OpenShift Container Platform 3.11

Service Mesh Release Notes

OpenShift Container Platform 3.11 Service Mesh Release Notes

Last Updated: 2019-08-19

OpenShift Container Platform 3.11 Service Mesh Release Notes

OpenShift Container Platform 3.11 Service Mesh Release Notes

Legal Notice

Abstract

Release Notes for Service Mesh

Table of Contents

CHAPTER 1. RED HAT OPENSHIFT SERVICE MESH RELEASE NOTES 3

1.1. INTRODUCTION TO RED HAT OPENSHIFT SERVICE MESH 0.12.TECHPREVIEW 3

1.1.1. Red Hat OpenShift Service Mesh overview 3

1.1.2. Getting support 3

1.2. NEW AND CHANGED FEATURES 4

1.2.1. New features Technology Preview 12 4

1.2.2. New features Technology Preview 11 4

1.2.3. New features Technology Preview 10 4

1.2.4. New features Technology Preview 9 4

1.2.5. New features Technology Preview 8 4

1.2.6. New features Technology Preview 7 5

1.2.7. New features Technology Preview 6 5

1.2.8. New features Technology Preview 5 5

1.2.9. New features Technology Preview 4 5

1.2.10. New features Technology Preview 3 5

1.2.11. New features Technology Preview 2 5

1.2.12. New features Technology Preview 1 5

1.3. RESOLVED ISSUES 5

1.3.1. Fixed issues 6

1.4. KNOWN ISSUES 7

1.4.1. Known issues 7

1.4.1.1. Red Hat OpenShift Service Mesh Issues 8

1.4.1.2. Kiali Issues 10

CHAPTER 1. RED HAT OPENSHIFT SERVICE MESH RELEASE NOTES

1.1. INTRODUCTION TO RED HAT OPENSHIFT SERVICE MESH 0.12.TECHPREVIEW

1.1.1. Red Hat OpenShift Service Mesh overview

IMPORTANT

This release of Red Hat OpenShift Service Mesh is a Technology Preview release only. Technology Preview releases are not supported with Red Hat production service-level agreements (SLAs) and might not be functionally complete, and Red Hat does NOT recommend using them for production. Using Red Hat OpenShift Service Mesh on a cluster renders the whole OpenShift cluster as a technology preview, that is, in an unsupported state. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process. For more information see Red Hat Technology Preview Features Support Scope.

Red Hat OpenShift Service Mesh is a platform that provides behavioral insight and operational control over the service mesh, providing a uniform way to connect, secure, and monitor microservice applications.

The term *service mesh* describes the network of microservices that make up applications in a distributed microservice architecture and the interactions between those microservices. As a service mesh grows in size and complexity, it can become harder to understand and manage.

Based on the open source Istio project, Red Hat OpenShift Service Mesh adds a transparent layer on existing distributed applications without requiring any changes to the service code. You add Red Hat OpenShift Service Mesh support to services by deploying a special sidecar proxy throughout your environment that intercepts all network communication between microservices. You configure and manage the service mesh using the control plane features.

Red Hat OpenShift Service Mesh provides an easy way to create a network of deployed services that provides discovery, load balancing, service-to-service authentication, failure recovery, metrics, and monitoring. A service mesh also provides more complex operational functionality, including A/B testing, canary releases, rate limiting, access control, and end-to-end authentication.

1.1.2. Getting support

If you experience difficulty with a procedure described in this documentation, visit the Red Hat Customer Portal at http://access.redhat.com. Through the customer portal, you can:

- Search or browse through the Red Hat Knowledgebase of technical support articles about Red Hat products
- Submit a support case to Red Hat Global Support Services (GSS)
- Access other product documentation

If you have a suggestion for improving this guide or have found an error, please submit a Bugzilla report at http://bugzilla.redhat.com against **Product** for the **Documentation** component. Please provide specific details, such as the section number, guide name, and {product-title_short} version so we can easily locate the content.

1.2. NEW AND CHANGED FEATURES

1.2.1. New features Technology Preview 12

This release of Red Hat OpenShift Service Mesh adds support for Istio 1.1.8, Jaeger 1.13.1, Kiali 1.0.0, and the 3scale Istio Adapter 0.7.1.

Other notable changes in this release include the following:

- Integrates the Kiali and Jaeger Operators into the installation.
- Adds support for Kubernetes Container Network Interface (CNI).
- Adds support for Operator Lifecycle Management (OLM).
- Updates the Istio OpenShift Router for multitenancy.
- Defaults to configuring the control planes for multitenancy. You can still configure a single tenant control plane in Red Hat OpenShift Service Mesh 0.12.TechPreview.

NOTE

To simplify installation and support, future releases will only support a multi-tenant control plane for one or more tenants.

1.2.2. New features Technology Preview 11

The release of Red Hat OpenShift Service Mesh adds support for multi-tenant installations, Red Hat Enterprise Linux (RHEL) Universal Base Images (UBI8), OpenSSL 1.1.1, Kiali 0.20.x, the 3scale Istio Adapter 0.6.0, and Istio 1.1.5.

1.2.3. New features Technology Preview 10

The release of Red Hat OpenShift Service Mesh adds support for Kiali 0.16.x, the 3scale Istio Adapter 0.5.0, and Istio 1.1.

1.2.4. New features Technology Preview 9

NOTE

Starting with Red Hat OpenShift Service Mesh 0.9.TechPreview, Mixer's policy enforcement is disabled by default, but you must enable it to run policy tasks. See Update Mixer policy enforcement for instructions on enabling Mixer policy enforcement.

The release of Red Hat OpenShift Service Mesh adds support for Kiali 0.15.x, Jaeger 1.11, the 3scale Istio Adapter 0.4.1, and Istio 1.1.0-rc.2.

1.2.5. New features Technology Preview 8

The release of Red Hat OpenShift Service Mesh adds support for Kiali 0.14.x and the 3scale Istio Adapter 0.3.

1.2.6. New features Technology Preview 7

The release of Red Hat OpenShift Service Mesh adds the 3scale Istio Adapter and support for Kiali 0.13.x, Jaeger 1.9.0, and Istio 1.1.

1.2.7. New features Technology Preview 6

The release of Red Hat OpenShift Service Mesh adds support for Kiali 0.11.x and and Istio 1.0.5.

1.2.8. New features Technology Preview 5

The release of Red Hat OpenShift Service Mesh adds support for Kiali 0.10.x, Jaeger 1.8.1, and Istio 1.0.4.

1.2.9. New features Technology Preview 4

The release of Red Hat OpenShift Service Mesh adds support for Kiali 0.9.x and Istio 1.0.3.

1.2.10. New features Technology Preview 3

The release of Red Hat OpenShift Service Mesh adds support for OpenShift 3.11, support for Kiali 0.8.x, and an updated base Ansible installer (3.11.16-3).

1.2.11. New features Technology Preview 2

The release adds the Kiali observability console to Red Hat OpenShift Service Mesh. Kiali provides a number of graphs that you can use to view the topography and health of the microservices that make up your service mesh. You can view predefined dashboards that provide detailed request and response metrics (volume, duration, size, TCP traffic) per inbound and outbound traffic. You can also browse your service mesh by application, workloads, and services to view the health of each element.

1.2.12. New features Technology Preview 1

Red Hat OpenShift Service Mesh provides a number of key capabilities uniformly across a network of services:

- **Traffic Management** - Control the flow of traffic and API calls between services, make calls more reliable, and make the network more robust in the face of adverse conditions.

- **Service Identity and Security**- Provide services in the mesh with a verifiable identity and provide the ability to protect service traffic as it flows over networks of varying degrees of trustworthiness.

- **Policy Enforcement** - Apply organizational policy to the interaction between services, ensure access policies are enforced and resources are fairly distributed among consumers. Policy changes are made by configuring the mesh, not by changing application code.

- **Telemetry** - Gain understanding of the dependencies between services and the nature and flow of traffic between them, providing the ability to quickly identify issues.

1.3. RESOLVED ISSUES

1.3.1. Fixed issues

The following issues been resolved in the current release:

- MAISTRA-4 - The uninstall does not remove all the files, and as a result, when you re-install the istio-operator installation fails because **customresourcedefinitions.apiextensions.k8s.io "installations.istio.openshift.com"** already exists.

- MAISTRA-5 - **openshift-ansible-istio-installer-job** pod tries to start but with errors.

- MAISTRA-13 - Installer should determine release version from installed components. At present, the installer queries the yaml file, however if the yaml has been modified, the installer is not able to remove an older version.

- MAISTRA-21 - The default in the installer of 512Mi was too low for tracing. Increased default Elasticsearch memory from 512 MB to 1 GB.

- MAISTRA-61 After all applicable resources are deployed to OpenShift, Istio sidecars may lose information about their routes and can no longer communicate with services until the next update is received.

- MAISTRA-79 - Running the **istiooc cluster up** command results in the istio-operator namespace deploying a pod responsible for continually ensuring the Elasticsearch sysctl requirements are met. This loop runs constantly causing a significant load on the system running the cluster.

- MAISTRA-110 In large clusters, citadel can take a significant amount of time to create secrets. This may cause the installation to fail.

- MAISTRA-157 The conditional rate limiting feature does not restrict access as expected.

- MAISTRA-196 If you edit the installation to modify a parameter, for example to enable authentication, the new installation will fail due to the existence of the new 1.1 CRD configmaps.

- MAISTRA-420 [Multi-tenant implementation] The Jaeger agent pods are unscheduled as a result of port collision in multi-tenancy deployment on OpenShift 4.1.rc.5.

- MAISTRA-245 The sidecar injector pod fails to start if you are running the upstream community version.

- MAISTRA-462 [Multi-tenant implementation] After adding a namespace member to a second control plane, Kiali does not display the namespace member in the namespace list because the namespace for the second control plane is missing the **maistra.io/member-of** and **istio.openshift.io/member-of** labels. This is a result of the installation of the second control plane failing due to MAISTRA-464(the operator can't create the **istio-ingressgateway** service in the second control plane, because the NodePort already being used by the first control plane). The workaround is to manually change the node ports of the **istio-ingressgateway** service in the first control plane's namespace (using **oc edit svc**). The operator will then be able to finish deploying the second control plane.

- MAISTRA-466 [Multi-tenant implementation] When you install more than one control plane, the operator overwrites the Kiali oauthclient yaml on any existing Kiali installations so that only the most recent installation functions. The Kiali oauthclient (**oc get oauthclients kiali**) contains a list of the authorized URLs that OpenShift OAuth will redirect to. If your URL is not part of this list, then the oauth login will fail and return the following message:

> `{"error":"invalid_request","error_description":"The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed."}

- MAISTRA-469 If you delete a project before deleting the ServiceMeshControlPlane, the cleanup process does not execute for resources in the deleted project. Service accounts added to the SecurityContextConstraints are not removed and the Kiali OAuthClient resource is not updated properly.

- MAISTRA-470 If you include the control plane namespace in the member roll, the reconciliation process produces an error that spams the logs and prevents the status of the configuredMembers list from updating even for members that were successfully configured.

- KIALI-1284 In Istio, a Workload can be any pod or group of pods, regardless where they originate from. They may come from Kubernetes Deployments, Replica Sets or even as a single "orphan" pod. In Kiali the current assumption is that a Workload comes from a Deployment. This should represent the vast majority of the cases.

- KIALI-1570 When a graph is loading in the Kiali console, a message that the graph is empty is displayed instead of a message that the graph is loading.

- KIALI-1572 If you see this ERROR message when you view the Kiali logs, you can ignore it:

  > Failed to determine console version from file [/opt/kiali/console/version.txt]. error=open /opt/kiali/console/version.txt: no such file or directory Kiali: Console version: unknown

- KIALI-1609 When dealing with very small values (for example, less than 0.0.1 rps) you might encounter some inconsistencies in the graph. We are working on making changes to have this function better when dealing with very small values.

- KIALI-2261 In the Kiali graph, unused links (that is, edges with no traffic) are being labeled as having 100% of the request traffic, even though there is currently no request traffic. See also KIALI-2296.

- KIALI-2403 The Istio version is no longer listed on the Kiali About page after moving to Istio 1.1.0-snapshot.6, because the latest Istio Pilot now listens on a different port. Istio Pilot listens on port 8080, and you can visit Pilot to determine the Istio version (http://istio-pilot:8080/version).

- KIALI-2430 When you click on a TCP edge, and then click on an HTTP edge the graph crashes in Kiali.

- KIALI-2671 If you **do not** specify a dashboard user/password in the control plane custom resource the operator will use Oauth for the installation. The OpenShift strategy for using Oauth does not work in Red Hat OpenShift Service Mesh 0.12.TechPreview Technology Preview 10. As a workaround, ensure that you provide a user and password in the custom resource.

- KIALI-2942 When using OpenShift OAuth, when you click the logout link, you are still logged into the Kiali console. When you go to the login URL it will check your cookies and then automatically log you back in. The workaround is to delete the Kiali cookie.

1.4. KNOWN ISSUES

1.4.1. Known issues

These limitations exist in Red Hat OpenShift Service Mesh at this time:

- Red Hat OpenShift Service Mesh does not support IPv6, as it it not supported by the upstream Istio project, nor fully supported by OpenShift.
- The istio-init container requires a privileged security context or at least to run as root and to have the NET_ADMIN capability. The istio-init container needs to be privileged because it needs to properly configure the iptables rules in the pod to intercept network connections. The team is currently investigating ideas for ways to reduce the privileges required by Istio.

  NOTE

  The Istio CNI plugin allows a pod to join the service mesh without requiring additional privileges to be granted for each pod. To enable the plugin, edit the control plane custom resource file to set the **enabled** field in the **istio_cni** section to **true**.

- Graph layout - The layout for the Kiali graph can render differently, depending on your application architecture and the data to display (number of graph nodes and their interactions). Because it is difficult if not impossible to create a single layout that renders nicely for every situation, Kiali offers a choice of several different layouts. To choose a different layout, you can choose a different **Layout Schema** from the **Graph Settings** menu.

NOTE

While Kafka publisher is included in the release as part of Jaeger, it is not supported.

1.4.1.1. Red Hat OpenShift Service Mesh Issues

These are the known issues in Red Hat OpenShift Service Mesh at this time:

- MAISTRA-684 The default Jaeger version in the **istio-operator** is 1.12.0, which does not match Jaeger version 1.13.1 that shipped in Red Hat OpenShift Service Mesh 0.12.TechPreview.
  If you install Red Hat OpenShift Service Mesh 0.12.TechPreview without changing the Jaeger version to 1.13.1, this is what you see when you check the pods in **istio-system**:

```
$ oc get pods -n istio-system

NAME                                      READY   STATUS              RESTARTS   AGE
elasticsearch-0                             1/1     Running            0          16m
grafana-694d54c786-m6dfc                    2/2     Running            0          18m
istio-citadel-7658c96954-r8p46              1/1     Running            0          18m
istio-egressgateway-d759556b8-hwc7n         1/1     Running            0          18m
istio-galley-7cf565999f-b729t               1/1     Running            0          18m
istio-ingressgateway-bc97545d5-5mpw4        1/1     Running            0          18m
istio-pilot-dd7c67fb5-r8nbt                 2/2     Running            0          29m
istio-policy-b5df8c557-5xbbl                2/2     Running            0          18m
istio-sidecar-injector-5bccb75987-xl6t6     1/1     Running            0          18m
istio-telemetry-7f86b4f6d9-kgl5p            2/2     Running            0          30m
jaeger-collector-85c597698c-54b2c           0/1     ImagePullBackOff   0          18m
jaeger-query-59b877c9d9-92vmj               1/3     ImagePullBackOff   0          18m
kiali-54ff784b57-8clh2                      1/1     Running            0          18m
prometheus-7b89468cf6-pbnqh                 2/2     Running            0          18m
```

Run this command to see **istio-system** events:

```
$ oc get events -n istio-system
```

You will see this error:

```
...
8m50s      Warning   Failed                    pod/jaeger-query-59b877c9d9-92vmj
Failed to pull image "registry.redhat.io/distributed-tracing-tech-preview/jaeger-agent:1.12.0":
rpc error: code = Unknown desc = Error reading manifest 1.12.0 in
registry.redhat.io/distributed-tracing-tech-preview/jaeger-agent: error parsing HTTP 404
response body: invalid character 'F' looking for beginning of value: "File not found.\""
...
```

The workaround is to make the following change to your custom resource to ensure you install Jaeger 1.13.1:

```
  tracing:
    enabled: true
    jaeger:
      tag: 1.13.1
```

- MAISTRA-622 In Maistra 0.12.0/TP12, permissive mode does not work. The user has the option to use Plain text mode or Mutual TLS mode, but not permissive.

- MAISTRA-572 Jaeger cannot be used with Kiali. In this release Jaeger is configured to use the OAuth proxy, but is also only configured to work through a browser and doesn't allow service access. Kiali cannot properly communicate with the Jaeger endpoint and it considers Jaeger to be disabled. See also TRACING-591.

- MAISTRA-465 The Maistra operator fails to create a service for operator metrics.

- MAISTRA-453 If you create a new project and deploy pods immediately, sidecar injection does not occur. The operator fails to add the **maistra.io/member-of** before the pods are created, therefore the pods must be deleted and recreated for sidecar injection to occur.

- MAISTRA-357 In OpenShift 4 Beta on AWS, it is not possible, out of the box, to access a TCP or HTTPS service through the ingress gateway on a port other than port 80. The AWS load balancer has a health check that verifies if port 80 on the service endpoint is active.
  The load balancer health check only checks the first port defined in the Istio ingress gateway ports list. This port is configured as 80/HTTP:31380/TCP. Without a service running on this port, the load balancer health check fails.

  To check HTTPS or TCP traffic by using an ingress gateway, you must have an existing HTTP service, for example, the Bookinfo sample application product page running on the ingress gateway port 80. Alternatively, using the AWS EC2 console, you can change the port that the load balancer uses to perform the health check, and replace 80 with the port your service actually uses.

- MAISTRA-348 To access a TCP service by using the ingress gateway on a port other than 80 or 443, use the service hostname provided by the AWS load balancer rather than the OpenShift router.
  The istio-ingressgateway route hostname (for example, **istio-ingressgateway-istio-system.apps.[cluster name].openshift.com**) works with port 80 or port 443 traffic. However, that route hostname does not support other port traffic.

To access service(s) running on the ingress gateway TCP port(s), you can retrieve the istio-ingressgateway external hostname (for example, **[uuid].[aws region].elb.amazonaws.com**) and then check traffic by using that external hostname value.

To retrieve the external IP hostname value, issue this command:

```
$ oc -n istio-system get service istio-ingressgateway -o
jsonpath='{.status.loadBalancer.ingress[0].hostname}'
```

- MAISTRA-193 Unexpected console info messages are visible when health checking is enabled for citadel.

- MAISTRA-158 Applying multiple gateways referencing the same hostname will cause all gateways to stop functioning.

- MAISTRA-108 Part of the process to install Operator Lifecycle Manager (OLM) in an OpenShift Container Platform cluster is to run the registry authorization playbook, but an error prevents the process from completing successfully.
  The task "openshift_control_plane : Check for file paths outside of /etc/origin/master in master's config" fails because if finds "/dev/null" string within the master-config.yaml file. This string is added when we patch the configuration when preparing the cluster to install Istio.

  Here are the two webhooks:

  ```
  MutatingAdmissionWebhook:
  configuration:
  apiVersion: apiserver.config.k8s.io/v1alpha1
  kind: WebhookAdmission
  kubeConfigFile: /dev/null
  ```

  ```
  ValidatingAdmissionWebhook:
  configuration:
  apiVersion: apiserver.config.k8s.io/v1alpha1s
  kind: WebhookAdmission
  kubeConfigFile: /dev/null
  ```

  Create a soft link from **/var/lib/origin/null** to **/dev/null** and replace the two kubeConfigFile variables to **/var/lib/origin/null**. This makes the task think /var/lib/origin/null is an asset in the origin "perimeter" and continue running.

- MAISTRA-62 After a successful Istio installation, when upgrading an OCP cluster from 3.10 to 3.11, the storage upgrade task fails causing the entire upgrade process to fail.

1.4.1.2. Kiali Issues

- KIALI-3118 After changes to the ServiceMeshMemberRoll, for example adding or removing namespaces, the Kiali pod restarts and then displays errors on the Graph page while the Kiali pod is restarting.

- KIALI-3096 Runtime metrics fail in the Service Mesh. There is an oauth filter between the the Service Mesh and Prometheus, requiring a bearer token to be passed to Prometheus before access will be granted. Kiali has been updated to use this token when communicating to the Prometheus server, but the application metrics are currently failing with 403 errors.

- KIALI-2206 When you are accessing the Kiali console for the first time, and there is no cached browser data for Kiali, the “View in Grafana” link on the Metrics tab of the Kiali Service Details page redirects to the wrong location. The only way you would encounter this issue is if you are accessing Kiali for the first time.

- KIALI-507 Kiali does not support Internet Explorer 11. This is because the underlying frameworks do not support Internet Explorer. To access the Kiali console, use one of the two most recent versions of the Chrome, Edge, Firefox or Safari browser.