the latest patch version is v1.5.28.

v1.5.28

Release Date: April 27, 2017

- Update to stemcell 3312.24

v1.5.27

Release Date: April 3, 2017

- Update to stemcell 3312.22

v1.5.26

Release Date: March 10, 2017

- Update to stemcell 3233.15

v1.5.25

Release Date: March 3, 2017

- Update to stemcell 3233.14

v1.5.24

Release Date: January 27, 2017

- Update to stemcell v3233.12
- Update to stemcell for security fix.
- You can only upgrade to v1.6.16 or later from this release

v1.5.23

Release Date: December 15, 2016

- Update to stemcell v3233.8
- Update to stemcell for security fix.
- You can only upgrade to v1.6.15 (when available) or above from this release

v1.5.22

Release Date: December 8, 2016

- Update to stemcell 3233.6
- Update to stemcell for security fix.
- You can only upgrade to v 1.6.12 or below from this release

v1.5.20

Release Date: November 22, 2016

- Update to stemcell 3233.4
- Update to OSS RabbitMQ 3.5.8 for security fix. For more information look here ⊠

v1.5.18

Release Date: October 21, 2016

- Update to stemcell 3233.3

v1.5.17

Release Date: October 13, 2016

- Updated stemcell to 3233.2

v1.5.15

Release Date: August 24, 2016

- Updated stemcell to 3232.21

v1.5.14

Release Date: August 24, 2016

- Updated stemcell to 3232.17

v1.5.13

Release Date: June 30, 2016

- Updated stemcell to 3232.12 for USN-3020-1

v1.5.12

Release Date: June 8, 2016

Features included in this release:

- This release incorporates stemcell 3232.6 which has fixes for the following:

    - USN-2985-2
    - USN-2981-1
    - USN-2970-1
    - USN-2966-1

v1.5.11

Release Date: May 26, 2016

Features included in this release:

- Updated to the latest version of broker_registrar
- Note you can only upgrade to version 1.6.1 and above

v1.5.10

Release Date: May 18, 2016

Features included in this release:

- Updated stemcell to 3232.4 for USN-2977-1

v1.5.9

Release Date: May 5, 2016

Features included in this release:

- Updated stemcell to 3146.11, including stemcell CVE updates

v1.5.8

Release Date: February 16, 2016

Features included in this release:

- Update stemcell to 3146.10 patches Ubuntu CVE 2016-3134

v1.5.7

Release Date: February 24, 2016

Features included in this release:

- Update stemcell to 3146.9 patches Ubuntu CVE USN-2910-1

v1.5.6

Release Date: February 18, 2016

Features included in this release:

- Update stemcell to 3146.8 patches Ubuntu CVE-2015-7547

v1.5.5

Release Date: February 2, 2016

Features included in this release:

- Update stemcell to 3146.6 patches Ubuntu CVEs

v1.5.4

Release Date: January 21, 2016

Features included in this release:

- Update stemcell to 3146.5 resolves CVE-2016-0728

v1.5.3

Release Date: January 18, 2016

Features included in this release:

- Bug fix that resolves issue with missing plugins causing RabbitMQ nodes to fail to start
- Update stemcell to 3146.3, resolves CVE-2016-0777 and CVE-2016-0778

v1.5.2

Release Date: January 7, 2016

Features included in this release:

- Bug fix with broker registrar errand failing if ERT has different system & app domains
- Update stemcell to 3146.2, resolves CVE USN-2857-1

v1.5.1

Release Date: December 21, 2015

Features included in this release:

- RabbitMQ 3.5.7
- Update stemcell to 3153

v1.5.0

Release Date: December 18, 2015

Features included in this release:

- RabbitMQ 3.5.6
- Erlang v18.1
- RabbitMQ HTTP logging enabled

- Update stemcell to 3147

Important: You will experience a **full cluster outage** during this particular deployment as the RabbitMQ & Erlang versions are updated. We recommend that you communicate with your application owners in advance to minimize the impact of this downtime.

v1.4.x

Pivotal released v1.4.0 in April 2015, and the latest patch version is v1.4.10.

v1.4.10

Release Date: December 3, 2015

Features included in this release:

- Update stemcell to 3146. Resolves CVE USN-2821-1

v1.4.9

Release Date: December 1, 2015

Features included in this release:

- Update stemcell to 3144. Resolves CVEs: USN-2815-1, USN-2812-1 and USN-2810-1

v1.4.8

Release Date: November 11, 2015

Features included in this release:

- Update stemcell to 3130. Resolves CVE USN-2806-1

v1.4.7

Release Date: October 30, 2015

Features included in this release:

- Update stemcell to 3112

v1.4.6

Release Date: October 14, 2015

Features included in this release:

- Update stemcell to 3100 for PCF Suite 1.6 release

v1.4.5

Release Date: October 7, 2015

Features included in this release:

- Update stemcell to 3094 to address USN-2765-1 ⬚

Known issues:

- Note one important known issue with the 1.5.6 patch for OpenStack deployments. BOSH stemcell v3094, which this version of Elastic Runtime references, has a limitation affecting OpenStack users only:
  - Elastic Runtime 1.5.6 on OpenStack does not work with S3/Swift blobstores.
  - Elastic Runtime 1.5.6 on OpenStack users must configure their object storage to use the internal blobstore option.
  - vSphere, AWS and vCloud users are not affected.

v1.4.4

Release Date: September 2, 2015

Features included in this release:

- Updated stemcell to 3062

v1.4.3

Release Date: July 29, 2015

Features included in this release:

- Updated stemcell to 3026 to resolve CVE-2015-3290

v1.4.2

Release Date: July 16, 2015

Features included in this release:

- Updated HAProxy to latest version in the 1.5.x branch to resolve CVE-2015-3281
- Requires stemcell 3012

Note: You may need to upload stemcell version 3012 to your Ops Manager installation. These are available here ⬚

Known Issues:

- The `manage` button for your RabbitMQ instance in Apps Manager will not automatically log you into the RabbitMQ Dashboard. You need to press `logout` and then login with your `username` and `password` which can be obtained from inspecting the environment variables for your instance.

v1.4.1

Release Date: July 6, 2015

Features included in this release:

- Support for Ops Manager v1.5.x or v1.4.x
- Support for Elastic Runtime v1.5.x or v1.4.x
- Support for HTTPS only environments
- Support for vSphere or AWS Deployments
- Requires stemcell 2989

Known Issues:

- The `manage` button for your RabbitMQ instance in Apps Manager will not automatically log you into the RabbitMQ Dashboard. You need to press `logout` and then login with your `username` and `password` which can be obtained from inspecting the environment variables for your instance.

v1.4.0

Release Date: April 10, 2015

Features included in this release:

- Support for multiple availability zones
- Ability to remove HAProxy SPOF
- Ability to configure an external load balancer
- Syslog output from RabbitMQ Nodes
- Queues mirrored to two nodes by default
- Requires Ops Manager v1.4.0 and Elastic Runtime v1.4.0 or greater
- Support for vSphere and AWS

Important: You may experience a **small window of downtime** during this particular deployment as the cluster nodes are renamed. We recommend that you communicate with your application owners in advance to minimize the impact of this downtime.

Additional known issues:

- On AWS, this version supports deployments in the US-East region. Multi-region support is coming in a future release.
- The experimental HTTPS-only feature in Elastic Runtime 1.5 may cause issues with this version of the product. Full support for HTTPS-only traffic is coming in a future release.

> **Note**: BOSH Stemcell 2865.1 is required for installation on Ops Manager 1.5.x and above.

v1.3.x

Pivotal released the first version of v1.3.x in October 2014, and the latest patch version is v1.3.6.

v1.3.6

Release Date: March 23, 2015

Features included in this release:

- Updated stemcell to 2889 to resolve these OpenSSL CVE alerts ⓧ

v1.3.5

Release Date: March 6, 2015

Features included in this release:

- Updated version of Jetty to 9.2.9

v1.3.4

Release Date: January 30, 2015

Features included in this release:

- Updated stemcell to 2824 to resolve CVE-2015-0235 Ghost ⊠
- Upgraded RabbitMQ version to 3.4.3
- Developers can add policies for their Vhost (instance)
- Admin username and password changes through Ops Manager are reflected correctly in RabbitMQ for the admin dashboard
- Bug fix for package dependencies and installation errors
- Bug fix for OAuth integration with UAA
- Bug fix to ensure config changes in Ops Manager are correctly reflected in RabbitMQ in a redeployment
- Ability to disable TLS V1.0

v1.3.3.2

Release Date: 14th November 14, 2014

Features included in this release:

- Management dashboard uses a registered route

v1.3.3.1

Release Date: November 4, 2014

Features included in this release:

- Fix for increased RAM usage on the service broker

v1.3.3.0

Release Date: October 31, 2014

Features included in this release:

- Disables SSLv3 to address the POODLE vulnerability

v1.3.2.2

Release Date: October 27, 2014

Features included in this release:

- Corrects installation errors on some Ops Manager versions

v1.3.2.1

Release Date: October 24, 2014

Features included in this release:

- Resolves issue with idle client connections being closed very quickly

Upgrading from 1.2.0

It is unfortunately **not** possible to upgrade from any prior versions to this tile version or greater. E.g. from 1.2.0 to 1.3.2.1

This is because tile versions 1.2.0 and earlier use v1 of the Services API, whilst all newer tiles use v2. The migration between the versions would have being risky and complicated due to the way RabbitMQ was using service names, therefore the decision was taken to not support tile upgrades.

We always aim for tiles to be upgradeable from previous versions where possible.

Options

We recommend the following:

- Backup any persisted data (if required)
- Stop any applications / services that are publishing to the queues
- Delete the existing 1.2.0 tile
- Deploy the >= 1.3.2.1 tile version
- Restore any data
- Restage any applications to refresh the binding information, as the IPs may have changed

v1.2.0

Release Date: May 16, 2014

Features included in this release:

- RabbitMQ 3.2.4

v1.1.0

Release Date: March 11, 2014

Features included in this release:

- RabbitMQ 3.2.2

v1.0.0

Release Date: November 22, 2013

Features included in this release:

- RabbitMQ 3.1.5

RabbitMQ for Pivotal Cloud Foundry® Documentation

Resource requirements

The following table shows the default resource and IP requirements for installing the tile:

Product	Resource	Instances	CPU	Ram	Ephemeral	Persistent	Static IP	Dynamic IP
RabbitMQ	RabbitMQ Node	2	2	8192	4096	8192	1	0
RabbitMQ	HAProxy for RabbitmQ	1	1	2048	4096	0	1	0
RabbitMQ	RabbitMQ Service Broker	1	1	2048	4096	0	0	1
RabbitMQ	Compilation	2	2	2048	4096	0	0	1
RabbitMQ	Broker Registrar	1	1	1024	2048	0	0	1
RabbitMQ	Broker De-Registrar	1	1	1024	2048	0	0	1

Notes:

- The number of `RabbitMQ Node` can be increased if required.