OpenShift Container Platform 4.15 Red Hat build of OpenTelemetry

Red Hat build of OpenTelemetry
Abstract

Use the Red Hat build of the open source OpenTelemetry project to collect unified, standardized, and vendor-neutral telemetry data collection for cloud-native software.
# Table of Contents

## CHAPTER 1. RELEASE NOTES

1.1. RELEASE NOTES FOR RED HAT BUILD OF OPENTELEMETRY 3.1
   1.1.1. Red Hat build of OpenTelemetry overview
   1.1.2. New features and enhancements
   1.1.3. Getting support
   1.1.4. Making open source more inclusive

1.2. RELEASE NOTES FOR PAST RELEASES OF RED HAT BUILD OF OPENTELEMETRY
   1.2.1. Distributed tracing overview
   1.2.2. Release notes for Red Hat build of OpenTelemetry 3.0
      1.2.2.1. New features and enhancements
      1.2.2.2. Removal notice
      1.2.2.3. Bug fixes
      1.2.2.4. Known issues
   1.2.3. Release notes for Red Hat build of OpenTelemetry 2.9.2
      1.2.3.1. CVEs
      1.2.3.2. Known issues
   1.2.4. Release notes for Red Hat build of OpenTelemetry 2.9.1
      1.2.4.1. CVEs
      1.2.4.2. Known issues
   1.2.5. Release notes for Red Hat build of OpenTelemetry 2.9
      1.2.5.1. New features and enhancements
      1.2.5.2. Known issues
   1.2.6. Release notes for Red Hat build of OpenTelemetry 2.8
      1.2.6.1. Bug fixes
   1.2.7. Release notes for Red Hat build of OpenTelemetry 2.7
      1.2.7.1. Bug fixes
   1.2.8. Release notes for Red Hat build of OpenTelemetry 2.6
      1.2.8.1. Bug fixes
   1.2.9. Release notes for Red Hat build of OpenTelemetry 2.5
      1.2.9.1. New features and enhancements
      1.2.9.2. Bug fixes
   1.2.10. Release notes for Red Hat build of OpenTelemetry 2.4
      1.2.10.1. Bug fixes
   1.2.11. Release notes for Red Hat build of OpenTelemetry 2.3
      1.2.11.1. Bug fixes
   1.2.12. Release notes for Red Hat build of OpenTelemetry 2.2
      1.2.12.1. Technology Preview features
      1.2.12.2. Bug fixes
   1.2.13. Release notes for Red Hat build of OpenTelemetry 2.1
      1.2.13.1. Technology Preview features
      1.2.13.2. Bug fixes
   1.2.14. Release notes for Red Hat build of OpenTelemetry 2.0
      1.2.15. Getting support
      1.2.16. Making open source more inclusive

## CHAPTER 2. INSTALLING THE RED HAT BUILD OF OPENTELEMETRY

2.1. INSTALLING THE RED HAT BUILD OF OPENTELEMETRY FROM THE WEB CONSOLE
2.2. INSTALLING THE RED HAT BUILD OF OPENTELEMETRY BY USING THE CLI
2.3. ADDITIONAL RESOURCES

## CHAPTER 3. CONFIGURATION OF THE OPENTELEMETRY COLLECTOR
3.1. OPENTELEMETRY COLLECTOR CONFIGURATION OPTIONS

3.2. OPENTELEMETRY COLLECTOR COMPONENTS

3.2.1. Receivers
   3.2.1.1. OTLP Receiver
   3.2.1.2. Jaeger Receiver
   3.2.1.3. Prometheus Receiver
   3.2.1.4. Zipkin Receiver
   3.2.1.5. Kafka Receiver
   3.2.1.6. OpenCensus receiver

3.2.2. Processors
   3.2.2.1. Batch processor
   3.2.2.2. Memory Limiter processor
   3.2.2.3. Resource Detection processor
   3.2.2.4. Attributes processor
   3.2.2.5. Resource processor
   3.2.2.6. Span processor
   3.2.2.7. Kubernetes Attributes processor
   3.2.2.8. Filter processor
   3.2.2.9. Routing processor

3.2.3. Exporters
   3.2.3.1. OTLP exporter
   3.2.3.2. OTLP HTTP exporter
   3.2.3.3. Debug exporter
   3.2.3.4. Prometheus exporter
   3.2.3.5. Kafka exporter

3.2.4. Connectors
   3.2.4.1. Spanmetrics connector

3.2.5. Extensions
   3.2.5.1. BearerTokenAuth extension
   3.2.5.2. OAuth2Client extension
   3.2.5.3. Jaeger Remote Sampling extension
   3.2.5.4. Performance Profiler extension
   3.2.5.5. Health Check extension
   3.2.5.6. Memory Ballast extension
   3.2.5.7. zPages extension

3.3. TARGET ALLOCATOR

CHAPTER 4. CONFIGURATION OF THE INSTRUMENTATION

4.1. OPENTELEMETRY INSTRUMENTATION CONFIGURATION OPTIONS

4.1.1. Instrumentation options

4.1.2. Using the instrumentation CR with Service Mesh
   4.1.2.1. Configuration of the Apache HTTP Server auto-instrumentation
   4.1.2.2. Configuration of the .NET auto-instrumentation
   4.1.2.3. Configuration of the Go auto-instrumentation
   4.1.2.4. Configuration of the Java auto-instrumentation
   4.1.2.5. Configuration of the Node.js auto-instrumentation
   4.1.2.6. Configuration of the Python auto-instrumentation
   4.1.2.7. Configuration of the OpenTelemetry SDK variables
   4.1.2.8. Multi-container pods

CHAPTER 5. SENDING TRACES AND METRICS TO THE OPENTELEMETRY COLLECTOR

5.1. SENDING TRACES AND METRICS TO THE OPENTELEMETRY COLLECTOR WITH SIDECAR INJECTION
5.2. Sending traces and metrics to the OpenTelemetry collector without sidecar injection

CHAPTER 6. Configuration for sending metrics to the monitoring stack

CHAPTER 7. Forwarding traces to a TemPostack

CHAPTER 8. Configuring the OpenTelemetry collector metrics

CHAPTER 9. Gathering the observability data from multiple clusters

CHAPTER 10. Troubleshooting the Red Hat build of OpenTelemetry

10.1. Getting the OpenTelemetry collector logs

10.2. Exposing the metrics

10.3. Debug exporter

CHAPTER 11. Migrating from the distributed tracing platform (Jaeger) to the Red Hat build of OpenTelemetry

11.1. Migrating from the distributed tracing platform (Jaeger) to the Red Hat build of OpenTelemetry with sidecars

11.2. Migrating from the distributed tracing platform (Jaeger) to the Red Hat build of OpenTelemetry without sidecars

CHAPTER 12. Updating the Red Hat build of OpenTelemetry

12.1. Additional resources

CHAPTER 13. Removing the Red Hat build of OpenTelemetry

13.1. Removing an OpenTelemetry collector instance by using the web console

13.2. Removing an OpenTelemetry collector instance by using the CLI

13.3. Additional resources
CHAPTER 1. RELEASE NOTES

1.1. RELEASE NOTES FOR RED HAT BUILD OF OPENTELEMETRY 3.1

1.1.1. Red Hat build of OpenTelemetry overview

Red Hat build of OpenTelemetry is based on the open source OpenTelemetry project, which aims to provide unified, standardized, and vendor-neutral telemetry data collection for cloud-native software. Red Hat build of OpenTelemetry product provides support for deploying and managing the OpenTelemetry Collector and simplifying the workload instrumentation.

The OpenTelemetry Collector can receive, process, and forward telemetry data in multiple formats, making it the ideal component for telemetry processing and interoperability between telemetry systems. The Collector provides a unified solution for collecting and processing metrics, traces, and logs.

The OpenTelemetry Collector has a number of features including the following:

- **Data Collection and Processing Hub**
  - It acts as a central component that gathers telemetry data like metrics and traces from various sources. This data can be created from instrumented applications and infrastructure.

- **Customizable telemetry data pipeline**
  - The OpenTelemetry Collector is designed to be customizable. It supports various processors, exporters, and receivers.

- **Auto-instrumentation features**
  - Automatic instrumentation simplifies the process of adding observability to applications. Developers don’t need to manually instrument their code for basic telemetry data.

Here are some of the use cases for the OpenTelemetry Collector:

- **Centralized data collection**
  - In a microservices architecture, the Collector can be deployed to aggregate data from multiple services.

- **Data enrichment and processing**
  - Before forwarding data to analysis tools, the Collector can enrich, filter, and process this data.

- **Multi-backend receiving and exporting**
  - The Collector can receive and send data to multiple monitoring and analysis platforms simultaneously.

1.1.2. New features and enhancements

This update introduces the following enhancements:

- Red Hat build of OpenTelemetry 3.1 is based on OpenTelemetry 0.93.0.

- Support for the target allocator in the OpenTelemetry Collector. The target allocator is an optional component of the OpenTelemetry Operator that shards Prometheus receiver scrape targets across the deployed fleet of OpenTelemetry Collector instances. The target allocator provides integration with the Prometheus PodMonitor and ServiceMonitor custom resources.

1.1.3. Getting support
If you experience difficulty with a procedure described in this documentation, or with OpenShift Container Platform in general, visit the Red Hat Customer Portal.

From the Customer Portal, you can:

- Search or browse through the Red Hat Knowledgebase of articles and solutions relating to Red Hat products.
- Submit a support case to Red Hat Support.
- Access other product documentation.

To identify issues with your cluster, you can use Insights in OpenShift Cluster Manager. Insights provides details about issues and, if available, information on how to solve a problem.

If you have a suggestion for improving this documentation or have found an error, submit a Jira issue for the most relevant documentation component. Please provide specific details, such as the section name and OpenShift Container Platform version.

1.1.4. Making open source more inclusive

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright’s message.

1.2. RELEASE NOTES FOR PAST RELEASES OF RED HAT BUILD OF OPENTELEMETRY

1.2.1. Distributed tracing overview

As a service owner, you can use distributed tracing to instrument your services to gather insights into your service architecture. You can use the Red Hat OpenShift distributed tracing platform for monitoring, network profiling, and troubleshooting the interaction between components in modern, cloud-native, microservices-based applications.

With the distributed tracing platform, you can perform the following functions:

- Monitor distributed transactions
- Optimize performance and latency
- Perform root cause analysis

The distributed tracing platform consists of three components:

- Red Hat OpenShift distributed tracing platform (Tempo) which is based on the open source Grafana Tempo project.
- Red Hat build of OpenTelemetry which is based on the open source OpenTelemetry project.
- Red Hat OpenShift distributed tracing platform (Jaeger) which is based on the open source Jaeger project.
1.2.2. Release notes for Red Hat build of OpenTelemetry 3.0

Red Hat build of OpenTelemetry 3.0 is based on OpenTelemetry 0.89.0.

1.2.2.1. New features and enhancements

This update introduces the following enhancements:

- The OpenShift distributed tracing data collection Operator is renamed as the Red Hat build of OpenTelemetry Operator.
- Support for the ARM architecture.
- Support for the Prometheus receiver for metrics collection.
- Support for the Kafka receiver and exporter for sending traces and metrics to Kafka.
- Support for cluster-wide proxy environments.
- The Red Hat build of OpenTelemetry Operator creates the Prometheus ServiceMonitor custom resource if the Prometheus exporter is enabled.
- The Operator enables the Instrumentation custom resource that allows injecting upstream OpenTelemetry auto-instrumentation libraries.

1.2.2.2. Removal notice

In Red Hat build of OpenTelemetry 3.0, the Jaeger exporter has been removed. Bug fixes and support are provided only through the end of the 2.9 lifecycle. As an alternative to the Jaeger exporter for sending data to the Jaeger collector, you can use the OTLP exporter instead.

1.2.2.3. Bug fixes

This update introduces the following bug fixes:

- Fixed support for disconnected environments when using the `oc adm catalog mirror` CLI command.

1.2.2.4. Known issues

There is currently a known issue:

- Currently, the cluster monitoring of the Red Hat build of OpenTelemetry Operator is disabled due to a bug (TRACING-3761). The bug is preventing the cluster monitoring from scraping metrics from the Red Hat build of OpenTelemetry Operator due to a missing label `openshift.io/cluster-monitoring=true` that is required for the cluster monitoring and service monitor object.

**Workaround**

You can enable the cluster monitoring as follows:
1. Add the following label in the Operator namespace: `oc label namespace openshift-opentelemetry-operator openshift.io/cluster-monitoring=true`

2. Create a service monitor, role, and role binding:

```yaml
apiVersion: monitoring.coreos.com/v1
kind: ServiceMonitor
metadata:
  name: opentelemetry-operator-controller-manager-metrics-service
  namespace: openshift-opentelemetry-operator
spec:
  endpoints:
    - bearerTokenFile: /var/run/secrets/kubernetes.io/serviceaccount/token
      path: /metrics
      port: https
      scheme: https
      tlsConfig:
        insecureSkipVerify: true
    selector:
      matchLabels:
      app.kubernetes.io/name: opentelemetry-operator
      control-plane: controller-manager
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: otel-operator-prometheus
  namespace: openshift-opentelemetry-operator
  annotations:
    include.release.openshift.io/self-managed-high-availability: "true"
    include.release.openshift.io/single-node-developer: "true"
rules:
- apiGroups:
  - ""
  resources:
  - services
  - endpoints
  - pods
  verbs:
  - get
  - list
  - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: otel-operator-prometheus
  namespace: openshift-opentelemetry-operator
  annotations:
    include.release.openshift.io/self-managed-high-availability: "true"
    include.release.openshift.io/single-node-developer: "true"
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: otel-operator-prometheus
subjects:
```
1.2.3. Release notes for Red Hat build of OpenTelemetry 2.9.2

IMPORTANT

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.9.2 is based on OpenTelemetry 0.81.0.

1.2.3.1. CVEs

- This release fixes CVE-2023-46234.

1.2.3.2. Known issues

There is currently a known issue:

- Currently, you must manually set operator maturity to Level IV, Deep Insights. (TRACING-3431)

1.2.4. Release notes for Red Hat build of OpenTelemetry 2.9.1

IMPORTANT

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.9.1 is based on OpenTelemetry 0.81.0.

1.2.4.1. CVEs

- This release fixes CVE-2023-44487.

1.2.4.2. Known issues
There is currently a known issue:

- Currently, you must manually set operator maturity to Level IV, Deep Insights. (TRACING-3431)

1.2.5. Release notes for Red Hat build of OpenTelemetry 2.9

**IMPORTANT**

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.9 is based on OpenTelemetry 0.81.0.

1.2.5.1. New features and enhancements

This release introduces the following enhancements for the Red Hat build of OpenTelemetry:

- Support OTLP metrics ingestion. The metrics can be forwarded and stored in the user-workload-monitoring via the Prometheus exporter.

- Support the operator maturity Level IV, Deep Insights, which enables upgrading and monitoring of OpenTelemetry Collector instances and the Red Hat build of OpenTelemetry Operator.

- Report traces and metrics from remote clusters using OTLP or HTTP and HTTPS.

- Collect OpenShift Container Platform resource attributes via the resourcedetection processor.

- Support the managed and unmanaged states in the OpenTelemetryCollector custom resource.

1.2.5.2. Known issues

There is currently a known issue:

- Currently, you must manually set operator maturity to Level IV, Deep Insights. (TRACING-3431)

1.2.6. Release notes for Red Hat build of OpenTelemetry 2.8
IMPORTANT

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.8 is based on OpenTelemetry 0.74.0.

1.2.6.1. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.

1.2.7. Release notes for Red Hat build of OpenTelemetry 2.7

IMPORTANT

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.7 is based on OpenTelemetry 0.63.1.

1.2.7.1. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.

1.2.8. Release notes for Red Hat build of OpenTelemetry 2.6

IMPORTANT

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.6 is based on OpenTelemetry 0.60.
1.2.8.1. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.

1.2.9. Release notes for Red Hat build of OpenTelemetry 2.5

IMPORTANT

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.5 is based on OpenTelemetry 0.56.

1.2.9.1. New features and enhancements

This update introduces the following enhancement:

- Support for collecting Kubernetes resource attributes to the Red Hat build of OpenTelemetry Operator.

1.2.9.2. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.

1.2.10. Release notes for Red Hat build of OpenTelemetry 2.4

IMPORTANT

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.4 is based on OpenTelemetry 0.49.

1.2.10.1. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.

1.2.11. Release notes for Red Hat build of OpenTelemetry 2.3

...
The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.3.1 is based on OpenTelemetry 0.44.1.

Red Hat build of OpenTelemetry 2.3.0 is based on OpenTelemetry 0.44.0.

1.2.11.1. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.

1.2.12. Release notes for Red Hat build of OpenTelemetry 2.2

Red Hat build of OpenTelemetry 2.2 is based on OpenTelemetry 0.42.0.

1.2.12.1. Technology Preview features

The unsupported OpenTelemetry Collector components included in the 2.1 release are removed.

1.2.12.2. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.

1.2.13. Release notes for Red Hat build of OpenTelemetry 2.1
IMPORTANT

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.1 is based on OpenTelemetry 0.41.1.

1.2.13.1. Technology Preview features

This release introduces a breaking change to how to configure certificates in the OpenTelemetry custom resource file. With this update, the `ca_file` moves under `tls` in the custom resource, as shown in the following examples.

CA file configuration for OpenTelemetry version 0.33

```yaml
spec:
  mode: deployment
  config:
    exporters:
      jaeger:
        endpoint: jaeger-production-collector-headless.tracing-system.svc:14250
        ca_file: /var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt
```

CA file configuration for OpenTelemetry version 0.41.1

```yaml
spec:
  mode: deployment
  config:
    exporters:
      jaeger:
        endpoint: jaeger-production-collector-headless.tracing-system.svc:14250
        tls:
          ca_file: /var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt
```

1.2.13.2. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.

1.2.14. Release notes for Red Hat build of OpenTelemetry 2.0
IMPORTANT

The Red Hat build of OpenTelemetry is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

Red Hat build of OpenTelemetry 2.0 is based on OpenTelemetry 0.33.0.

This release adds the Red Hat build of OpenTelemetry as a Technology Preview, which you install using the Red Hat build of OpenTelemetry Operator. Red Hat build of OpenTelemetry is based on the OpenTelemetry APIs and instrumentation. The Red Hat build of OpenTelemetry includes the OpenTelemetry Operator and Collector. You can use the Collector to receive traces in the OpenTelemetry or Jaeger protocol and send the trace data to the Red Hat build of OpenTelemetry. Other capabilities of the Collector are not supported at this time. The OpenTelemetry Collector allows developers to instrument their code with vendor agnostic APIs, avoiding vendor lock-in and enabling a growing ecosystem of observability tooling.

1.2.15. Getting support

If you experience difficulty with a procedure described in this documentation, or with OpenShift Container Platform in general, visit the Red Hat Customer Portal.

From the Customer Portal, you can:

- Search or browse through the Red Hat Knowledgebase of articles and solutions relating to Red Hat products.
- Submit a support case to Red Hat Support.
- Access other product documentation.

To identify issues with your cluster, you can use Insights in OpenShift Cluster Manager. Insights provides details about issues and, if available, information on how to solve a problem.

If you have a suggestion for improving this documentation or have found an error, submit a Jira issue for the most relevant documentation component. Please provide specific details, such as the section name and OpenShift Container Platform version.

1.2.16. Making open source more inclusive

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright’s message.
CHAPTER 2. INSTALLING THE RED HAT BUILD OF OPENTELEMETRY

Installing the Red Hat build of OpenTelemetry involves the following steps:

1. Installing the Red Hat build of OpenTelemetry Operator.

2. Creating a namespace for an OpenTelemetry Collector instance.

3. Creating an `OpenTelemetryCollector` custom resource to deploy the OpenTelemetry Collector instance.

2.1. INSTALLING THE RED HAT BUILD OF OPENTELEMETRY FROM THE WEB CONSOLE

You can install the Red Hat build of OpenTelemetry from the Administrator view of the web console.

Prerequisites

- You are logged in to the web console as a cluster administrator with the `cluster-admin` role.

- For Red Hat OpenShift Dedicated, you must be logged in using an account with the `dedicated-admin` role.

Procedure

1. Install the Red Hat build of OpenTelemetry Operator:

   a. Go to Operators → OperatorHub and search for Red Hat build of OpenTelemetry Operator.

   b. Select the Red Hat build of OpenTelemetry Operator that is provided by Red Hat → Install → Install → View Operator.

   IMPORTANT

   This installs the Operator with the default presets:

   - Update channel → stable
   - Installation mode → All namespaces on the cluster
   - Installed Namespace → openshift-operators
   - Update approval → Automatic

   c. In the Details tab of the installed Operator page, under ClusterServiceVersion details, verify that the installation Status is Succeeded.

2. Create a project of your choice for the OpenTelemetry Collector instance that you will create in the next step by going to Home → Projects → Create Project.

3. Create an OpenTelemetry Collector instance.
a. Go to **Operators → Installed Operators**.

b. Select **OpenTelemetry Collector → Create OpenTelemetry Collector → YAML view**.

c. In the **YAML view**, customize the **OpenTelemetryCollector** custom resource (CR) with the OTLP, Jaeger, Zipkin receivers and the debug exporter.

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: otel
  namespace: <project_of_opentelemetry_collector_instance>
spec:
  mode: deployment
  config:
    receivers:
      otlp:
        protocols:
          grpc:
          http:
      jaeger:
        protocols:
          grpc:
          thrift_binary:
          thrift_compact:
          thrift_http:
      zipkin:
    processors:
      batch:
        memory_limiter:
          check_interval: 1s
          limit_percentage: 50
          spike_limit_percentage: 30
    exporters:
      debug:
    service:
    pipelines:
      traces:
        receivers: [otlp,jaeger,zipkin]
        processors: [memory_limiter,batch]
        exporters: [debug]
```

d. Select **Create**.

**Verification**

1. Use the **Project**: dropdown list to select the project of the **OpenTelemetry Collector** instance.

2. Go to **Operators → Installed Operators** to verify that the **Status** of the **OpenTelemetry Collector** instance is **Condition: Ready**.

3. Go to **Workloads → Pods** to verify that all the component pods of the **OpenTelemetry Collector** instance are running.
2.2. INSTALLING THE RED HAT BUILD OF OPENTELEMETRY BY USING THE CLI

You can install the Red Hat build of OpenTelemetry from the command line.

Prerequisites

- An active OpenShift CLI (oc) session by a cluster administrator with the `cluster-admin` role.

TIP

- Ensure that your OpenShift CLI (oc) version is up to date and matches your OpenShift Container Platform version.
- Run `oc login`:
  ```
  $ oc login --username=<your_username>
  ```

Procedure

1. Install the Red Hat build of OpenTelemetry Operator:
   a. Create a project for the Red Hat build of OpenTelemetry Operator by running the following command:
      ```
      $ oc apply -f - << EOF
      apiVersion: project.openshift.io/v1
      kind: Project
      metadata:
        labels:
          kubernetes.io/metadata.name: openshift-opentelemetry-operator
          openshift.io/cluster-monitoring: "true"
          name: openshift-opentelemetry-operator
      EOF
      ```
   b. Create an Operator group by running the following command:
      ```
      $ oc apply -f - << EOF
      apiVersion: operators.coreos.com/v1
      kind: OperatorGroup
      metadata:
        name: openshift-opentelemetry-operator
      spec:
        upgradeStrategy: Default
      EOF
      ```
   c. Create a subscription by running the following command:
      ```
      $ oc apply -f - << EOF
      apiVersion: operators.coreos.com/v1alpha1
      kind: Subscription
      metadata:
        name: opentelemetry-product
      EOF
      ```
d. Check the Operator status by running the following command:

```
$ oc get csv -n openshift-opentelemetry-operator
```

2. Create a project of your choice for the OpenTelemetry Collector instance that you will create in a subsequent step:

- To create a project without metadata, run the following command:

```
$ oc new-project <project_of_opentelemetry_collector_instance>
```

- To create a project with metadata, run the following command:

```
$ oc apply -f - << EOF
apiVersion: project.openshift.io/v1
kind: Project
metadata:
  name: <project_of_opentelemetry_collector_instance>
EOF
```

3. Create an OpenTelemetry Collector instance in the project that you created for it.

**NOTE**

You can create multiple OpenTelemetry Collector instances in separate projects on the same cluster.

a. Customize the **OpenTelemetry Collector** custom resource (CR) with the OTLP, Jaeger, and Zipkin receivers and the debug exporter:

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: otel
  namespace: <project_of_opentelemetry_collector_instance>
spec:
  mode: deployment
  config:
    receivers:
      otlp:
        protocols:
          grpc:
          http:
      jaeger:
        protocols:
```
Apply the customized CR by running the following command:

```
$ oc apply -f - << EOF
<OpenTelemetryCollector_custom_resource>
EOF
```

**Verification**

1. Verify that the `status.phase` of the OpenTelemetry Collector pod is **Running** and the `conditions` are **type: Ready** by running the following command:

```
$ oc get pod -l app.kubernetes.io/managed-by=opentelemetry-operator,app.kubernetes.io/instance=<namespace>.<instance_name> -o yaml
```

2. Get the OpenTelemetry Collector service by running the following command:

```
$ oc get service -l app.kubernetes.io/managed-by=opentelemetry-operator,app.kubernetes.io/instance=<namespace>.<instance_name>
```

### 2.3. ADDITIONAL RESOURCES

- Creating a cluster admin
- OperatorHub.io
- Accessing the web console
- Installing from OperatorHub using the web console
- Creating applications from installed Operators
- Getting started with the OpenShift CLI
CHAPTER 3. CONFIGURATION OF THE OPENTELEMETRY COLLECTOR

The Red Hat build of OpenTelemetry Operator uses a custom resource definition (CRD) file that defines the architecture and configuration settings to be used when creating and deploying the Red Hat build of OpenTelemetry resources. You can install the default configuration or modify the file.

3.1. OPENTELEMETRY COLLECTOR CONFIGURATION OPTIONS

The OpenTelemetry Collector consists of five types of components that access telemetry data:

**Receivers**

A receiver, which can be push or pull based, is how data gets into the Collector. Generally, a receiver accepts data in a specified format, translates it into the internal format, and passes it to processors and exporters defined in the applicable pipelines. By default, no receivers are configured. One or more receivers must be configured. Receivers may support one or more data sources.

**Processors**

Optional. Processors process the data between it is received and exported. By default, no processors are enabled. Processors must be enabled for every data source. Not all processors support all data sources. Depending on the data source, multiple processors might be enabled. Note that the order of processors matters.

**Exporters**

An exporter, which can be push or pull based, is how you send data to one or more back ends or destinations. By default, no exporters are configured. One or more exporters must be configured. Exporters can support one or more data sources. Exporters might be used with their default settings, but many exporters require configuration to specify at least the destination and security settings.

**Connectors**

A connector connects two pipelines. It consumes data as an exporter at the end of one pipeline and emits data as a receiver at the start of another pipeline. It can consume and emit data of the same or different data type. It can generate and emit data to summarize the consumed data, or it can merely replicate or route data.

**Extensions**

An extension adds capabilities to the Collector. For example, authentication can be added to the receivers and exporters automatically.

You can define multiple instances of components in a custom resource YAML file. When configured, these components must be enabled through pipelines defined in the `spec.config.service` section of the YAML file. As a best practice, only enable the components that you need.

**Example of the OpenTelemetry Collector custom resource file**

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: cluster-collector
  namespace: tracing-system
spec:
  mode: deployment
  observability:
    metrics:
      enableMetrics: true
```
If a component is configured but not defined in the `service` section, the component is not enabled.

### Table 3.1. Parameters used by the Operator to define the OpenTelemetry Collector

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>receivers:</td>
<td>A receiver is how data gets into the Collector. By default, no receivers are configured. There must be at least one enabled receiver for a configuration to be considered valid. Receivers are enabled by being added to a pipeline.</td>
<td>otlp, jaeger, prometheus, zipkin, kafka, opencensus</td>
<td>None</td>
</tr>
<tr>
<td>processors:</td>
<td>Processors run through the received data before it is exported. By default, no processors are enabled.</td>
<td>batch, memorylimiter, resourcedetection, attributes, span, k8sattributes, filter, routing</td>
<td>None</td>
</tr>
</tbody>
</table>
An exporter sends data to one or more back ends or destinations. By default, no exporters are configured. There must be at least one enabled exporter for a configuration to be considered valid. Exporters are enabled by being added to a pipeline. Exporters might be used with their default settings, but many require configuration to specify at least the destination and security settings.

Connectors join pairs of pipelines by consuming data as end-of-pipeline exporters and emitting data as start-of-pipeline receivers. Connectors can be used to summarize, replicate, or route consumed data.

Optional components for tasks that do not involve processing telemetry data.

Components are enabled by adding them to a pipeline under `services.pipeline`. You enable receivers for tracing by adding them under `service.pipelines.traces`.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>exporters:</td>
<td>An exporter sends data to one or more back ends or destinations. By default, no exporters are configured. There must be at least one enabled exporter for a configuration to be considered valid. Exporters are enabled by being added to a pipeline. Exporters might be used with their default settings, but many require configuration to specify at least the destination and security settings.</td>
<td>otlp, otlphttp, debug, prometheus, kafka</td>
<td>None</td>
</tr>
<tr>
<td>connectors:</td>
<td>Connectors join pairs of pipelines by consuming data as end-of-pipeline exporters and emitting data as start-of-pipeline receivers. Connectors can be used to summarize, replicate, or route consumed data.</td>
<td>spanmetrics</td>
<td>None</td>
</tr>
<tr>
<td>extensions:</td>
<td>Optional components for tasks that do not involve processing telemetry data.</td>
<td>bearertokenauth, oauth2client, jaegerremotesampler, pprof, health_check, memory_ballast, zpages</td>
<td>None</td>
</tr>
<tr>
<td>service: pipelines:</td>
<td>Components are enabled by adding them to a pipeline under <code>services.pipeline</code>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>service: pipelines: traces: receivers:</td>
<td>You enable receivers for tracing by adding them under <code>service.pipelines.traces</code>.</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>service:</td>
<td>You enable processors for tracing by adding them under service.pipelines.traces</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>pipelines:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>traces:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processors:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| service:        | You enable exporters for tracing by adding them under service.pipelines.traces | None        | None       |
| pipelines:      |                                                                              |             |            |
| traces:         |                                                                              |             |            |
| exporters:      |                                                                              |             |            |

| service:        | You enable receivers for metrics by adding them under service.pipelines.metrics | None        | None       |
| pipelines:      |                                                                              |             |            |
| metrics:        |                                                                              |             |            |
| receivers:      |                                                                              |             |            |

| service:        | You enable processors for metrics by adding them under service.pipelines.metrics | None        | None       |
| pipelines:      |                                                                              |             |            |
| metrics:        |                                                                              |             |            |
| processors:     |                                                                              |             |            |

| service:        | You enable exporters for metrics by adding them under service.pipelines.metrics | None        | None       |
| pipelines:      |                                                                              |             |            |
| metrics:        |                                                                              |             |            |
| exporters:      |                                                                              |             |            |

### 3.2. OPENTELEMETRY COLLECTOR COMPONENTS

#### 3.2.1. Receivers

Receivers get data into the Collector.

#### 3.2.1.1. OTLP Receiver

The OTLP receiver ingests traces and metrics using the OpenTelemetry protocol (OTLP).

**OpenTelemetry Collector custom resource with an enabled OTLP receiver**

```yaml
cfg:
  | receivers:
```
The OTLP gRPC endpoint. If omitted, the default **0.0.0.0:4317** is used.

The server-side TLS configuration. Defines paths to TLS certificates. If omitted, TLS is disabled.

The path to the TLS certificate at which the server verifies a client certificate. This sets the value of `ClientCA` and `ClientAuth` to `RequireAndVerifyClientCert` in the `TLSConfig`. For more information, see the Config of the Golang TLS package.

Specifies the time interval at which the certificate is reloaded. If the value is not set, the certificate is never reloaded. The `reload_interval` accepts a string containing valid units of time such as **ns, us** (or **µs**), **ms, s, m, h**.

The OTLP HTTP endpoint. The default value is **0.0.0.0:4318**.

The server-side TLS configuration. For more information, see the `grpc` protocol configuration section.

### 3.2.1.2. Jaeger Receiver

The Jaeger receiver ingests traces in the Jaeger formats.

**OpenTelemetry Collector custom resource with an enabled Jaeger receiver**
The Jaeger gRPC endpoint. If omitted, the default 0.0.0.0:14250 is used.

The Jaeger Thrift HTTP endpoint. If omitted, the default 0.0.0.0:14268 is used.

The Jaeger Thrift Compact endpoint. If omitted, the default 0.0.0.0:6831 is used.

The Jaeger Thrift Binary endpoint. If omitted, the default 0.0.0.0:6832 is used.

The server-side TLS configuration. See the OTLP receiver configuration section for more details.

3.2.1.3. Prometheus Receiver

The Prometheus receiver is currently a Technology Preview feature only.

The Prometheus receiver scrapes the metrics endpoints.

**OpenTelemetry Collector custom resource with an enabled Prometheus receiver**

```yaml
config:
  receivers:
    prometheus:
      config:
        scrape_configs:
        - job_name: 'my-app'
          scrape_interval: 5s
          static_configs:
            - targets: ['my-app.example.svc.cluster.local:8888']

service:
  pipelines:
    metrics:
      receivers: [prometheus]
```

1. Scrapes configurations using the Prometheus format.
2. The Prometheus job name.
3. The Interval for scraping the metrics data. Accepts time units. The default value is 1m.
4. The targets at which the metrics are exposed. This example scrapes the metrics from a my-app application in the example project.

3.2.1.4. Zipkin Receiver

The Zipkin receiver ingests traces in the Zipkin v1 and v2 formats.
OpenTelemetry Collector custom resource with the enabled Zipkin receiver

```yaml
config:
  receivers:
    zipkin:
      endpoint: 0.0.0.0:9411 1
      tls: 2

    service:
      pipelines:
        traces:
          receivers: [zipkin]
```

1. The Zipkin HTTP endpoint. If omitted, the default `0.0.0.0:9411` is used.
2. The server-side TLS configuration. See the OTLP receiver configuration section for more details.

### 3.2.1.5. Kafka Receiver

The Kafka receiver is currently a Technology Preview feature only.

The Kafka receiver receives traces, metrics, and logs from Kafka in the OTLP format.

OpenTelemetry Collector custom resource with the enabled Kafka receiver

```yaml
config:
  receivers:
    kafka:
      brokers: ["localhost:9092"] 1
      protocol_version: 2.0.0 2
      topic: otlp_spans 3
      auth:
        plain_text: 4
        username: example
        password: example
      tls: 5
        ca_file: ca.pem
        cert_file: cert.pem
        key_file: key.pem
        insecure: false 6
        server_name_override: kafka.example.corp 7

    service:
      pipelines:
        traces:
          receivers: [kafka]
```

1. The list of Kafka brokers. The default is `localhost:9092`.
2. The Kafka protocol version. For example, `2.0.0`. This is a required field.
3. The name of the Kafka topic to read from. The default is `otlp_spans`.
4. The plaintext authentication configuration. If omitted, plaintext authentication is disabled.
The client-side TLS configuration. Defines paths to the TLS certificates. If omitted, TLS authentication is disabled.

Disables verifying the server’s certificate chain and host name. The default is false.

ServerName indicates the name of the server requested by the client to support virtual hosting.

3.2.1.6. OpenCensus receiver

The OpenCensus receiver provides backwards compatibility with the OpenCensus project for easier migration of instrumented codebases. It receives metrics and traces in the OpenCensus format via gRPC or HTTP and Json.

OpenTelemetry Collector custom resource with the enabled OpenCensus receiver

config:
receivers:
  opencensus:
    endpoint: 0.0.0.0:9411
    tls:
      cors_allowed_origins:
        - https://*.<example>.com

service:
  pipelines:
    traces:
      receivers: [opencensus]

1. The OpenCensus endpoint. If omitted, the default is 0.0.0.0:55678.
2. The server-side TLS configuration. See the OTLP receiver configuration section for more details.
3. You can also use the HTTP JSON endpoint to optionally configure CORS, which is enabled by specifying a list of allowed CORS origins in this field. Wildcards with * are accepted under the cors_allowed_origins. To match any origin, enter only *.

3.2.2. Processors

Processors run through the data between it is received and exported.

3.2.2.1. Batch processor

The Batch processor batches traces and metrics to reduce the number of outgoing connections needed to transfer the telemetry information.

Example of the OpenTelemetry Collector custom resource when using the Batch processor

config:
  processor:
    batch:
      timeout: 5s
      send_batch_max_size: 10000
Table 3.2. Parameters used by the Batch processor

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>Sends the batch after a specific time duration and irrespective of the batch size.</td>
<td>200ms</td>
</tr>
<tr>
<td>send_batch_size</td>
<td>Sends the batch of telemetry data after the specified number of spans or metrics.</td>
<td>8192</td>
</tr>
<tr>
<td>send_batch_max_size</td>
<td>The maximum allowable size of the batch. Must be equal or greater than the send_batch_size.</td>
<td>0</td>
</tr>
<tr>
<td>metadata_keys</td>
<td>When activated, a batcher instance is created for each unique set of values found in the client.Metadata.</td>
<td>[]</td>
</tr>
<tr>
<td>metadata_cardinality_limit</td>
<td>When the metadata_keys are populated, this configuration restricts the number of distinct metadata key-value combinations processed throughout the duration of the process.</td>
<td>1000</td>
</tr>
</tbody>
</table>

3.2.2.2. Memory Limiter processor

The Memory Limiter processor periodically checks the Collector’s memory usage and pauses data processing when the soft memory limit is reached. This processor supports traces, metrics, and logs. The preceding component, which is typically a receiver, is expected to retry sending the same data and may apply a backpressure to the incoming data. When memory usage exceeds the hard limit, the Memory Limiter processor forces garbage collection to run.

Example of the OpenTelemetry Collector custom resource when using the Memory Limiter processor

```
config: |
  processor: |
    memory_limiter: |
      check_interval: 1s
      limit_mib: 4000
      spike_limit_mib: 800
```
Table 3.3. Parameters used by the Memory Limiter processor

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>check_interval</td>
<td>Time between memory usage measurements. The optimal value is 1s. For spiky traffic patterns, you can decrease the check_interval or increase the spike_limit_mib.</td>
<td>0s</td>
</tr>
<tr>
<td>limit_mib</td>
<td>The hard limit, which is the maximum amount of memory in MiB allocated on the heap. Typically, the total memory usage of the OpenTelemetry Collector is about 50 MiB greater than this value.</td>
<td>0</td>
</tr>
<tr>
<td>spike_limit_mib</td>
<td>Spike limit, which is the maximum expected spike of memory usage in MiB. The optimal value is approximately 20% of limit_mib. To calculate the soft limit, subtract the spike_limit_mib from the limit_mib.</td>
<td>20% of limit_mib</td>
</tr>
<tr>
<td>limit_percentage</td>
<td>Same as the limit_mib but expressed as a percentage of the total available memory. The limit_mib setting takes precedence over this setting.</td>
<td>0</td>
</tr>
<tr>
<td>spike_limit_percentage</td>
<td>Same as the spike_limit_mib but expressed as a percentage of the total available memory. Intended to be used with the limit_percentage setting.</td>
<td>0</td>
</tr>
</tbody>
</table>

3.2.2.3. Resource Detection processor

The Resource Detection processor is currently a Technology Preview feature only.

The Resource Detection processor identifies host resource details in alignment with OpenTelemetry’s resource semantic standards. Using the detected information, it can add or replace the resource values in telemetry data. This processor supports traces, metrics, and can be used with multiple detectors such
as the Docket metadata detector or the **OTEL_RESOURCE_ATTRIBUTES** environment variable detector.

**OpenShift Container Platform permissions required for the Resource Detection processor**

```yaml
kind: ClusterRole
metadata:
  name: otel-collector
rules:
- apiGroups: ["config.openshift.io"]
  resources: ["infrastructures", "infrastructures/status"]
  verbs: ["get", "watch", "list"]
```

**OpenTelemetry Collector using the Resource Detection processor**

```yaml
config: |
  processor:
    resourcedetection:
      detectors: [openshift]
      override: true
  service:
    pipelines:
      traces:
        processors: [resourcedetection]
      metrics:
        processors: [resourcedetection]
```

**OpenTelemetry Collector using the Resource Detection Processor with an environment variable detector**

```yaml
config: |
  processors:
    resourcedetection/env:
      detectors: [env]
      timeout: 2s
      override: false
```

1. Specifies which detector to use. In this example, the environment detector is specified.

### 3.2.2.4. Attributes processor

The Attributes processor is currently a **Technology Preview** feature only.

The Attributes processor can modify attributes of a span, log, or metric. You can configure this processor to filter and match input data and include or exclude such data for specific actions.

The processor operates on a list of actions, executing them in the order specified in the configuration. The following actions are supported:

- **Insert**
  
  Inserts a new attribute into the input data when the specified key does not already exist.

- **Update**
Updates an attribute in the input data if the key already exists.

**Upset**

Combines the insert and update actions: Inserts a new attribute if the key does not exist yet. Updates the attribute if the key already exists.

**Delete**

Removes an attribute from the input data.

**Hash**

Hashes an existing attribute value as SHA1.

**Extract**

Extracts values by using a regular expression rule from the input key to the target keys defined in the rule. If a target key already exists, it will be overridden similarly to the Span processor’s `to_attributes` setting with the existing attribute as the source.

**Convert**

Converts an existing attribute to a specified type.

### OpenTelemetry Collector using the Attributes processor

```yaml
config:
  processors:
    attributes/example:
      actions:
        - key: db.table
          action: delete
        - key: redacted_span
          value: true
          action: upsert
        - key: copy_key
          from_attribute: key_original
          action: update
        - key: account_id
          value: 2245
          action: insert
        - key: account_password
          action: delete
        - key: account_email
          action: hash
        - key: http.status_code
          action: convert
          converted_type: int
```

### 3.2.2.5. Resource processor

The Resource processor is currently a Technology Preview feature only.

The Resource processor applies changes to the resource attributes. This processor supports traces, metrics, and logs.

### OpenTelemetry Collector using the Resource Detection processor

```yaml
config:
  processor:
```
Attributes represent the actions that are applied to the resource attributes, such as delete the attribute, insert the attribute, or upsert the attribute.

### 3.2.2.6. Span processor

The Span processor is currently a Technology Preview feature only.

The Span processor modifies the span name based on its attributes or extracts the span attributes from the span name. It can also change the span status. It can also include or exclude spans. This processor supports traces.

Span renaming requires specifying attributes for the new name by using the `from_attributes` configuration.

**OpenTelemetry Collector using the Span processor for renaming a span**

```yaml
config: |
  processor:
    span:
      name:
        from_attributes: [<key1>, <key2>, ...] ①
        separator: <value> ②

① Defines the keys to form the new span name.
② An optional separator.
```

You can use the processor to extract attributes from the span name.

**OpenTelemetry Collector using the Span processor for extracting attributes from a span name**

```yaml
config: |
  processor:
    span/to_attributes:
      name:
        to_attributes:
          rules:
            - ^/api/v1/document/(.*)/update$ ①

① This rule defines how the extraction is to be executed. You can define more rules: for example, in this case, if the regular expression matches the name, a `documentID` attribute is created. In this example, if the input span name is `/api/v1/document/12345678/update`, this results in the
You can have the span status modified.

OpenTelemetry Collector using the Span Processor for status change

```yaml
config: |
  processor:
    span/set_status:
      status:
        code: Error
        description: "<error_description>"
```

3.2.2.7. Kubernetes Attributes processor

The Kubernetes Attributes processor is currently a Technology Preview feature only.

The Kubernetes Attributes processor enables automatic configuration of spans, metrics, and log resource attributes by using the Kubernetes metadata. This processor supports traces, metrics, and logs. This processor automatically identifies the Kubernetes resources, extracts the metadata from them, and incorporates this extracted metadata as resource attributes into relevant spans, metrics, and logs. It utilizes the Kubernetes API to discover all pods operating within a cluster, maintaining records of their IP addresses, pod UIDs, and other relevant metadata.

Minimum OpenShift Container Platform permissions required for the Kubernetes Attributes processor

```yaml
kind: ClusterRole
metadata:
  name: otel-collector
rules:
  - apiGroups: ['']
    resources: ['pods', 'namespaces']
    verbs: ['get', 'watch', 'list']
```

OpenTelemetry Collector using the Kubernetes Attributes processor

```yaml
config: |
  processors:
    k8sattributes:
      filter:
        node_from_env_var: KUBE_NODE_NAME
```

3.2.2.8. Filter processor

The Filter processor is currently a Technology Preview feature only.

The Filter processor leverages the OpenTelemetry Transformation Language to establish criteria for discarding telemetry data. If any of these conditions are satisfied, the telemetry data are discarded. The conditions can be combined by using the logical OR operator. This processor supports traces, metrics, and logs.
OpenTelemetry Collector custom resource with an enabled OTLP exporter

```
config:
  processors:
    filter/ottl:
      error_mode: ignore
    traces:
      span:
        - 'attributes["container.name"] == "app_container_1"'
        - 'resource.attributes["host.name"] == "localhost"'
```

1. Defines the error mode. When set to `ignore`, ignores errors returned by conditions. When set to `propagate`, returns the error up the pipeline. An error causes the payload to be dropped from the Collector.

2. Filters the spans that have the `container.name == app_container_1` attribute.

3. Filters the spans that have the `host.name == localhost` resource attribute.

### 3.2.2.9. Routing processor

The Routing processor is currently a Technology Preview feature only.

The Routing processor routes logs, metrics, or traces to specific exporters. This processor can read a header from an incoming HTTP request (gRPC or plain HTTP) or can read a resource attribute, and then directs the trace information to relevant exporters according to the read value.

OpenTelemetry Collector custom resource with an enabled OTLP exporter

```
config:
  processors:
    routing:
      from_attribute: X-Tenant
    default_exporters:
      - jaeger
      table:
        - value: acme
          exporters: [jaeger/acme]
    exporters:
      jaeger:
        endpoint: localhost:14250
      jaeger/acme:
        endpoint: localhost:24250
```

1. The HTTP header name for the lookup value when performing the route.

2. The default exporter when the attribute value is not present in the table in the next section.

3. The table that defines which values are to be routed to which exporters.
You can optionally create an `attribute_source` configuration, which defines where to look for the attribute in `from_attribute`. The allowed value is `context` to search the context, which includes the HTTP headers, or `resource` to search the resource attributes.

### 3.2.3. Exporters

Exporters send data to one or more back ends or destinations.

#### 3.2.3.1. OTLP exporter

The OTLP gRPC exporter exports traces and metrics using the OpenTelemetry protocol (OTLP).

**OpenTelemetry Collector custom resource with an enabled OTLP exporter**

```yaml
config:
  exporters:
    otlp:
      endpoint: tempo-ingester:4317
      tls:
        ca_file: ca.pem
        cert_file: cert.pem
        key_file: key.pem
        insecure: false
        insecure_skip_verify: false
        reload_interval: 1h
        server_name_override: <name>
      headers:
        X-Scope-OrgID: "dev"

service:
  pipelines:
    traces:
      exporters: [otlp]
    metrics:
      exporters: [otlp]
```

1. The OTLP gRPC endpoint. If the `https://` scheme is used, then client transport security is enabled and overrides the `insecure` setting in the `tls`.
2. The client-side TLS configuration. Defines paths to TLS certificates.
3. Disables client transport security when set to `true`. The default value is `false` by default.
4. Skips verifying the certificate when set to `true`. The default value is `false`.
5. Specifies the time interval at which the certificate is reloaded. If the value is not set, the certificate is never reloaded. The `reload_interval` accepts a string containing valid units of time such as `ns, us` (or `µs`), `ms, s, m, h`.
6. Overrides the virtual host name of authority such as the authority header field in requests. You can use this for testing.
7. Headers are sent for every request performed during an established connection.
3.2.3.2. OTLP HTTP exporter

The OTLP HTTP exporter exports traces and metrics using the OpenTelemetry protocol (OTLP).

OpenTelemetry Collector custom resource with an enabled OTLP exporter

```yaml
config:
  exporters:
    otlphttp:
      endpoint: http://tempo-ingester:4318
      tls: 2
      headers: 3
      X-Scope-OrgID: "dev"
      disable_keep_alives: false 4

  service:
    pipelines:
      traces:
        exporters: [otlphttp]
      metrics:
        exporters: [otlphttp]
```

1. The OTLP HTTP endpoint. If the `https://` scheme is used, then client transport security is enabled and overrides the `insecure` setting in the `tls`.

2. The client side TLS configuration. Defines paths to TLS certificates.

3. Headers are sent in every HTTP request.

4. If true, disables HTTP keep-alives. It will only use the connection to the server for a single HTTP request.

3.2.3.3. Debug exporter

The Debug exporter prints traces and metrics to the standard output.

OpenTelemetry Collector custom resource with an enabled Debug exporter

```yaml
config:
  exporters:
    debug:
      verbosity: detailed 1

  service:
    pipelines:
      traces:
        exporters: [logging]
      metrics:
        exporters: [logging]
```

1. Verbosity of the debug export: `detailed` or `normal` or `basic`. When set to `detailed`, pipeline data is verbosely logged. Defaults to `normal`.  

---

37
### 3.2.3.4. Prometheus exporter

The Prometheus exporter is currently a Technology Preview feature only.

The Prometheus exporter exports metrics in the Prometheus or OpenMetrics formats.

**OpenTelemetry Collector custom resource with an enabled Prometheus exporter**

```yaml
ports:
  - name: promexporter
    port: 8889
    protocol: TCP
    config:
      exporters:
        prometheus:
          endpoint: 0.0.0.0:8889
          tls:
            ca_file: ca.pem
            cert_file: cert.pem
            key_file: key.pem
          namespace: prefix
          const_labels:
            label1: value1
          enable_open_metrics: true
          resource_to_telemetry_conversion: enabled
          metric_expiration: 180m
          add_metric_suffixes: false

service:
  pipelines:
  metrics:
    exporters: [prometheus]
```

1. Exposes the Prometheus port from the Collector pod and service. You can enable scraping of metrics by Prometheus by using the port name in `ServiceMonitor` or `PodMonitor` custom resource.

2. The network endpoint where the metrics are exposed.

3. The server-side TLS configuration. Defines paths to TLS certificates.

4. If set, exports metrics under the provided value. No default.

5. Key-value pair labels that are applied for every exported metric. No default.

6. If `true`, metrics are exported using the OpenMetrics format. Exemplars are only exported in the OpenMetrics format and only for histogram and monotonic sum metrics such as `counter`. Disabled by default.

7. If `enabled` is `true`, all the resource attributes are converted to metric labels by default. Disabled by default.

8. Defines how long metrics are exposed without updates. The default is `5m`.

9. Adds the metrics types and units suffixes. Must be disabled if the monitor tab in Jaeger console is enabled. The default is `true`. 
3.2.3.5. Kafka exporter

The Kafka exporter is currently a Technology Preview feature only.

The Kafka exporter exports logs, metrics, and traces to Kafka. This exporter uses a synchronous producer that blocks and does not batch messages. It must be used with batch and queued retry processors for higher throughput and resiliency.

OpenTelemetry Collector custom resource with an enabled Kafka exporter

```yaml
config:
  exporters:
    kafka:
      brokers: ["localhost:9092"]
      protocol_version: 2.0.0
      topic: otlp_spans
      auth:
        plain_text:
          username: example
          password: example
      tls:
        ca_file: ca.pem
        cert_file: cert.pem
        key_file: key.pem
        insecure: false
        server_name_override: kafka.example.corp
  service:
    pipelines:
      traces:
        exporters: [kafka]
```

1. The list of Kafka brokers. The default is `localhost:9092`.
2. The Kafka protocol version. For example, `2.0.0`. This is a required field.
3. The name of the Kafka topic to read from. The following are the defaults: `otlp_spans` for traces, `otlp_metrics` for metrics, `otlp_logs` for logs.
4. The plaintext authentication configuration. If omitted, plaintext authentication is disabled.
5. The client-side TLS configuration. Defines paths to the TLS certificates. If omitted, TLS authentication is disabled.
6. Disables verifying the server's certificate chain and host name. The default is `false`.
7. ServerName indicates the name of the server requested by the client to support virtual hosting.

3.2.4. Connectors

Connectors connect two pipelines.

3.2.4.1. Spanmetrics connector

The Spanmetrics connector is currently a Technology Preview feature only.
The Spanmetrics connector aggregates Request, Error, and Duration (R.E.D) OpenTelemetry metrics from span data.

**OpenTelemetry Collector custom resource with an enabled spanmetrics connector**

```
config:
  connectors:
    spanmetrics:
      metrics_flush_interval: 15s
  service:
    pipelines:
      traces:
        exporters: [spanmetrics]
        metrics:
          receivers: [spanmetrics]
```

1. Defines the flush interval of the generated metrics. Defaults to 15s.

### 3.2.5. Extensions

Extensions add capabilities to the Collector.

#### 3.2.5.1. BearerTokenAuth extension

The BearerTokenAuth extension is currently a Technology Preview feature only.

The BearerTokenAuth extension is an authenticator for receivers and exporters that are based on the HTTP and the gRPC protocol. You can use the OpenTelemetry Collector custom resource to configure client authentication and server authentication for the BearerTokenAuth extension on the receiver and exporter side. This extension supports traces, metrics, and logs.

**OpenTelemetry Collector custom resource with client and server authentication configured for the BearerTokenAuth extension**

```
config:
  extensions:
    bearertokenauth:
      scheme: "Bearer" 1
      token: "<token>" 2
      filename: "<token_file>" 3

  receivers:
    otlp:
      protocols:
        http:
          auth:
            authenticator: bearertokenauth 4
  exporters:
    otlp:
      auth:
        authenticator: bearertokenauth 5
  service:
```

1. Scheme for client authentication
2. Token for client authentication
3. Filename for token file
4. Authenticator for HTTP protocol
5. Authenticator for Otlp exporter
You can configure the BearerTokenAuth extension to send a custom scheme. The default is Bearer.

You can add the BearerTokenAuth extension token as metadata to identify a message.

Path to a file that contains an authorization token that is transmitted with every message.

You can assign the authenticator configuration to an OTLP receiver.

You can assign the authenticator configuration to an OTLP exporter.

### 3.2.5.2. OAuth2Client extension

The OAuth2Client extension is currently a Technology Preview feature only.

The OAuth2Client extension is an authenticator for exporters that are based on the HTTP and the gRPC protocol. Client authentication for the OAuth2Client extension is configured in a separate section in the OpenTelemetry Collector custom resource. This extension supports traces, metrics, and logs.

**OpenTelemetry Collector custom resource with client authentication configured for the OAuth2Client extension**

```yaml
config:
  extensions:
    oauth2client:
      client_id: <client_id>  # 1
      client_secret: <client_secret>  # 2
      endpoint_params:  # 3
        audience: <audience>
      token_url: https://example.com/oauth2/default/v1/token  # 4
      scopes: ["api.metrics"]  # 5
    # tls settings for the token client
    tls:
      insecure: true  # 7
      ca_file: /var/lib/mycert.pem  # 8
      cert_file: <cert_file>  # 9
      key_file: <key_file>  # 10
      timeout: 2s  # 11
  receivers:
    otlp:
      protocols:
        http:
  exporters:
    otlp:
      auth:
```
Client identifier, which is provided by the identity provider.

Confidential key used to authenticate the client to the identity provider.

Further metadata, in the key-value pair format, which is transferred during authentication. For example, **audience** specifies the intended audience for the access token, indicating the recipient of the token.

The URL of the OAuth2 token endpoint, where the Collector requests access tokens.

The scopes define the specific permissions or access levels requested by the client.

The Transport Layer Security (TLS) settings for the token client, which is used to establish a secure connection when requesting tokens.

When set to **true**, configures the Collector to use an insecure or non-verified TLS connection to call the configured token endpoint.

The path to a Certificate Authority (CA) file that is used to verify the server’s certificate during the TLS handshake.

The path to the client certificate file that the client must use to authenticate itself to the OAuth2 server if required.

The path to the client’s private key file that is used with the client certificate if needed for authentication.

Sets a timeout for the token client’s request.

You can assign the authenticator configuration to an OTLP exporter.

### 3.2.5.3. Jaeger Remote Sampling extension

The Jaeger Remote Sampling extension is currently a **Technology Preview** feature only.

The Jaeger Remote Sampling extension allows serving sampling strategies after Jaeger’s remote sampling API. You can configure this extension to proxy requests to a backing remote sampling server such as a Jaeger collector down the pipeline or to a static JSON file from the local file system.

**OpenTelemetry Collector custom resource with a configured Jaeger Remote Sampling extension**

```yaml
config:
  extensions:
    jaegerremotesampling:
      source:
```

---

1. Client identifier, which is provided by the identity provider.
2. Confidential key used to authenticate the client to the identity provider.
3. Further metadata, in the key-value pair format, which is transferred during authentication. For example, **audience** specifies the intended audience for the access token, indicating the recipient of the token.
4. The URL of the OAuth2 token endpoint, where the Collector requests access tokens.
5. The scopes define the specific permissions or access levels requested by the client.
6. The Transport Layer Security (TLS) settings for the token client, which is used to establish a secure connection when requesting tokens.
7. When set to **true**, configures the Collector to use an insecure or non-verified TLS connection to call the configured token endpoint.
8. The path to a Certificate Authority (CA) file that is used to verify the server’s certificate during the TLS handshake.
9. The path to the client certificate file that the client must use to authenticate itself to the OAuth2 server if required.
10. The path to the client’s private key file that is used with the client certificate if needed for authentication.
11. Sets a timeout for the token client’s request.
12. You can assign the authenticator configuration to an OTLP exporter.
The time interval at which the sampling configuration is updated.

The endpoint for reaching the Jaeger remote sampling strategy provider.

The path to a local file that contains a sampling strategy configuration in the JSON format.

Example of a Jaeger Remote Sampling strategy file

```json
{
    "service_strategies": [
        {
            "service": "foo",
            "type": "probabilistic",
            "param": 0.8,
            "operation_strategies": [
                {
                    "operation": "op1",
                    "type": "probabilistic",
                    "param": 0.2
                },
                {
                    "operation": "op2",
                    "type": "probabilistic",
                    "param": 0.4
                }
            ]
        },
        {
            "service": "bar",
            "type": "ratelimiting",
            "param": 5
        }
    ],
    "default_strategy": {
```
3.2.5.4. Performance Profiler extension

The Performance Profiler extension is currently a Technology Preview feature only.

The Performance Profiler extension enables the Go net/http/pprof endpoint. This is typically used by developers to collect performance profiles and investigate issues with the service.

**OpenTelemetry Collector custom resource with the configured Performance Profiler extension**

```yaml
config:
  extensions:
    pprof:
      endpoint: localhost:1777
      block_profile_fraction: 0
      mutex_profile_fraction: 0
      save_to_file: test.pprof

receivers:
  otlp:
    protocols:
      http:

exporters:
  otlp:

service:
  extensions: [pprof]
  pipelines:
    traces:
      receivers: [otlp]
      exporters: [otlp]
```

1. The endpoint at which this extension listens. Use `localhost:` to make it available only locally or `:0` to make it available on all network interfaces. The default value is `localhost:1777`.

2. Sets a fraction of blocking events to be profiled. To disable profiling, set this to 0 or a negative integer. See the documentation for the runtime package. The default value is 0.
Set a fraction of mutex contention events to be profiled. To disable profiling, set this to 0 or a negative integer. See the documentation for the runtime package. The default value is 0.

The name of the file in which the CPU profile is to be saved. Profiling starts when the Collector starts. Profiling is saved to the file when the Collector is terminated.

3.2.5.5. Health Check extension

The Health Check extension is currently a Technology Preview feature only.

The Health Check extension provides an HTTP URL for checking the status of the OpenTelemetry Collector. You can use this extension as a liveness and readiness probe on OpenShift.

OpenTelemetry Collector custom resource with the configured Health Check extension

```yaml
config:
  extensions:
    health_check:
      endpoint: "0.0.0.0:13133" 1
      tls: 2
        ca_file: "/path/to/ca.crt"
        cert_file: "/path/to/cert.crt"
        key_file: "/path/to/key.key"
        path: "/health/status" 3
      check_collector_pipeline: 4
        enabled: true 5
        interval: "5m" 6
        exporter_failure_threshold: 5 7

    receivers:
      otlp:
        protocols:
          http:

    exporters:
      otlp:

    service:
      extensions: [health_check]
      pipelines:
        traces:
          receivers: [otlp]
          exporters: [otlp]
```

1 The target IP address for publishing the health check status. The default is 0.0.0.0:13133.

2 The TLS server-side configuration. Defines paths to TLS certificates. If omitted, the TLS is disabled.

3 The path for the health check server. The default is /.

4 Settings for the Collector pipeline health check.
Enables the Collector pipeline health check. The default is false.

The time interval for checking the number of failures. The default is 5m.

The threshold of a number of failures until which a container is still marked as healthy. The default is 5.

3.2.5.6. Memory Ballast extension

The Memory Ballast extension is currently a Technology Preview feature only.

The Memory Ballast extension enables applications to configure memory ballast for the process.

OpenTelemetry Collector custom resource with the configured Memory Ballast extension

```yaml
config:
  extensions:
    memory_ballast:
      size_mib: 64
      size_in_percentage: 20

receivers:
  otlp:
    protocols:
      http:

exporters:
  otlp:

service:
  extensions: [memory_ballast]
  pipelines:
    traces:
      receivers: [otlp]
      exporters: [otlp]
```

1. Sets the memory ballast size in MiB. Takes priority over the size_in_percentage if both are specified.

2. Sets the memory ballast as a percentage, 1-100, of the total memory. Supports containerized and physical host environments.

3.2.5.7. zPages extension

The zPages extension is currently a Technology Preview feature only.

The zPages extension provides an HTTP endpoint for extensions that serve zPages. At the endpoint, this extension serves live data for debugging instrumented components. All core exporters and receivers provide some zPages instrumentation.

zPages are useful for in-process diagnostics without having to depend on a back end to examine traces or metrics.
OpenTelemetry Collector custom resource with the configured zPages extension

```yaml
config:
  extensions:
    zpages:
      endpoint: "localhost:55679"

receivers:
  otlp:
    protocols:
      http:
    exporters:
      otlp:

service:
  extensions: [zpages]
  pipelines:
    traces:
      receivers: [otlp]
      exporters: [otlp]
```

1. Specifies the HTTP endpoint that serves zPages. Use `localhost` to make it available only locally, or `*:` to make it available on all network interfaces. The default is `localhost:55679`.

### 3.3. TARGET ALLOCATOR

The target allocator is an optional component of the OpenTelemetry Operator that shards scrape targets across the deployed fleet of OpenTelemetry Collector instances. The target allocator integrates with the Prometheus PodMonitor and ServiceMonitor custom resources (CR). When the target allocator is enabled, the OpenTelemetry Operator adds the `http_sd_config` field to the enabled prometheus receiver that connects to the target allocator service.

**Example OpenTelemetryCollector CR with the enabled target allocator**

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: otel
  namespace: observability
spec:
  mode: statefulset
  targetAllocator:
    enabled: true
    serviceAccount: 
    prometheusCR:
      enabled: true
      scrapeInterval: 10s
      serviceMonitorSelector:
        name: app1
        podMonitorSelector:
          name: app2
      config: |
      receivers:
```

1. Specifies the HTTP endpoint that serves zPages. Use `localhost` to make it available only locally, or `*:` to make it available on all network interfaces. The default is `localhost:55679`.
When the target allocator is enabled, the deployment mode must be set to `statefulset`.

1. Enables the target allocator. Defaults to `false`.

2. The service account name of the target allocator deployment. The service account needs to have RBAC to get the `ServiceMonitor`, `PodMonitor` custom resources, and other objects from the cluster to properly set labels on scraped metrics. The default service name is `<collector_name>-targetallocator`.

3. Enables integration with the Prometheus `PodMonitor` and `ServiceMonitor` custom resources.

4. Label selector for the Prometheus `ServiceMonitor` custom resources. When left empty, enables all service monitors.

5. Label selector for the Prometheus `PodMonitor` custom resources. When left empty, enables all pod monitors.

6. Prometheus receiver with the minimal, empty `scrape_config: []` configuration option.

7. The target allocator deployment uses the Kubernetes API to get relevant objects from the cluster, so it requires a custom RBAC configuration.

**RBAC configuration for the target allocator service account**

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: otel-targetallocator
rules:
- apiGroups: [""
  resources:
  - services
  - pods
  verbs: ["get", "list", "watch"]
- apiGroups: ["monitoring.coreos.com"
  resources:
  - servicemonitors
  - podmonitors
  verbs: ["get", "list", "watch"]
- apiGroups: ["discovery.k8s.io"
  resources:
  - endpointslices
```
The name of the target allocator service account name.

The namespace of the target allocator service account.
CHAPTER 4. CONFIGURATION OF THE INSTRUMENTATION

IMPORTANT

OpenTelemetry instrumentation injection is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

The Red Hat build of OpenTelemetry Operator uses a custom resource definition (CRD) file that defines the configuration of the instrumentation.

4.1. OPENTELEMETRY INSTRUMENTATION CONFIGURATION OPTIONS

The Red Hat build of OpenTelemetry can inject and configure the OpenTelemetry auto-instrumentation libraries into your workloads. Currently, the project supports injection of the instrumentation libraries from Go, Java, Node.js, Python, .NET, and the Apache HTTP Server (httpd).

Auto-instrumentation in OpenTelemetry refers to the capability where the framework automatically instruments an application without manual code changes. This enables developers and administrators to get observability into their applications with minimal effort and changes to the existing codebase.

IMPORTANT

The Red Hat build of OpenTelemetry Operator only supports the injection mechanism of the instrumentation libraries but does not support instrumentation libraries or upstream images. Customers can build their own instrumentation images or use community images.

4.1.1. Instrumentation options

Instrumentation options are specified in the OpenTelemetryCollector custom resource.

Sample OpenTelemetryCollector custom resource file

```yaml
apiVersion: opentelemetry.io/v1alpha1
customResourceDefinition
metadata:
  name: java-instrumentation
spec:
  env:
    - name: OTEL_EXPORTER_OTLP_TIMEOUT
      value: "20"
  exporter:
    endpoint: http://production-collector.observability.svc.cluster.local:4317
    propagators:
      - w3c
    sampler:
```

50
Table 4.1. Parameters used by the Operator to define the Instrumentation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>env</td>
<td>Common environment variables to define across all the instrumentations.</td>
<td></td>
</tr>
<tr>
<td>exporter</td>
<td>Exporter configuration.</td>
<td></td>
</tr>
<tr>
<td>propagators</td>
<td>Propagators defines inter-process context propagation configuration.</td>
<td>tracecontext, baggage, b3, b3multi, jaeger, ottrace, none</td>
</tr>
<tr>
<td>resource</td>
<td>Resource attributes configuration.</td>
<td></td>
</tr>
<tr>
<td>sampler</td>
<td>Sampling configuration.</td>
<td></td>
</tr>
<tr>
<td>apacheHttpd</td>
<td>Configuration for the Apache HTTP Server instrumentation.</td>
<td></td>
</tr>
<tr>
<td>dotnet</td>
<td>Configuration for the .NET instrumentation.</td>
<td></td>
</tr>
<tr>
<td>go</td>
<td>Configuration for the Go instrumentation.</td>
<td></td>
</tr>
<tr>
<td>java</td>
<td>Configuration for the Java instrumentation.</td>
<td></td>
</tr>
<tr>
<td>nodejs</td>
<td>Configuration for the Node.js instrumentation.</td>
<td></td>
</tr>
<tr>
<td>python</td>
<td>Configuration for the Python instrumentation.</td>
<td></td>
</tr>
</tbody>
</table>
4.1.2. Using the instrumentation CR with Service Mesh

When using the instrumentation custom resource (CR) with Red Hat OpenShift Service Mesh, you must use the \texttt{b3multi} propagator.

4.1.2.1. Configuration of the Apache HTTP Server auto-instrumentation

Table 4.2. Parameters for the \texttt{.spec.apacheHttpd} field

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{attrs}</td>
<td>Attributes specific to the Apache HTTP Server.</td>
<td></td>
</tr>
<tr>
<td>\texttt{configPath}</td>
<td>Location of the Apache HTTP Server configuration.</td>
<td>/usr/local/apache2/conf</td>
</tr>
<tr>
<td>\texttt{env}</td>
<td>Environment variables specific to the Apache HTTP Server.</td>
<td></td>
</tr>
<tr>
<td>\texttt{image}</td>
<td>Container image with the Apache SDK and auto-instrumentation.</td>
<td></td>
</tr>
<tr>
<td>\texttt{resourceRequirements}</td>
<td>The compute resource requirements.</td>
<td></td>
</tr>
<tr>
<td>\texttt{version}</td>
<td>Apache HTTP Server version.</td>
<td>2.4</td>
</tr>
</tbody>
</table>

The \texttt{PodSpec} annotation to enable injection

\texttt{instrumentation.opentelemetry.io/inject-apache-httpd: "true"}

4.1.2.2. Configuration of the .NET auto-instrumentation

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{env}</td>
<td>Environment variables specific to .NET.</td>
</tr>
<tr>
<td>\texttt{image}</td>
<td>Container image with the .NET SDK and auto-instrumentation.</td>
</tr>
<tr>
<td>\texttt{resourceRequirements}</td>
<td>The compute resource requirements.</td>
</tr>
</tbody>
</table>
For the .NET auto-instrumentation, the required `OTEL_EXPORTER_OTLP_ENDPOINT` environment variable must be set if the endpoint of the exporters is set to 4317. The .NET autoinstrumentation uses `http/proto` by default, and the telemetry data must be set to the 4318 port.

The **PodSpec** annotation to enable injection

```
instrumentation.opentelemetry.io/inject-dotnet: "true"
```

### 4.1.2.3. Configuration of the Go auto-instrumentation

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>env</td>
<td>Environment variables specific to Go.</td>
</tr>
<tr>
<td>image</td>
<td>Container image with the Go SDK and auto-instrumentation.</td>
</tr>
<tr>
<td>resourceRequirements</td>
<td>The compute resource requirements.</td>
</tr>
</tbody>
</table>

The **PodSpec** annotation to enable injection

```
instrumentation.opentelemetry.io/inject-go: "true"
```

**Additional permissions required for the Go auto-instrumentation in the OpenShift cluster**

```yaml
apiVersion: security.openshift.io/v1
description: SecurityContextConstraints
metadata:
  name: otel-go-instrumentation-scc
spec:
  allowHostDirVolumePlugin: true
  allowPrivilegeEscalation: true
  allowPrivilegedContainer: true
  allowedCapabilities:
  - "SYS_PTRACE"
  fsGroup:
    type: RunAsAny
  runAsUser:
    type: RunAsAny
  seLinuxContext:
    type: RunAsAny
  seccompProfiles:
    - "*"
  supplementalGroups:
    type: RunAsAny
```
TIP

The CLI command for applying the permissions for the Go auto-instrumentation in the OpenShift cluster is as follows:

```
$ oc adm policy add-scc-to-user otel-go-instrumentation-scc -z <service_account>
```

### 4.1.2.4. Configuration of the Java auto-instrumentation

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>env</td>
<td>Environment variables specific to Java.</td>
</tr>
<tr>
<td>image</td>
<td>Container image with the Java SDK and auto-instrumentation.</td>
</tr>
<tr>
<td>resourceRequirements</td>
<td>The compute resource requirements.</td>
</tr>
</tbody>
</table>

The **PodSpec** annotation to enable injection

```
instrumentation.opentelemetry.io/inject-java: "true"
```

### 4.1.2.5. Configuration of the Node.js auto-instrumentation

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>env</td>
<td>Environment variables specific to Node.js.</td>
</tr>
<tr>
<td>image</td>
<td>Container image with the Node.js SDK and auto-instrumentation.</td>
</tr>
<tr>
<td>resourceRequirements</td>
<td>The compute resource requirements.</td>
</tr>
</tbody>
</table>

The **PodSpec** annotations to enable injection

```
instrumentation.opentelemetry.io/inject-nodejs: "true"
instrumentation.opentelemetry.io/otel-go-auto-target-exe: "/path/to/container/executable"
```

The **instrumentation.opentelemetry.io/otel-go-auto-target-exe** annotation sets the value for the required **OTEL_GO_AUTO_TARGET_EXE** environment variable.
### 4.1.2.6. Configuration of the Python auto-instrumentation

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>env</td>
<td>Environment variables specific to Python.</td>
</tr>
<tr>
<td>image</td>
<td>Container image with the Python SDK and auto-instrumentation.</td>
</tr>
<tr>
<td>resourceRequirements</td>
<td>The compute resource requirements.</td>
</tr>
</tbody>
</table>

For Python auto-instrumentation, the **OTEL_EXPORTER_OTLP_ENDPOINT** environment variable must be set if the endpoint of the exporters is set to 4317. Python auto-instrumentation uses **http/proto** by default, and the telemetry data must be set to the 4318 port.

**The PodSpec annotation to enable injection**

```text
instrumentation.opentelemetry.io/inject-python: "true"
```

### 4.1.2.7. Configuration of the OpenTelemetry SDK variables

The OpenTelemetry SDK variables in your pod are configurable by using the following annotation:

```text
instrumentation.opentelemetry.io/inject-sdk: "true"
```

Note that all the annotations accept the following values:

- **true**
  - Injects the **Instrumentation** resource from the namespace.
- **false**
  - Does not inject any instrumentation.
- **instrumentation-name**
  - The name of the instrumentation resource to inject from the current namespace.
- **other-namespace/instrumentation-name**
  - The name of the instrumentation resource to inject from another namespace.

### 4.1.2.8. Multi-container pods

The instrumentation is run on the first container that is available by default according to the pod specification. In some cases, you can also specify target containers for injection.

**Pod annotation**

```text
instrumentation.opentelemetry.io/container-names: "<container_1>,<container_2>"
```
NOTE

The Go auto-instrumentation does not support multi-container auto-instrumentation injection.
CHAPTER 5. SENDING TRACES AND METRICS TO THE OPENTELEMETRY COLLECTOR

You can set up and use the Red Hat build of OpenTelemetry to send traces to the OpenTelemetry Collector or the TempoStack.

Sending traces and metrics to the OpenTelemetry Collector is possible with or without sidecar injection.

5.1. SENDING TRACES AND METRICS TO THE OPENTELEMETRY COLLECTOR WITH SIDECAR INJECTION

You can set up sending telemetry data to an OpenTelemetry Collector instance with sidecar injection.

The Red Hat build of OpenTelemetry Operator allows sidecar injection into deployment workloads and automatic configuration of your instrumentation to send telemetry data to the OpenTelemetry Collector.

Prerequisites

- The Red Hat OpenShift distributed tracing platform (Tempo) is installed, and a TempoStack instance is deployed.
- You have access to the cluster through the web console or the OpenShift CLI (oc):
  - You are logged in to the web console as a cluster administrator with the cluster-admin role.
  - An active OpenShift CLI (oc) session by a cluster administrator with the cluster-admin role.
  - For Red Hat OpenShift Dedicated, you must have an account with the dedicated-admin role.

Procedure

1. Create a project for an OpenTelemetry Collector instance.

   ```yaml
   apiVersion: project.openshift.io/v1
   kind: Project
   metadata:
     name: observability
   ```

2. Create a service account.

   ```yaml
   apiVersion: v1
   kind: ServiceAccount
   metadata:
     name: otep-collector-sidecar
     namespace: observability
   ```

3. Grant the permissions to the service account for the k8sattributes and resourcedetection processors.

   ```yaml
   apiVersion: rbac.authorization.k8s.io/v1
   kind: ClusterRole
   ```
4. Deploy the OpenTelemetry Collector as a sidecar.

apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: otel
namespace: observability
spec:
  serviceAccount: otel-collector-sidecar
  mode: sidecar
  config:
    serviceAccount: otel-collector-sidecar
    receivers:
      otlp:
        protocols:
          grpc:
          http:
    processors:
      batch:
        memory_limiter:
          check_interval: 1s
          limit_percentage: 50
          spike_limit_percentage: 30
    resourcedetection:
      detectors: [openshift]
      timeout: 2s
    exporters:
      otlp:
        endpoint: "tempo<>-gateway:8090"
        tls:
          insecure: true
    service:
      pipelines:
      traces:
This points to the Gateway of the TempoStack instance deployed by using the `<example>` Tempo Operator.

5. Create your deployment using the `otel-collector-sidecar` service account.

6. Add the `sidecar.opentelemetry.io/inject: "true"` annotation to your Deployment object. This will inject all the needed environment variables to send data from your workloads to the OpenTelemetry Collector instance.

### 5.2. SENDING TRACES AND METRICS TO THE OPENTELEMETRY COLLECTOR WITHOUT SIDECAR INJECTION

You can set up sending telemetry data to an OpenTelemetry Collector instance without sidecar injection, which involves manually setting several environment variables.

#### Prerequisites

- The Red Hat OpenShift distributed tracing platform (Tempo) is installed, and a TempoStack instance is deployed.
- You have access to the cluster through the web console or the OpenShift CLI (`oc`):
  - You are logged in to the web console as a cluster administrator with the `cluster-admin` role.
  - An active OpenShift CLI (`oc`) session by a cluster administrator with the `cluster-admin` role.
  - For Red Hat OpenShift Dedicated, you must have an account with the `dedicated-admin` role.

#### Procedure

1. Create a project for an OpenTelemetry Collector instance.

   ```yaml
   apiVersion: project.openshift.io/v1
   kind: Project
   metadata:
     name: observability
   ```

2. Create a service account.

   ```yaml
   apiVersion: v1
   kind: ServiceAccount
   metadata:
     name: otel-collector-deployment
     namespace: observability
   ```

3. Grant the permissions to the service account for the `k8sattributes` and `resourcedetection` processors.
Deploy the OpenTelemetry Collector instance with the `OpenTelemetryCollector` custom resource.

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: otel-collector
rules:
  - apiGroups: ["", "config.openshift.io"]
    resources: ["pods", "namespaces", "infrastructures", "infrastructures/status"]
    verbs: ["get", "watch", "list"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: otel-collector
subjects:
  - kind: ServiceAccount
    name: otel-collector
    namespace: observability
roleRef:
  kind: ClusterRole
  name: otel-collector
  apiGroup: rbac.authorization.k8s.io
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: otel
  namespace: observability
spec:
  mode: deployment
  serviceAccount: otel-collector-deployment
  config:
    receivers:
      jaeger:
        protocols:
          grpc:
            thrift_binary:
            thrift_compact:
            thrift_http:
          opencensus:
          otlp:
            protocols:
              grpc:
              http:
            zipkin:
  processors:
    batch:
    k8sattributes:
    memory_limiter:
      check_interval: 1s
      limit_percentage: 50
      spike_limit_percentage: 30
  resourcedetection:
```

4. Deploy the OpenTelemetry Collector instance with the **OpenTelemetryCollector** custom resource.
detectors: [openshift]
exporters:
  otlp:
    endpoint: "tempo-<example>-distributor:4317"
  tls:
    insecure: true
service:
  pipelines:
    traces:
      receivers: [jaeger, opencensus, otlp, zipkin]
      processors: [memory_limiter, k8sattributes, resourcedetection, batch]
      exporters: [otlp]

This points to the Gateway of the TempoStack instance deployed by using the <example> Tempo Operator.

5. Set the environment variables in the container with your instrumented application.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTEL_SERVICE_NAME</td>
<td>Sets the value of the service.name resource attribute.</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>OTEL_EXPORTER_OTLP_ENDPOINT</td>
<td>Base endpoint URL for any signal type with an optionally specified port number.</td>
<td><a href="https://localhost:4317">https://localhost:4317</a></td>
</tr>
<tr>
<td>OTEL_EXPORTER_OTLP_CERTIFICATE</td>
<td>Path to the certificate file for the TLS credentials of the gRPC client.</td>
<td><a href="https://localhost:4317">https://localhost:4317</a></td>
</tr>
<tr>
<td>OTEL_TRACES_SAMPLER</td>
<td>Sampler to be used for traces.</td>
<td>parentbased_always_on</td>
</tr>
<tr>
<td>OTEL_EXPORTER_OTLP_PROTOCOL</td>
<td>Transport protocol for the OTLP exporter.</td>
<td>grpc</td>
</tr>
<tr>
<td>OTEL_EXPORTER_OTLP_TIMEOUT</td>
<td>Maximum time interval for the OTLP exporter to wait for each batch export.</td>
<td>10s</td>
</tr>
<tr>
<td>OTEL_EXPORTER_OTLP_INSECURE</td>
<td>Disables client transport security for gRPC requests. An HTTPS schema overrides it.</td>
<td>False</td>
</tr>
</tbody>
</table>
CHAPTER 6. CONFIGURATION FOR SENDING METRICS TO THE MONITORING STACK

The OpenTelemetry Collector custom resource (CR) can be configured to create a Prometheus ServiceMonitor CR for scraping the Collector’s pipeline metrics and the enabled Prometheus exporters.

Example of the OpenTelemetry Collector custom resource with the Prometheus exporter

```yaml
spec:
  mode: deployment
  observability:
    metrics:
      enableMetrics: true
  config: |
  exporters:
    prometheus:
      endpoint: 0.0.0.0:8889
      resource_to_telemetry_conversion:
        enabled: true # by default resource attributes are dropped
  service:
    telemetry:
      metrics:
        address: ":8888"
    pipelines:
      metrics:
        receivers: [otlp]
        exporters: [prometheus]
```

1 Configures the operator to create the Prometheus ServiceMonitor CR to scrape the collector’s internal metrics endpoint and Prometheus exporter metric endpoints. The metrics will be stored in the OpenShift monitoring stack.

Alternatively, a manually created Prometheus PodMonitor can provide fine control, for example removing duplicated labels added during Prometheus scraping.

Example of the PodMonitor custom resource that configures the monitoring stack to scrape the Collector metrics

```yaml
apiVersion: monitoring.coreos.com/v1
kind: PodMonitor
metadata:
  name: otel-collector
spec:
  selector:
    matchLabels:
      app.kubernetes.io/name: `<cr_name>-collector`
  podMetricsEndpoints:
    - port: metrics
    - port: promexporter
  relabelings:
    - action: labeldrop
      regex: pod
    - action: labeldrop
```

1 Configures the operator to scrape the Collector metrics.
- action: labeldrop
  regex: endpoint

metricRelabelings:
- action: labeldrop
  regex: instance
- action: labeldrop
  regex: job

1. The name of the OpenTelemetry Collector custom resource.
2. The name of the internal metrics port for the OpenTelemetry Collector. This port name is always metrics.
3. The name of the Prometheus exporter port for the OpenTelemetry Collector.
CHAPTER 7. FORWARDING TRACES TO A TEMPOSTACK

To configure forwarding traces to a TempoStack, you can deploy and configure the OpenTelemetry Collector. You can deploy the OpenTelemetry Collector in the deployment mode by using the specified processors, receivers, and exporters. For other modes, see the OpenTelemetry Collector documentation linked in Additional resources.

Prerequisites

- The Red Hat build of OpenTelemetry Operator is installed.
- The Tempo Operator is installed.
- A TempoStack is deployed on the cluster.

Procedure

1. Create a service account for the OpenTelemetry Collector.

Example ServiceAccount

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: otel-collector-deployment
```

2. Create a cluster role for the service account.

Example ClusterRole

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: otel-collector
rules:
  - apiGroups: ['", "config.openshift.io"
    resources: ['"pods", "namespaces", "infrastructures", "infrastructures/status"
    verbs: ['"get", "watch", "list"
```

1. The `k8sattributesprocessor` requires permissions for pods and namespaces resources.
2. The `resourcedetectionprocessor` requires permissions for infrastructures and status.

3. Bind the cluster role to the service account.

Example ClusterRoleBinding

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: otel-collector
```
4. Create the YAML file to define the `OpenTelemetryCollector` custom resource (CR).

**Example OpenTelemetryCollector**

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: otel
spec:
  mode: deployment
  serviceAccount: otel-collector-deployment
  config:
    receivers:
      jaeger:
        protocols:
          grpc:
            thrift_binary:
            thrift_compact:
            thrift_http:
          opencensus:
          otlp:
            protocols:
              grpc:
              http:
            endpoint: "tempo-simplest-distributor:4317"
            insecure: true
    processors:
      batch:
      k8sattributes:
      memory_limiter:
        check_interval: 1s
        limit_percentage: 50
        spike_limit_percentage: 30
    resourcedetection:
      detectors: [openshift]
    exporters:
      otlp:
        endpoint: "tempo-simplest-distributor:4317"
        tls:
          insecure: true
    service:
      pipelines:
        traces:
          receivers: [jaeger, opencensus, otlp, zipkin]
          processors: [memory_limiter, k8sattributes, resourcedetection, batch]
          exporters: [otlp]
```
The Collector exporter is configured to export OTLP and points to the Tempo distributor endpoint, \texttt{"tempo-simplest-distributor:4317"} in this example, which is already created.

The Collector is configured with a receiver for Jaeger traces, OpenCensus traces over the OpenCensus protocol, Zipkin traces over the Zipkin protocol, and OTLP traces over the GRPC protocol.

\section*{TIP}

You can deploy \texttt{tracegen} as a test:

```yaml
apiVersion: batch/v1
kind: Job
metadata:
  name: tracegen
spec:
  template:
    spec:
      containers:
        - name: tracegen
          image: ghcr.io/open-telemetry/opentelemetry-collector-contrib/tracegen:latest
          command: 
            - "/tracegen"
          args:
            - -otlp-endpoint=otel-collector:4317
            - -otlp-insecure
            - -duration=30s
            - -workers=1
          restartPolicy: Never
          backoffLimit: 4
```

\section*{Additional resources}

- OpenTelemetry Collector documentation
- Deployment examples on GitHub
You can enable metrics and alerts of OpenTelemetry Collector instances.

**Prerequisites**

- Monitoring for user-defined projects is enabled in the cluster.

**Procedure**

- To enable metrics of an OpenTelemetry Collector instance, set the `spec.observability.metrics.enableMetrics` field to `true`:

  ```yaml
  apiVersion: opentelemetry.io/v1alpha1
  kind: OpenTelemetryCollector
  metadata:
    name: <name>
  spec:
    observability:
      metrics:
        enableMetrics: true
  ```

**Verification**

You can use the Administrator view of the web console to verify successful configuration:

- Go to Observe → Targets, filter by Source: User, and check that the ServiceMonitors in the `opentelemetry-collector-<instance_name>` format have the Up status.

**Additional resources**

- Enabling monitoring for user-defined projects
CHAPTER 9. GATHERING THE OBSERVABILITY DATA FROM MULTIPLE CLUSTERS

For a multicluster configuration, you can create one OpenTelemetry Collector instance in each one of the remote clusters and then forward all the telemetry data to one OpenTelemetry Collector instance.

Prerequisites

- The Red Hat build of OpenTelemetry Operator is installed.
- The Tempo Operator is installed.
- A TempoStack instance is deployed on the cluster.
- The following mounted certificates: Issuer, self-signed certificate, CA issuer, client and server certificates. To create any of these certificates, see step 1.

Procedure

1. Mount the following certificates in the OpenTelemetry Collector instance, skipping already mounted certificates.
   a. An Issuer to generate the certificates by using the cert-manager Operator for Red Hat OpenShift.

```yaml
apiVersion: cert-manager.io/v1
kind: Issuer
metadata:
  name: selfsigned-issuer
spec:
  selfSigned: {}
```

b. A self-signed certificate.

```yaml
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: ca
spec:
  isCA: true
  commonName: ca
  subject:
    organizations:
      - Organization # <your_organization_name>
  organizationalUnits:
    - Widgets
  secretName: ca-secret
  privateKey:
    algorithm: ECDSA
    size: 256
  issuerRef:
    name: selfsigned-issuer
    kind: Issuer
    group: cert-manager.io
```
c. A CA issuer.

```yaml
apiVersion: cert-manager.io/v1
kind: Issuer
metadata:
  name: test-ca-issuer
spec:
  ca:
    secretName: ca-secret
```

d. The client and server certificates.

```yaml
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: server
spec:
  secretName: server-tls
  isCA: false
  usages:
    - server auth
    - client auth
  dnsNames:
    - "otel.observability.svc.cluster.local"  # 1
  issuerRef:
    name: ca-issuer
---
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: client
spec:
  secretName: client-tls
  isCA: false
  usages:
    - server auth
    - client auth
  dnsNames:
    - "otel.observability.svc.cluster.local"  # 2
  issuerRef:
    name: ca-issuer
```

1 List of exact DNS names to be mapped to a solver in the server OpenTelemetry Collector instance.

2 List of exact DNS names to be mapped to a solver in the client OpenTelemetry Collector instance.

2. Create a service account for the OpenTelemetry Collector instance.

**Example ServiceAccount**

```yaml
apiVersion: v1
kind: ServiceAccount
```
3. Create a cluster role for the service account.

**Example ClusterRole**

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: otel-collector
rules:
- apiGroups: ["", "config.openshift.io"]
  resources: ["pods", "namespaces", "infrastructures", "infrastructures/status"]
  verbs: ["get", "watch", "list"]
```

1. The `k8sattributesprocessor` requires permissions for pods and namespace resources.
2. The `resourcedetectionprocessor` requires permissions for infrastructures and status.

4. Bind the cluster role to the service account.

**Example ClusterRoleBinding**

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: otel-collector
subjects:
- kind: ServiceAccount
  name: otel-collector-deployment
  namespace: otel-collector-<example>
roleRef:
  kind: ClusterRole
  name: otel-collector
  apiGroup: rbac.authorization.k8s.io
```

5. Create the YAML file to define the **OpenTelemetryCollector** custom resource (CR) in the edge clusters.

**Example OpenTelemetryCollector custom resource for the edge clusters**

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: otel
  namespace: otel-collector-<example>
spec:
  mode: daemonset
  serviceAccount: otel-collector-deployment
  config: |
```
The Collector exporter is configured to export OTLP HTTP and points to the OpenTelemetry Collector from the central cluster.

6. Create the YAML file to define the **OpenTelemetryCollector** custom resource (CR) in the central cluster.

**Example OpenTelemetryCollector custom resource for the central cluster**

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
```
The Collector receiver requires the certificates listed in the first step.

The Collector exporter is configured to export OTLP and points to the Tempo distributor endpoint, which in this example is "tempo-simplest-distributor:4317" and already created.
CHAPTER 10. TROUBLESHOOTING THE RED HAT BUILD OF OPENTELEMETRY

The OpenTelemetry Collector offers multiple ways to measure its health as well as investigate data ingestion issues.

10.1. GETTING THE OPENTELEMETRY COLLECTOR LOGS

You can get the logs for the OpenTelemetry Collector as follows.

Procedure

1. Set the relevant log level in the `OpenTelemetryCollector` custom resource (CR):

   ```yaml
   config: |
     service:
       telemetry:
         logs:
           level: debug
   ```

   Collector’s log level. Supported values include *info*, *warn*, *error*, or *debug*. Defaults to *info*.

2. Use the `oc logs` command or the web console to retrieve the logs.

10.2. EXPOSING THE METRICS

The OpenTelemetry Collector exposes the metrics about the data volumes it has processed. The following metrics are for spans, although similar metrics are exposed for metrics and logs signals:

- **otelcol_receiver_accepted_spans**
  - The number of spans successfully pushed into the pipeline.

- **otelcol_receiver_refused_spans**
  - The number of spans that could not be pushed into the pipeline.

- **otelcol_exporter_sent_spans**
  - The number of spans successfully sent to the destination.

- **otelcol_exporter_enqueue_failed_spans**
  - The number of spans failed to be added to the sending queue.

The operator creates a `<cr_name>-collector-monitoring` telemetry service that you can use to scrape the metrics endpoint.

Procedure

1. Enable the telemetry service by adding the following lines in the `OpenTelemetryCollector` custom resource:

   ```yaml
   config: |
     service:
       telemetry:
   ```
The address at which the internal collector metrics are exposed. Defaults to :8888.

1. Retrieve the metrics by running the following command, which uses the port-forwarding Collector pod:

   $ oc port-forward <collector_pod>


10.3. DEBUG EXPORTER

You can configure the debug exporter to export the collected data to the standard output.

Procedure

1. Configure the OpenTelemetryCollector custom resource as follows:

   config:
   exporters:
     debug:
       verbosity: detailed
     service:
     pipelines:
     traces:
       exporters: [debug]
     metrics:
       exporters: [debug]
     logs:
       exporters: [debug]

2. Use the oc logs command or the web console to export the logs to the standard output.
If you are already using the Red Hat OpenShift distributed tracing platform (Jaeger) for your applications, you can migrate to the Red Hat build of OpenTelemetry, which is based on the OpenTelemetry open-source project.

The Red Hat build of OpenTelemetry provides a set of APIs, libraries, agents, and instrumentation to facilitate observability in distributed systems. The OpenTelemetry Collector in the Red Hat build of OpenTelemetry can ingest the Jaeger protocol, so you do not need to change the SDKs in your applications.

Migration from the distributed tracing platform (Jaeger) to the Red Hat build of OpenTelemetry requires configuring the OpenTelemetry Collector and your applications to report traces seamlessly. You can migrate sidecar and sidecarless deployments.

### 11.1. MIGRATING FROM THE DISTRIBUTED TRACING PLATFORM (JAEGER) TO THE RED HAT BUILD OF OPENTELEMETRY WITH SIDECARs

The Red Hat build of OpenTelemetry Operator supports sidecar injection into deployment workloads, so you can migrate from a distributed tracing platform (Jaeger) sidecar to a Red Hat build of OpenTelemetry sidecar.

#### Prerequisites

- The Red Hat OpenShift distributed tracing platform (Jaeger) is used on the cluster.
- The Red Hat build of OpenTelemetry is installed.

#### Procedure

1. Configure the OpenTelemetry Collector as a sidecar.

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: otel
  namespace: <otel-collector-namespace>
spec:
```
This endpoint points to the Gateway of a TempoStack instance deployed by using the `<example>` Tempo Operator.

2. Create a service account for running your application.

   ```yaml
   apiVersion: v1
   kind: ServiceAccount
   metadata:
     name: otel-collector-sidecar
   ```

3. Create a cluster role for the permissions needed by some processors.

   ```yaml
   apiVersion: rbac.authorization.k8s.io/v1
   kind: ClusterRole
   metadata:
     name: otel-collector-sidecar
   rules:
     - apiGroups: ["config.openshift.io"]
       resources: ["infrastructures", "infrastructures/status"]
       verbs: ["get", "watch", "list"]
   ```

   The `resourcedetectionprocessor` requires permissions for infrastructures and infrastructures/status.
4. Create a **ClusterRoleBinding** to set the permissions for the service account.

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: otel-collector-sidecar
subjects:
- kind: ServiceAccount
  name: otel-collector-deployment
  namespace: otel-collector-example
roleRef:
  kind: ClusterRole
  name: otel-collector
  apiGroup: rbac.authorization.k8s.io
```

5. Deploy the OpenTelemetry Collector as a sidecar.

6. Remove the injected Jaeger Agent from your application by removing the "**sidecar.jaegertracing.io/inject**: "true" annotation from your Deployment object.

7. Enable automatic injection of the OpenTelemetry sidecar by adding the `**sidecar.opentelemetry.io/inject**: "true"` annotation to the `.spec.template.metadata.annotations` field of your Deployment object.

8. Use the created service account for the deployment of your application to allow the processors to get the correct information and add it to your traces.

### 11.2. MIGRATING FROM THE DISTRIBUTED TRACING PLATFORM (JAEGER) TO THE RED HAT BUILD OF OPENTELEMETRY WITHOUT SIDECARs

You can migrate from the distributed tracing platform (Jaeger) to the Red Hat build of OpenTelemetry without sidecar deployment.

#### Prerequisites

- The Red Hat OpenShift distributed tracing platform (Jaeger) is used on the cluster.
- The Red Hat build of OpenTelemetry is installed.

#### Procedure

1. Configure OpenTelemetry Collector deployment.

2. Create the project where the OpenTelemetry Collector will be deployed.

   ```yaml
   apiVersion: project.openshift.io/v1
   kind: Project
   metadata:
     name: observability
   ```

3. Create a service account for running the OpenTelemetry Collector instance.

   ```yaml
   apiVersion: v1
   ```
4. Create a cluster role for setting the required permissions for the processors.

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: otel-collector
rules:
- apiGroups: ["", "config.openshift.io"]
  resources: ["pods", "namespaces", "infrastructures", "infrastructures/status"]
  verbs: ["get", "watch", "list"]
```

1 Permissions for the **pods** and **namespaces** resources are required for the **k8sattributesprocessor**.

2 Permissions for **infrastructures** and **infrastructures/status** are required for **resourcedetectionprocessor**.

5. Create a ClusterRoleBinding to set the permissions for the service account.

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: otel-collector
subjects:
- kind: ServiceAccount
  name: otel-collector-deployment
  namespace: observability
roleRef:
  kind: ClusterRole
  name: otel-collector
  apiGroup: rbac.authorization.k8s.io
```

6. Create the OpenTelemetry Collector instance.

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
metadata:
  name: otel
  namespace: observability
spec:
```

**NOTE**

This collector will export traces to a TempoStack instance. You must create your TempoStack instance by using the Red Hat Tempo Operator and place here the correct endpoint.
7. Point your tracing endpoint to the OpenTelemetry Operator.

8. If you are exporting your traces directly from your application to Jaeger, change the API endpoint from the Jaeger endpoint to the OpenTelemetry Collector endpoint.

**Example of exporting traces by using the `jaegerexporter` with Golang**

```go
exp, err := jaeger.New(jaeger.WithCollectorEndpoint(jaeger.WithEndpoint(url)))
```

1 The URL points to the OpenTelemetry Collector API endpoint.
CHAPTER 12. UPDATING THE RED HAT BUILD OF OPENTELEMETRY

For version upgrades, the Red Hat build of OpenTelemetry Operator uses the Operator Lifecycle Manager (OLM), which controls installation, upgrade, and role-based access control (RBAC) of Operators in a cluster.

The OLM runs in the OpenShift Container Platform by default. The OLM queries for available Operators as well as upgrades for installed Operators.

When the Red Hat build of OpenTelemetry Operator is upgraded to the new version, it scans for running OpenTelemetry Collector instances that it manages and upgrades them to the version corresponding to the Operator’s new version.

12.1. ADDITIONAL RESOURCES

- Operator Lifecycle Manager concepts and resources
- Updating installed Operators
CHAPTER 13. REMOVING THE RED HAT BUILD OF OPENTELEMETRY

The steps for removing the Red Hat build of OpenTelemetry from an OpenShift Container Platform cluster are as follows:

1. Shut down all Red Hat build of OpenTelemetry pods.
2. Remove any OpenTelemetryCollector instances.
3. Remove the Red Hat build of OpenTelemetry Operator.

13.1. REMOVING AN OPENTELEMETRY COLLECTOR INSTANCE BY USING THE WEB CONSOLE

You can remove an OpenTelemetry Collector instance in the Administrator view of the web console.

**Prerequisites**

- You are logged in to the web console as a cluster administrator with the `cluster-admin` role.
- For Red Hat OpenShift Dedicated, you must be logged in using an account with the `dedicated-admin` role.

**Procedure**

1. Go to **Operators → Installed Operators → Red Hat build of OpenTelemetry Operator → OpenTelemetryInstrumentation** or **OpenTelemetryCollector**.

2. To remove the relevant instance, select → **Delete** → **Delete**.

3. Optional: Remove the Red Hat build of OpenTelemetry Operator.

13.2. REMOVING AN OPENTELEMETRY COLLECTOR INSTANCE BY USING THE CLI

You can remove an OpenTelemetry Collector instance on the command line.

**Prerequisites**

- An active OpenShift CLI (`oc`) session by a cluster administrator with the `cluster-admin` role.

**TIP**

- Ensure that your OpenShift CLI (`oc`) version is up to date and matches your OpenShift Container Platform version.

- Run `oc login`:
  
  ```
  $ oc login --username=<your_username>
  ```
Procedure

1. Get the name of the OpenTelemetry Collector instance by running the following command:

   ```bash
   $ oc get deployments -n <project_of_opentelemetry_instance>
   ```

2. Remove the OpenTelemetry Collector instance by running the following command:

   ```bash
   $ oc delete opentelemetrycollectors <opentelemetry_instance_name> -n <project_of_opentelemetry_instance>
   ```

3. Optional: Remove the Red Hat build of OpenTelemetry Operator.

Verification

- To verify successful removal of the OpenTelemetry Collector instance, run `oc get deployments` again:

  ```bash
  $ oc get deployments -n <project_of_opentelemetry_instance>
  ```

13.3. ADDITIONAL RESOURCES

- Deleting Operators from a cluster
- Getting started with the OpenShift CLI