Redis Enterprise for Kubernetes
Release Notes 6.0.8-1 (October 2020)

The Redis Enterprise K8s 6.0.8-1 release is a major release on top of 6.0.6-24 providing support for the latest Redis Enterprise Software release 6.0.8-28 and includes several enhancements (including OpenShift 4.5 and Kubernetes 1.18 support) and bug fixes.

Overview

This release of the operator provides:

- New features
- New support K8s distributions and platforms
- Various bug fixes

To upgrade your deployment to this latest release, see “Upgrade a Redis Enterprise cluster (REC) on Kubernetes”.

Images

- **Redis Enterprise** - redislabs/redis:6.0.8-28 or redislabs/redis:6.0.8-28.rhel7-openshift
- **Operator** - redislabs/operator:6.0.8-1
- **Services Rigger** - redislabs/k8s-controller:6.0.8-1 or redislabs/services-manager:6.0.8-1 (Red Hat registry)

New features

- Redis Modules can now be configured in the database custom resource.
- Support was added for OpenShift 4.5
- Support was added for Kubernetes 1.18
- Added support for the Gesher admission control proxy to provide an administrator the ability to setup delegation to avoid the need for administrator intervention on every namespaced deployed operator.

Important fixes

- Added the missing Services Rigger health check (RED47062)
- Fixed failures when updating the ui service type (RED45771)

Known limitations

CrashLoopBackOff causes cluster recovery to be incomplete (RED33713)
When a pod status is CrashLoopBackOff and we run the cluster recovery, the process will not complete. The workaround is to delete the crashing pods manually and recovery process will continue.

**Long cluster names cause routes to be rejected (RED25871)**

A cluster name longer than 20 characters will result in a rejected route configuration as the host part of the domain name exceeds 63 characters. The workaround is to limit cluster name to 20 characters or less.

**Cluster CR (REC) errors are not reported after invalid updates (RED25542)**

A cluster CR specification error is not reported if two or more invalid CR resources are updated in sequence.

**An unreachable cluster has status running (RED32805)**

When a cluster is in an unreachable state the state is still running instead of being reported as an error.

**Readiness probe incorrect on failures (RED39300)**

STS Readiness probe doesn’t mark a node as not ready when radmin status on the node fails.

**Role missing on replica sets (RED39002)**

The redis-enterprise-operator role is missing permission on replica sets.

**Private registries are not supported on OpenShift 3.11 (RED38579)**

OpenShift 3.11 doesn’t support dockerhub private registry. This is a known OpenShift issue.

**Internal DNS and Kubernetes DNS may have conflicts (RED37462)**

DNS conflicts are possible between the cluster mdns_server and the K8s DNS. This only impacts DNS resolution from within cluster nodes for Kubernetes DNS names.

**5.4.10 negatively impacts 5.4.6 (RED37233)**

Kubernetes-based 5.4.10 deployments seem to negatively impact existing 5.4.6 deployments that share a Kubernetes cluster.

**Node CPU usage is reported instead of pod CPU usage (RED36884)**

In Kubernetes, the node CPU usage we report on is the usage of the Kubernetes worker node hosting the REC pod.

**Master pod label in Rancher (RED42896)**

Master pod is not always labeled in Rancher.

**Cluster fail to start for clusters with unsynchronized clocks (RED47254)**

When REC clusters are deployed on clusters with unsynchronized clocks, the cluster does not start correctly. The fix is to use NTP to synchronize the underlying K8s nodes.

**Errors in operator log for REDB status (RED44919)**

Benign errors are reported in the operator log when using database controller (REDB) (e.g., “failed to update database status”. These errors can be ignored.

**Compatibility Notes**
• Support for OpenShift 4.5 was added.
• Support for Kubernetes 1.18 was added.
• Support for the previous deprecated Kubernetes 1.11 and 1.12 has been removed.

Updated: January 11, 2022