Redis Enterprise for Kubernetes
Release Notes 6.0.8-20 (December 2020)

The Redis Enterprise K8s 6.0.8-20 release is a major release on top of 6.0.8-1 providing support for the Redis Enterprise Software release 6.0.8-30 and includes several enhancements and bug fixes.

Overview

This release of the operator provides:

- New features
- Various bug fixes

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

Images

This release includes the following container images:

- **Redis Enterprise**: redislabs/redis:6.0.8-30 or redislabs/redis:6.0.8-30.rhel7-openshift
- **Operator and Bootstrapper**: redislabs/operator:6.0.8-20
- **Services Rigger**: redislabs/k8s-controller:6.0.8-20 or redislabs/services-manager:6.0.8-20 (Red Hat registry)

New features

- You can now create database custom resources (REDB CRs) in consumer namespaces that are separate from the operator and cluster namespace. You configured the operator deployment to watch specific namespaces for these REDB CRs.
- The Gesher admission control proxy is now certified by Red Hat.
- REDB CRs no longer require a Redis Enterprise cluster name. The name will default to the cluster in the context of the operator.
- REC and REDB CRs are now validated via a schema.

Important fixes

- The database controller (REDB) no longer generates the following error message: “failed to update database status”
- Issues with configuring replica-of through the database controller (REDB) and TLS have been fixed. (RED48285)
- A timeout issue with rlutil upgrade was fixed. (RED48700)

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

Long cluster names cause routes to be rejected (RED25871)
A cluster name longer than 20 characters will result in a rejected route configuration because the host part of the domain name will exceed 63 characters. The workaround is to limit cluster name to 20 characters or fewer.

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 does not mark a node as “not ready” when running rladmin 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 does not support DockerHub private registries. 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.

Clusters must be named “rec” in OLM-based deployments (RED39825)
In OLM-deployed operators, the deployment of the cluster will fail if the name is not “rec”. When the operator is deployed via the OLM, the security context constraints (scc) is bound to a specific service account name (i.e., “rec”). The workaround is to name the cluster “rec”.

Master pod label in Rancher (RED42896)
The master pod is not always labeled in Rancher.

REC clusters fail to start on Kubernetes clusters with unsynchronized clocks (RED47254)
When REC clusters are deployed on Kubernetes clusters with unsynchronized clocks, the REC cluster does not start correctly. The fix is to use NTP to synchronize the underlying K8s nodes.