Redis Enterprise for Kubernetes
Release Notes 6.0.20-12 (July 2021)

Overview

The Redis Enterprise K8s 6.0.20-12 release is a major release on top of 6.0.20-4 providing support for the Redis Enterprise Software release 6.0.20-97 and includes several enhancements and bug fixes.

This release of the operator provides:

- New features
- Various bug fixes

Images

This release includes the following container images:

- **Redis Enterprise**: reddlabs/redis:6.0.20-97 or reddlabs/redis:6.0.20-97.rhel7-openshift
- **Operator and Bootstrapper**: reddlabs/operator:6.0.20-12
- **Services Rigger**: reddlabs/k8s-controller:6.0.20-12 or reddlabs/services-manager:6.0.20-12 (on the Red Hat registry)

New features

- EKS support
- Feature parity for Openshift OLM; added support for:
  - REDB
  - admission
  - Hashicorp Vault integration
- Hashicorp Vault integration is now GA
- Moved Operator environment variables to configmap

Important fixes

- Admission controller deployment combined with operator deployment to simplify deployment (RED-52701)
- Additional verbosity in the kubectl get redb command output (RED-55042)
- Support for Redis Enterprise license storage within secrets; Vault and K8s secrets (RED-55587)
- Support for manual procedure to replace the REC credentials (RED-56529, RED-56530)
- Fixed cluster recovery issue - recovery process was not starting (RED-55500)
- When a pod status is CrashLoopBackOff and we run the cluster recovery, the process will not complete (RED-33713)
Known limitations

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

Nodes down indefinitely after the redis-enterprise-node container of a REC pod is restarted (53042)
In some cases where the Redis Enterprise Cluster container in the Redis Enterprise Cluster (REC) pod is restarted, the REC node remains down. Workaround: restart the pod, while ensuring the majority of REC nodes are available.

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.

Deleting an OpenShift project with an REC deployed may hang (RED47192)

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 (RED51921)

In K8s 1.15 or older, the PVC labels come from the match selectors and not the PVC templates. As such, these versions can not support PVC labels. If this feature is required, the only fix is to upgrade the K8s cluster to a newer version.

Compatibility Notes

- EKS is now supported (K8s 1.18)
- OpenShift 4.4 (previously deprecated) is no longer supported
- GKE K8s versions 1.15, 1.16 (previously deprecated) is no longer supported
- VMWare TKGI 1.10 (K8s 1.19) is now supported

Deprecation notice

- GKE K8s version 1.17 (no longer supported by Google) is deprecated
- kOps 1.15 is deprecated
- VMWare TKGI 1.7 (K8s 1.16), VMWare TKGI 1.8 (K8s 1.17) are deprecated (no longer supported by VMWare)

Updated: January 11, 2022