Redis Enterprise for Kubernetes
Release Notes 6.2.8-11 (January 2022)

Overview

The Redis Enterprise K8s 6.2.8-11 release provides support for the Redis Enterprise Software release 6.2.8 and includes several enhancements and bug fixes.

The key new features, bug fixes, and known limitations are described below.

Images

This release includes the following container images:

- **Redis Enterprise**: redislabs/redis:6.2.8-53 or redislabs/redis:6.2.8-53.rhel7-openshift
- **Operator**: redislabs/operator:6.2.8-11
- **Services Rigger**: redislabs/k8s-controller:6.2.8-11 or redislabs/services-manager:6.2.8-11 (on the Red Hat registry)

Feature improvements

- Istio gateway/virtual services are supported as ingress controllers. Note that for Active-Active databases, the operator doesn’t create ingress rules, and those should be manually configured. The version of Istio that was tested is Istio 1.12.0 (RED-64020)
- Support for K8s 1.22 (AKS, kOps, GKE) and OpenShift 4.9 (RED-64016)
- Support for pod termination grace period customization in the REC (advanced use case) (RED-67217)
- Improved security granularity of SCC configuration steps in documentation (RED-67321)
- Changed behavior when two databases with the same name are created on the cluster. The operator avoids creating a service for them to prevent possible corruption (RED-64535)
- Improved documentation about changing cluster credentials when using Hashicorp Vault (RED-65304)

Fixed bugs

- Upgraded Go dependencies marked as vulnerable (RED-63858, RED-68651)
- Avoided flooding operator logs with deprecation notices on K8s 1.21 (RED-67544)
- Fixed log collector utility issues running on Microsoft Windows (RED-67682)
- Fixed excessive updates to the RS cluster when using Windows line endings for TLS certificates (RED-67874)

Known limitations
Upgrading with the bundle using `kubectl apply -f` fails (RED-69515)

Upgrading with the bundle using `kubectl apply -f` fails, giving the following error:

The CustomResourceDefinition "redisenterpriseclusters.app.redislabs.com" is invalid:
spec.preserveUnknownFields: Invalid value: true: must be false in order to use defaults in the schema

Workaround: Before the upgrade, set the `spec.preserveUnknownFields` value to false on the REC custom resource. You can use the following command:

```
kubectl patch crd redisenterpriseclusters.app.redislabs.com -p $'spec:
  preserveUnknownFields: false'
```

Long cluster names cause routes to be rejected (RED-25871)

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 less.

Cluster CR (REC) errors are not reported after invalid updates (RED-25542)

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 (RED-32805)

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 (RED-39300)

STS Readiness probe does not mark a node as "not ready" when running `rladmin status` on node failure.

Role missing on replica sets (RED-39002)

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

Private registries are not supported on OpenShift 3.11 (RED-38579)

OpenShift 3.11 does not support DockerHub private registries. This is a known OpenShift issue.

Internal DNS and Kubernetes DNS may have conflicts (RED-37462)

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 (RED-37233)

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 (RED-36884)

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 (RED-39825)

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) are bound to a specific service account name (i.e., "rec"). The workaround is to name the cluster "rec".
REC clusters fail to start on Kubernetes clusters with unsynchronized clocks (RED-47254)
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.

Deleting an OpenShift project with an REC deployed may hang (RED-47192)
When a REC cluster is deployed in a project (namespace) and has REDB resources, the REDB resources must be deleted first before the REC can be deleted. As such, until the REDB resources are deleted, the project deletion will hang. The fix is to delete the REDB resources first and the REC second. Afterwards, you may delete the project.

REC extraLabels are not applied to PVCs on K8s versions 1.15 or older (RED-51921)
In K8s 1.15 or older, the PVC labels come from the match selectors and not the PVC templates. As such, these versions cannot support PVC labels. If this feature is required, the only fix is to upgrade the K8s cluster to a newer version.

Hashicorp Vault integration - no support for Gesher (RED-55080)
There is no workaround at this time

REC might report error states on initial startup (RED-61707)
There is no workaround at this time except to ignore the errors.

PVC size issues when using decimal value in spec (RED-62132)
The workaround for this issue is to make sure you use integer values for the PVC size.

Following old revision of quick start guide causes issues creating an REDB due to unrecognized memory field name
The workaround is to use the newer (current) revision of the quick start document available online.

Compatibility Notes
See Supported Kubernetes distributions for the full list of supported distributions.

Now supported
This release adds support for the following:

- K8s 1.22 for GKE, AKS, and kOps
- OpenShift 4.9 (uses K8s 1.22)

Deprecated
- Rancher 2.5/K8s 1.17 support is deprecated

No longer supported
This release removes support for the following:

- Rancher 2.4 (previously deprecated)