OpenShift Container Platform 4.11 Distributed tracing

Distributed tracing installation, usage, and release notes
Abstract

This document provides information on how to use distributed tracing in OpenShift Container Platform.
# Table of Contents

**CHAPTER 1. DISTRIBUTED TRACING RELEASE NOTES** ................................................. 6

1.1. RELEASE NOTES FOR RED HAT OPENSSHIFT DISTRIBUTED TRACING PLATFORM 3.0 6
   1.1.1. Distributed tracing overview 6
   1.1.2. Component versions in the Red Hat OpenShift distributed tracing platform 3.0 6
   1.1.3. Red Hat OpenShift distributed tracing platform (Jaeger) 6
      1.1.3.1. Deprecated functionality 6
      1.1.3.2. New features and enhancements 7
      1.1.3.3. Bug fixes 7
      1.1.3.4. Known issues 7
   1.1.4. Red Hat OpenShift distributed tracing platform (Tempo) 7
      1.1.4.1. New features and enhancements 7
      1.1.4.2. Bug fixes 7
      1.1.4.3. Known issues 7
   1.1.5. Getting support 8
   1.1.6. Making open source more inclusive 8

1.2. RELEASE NOTES FOR RED HAT OPENSIFT DISTRIBUTED TRACING PLATFORM 2.9.2 8
   1.2.1. Distributed tracing overview 8
   1.2.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.9.2 9
   1.2.3. CVEs 9
   1.2.4. Red Hat OpenShift distributed tracing platform (Jaeger) 9
      1.2.4.1. Known issues 9
   1.2.5. Red Hat OpenShift distributed tracing platform (Tempo) 9
      1.2.5.1. Known issues 9
   1.2.6. Red Hat build of OpenTelemetry 11
      1.2.6.1. Known issues 11
   1.2.7. Getting support 11
   1.2.8. Making open source more inclusive 11

1.3. RELEASE NOTES FOR RED HAT OPENSIFT DISTRIBUTED TRACING PLATFORM 2.9.1 12
   1.3.1. Distributed tracing overview 12
   1.3.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.9.1 12
   1.3.3. CVEs 12
   1.3.4. Red Hat OpenShift distributed tracing platform (Jaeger) 12
      1.3.4.1. Known issues 13
   1.3.5. Red Hat OpenShift distributed tracing platform (Tempo) 13
      1.3.5.1. Known issues 13
   1.3.6. Red Hat build of OpenTelemetry 14
      1.3.6.1. Known issues 15
   1.3.7. Getting support 15
   1.3.8. Making open source more inclusive 15

1.4. RELEASE NOTES FOR RED HAT OPENSIFT DISTRIBUTED TRACING PLATFORM 2.9 15
   1.4.1. Distributed tracing overview 15
   1.4.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.9 16
   1.4.3. Red Hat OpenShift distributed tracing platform (Jaeger) 16
      1.4.3.1. New features and enhancements 16
      1.4.3.2. Bug fixes 16
      1.4.3.3. Known issues 17
   1.4.4. Red Hat OpenShift distributed tracing platform (Tempo) 17
      1.4.4.1. New features and enhancements 17
      1.4.4.2. Bug fixes 17
      1.4.4.3. Known issues 17
   1.4.5. Red Hat build of OpenTelemetry 19
1.12. RELEASE NOTES FOR RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM 2.1
  1.12.1. Distributed tracing overview
  1.12.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.1.0
  1.12.3. Technology Preview features
  1.12.4. Bug fixes
  1.12.5. Getting support
  1.12.6. Making open source more inclusive

1.13. RELEASE NOTES FOR RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM 2.0
  1.13.1. Distributed tracing overview
  1.13.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.0.0
  1.13.3. New features and enhancements
  1.13.4. Technology Preview features
  1.13.5. Bug fixes
  1.13.6. Getting support
  1.13.7. Making open source more inclusive

CHAPTER 2. DISTRIBUTED TRACING ARCHITECTURE
  2.1. DISTRIBUTED TRACING ARCHITECTURE
  2.1.1. Distributed tracing overview
  2.1.2. Red Hat OpenShift distributed tracing platform features
  2.1.3. Red Hat OpenShift distributed tracing platform architecture

CHAPTER 3. DISTRIBUTED TRACING PLATFORM (JAEGER)
  3.1. INSTALLING THE DISTRIBUTED TRACING PLATFORM JAEGER
    3.1.1. Prerequisites
    3.1.2. Red Hat OpenShift distributed tracing platform installation overview
    3.1.3. Installing the OpenShift Elasticsearch Operator
    3.1.4. Installing the Red Hat OpenShift distributed tracing platform (Jaeger) Operator
  3.2. CONFIGURING AND DEPLOYING THE DISTRIBUTED TRACING PLATFORM JAEGER
    3.2.1. Supported deployment strategies
    3.2.2. Deploying the distributed tracing platform default strategy from the web console
      3.2.2.1. Deploying the distributed tracing platform default strategy from the CLI
    3.2.3. Deploying the distributed tracing platform production strategy from the web console
      3.2.3.1. Deploying the distributed tracing platform production strategy from the CLI
    3.2.4. Deploying the distributed tracing platform streaming strategy from the web console
      3.2.4.1. Deploying the distributed tracing platform streaming strategy from the CLI
    3.2.5. Validating your deployment
      3.2.5.1. Accessing the Jaeger console
    3.2.6. Customizing your deployment
      3.2.6.1. Deployment best practices
      3.2.6.2. Distributed tracing default configuration options
      3.2.6.3. Jaeger Collector configuration options
      3.2.6.4. Distributed tracing sampling configuration options
      3.2.6.5. Distributed tracing storage configuration options
        3.2.6.5.1. Auto-provisioning an Elasticsearch instance
        3.2.6.5.2. Connecting to an existing Elasticsearch instance
      3.2.6.6. Managing certificates with Elasticsearch
      3.2.6.7. Query configuration options
      3.2.6.8. Ingester configuration options
    3.2.7. Injecting sidecars
      3.2.7.1. Automatically injecting sidecars
      3.2.7.2. Manually injecting sidecars
  3.3. UPDATING THE DISTRIBUTED TRACING PLATFORM JAEGER
3.3.1. Additional resources

3.4. REMOVING THE DISTRIBUTED TRACING PLATFORM JAEGER

3.4.1. Removing a distributed tracing platform (Jaeger) instance by using the web console

3.4.2. Removing a distributed tracing platform (Jaeger) instance by using the CLI

3.4.3. Removing the Red Hat OpenShift distributed tracing platform Operators

CHAPTER 4. DISTRIBUTED TRACING PLATFORM (TEMPO)

4.1. INSTALLING THE DISTRIBUTED TRACING PLATFORM (TEMPO)

4.1.1. Installing the distributed tracing platform (Tempo) from the web console

4.1.2. Installing the distributed tracing platform (Tempo) by using the CLI

4.1.3. Additional resources

4.2. CONFIGURING AND DEPLOYING THE DISTRIBUTED TRACING PLATFORM (TEMPO)

4.2.1. Customizing your deployment

4.2.1.1. Distributed tracing default configuration options

4.2.1.2. The distributed tracing platform (Tempo) storage configuration

4.2.1.3. Query configuration options

4.2.1.4. Configuration of the monitor tab in Jaeger UI

4.2.1.4.1. OpenTelemetry Collector configuration

4.2.1.4.2. Tempo configuration

4.2.1.5. Multitenancy

4.2.2. Setting up monitoring for the distributed tracing platform (Tempo)

4.2.2.1. Configuring TempoStack metrics and alerts

4.2.2.2. Configuring Tempo Operator metrics and alerts

4.3. UPDATING THE DISTRIBUTED TRACING PLATFORM (TEMPO)

4.3.1. Additional resources

4.4. REMOVING THE RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM (TEMPO)

4.4.1. Removing a TempoStack instance by using the web console

4.4.2. Removing a TempoStack instance by using the CLI

4.4.3. Additional resources
CHAPTER 1. DISTRIBUTED TRACING RELEASE NOTES

1.1. RELEASE NOTES FOR RED HAT OPENS shift DISTRIBUTED TRACING PLATFORM 3.0

1.1.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.

1.1.2. Component versions in the Red Hat OpenShift distributed tracing platform 3.0

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.51.0</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.89.0</td>
</tr>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>2.3.0</td>
</tr>
</tbody>
</table>

1.1.3. Red Hat OpenShift distributed tracing platform (Jaeger)

1.1.3.1. Deprecated functionality

In Red Hat OpenShift distributed tracing 3.0, Jaeger and Elasticsearch are deprecated, and both are planned to be removed in a future release. Red Hat will provide critical and above CVE bug fixes and support for these components during the current release lifecycle, but these components will no longer receive feature enhancements.
In Red Hat OpenShift distributed tracing 3.0, Tempo provided by the Tempo Operator and the OpenTelemetry collector provided by the Red Hat build of OpenTelemetry are the preferred Operators for distributed tracing collection and storage. The OpenTelemetry and Tempo distributed tracing stack is to be adopted by all users because this will be the stack that will be enhanced going forward.

1.1.3.2. New features and enhancements
This update introduces the following enhancements for the distributed tracing platform (Jaeger):

- Support for the ARM architecture.
- Support for cluster-wide proxy environments.

1.1.3.3. Bug fixes
This update introduces the following bug fixes for the distributed tracing platform (Jaeger):

- Fixed support for disconnected environments when using the `oc adm catalog mirror` CLI command. (TRACING-3546)

1.1.3.4. Known issues

- Currently, Apache Spark is not supported.
- Currently, the streaming deployment via AMQ/Kafka is not supported on the IBM Z and IBM Power Systems architectures.

1.1.4. Red Hat OpenShift distributed tracing platform (Tempo)

1.1.4.1. New features and enhancements
This update introduces the following enhancements for the distributed tracing platform (Tempo):

- Support for the ARM architecture.
- Support for span request count, duration, and error count (RED) metrics. The metrics can be visualized in the Jaeger console deployed as part of Tempo or in the web console in the Observe menu.

1.1.4.2. Bug fixes
This update introduces the following bug fixes for the distributed tracing platform (Tempo):

- Fixed support for the custom TLS CA option for connecting to object storage. (TRACING-3462)
- Fixed support for disconnected environments when using the `oc adm catalog mirror` CLI command. (TRACING-3523)
- Fixed mTLS when Gateway is not deployed. (TRACING-3510)

1.1.4.3. Known issues

- Currently, when used with the Tempo Operator, the Jaeger UI only displays services that have
Currently, when used with the Tempo Operator, the Jaeger UI only displays services that have sent traces in the last 15 minutes. For services that did not send traces in the last 15 minutes, traces are still stored but not displayed in the Jaeger UI. (TRACING-3139)

Currently, the distributed tracing platform (Tempo) fails on the IBM Z (s390x) architecture. (TRACING-3545)

1.1.5. 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 Hybrid Cloud Console. 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.

1.1.6. 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 RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM 2.9.2

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 (Jaeger) which is based on the open source Jaeger project.
• 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.

### 1.2.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.9.2

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.47.0</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.81.0</td>
</tr>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>2.1.1</td>
</tr>
</tbody>
</table>

### 1.2.3. CVEs

This release fixes [CVE-2023-46234](#).

### 1.2.4. Red Hat OpenShift distributed tracing platform (Jaeger)

#### 1.2.4.1. Known issues

- Apache Spark is not supported.
- The streaming deployment via AMQ/Kafka is unsupported on IBM Z and IBM Power Systems.

### 1.2.5. Red Hat OpenShift distributed tracing platform (Tempo)

**IMPORTANT**

The Red Hat OpenShift distributed tracing platform (Tempo) 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](#).

#### 1.2.5.1. Known issues

- Currently, the custom TLS CA option is not implemented for connecting to object storage. ([TRACING-3462](#))
Currently, when used with the Tempo Operator, the Jaeger UI only displays services that have sent traces in the last 15 minutes. For services that did not send traces in the last 15 minutes, traces are still stored but not displayed in the Jaeger UI. (TRACING-3139)

Currently, the distributed tracing platform (Tempo) fails on the IBM Z (s390x) architecture. (TRACING-3545)

Currently, the Tempo query frontend service must not use internal mTLS when Gateway is not deployed. This issue does not affect the Jaeger Query API. The workaround is to disable mTLS. (TRACING-3510)

**Workaround**

Disable mTLS as follows:

1. Open the Tempo Operator ConfigMap for editing by running the following command:

   ```bash
   $ oc edit configmap tempo-operator-manager-config -n openshift-tempo-operator
   ``

   The project where the Tempo Operator is installed.

2. Disable the mTLS in the operator configuration by updating the YAML file:

   ```yaml
   data:
   controller_manager_config.yaml:
   featureGates:
   httpEncryption: false
   grpcEncryption: false
   builtinCertManagement:
   enabled: false
   
   $ oc rollout restart deployment.apps/tempo-operator-controller -n openshift-tempo-operator
   ``

3. Restart the Tempo Operator pod by running the following command:

   ```bash
   $ oc rollout restart deployment.apps/tempo-operator-controller -n openshift-tempo-operator
   ``

**Workaround**

Add the Tempo Operator related images in the mirroring tool to mirror the images to the registry:

```yaml
kind: ImageSetConfiguration
apiVersion: mirror.openshift.io/v1alpha2
archiveSize: 20
storageConfig:
  local:
    path: /home/user/images
  mirror:
    operators:
        packages:
```

Missing images for running the Tempo Operator in restricted environments. The Red Hat OpenShift distributed tracing platform (Tempo) CSV is missing references to the operand images. (TRACING-3523)
1.2.6. Red Hat build of OpenTelemetry

**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](#).

1.2.6.1. Known issues

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

1.2.7. 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 Hybrid Cloud Console](#). 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.

1.2.8. 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.

1.3. RELEASE NOTES FOR RED HAT OPENSIST DISTRIBUTED TRACING PLATFORM 2.9.1

1.3.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.

1.3.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.9.1

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.47.0</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.81.0</td>
</tr>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>2.1.1</td>
</tr>
</tbody>
</table>

1.3.3. CVEs

This release fixes **CVE-2023-44487**.

1.3.4. Red Hat OpenShift distributed tracing platform (Jaeger)
1.3.4.1. Known issues

- Apache Spark is not supported.
- The streaming deployment via AMQ/Kafka is unsupported on IBM Z and IBM Power Systems.

1.3.5. Red Hat OpenShift distributed tracing platform (Tempo)

**IMPORTANT**

The Red Hat OpenShift distributed tracing platform (Tempo) 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.

1.3.5.1. Known issues

- Currently, the custom TLS CA option is not implemented for connecting to object storage. ([TRACING-3462](#))

- Currently, when used with the Tempo Operator, the Jaeger UI only displays services that have sent traces in the last 15 minutes. For services that did not send traces in the last 15 minutes, traces are still stored but not displayed in the Jaeger UI. ([TRACING-3139](#))

- Currently, the distributed tracing platform (Tempo) fails on the IBM Z (s390x) architecture. ([TRACING-3545](#))

- Currently, the Tempo query frontend service must not use internal mTLS when Gateway is not deployed. This issue does not affect the Jaeger Query API. The workaround is to disable mTLS. ([TRACING-3510](#))

**Workaround**

Disable mTLS as follows:

1. Open the Tempo Operator ConfigMap for editing by running the following command:

   ```bash
   $ oc edit configmap tempo-operator-manager-config -n openshift-tempo-operator
   ```

   1. The project where the Tempo Operator is installed.

2. Disable the mTLS in the operator configuration by updating the YAML file:

   ```yaml
   data:
   controller_manager_config.yaml:
   featureGates:
   httpEncryption: false
   ```
3. Restart the Tempo Operator pod by running the following command:

```bash
$ oc rollout restart deployment.apps/tempo-operator-controller -n openshift-tempo-operator
```

- Missing images for running the Tempo Operator in restricted environments. The Red Hat OpenShift distributed tracing platform (Tempo) CSV is missing references to the operand images. (TRACING-3523)

**Workaround**

Add the Tempo Operator related images in the mirroring tool to mirror the images to the registry:

```yaml
kind: ImageSetConfiguration
apiVersion: mirror.openshift.io/v1alpha2
archiveSize: 20
storageConfig:
  local:
    path: /home/user/images
  mirror:
    operators:
        packages:
          - name: tempo-product
            channels:
              - name: stable
  additionalImages:
    - name: registry.redhat.io/rhosdt/tempo-rhel8@sha256:e4295f837066efb05bcc5897f31eb2bddd81684a8c59d6f9498dd3590c62c12a
    - name: registry.redhat.io/rhosdt/tempo-gateway-rhel8@sha256:b62f5cedfeb5907b638f14ca6aaeea50f41642980a8a6f87b7061e88d90fac23
    - name: registry.redhat.io/rhosdt/tempo-query-rhel8@sha256:8cd134deca47d6817b26566e272e6c3f75367653d589f5c90855c59b2fab01e9
    - name: registry.redhat.io/rhosdt/tempo-gateway-opa-rhel8@sha256:0da43034f440b8258a48a0697ba6435643d48b615cdb882ac7f4f1f80aad08e
```

1.3.6. Red Hat build of OpenTelemetry
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.

1.3.6.1. Known issues

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

1.3.7. 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 Hybrid Cloud Console. 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.

1.3.8. 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.

1.4. RELEASE NOTES FOR RED HAT OPENSOURCE DISTRIBUTED TRACING PLATFORM 2.9

1.4.1. 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 (Jaeger)** which is based on the open source Jaeger project.

- **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.

### 1.4.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.9

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.47.0</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.81.0</td>
</tr>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>2.11</td>
</tr>
</tbody>
</table>

### 1.4.3. Red Hat OpenShift distributed tracing platform (Jaeger)

#### 1.4.3.1. New features and enhancements

- None.

#### 1.4.3.2. Bug fixes

- Before this update, connection was refused due to a missing gRPC port on the jaeger-query deployment. This issue resulted in transport: Error while dialing: dial tcp :16685: connect: connection refused error message. With this update, the Jaeger Query gRPC port (16685) is successfully exposed on the Jaeger Query service. (TRACING-3322)

- Before this update, the wrong port was exposed for jaeger-production-query, resulting in refused connection. With this update, the issue is fixed by exposing the Jaeger Query gRPC port (16685) on the Jaeger Query deployment. (TRACING-2968)

- Before this update, when deploying Service Mesh on single-node OpenShift clusters in disconnected environments, the Jaeger pod frequently went into the Pending state. With this update, the issue is fixed. (TRACING-3312)

- Before this update, the Jaeger Operator pod restarted with the default memory value due to the reason: OOMKilled error message. With this update, this issue is fixed by removing the resource limits. (TRACING-3173)
1.4.3.3. Known issues

- Apache Spark is not supported.
- The streaming deployment via AMQ/Kafka is unsupported on IBM Z and IBM Power Systems.

1.4.4. Red Hat OpenShift distributed tracing platform (Tempo)

**IMPORTANT**

The Red Hat OpenShift distributed tracing platform (Tempo) 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](#).

1.4.4.1. New features and enhancements

This release introduces the following enhancements for the distributed tracing platform (Tempo):

- Support the **operator maturity** Level IV, Deep Insights, which enables upgrading, monitoring, and alerting of **TempoStack** instances and the Tempo Operator.

- Add Ingress and Route configuration for the Gateway.

- Support the **managed** and **unmanaged** states in the **TempoStack** custom resource.

- Expose the following additional ingestion protocols in the Distributor service: Jaeger Thrift binary, Jaeger Thrift compact, Jaeger gRPC, and Zipkin. When the Gateway is enabled, only the OpenTelemetry protocol (OTLP) gRPC is enabled.

- Expose the Jaeger Query gRPC endpoint on the Query Frontend service.

- Support multitenancy without Gateway authentication and authorization.

1.4.4.2. Bug fixes

- Before this update, the Tempo Operator was not compatible with disconnected environments. With this update, the Tempo Operator supports disconnected environments. ([TRACING-3145](#))

- Before this update, the Tempo Operator with TLS failed to start on OpenShift Container Platform. With this update, the mTLS communication is enabled between Tempo components, the Operand starts successfully, and the Jaeger UI is accessible. ([TRACING-3091](#))

- Before this update, the resource limits from the Tempo Operator caused error messages such as `reason: OOMKilled`. With this update, the resource limits for the Tempo Operator are removed to avoid such errors. ([TRACING-3204](#))

1.4.4.3. Known issues
Currently, the custom TLS CA option is not implemented for connecting to object storage. (TRACING-3462)

Currently, when used with the Tempo Operator, the Jaeger UI only displays services that have sent traces in the last 15 minutes. For services that did not send traces in the last 15 minutes, traces are still stored but not displayed in the Jaeger UI. (TRACING-3139)

Currently, the distributed tracing platform (Tempo) fails on the IBM Z (s390x) architecture. (TRACING-3545)

Currently, the Tempo query frontend service must not use internal mTLS when Gateway is not deployed. This issue does not affect the Jaeger Query API. The workaround is to disable mTLS. (TRACING-3510)

**Workaround**

Disable mTLS as follows:

1. Open the Tempo Operator ConfigMap for editing by running the following command:

   ```bash
   $ oc edit configmap tempo-operator-manager-config -n openshift-tempo-operator
   ``

   The project where the Tempo Operator is installed.

2. Disable the mTLS in the operator configuration by updating the YAML file:

   ```yaml
   data:
   controller_manager_config.yaml: |
     featureGates:
       httpEncryption: false
       grpcEncryption: false
       builtinCertManagement:
         enabled: false
   ```

3. Restart the Tempo Operator pod by running the following command:

   ```bash
   $ oc rollout restart deployment.apps/tempo-operator-controller -n openshift-tempo-operator
   ```

**Workaround**

Add the Tempo Operator related images in the mirroring tool to mirror the images to the registry:

```yaml
kind: ImageSetConfiguration
apiVersion: mirror.openshift.io/v1alpha2
archiveSize: 20
storageConfig:
  local:
    path: /home/user/images
mirror:
```

Missing images for running the Tempo Operator in restricted environments. The Red Hat OpenShift distributed tracing platform (Tempo) CSV is missing references to the operand images. (TRACING-3523)
1.4.5. Red Hat build of OpenTelemetry

**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](#).

1.4.5.1. 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.

1.4.5.2. Bug fixes

None.

1.4.5.3. Known issues

operators:
  packages:
  - name: tempo-product
    channels:
    - name: stable
      additionalImages:
      - name: registry.redhat.io/rhosdt/tempo-rhel8@sha256:e4295f837066efb05bcc5897f31eb2bd81684a8c59d6f9498dd3590c62c12a
        - name: registry.redhat.io/rhosdt/tempo-gateway-rhel8@sha256:b62f5cedfe65907b638f14ca6aaeaa50f41642980a8a6f87b7061e88d90fac23
        - name: registry.redhat.io/rhosdt/tempo-gateway-opa-rhel8@sha256:8cd134deca47d6817b26566e272e6c3f75367653d589f5c90855c59b2f6be01e9
        - name: registry.redhat.io/rhosdt/tempo-query-rhel8@sha256:0da43034f440b8258a48a0697ba643b5643d48b615cdeb82ac7f4f1f80aad08e
1.4.6. 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 Hybrid Cloud Console. 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.

1.4.7. 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.

1.5. RELEASE NOTES FOR RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM 2.8

1.5.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.
1.5.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.8

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.42</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.74.0</td>
</tr>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>0.1.0</td>
</tr>
</tbody>
</table>

1.5.3. Technology Preview features

This release introduces support for the Red Hat OpenShift distributed tracing platform (Tempo) as a Technology Preview feature for Red Hat OpenShift distributed tracing platform.

**IMPORTANT**

The Red Hat OpenShift distributed tracing platform (Tempo) 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 feature uses version 0.1.0 of the Red Hat OpenShift distributed tracing platform (Tempo) and version 2.0.1 of the upstream distributed tracing platform (Tempo) components.

You can use the distributed tracing platform (Tempo) to replace Jaeger so that you can use S3-compatible storage instead of ElasticSearch. Most users who use the distributed tracing platform (Tempo) instead of Jaeger will not notice any difference in functionality because the distributed tracing platform (Tempo) supports the same ingestion and query protocols as Jaeger and uses the same user interface.

If you enable this Technology Preview feature, note the following limitations of the current implementation:

- The distributed tracing platform (Tempo) currently does not support disconnected installations. (TRACING-3145)
- When you use the Jaeger user interface (UI) with the distributed tracing platform (Tempo), the Jaeger UI lists only services that have sent traces within the last 15 minutes. For services that have not sent traces within the last 15 minutes, those traces are still stored even though they are not visible in the Jaeger UI. (TRACING-3139)

Expanded support for the Tempo Operator is planned for future releases of the Red Hat OpenShift distributed tracing platform. Possible additional features might include support for TLS authentication, multitenancy, and multiple clusters. For more information about the Tempo Operator, see the Tempo community documentation.
1.5.4. Bug fixes

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

1.5.5. 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 Hybrid Cloud Console. 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.

1.5.6. 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.

1.6. RELEASE NOTES FOR RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM 2.7

1.6.1. 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 (Jaeger) which is based on the open source Jaeger project.
- 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.

1.6.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.7

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.39</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.63.1</td>
</tr>
</tbody>
</table>

1.6.3. Bug fixes

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

1.6.4. 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 Hybrid Cloud Console. 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.

1.6.5. 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.

1.7. RELEASE NOTES FOR RED HAT OPENSSHIFT DISTRIBUTED TRACING PLATFORM 2.6

1.7.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.

### 1.7.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.6

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.38</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.60</td>
</tr>
</tbody>
</table>

### 1.7.3. Bug fixes

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

### 1.7.4. 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](https://www.redhat.com). 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 Hybrid Cloud Console](https://cloud.redhat.com/ocs/). 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.

### 1.7.5. 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.

1.8. RELEASE NOTES FOR RED HAT OPENSSHIFT DISTRIBUTED TRACING PLATFORM 2.5

1.8.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.

1.8.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.5

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.36</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.56</td>
</tr>
</tbody>
</table>

1.8.3. New features and enhancements

This release introduces support for ingesting OpenTelemetry protocol (OTLP) to the Red Hat OpenShift distributed tracing platform (Jaeger) Operator. The Operator now automatically enables the OTLP ports:

- Port 4317 for the OTLP gRPC protocol.
- Port 4318 for the OTLP HTTP protocol.

This release also adds support for collecting Kubernetes resource attributes to the Red Hat build of OpenTelemetry Operator.
1.8.4. Bug fixes

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

1.8.5. 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 Hybrid Cloud Console. 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.

1.8.6. 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.

1.9. RELEASE NOTES FOR RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM 2.4

1.9.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.

1.9.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.4

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.34.1</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.49</td>
</tr>
</tbody>
</table>

1.9.3. New features and enhancements

This release adds support for auto-provisioning certificates using the Red Hat Elasticsearch Operator.

• Self-provisioning by using the Red Hat OpenShift distributed tracing platform (Jaeger) Operator to call the Red Hat Elasticsearch Operator during installation.

IMPORTANT

When upgrading to the Red Hat OpenShift distributed tracing platform 2.4, the operator recreates the Elasticsearch instance, which might take five to ten minutes. Distributed tracing will be down and unavailable for that period.

1.9.4. Technology Preview features

• Creating the Elasticsearch instance and certificates first and then configuring the distributed tracing platform (Jaeger) to use the certificate is a Technology Preview for this release.

1.9.5. Bug fixes

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

1.9.6. 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 Hybrid Cloud Console. 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.
1.9.7. 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.

1.10. RELEASE NOTES FOR RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM 2.3

1.10.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.

1.10.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.3.0

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.30.1</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.44.0</td>
</tr>
</tbody>
</table>

1.10.3. Component versions in the Red Hat OpenShift distributed tracing platform 2.3.1
## 1.10.4. New features and enhancements

With this release, the Red Hat OpenShift distributed tracing platform (Jaeger) Operator is now installed to the `openshift-distributed-tracing` namespace by default. Before this update, the default installation had been in the `openshift-operators` namespace.

## 1.10.5. Bug fixes

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

## 1.10.6. 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](https://www.redhat.com). 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 Hybrid Cloud Console](https://docs.openshift.com/container-platform/4.4/cluster管理员/insights-console.html). 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](https://issues.redhat.com/new Issue) for the most relevant documentation component. Please provide specific details, such as the section name and OpenShift Container Platform version.

## 1.10.7. 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](https://www.redhat.com/blog/cto-chris-wright-message).

## 1.11. RELEASE NOTES FOR RED HAT OPENSSHIFT DISTRIBUTED TRACING PLATFORM 2.2

### 1.11.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.

1.11.2. Technology Preview features

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

1.11.3. Bug fixes

This release of the Red Hat OpenShift distributed tracing platform addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.

1.11.4. 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 Hybrid Cloud Console. 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.

1.11.5. 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.
1.12. RELEASE NOTES FOR RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM 2.1

1.12.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.

1.12.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.1.0

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.29.1</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.41.1</td>
</tr>
</tbody>
</table>

1.12.3. 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:
```

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"

1.12.4. Bug fixes

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

1.12.5. 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 Hybrid Cloud Console. 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.

1.12.6. 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.

1.13. RELEASE NOTES FOR RED HAT OPENShift DISTRIBUTED TRACING PLATFORM 2.0

1.13.1. 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 (Jaeger)** which is based on the open source Jaeger project.
- **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.

### 1.13.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.0.0

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger)</td>
<td>Jaeger</td>
<td>1.28.0</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.33.0</td>
</tr>
</tbody>
</table>

### 1.13.3. New features and enhancements

This release introduces the following new features and enhancements:

- Rebrands Red Hat OpenShift Jaeger as the Red Hat OpenShift distributed tracing platform.
- Updates Red Hat OpenShift distributed tracing platform (Jaeger) Operator to Jaeger 1.28. Going forward, the Red Hat OpenShift distributed tracing platform will only support the stable Operator channel. Channels for individual releases are no longer supported.
- Adds support for OpenTelemetry protocol (OTLP) to the Query service.
- Introduces a new distributed tracing icon that appears in the OperatorHub.
- Includes rolling updates to the documentation to support the name change and new features.

### 1.13.4. Technology Preview features

- 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 OpenShift distributed tracing platform. 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.

1.13.5. Bug fixes

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

1.13.6. 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 Hybrid Cloud Console. 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.

1.13.7. 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. DISTRIBUTED TRACING ARCHITECTURE

2.1. DISTRIBUTED TRACING ARCHITECTURE

Every time a user takes an action in an application, a request is executed by the architecture that may require dozens of different services to participate to produce a response. Red Hat OpenShift distributed tracing platform lets you perform distributed tracing, which records the path of a request through various microservices that make up an application.

Distributed tracing is a technique that is used to tie the information about different units of work together – usually executed in different processes or hosts – to understand a whole chain of events in a distributed transaction. Developers can visualize call flows in large microservice architectures with distributed tracing. It is valuable for understanding serialization, parallelism, and sources of latency.

Red Hat OpenShift distributed tracing platform records the execution of individual requests across the whole stack of microservices, and presents them as traces. A trace is a data/execution path through the system. An end-to-end trace is comprised of one or more spans.

A span represents a logical unit of work in Red Hat OpenShift distributed tracing platform that has an operation name, the start time of the operation, and the duration, as well as potentially tags and logs. Spans may be nested and ordered to model causal relationships.

2.1.1. 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 (Jaeger) which is based on the open source Jaeger project.
- 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.

2.1.2. Red Hat OpenShift distributed tracing platform features

Red Hat OpenShift distributed tracing platform provides the following capabilities:

- Integration with Kiali – When properly configured, you can view distributed tracing platform data from the Kiali console.
• High scalability – The distributed tracing platform back end is designed to have no single points of failure and to scale with the business needs.

• Distributed Context Propagation – Enables you to connect data from different components together to create a complete end-to-end trace.

• Backwards compatibility with Zipkin – Red Hat OpenShift distributed tracing platform has APIs that enable it to be used as a drop-in replacement for Zipkin, but Red Hat is not supporting Zipkin compatibility in this release.

2.1.3. Red Hat OpenShift distributed tracing platform architecture

Red Hat OpenShift distributed tracing platform is made up of several components that work together to collect, store, and display tracing data.

• **Red Hat OpenShift distributed tracing platform (Jaeger)** - This component is based on the open source Jaeger project.
  
  • **Client** (Jaeger client, Tracer, Reporter, instrumented application, client libraries) - The distributed tracing platform (Jaeger) clients are language-specific implementations of the OpenTracing API. They can be used to instrument applications for distributed tracing either manually or with a variety of existing open source frameworks, such as Camel (Fuse), Spring Boot (RHOAR), MicroProfile (RHOAR/Thorntail), Wildfly (EAP), and many more, that are already integrated with OpenTracing.

  • **Agent** (Jaeger agent, Server Queue, Processor Workers) - The distributed tracing platform (Jaeger) agent is a network daemon that listens for spans sent over User Datagram Protocol (UDP), which it batches and sends to the Collector. The agent is meant to be placed on the same host as the instrumented application. This is typically accomplished by having a sidecar in container environments such as Kubernetes.

  • **Jaeger Collector** (Collector, Queue, Workers) - Similar to the Jaeger agent, the Jaeger Collector receives spans and places them in an internal queue for processing. This allows the Jaeger Collector to return immediately to the client/agent instead of waiting for the span to make its way to the storage.

  • **Storage** (Data Store) - Collectors require a persistent storage backend. Red Hat OpenShift distributed tracing platform (Jaeger) has a pluggable mechanism for span storage. Note that for this release, the only supported storage is Elasticsearch.

  • **Query** (Query Service) - Query is a service that retrieves traces from storage.

  • **Ingester** (Ingester Service) - Red Hat OpenShift distributed tracing platform can use Apache Kafka as a buffer between the Collector and the actual Elasticsearch backing storage. Ingester is a service that reads data from Kafka and writes to the Elasticsearch storage backend.

  • **Jaeger Console** – With the Red Hat OpenShift distributed tracing platform (Jaeger) user interface, you can visualize your distributed tracing data. On the Search page, you can find traces and explore details of the spans that make up an individual trace.

• **Red Hat OpenShift distributed tracing platform (Tempo)** - This component is based on the open source Grafana Tempo project.

  • **Gateway** – The Gateway handles authentication, authorization, and forwarding requests to the Distributor or Query front-end service.
- **Distributor** – The Distributor accepts spans in multiple formats including Jaeger, OpenTelemetry, and Zipkin. It routes spans to Ingesters by hashing the `traceID` and using a distributed consistent hash ring.

- **Ingester** – The Ingester batches a trace into blocks, creates bloom filters and indexes, and then flushes it all to the back end.

- **Query Frontend** – The Query Frontend is responsible for sharding the search space for an incoming query. The search query is then sent to the Queriers. The Query Frontend deployment exposes the Jaeger UI through the Tempo Query sidecar.

- **Querier** – The Querier is responsible for finding the requested trace ID in either the Ingesters or the back-end storage. Depending on parameters, it can query the Ingesters and pull Bloom indexes from the back end to search blocks in object storage.

- **Compactor** – The Compactors stream blocks to and from the back-end storage to reduce the total number of blocks.

- **Red Hat build of OpenTelemetry** – This component is based on the open source OpenTelemetry project.

- **OpenTelemetry Collector** – The OpenTelemetry Collector is a vendor-agnostic way to receive, process, and export telemetry data. The OpenTelemetry Collector supports open-source observability data formats, for example, Jaeger and Prometheus, sending to one or more open-source or commercial back-ends. The Collector is the default location instrumentation libraries export their telemetry data.
CHAPTER 3. DISTRIBUTED TRACING PLATFORM (JAEGGER)

3.1. INSTALLING THE DISTRIBUTED TRACING PLATFORM JAEGGER

WARNING
Jaeger is deprecated in Red Hat OpenShift distributed tracing 3.0.

You can install Red Hat OpenShift distributed tracing platform on OpenShift Container Platform in either of two ways:

- You can install Red Hat OpenShift distributed tracing platform as part of Red Hat OpenShift Service Mesh. Distributed tracing is included by default in the Service Mesh installation. To install Red Hat OpenShift distributed tracing platform as part of a service mesh, follow the Red Hat Service Mesh Installation instructions. You must install Red Hat OpenShift distributed tracing platform in the same namespace as your service mesh, that is, the ServiceMeshControlPlane and the Red Hat OpenShift distributed tracing platform resources must be in the same namespace.

- If you do not want to install a service mesh, you can use the Red Hat OpenShift distributed tracing platform Operators to install distributed tracing platform by itself. To install Red Hat OpenShift distributed tracing platform without a service mesh, use the following instructions.

3.1.1. Prerequisites
Before you can install Red Hat OpenShift distributed tracing platform, review the installation activities, and ensure that you meet the prerequisites:

- Possess an active OpenShift Container Platform subscription on your Red Hat account. If you do not have a subscription, contact your sales representative for more information.

- Review the OpenShift Container Platform 4.11 overview.

- Install OpenShift Container Platform 4.11.
  - Install OpenShift Container Platform 4.11 on AWS
  - Install OpenShift Container Platform 4.11 on user-provisioned AWS
  - Install OpenShift Container Platform 4.11 on bare metal
  - Install OpenShift Container Platform 4.11 on vSphere

- Install the version of the oc CLI tool that matches your OpenShift Container Platform version and add it to your path.

- An account with the cluster-admin role.

3.1.2. Red Hat OpenShift distributed tracing platform installation overview
The steps for installing Red Hat OpenShift distributed tracing platform are as follows:

- Review the documentation and determine your deployment strategy.
- If your deployment strategy requires persistent storage, install the OpenShift Elasticsearch Operator via the OperatorHub.
- Install the Red Hat OpenShift distributed tracing platform (Jaeger) Operator via the OperatorHub.
- Modify the custom resource YAML file to support your deployment strategy.
- Deploy one or more instances of Red Hat OpenShift distributed tracing platform (Jaeger) to your OpenShift Container Platform environment.

### 3.1.3. Installing the OpenShift Elasticsearch Operator

The default Red Hat OpenShift distributed tracing platform (Jaeger) deployment uses in-memory storage because it is designed to be installed quickly for those evaluating Red Hat OpenShift distributed tracing platform, giving demonstrations, or using Red Hat OpenShift distributed tracing platform (Jaeger) in a test environment. If you plan to use Red Hat OpenShift distributed tracing platform (Jaeger) in production, you must install and configure a persistent storage option, in this case, Elasticsearch.

#### Prerequisites

- You have access to the OpenShift Container Platform web console.
- You have access to the cluster as a user with the `cluster-admin` role. If you use Red Hat OpenShift Dedicated, you must have an account with the `dedicated-admin` role.

**WARNING**

Do not install Community versions of the Operators. Community Operators are not supported.

**NOTE**

If you have already installed the OpenShift Elasticsearch Operator as part of OpenShift Logging, you do not need to install the OpenShift Elasticsearch Operator again. The Red Hat OpenShift distributed tracing platform (Jaeger) Operator creates the Elasticsearch instance using the installed OpenShift Elasticsearch Operator.

#### Procedure

1. Log in to the OpenShift Container Platform web console as a user with the `cluster-admin` role. If you use Red Hat OpenShift Dedicated, you must have an account with the `dedicated-admin` role.

3. Type Elasticsearch into the filter box to locate the OpenShift Elasticsearch Operator.

4. Click the **OpenShift Elasticsearch Operator** provided by Red Hat to display information about the Operator.

5. Click **Install**.

6. On the **Install Operator** page, select the **stable** Update Channel. This automatically updates your Operator as new versions are released.

7. Accept the default **All namespaces on the cluster (default)** This installs the Operator in the default **openshift-operators-redhat** project and makes the Operator available to all projects in the cluster.

   **NOTE**

   The Elasticsearch installation requires the **openshift-operators-redhat** namespace for the OpenShift Elasticsearch Operator. The other Red Hat OpenShift distributed tracing platform Operators are installed in the **openshift-operators** namespace.

8. Accept the default **Automatic** approval strategy. By accepting the default, when a new version of this Operator is available, Operator Lifecycle Manager (OLM) automatically upgrades the running instance of your Operator without human intervention. If you select **Manual** updates, when a newer version of an Operator is available, OLM creates an update request. As a cluster administrator, you must then manually approve that update request to have the Operator updated to the new version.

   **NOTE**

   The **Manual** approval strategy requires a user with appropriate credentials to approve the Operator install and subscription process.

9. Click **Install**.

10. On the **Installed Operators** page, select the **openshift-operators-redhat** project. Wait until you see that the OpenShift Elasticsearch Operator shows a status of "InstallSucceeded" before continuing.

### 3.1.4. Installing the Red Hat OpenShift distributed tracing platform (Jaeger) Operator

To install Red Hat OpenShift distributed tracing platform (Jaeger), you use the **OperatorHub** to install the Red Hat OpenShift distributed tracing platform (Jaeger) Operator.

By default, the Operator is installed in the **openshift-operators** project.

**Prerequisites**

- You have access to the OpenShift Container Platform web console.
- You have access to the cluster as a user with the **cluster-admin** role. If you use Red Hat OpenShift Dedicated, you must have an account with the **dedicated-admin** role.
If you require persistent storage, you must also install the OpenShift Elasticsearch Operator before installing the Red Hat OpenShift distributed tracing platform (Jaeger) Operator.

**WARNING**

Do not install Community versions of the Operators. Community Operators are not supported.

**Procedure**

1. Log in to the OpenShift Container Platform web console as a user with the `cluster-admin` role. If you use Red Hat OpenShift Dedicated, you must have an account with the `dedicated-admin` role.

2. Navigate to **Operators → OperatorHub**.

3. Type **distributed tracing platform** into the filter to locate the Red Hat OpenShift distributed tracing platform (Jaeger) Operator.

4. Click the **Red Hat OpenShift distributed tracing platform (Jaeger) Operator** provided by Red Hat to display information about the Operator.

5. Click **Install**.

6. On the **Install Operator** page, select the **stable** Update Channel. This automatically updates your Operator as new versions are released.

7. Accept the default **All namespaces on the cluster (default)** This installs the Operator in the default `openshift-operators` project and makes the Operator available to all projects in the cluster.

   - Accept the default **Automatic** approval strategy. By accepting the default, when a new version of this Operator is available, Operator Lifecycle Manager (OLM) automatically upgrades the running instance of your Operator without human intervention. If you select **Manual** updates, when a newer version of an Operator is available, OLM creates an update request. As a cluster administrator, you must then manually approve that update request to have the Operator updated to the new version.

   **NOTE**

   The **Manual** approval strategy requires a user with appropriate credentials to approve the Operator install and subscription process.

8. Click **Install**.

9. Navigate to **Operators → Installed Operators**.

10. On the **Installed Operators** page, select the **openshift-operators** project. Wait until you see that the Red Hat OpenShift distributed tracing platform (Jaeger) Operator shows a status of "Succeeded" before continuing.
3.2. CONFIGURING AND DEPLOYING THE DISTRIBUTED TRACING PLATFORM JAEGER

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

If you have installed distributed tracing platform as part of Red Hat OpenShift Service Mesh, you can perform basic configuration as part of the ServiceMeshControlPlane, but for complete control, you must configure a Jaeger CR and then reference your distributed tracing configuration file in the ServiceMeshControlPlane.

The Red Hat OpenShift distributed tracing platform (Jaeger) has predefined deployment strategies. You specify a deployment strategy in the custom resource file. When you create a distributed tracing platform (Jaeger) instance, the Operator uses this configuration file to create the objects necessary for the deployment.

Jaeger custom resource file showing deployment strategy

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: MyConfigFile
spec:
  strategy: production
```

Deployment strategy.

3.2.1. Supported deployment strategies

The Red Hat OpenShift distributed tracing platform (Jaeger) Operator currently supports the following deployment strategies:

**allInOne**

- This strategy is intended for development, testing, and demo purposes; it is not intended for production use. The main backend components, Agent, Collector, and Query service, are all packaged into a single executable which is configured, by default, to use in-memory storage.

**NOTE**

In-memory storage is not persistent, which means that if the distributed tracing platform (Jaeger) instance shuts down, restarts, or is replaced, that your trace data will be lost. And in-memory storage cannot be scaled, since each pod has its own memory. For persistent storage, you must use the production or streaming strategies, which use Elasticsearch as the default storage.

**production**

The production strategy is intended for production environments, where long term storage of trace data is important, as well as a more scalable and highly available architecture is required. Each of the backend components is therefore deployed separately. The Agent can be injected as a sidecar on
the instrumented application. The Query and Collector services are configured with a supported storage type - currently Elasticsearch. Multiple instances of each of these components can be provisioned as required for performance and resilience purposes.

streaming

The streaming strategy is designed to augment the production strategy by providing a streaming capability that effectively sits between the Collector and the Elasticsearch backend storage. This provides the benefit of reducing the pressure on the backend storage, under high load situations, and enables other trace post-processing capabilities to tap into the real time span data directly from the streaming platform (AMQ Streams/ Kafka).

NOTE

- The streaming strategy requires an additional Red Hat subscription for AMQ Streams.
- The streaming deployment strategy is currently unsupported on IBM Z.

3.2.2. Deploying the distributed tracing platform default strategy from the web console

The custom resource definition (CRD) defines the configuration used when you deploy an instance of Red Hat OpenShift distributed tracing platform. The default CR is named jaeger-all-in-one-inmemory and it is configured with minimal resources to ensure that you can successfully install it on a default OpenShift Container Platform installation. You can use this default configuration to create a Red Hat OpenShift distributed tracing platform (Jaeger) instance that uses the AllInOne deployment strategy, or you can define your own custom resource file.

NOTE

In-memory storage is not persistent. If the Jaeger pod shuts down, restarts, or is replaced, your trace data will be lost. For persistent storage, you must use the production or streaming strategies, which use Elasticsearch as the default storage.

Prerequisites

- The Red Hat OpenShift distributed tracing platform (Jaeger) Operator has been installed.
- You have reviewed the instructions for how to customize the deployment.
- You have access to the cluster as a user with the cluster-admin role.

Procedure

1. Log in to the OpenShift Container Platform web console as a user with the cluster-admin role.

2. Create a new project, for example tracing-system.

NOTE

If you are installing as part of Service Mesh, the distributed tracing platform resources must be installed in the same namespace as the ServiceMeshControlPlane resource, for example istio-system.
3.2.2.1. Deploying the distributed tracing platform default strategy from the CLI

Follow this procedure to create an instance of distributed tracing platform (Jaeger) from the command line.

Prerequisites

- The Red Hat OpenShift distributed tracing platform (Jaeger) Operator has been installed and verified.
- You have reviewed the instructions for how to customize the deployment.
- You have access to the OpenShift CLI (oc) that matches your OpenShift Container Platform version.
- You have access to the cluster as a user with the cluster-admin role.

Procedure

1. Log in to the OpenShift Container Platform CLI as a user with the cluster-admin role by running the following command:

   ```bash
   $ oc login --username=<NAMEOFUSER> https://<HOSTNAME>:8443
   ```

2. Create a new project named tracing-system by running the following command:

   ```bash
   $ oc new-project tracing-system
   ```
3. Create a custom resource file named `jaeger.yaml` that contains the following text:

Example `jaeger-all-in-one.yaml`

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: jaeger-all-in-one-inmemory
```

4. Run the following command to deploy distributed tracing platform (Jaeger):

```
$ oc create -n tracing-system -f jaeger.yaml
```

5. Run the following command to watch the progress of the pods during the installation process:

```
$ oc get pods -n tracing-system -w
```

After the installation process has completed, the output is similar to the following example:

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>jaeger-all-in-one-inmemory-cdf17897b-qhfdx</td>
<td>2/2</td>
<td>Running</td>
<td>0</td>
<td>24s</td>
</tr>
</tbody>
</table>

3.2.3. Deploying the distributed tracing platform production strategy from the web console

The **production** deployment strategy is intended for production environments that require a more scalable and highly available architecture, and where long-term storage of trace data is important.

**Prerequisites**

- The OpenShift Elasticsearch Operator has been installed.
- The Red Hat OpenShift distributed tracing platform (Jaeger) Operator has been installed.
- You have reviewed the instructions for how to customize the deployment.
- You have access to the cluster as a user with the `cluster-admin` role.

**Procedure**

1. Log in to the OpenShift Container Platform web console as a user with the `cluster-admin` role.

2. Create a new project, for example `tracing-system`.

   **NOTE**

   If you are installing as part of Service Mesh, the distributed tracing platform resources must be installed in the same namespace as the `ServiceMeshControlPlane` resource, for example `istio-system`.


   b. Click `Create Project`
c. Enter `tracing-system` in the Name field.

d. Click Create.

3. Navigate to Operators → Installed Operators.

4. If necessary, select `tracing-system` from the Project menu. You may have to wait a few moments for the Operators to be copied to the new project.

5. Click the Red Hat OpenShift distributed tracing platform (Jaeger) Operator. On the Overview tab, under Provided APIs, the Operator provides a single link.

6. Under Jaeger, click Create Instance.

7. On the Create Jaeger page, replace the default all-in-one YAML text with your production YAML configuration, for example:

   **Example jaeger-production.yaml file with Elasticsearch**

   ```yaml
   apiVersion: jaegertracing.io/v1
   kind: Jaeger
   metadata:
     name: jaeger-production
     namespace: 
   spec:
     strategy: production
     ingress:
       security: oauth-proxy
       storage:
         type: elasticsearch
         elasticsearch:
           nodeCount: 3
           redundancyPolicy: SingleRedundancy
         esIndexCleaner:
           enabled: true
           numberOfDays: 7
           schedule: 55 23 * * *
         esRollover:
           schedule: */30 * * * *
   ```

8. Click Create to create the distributed tracing platform (Jaeger) instance.

9. On the Jaegers page, click the name of the distributed tracing platform (Jaeger) instance, for example, `jaeger-prod-elasticsearch`.

10. On the Jaeger Details page, click the Resources tab. Wait until all the pods have a status of "Running" before continuing.

**3.2.3.1. Deploying the distributed tracing platform production strategy from the CLI**

Follow this procedure to create an instance of distributed tracing platform (Jaeger) from the command line.

**Prerequisites**

- The OpenShift Elasticsearch Operator has been installed.
The Red Hat OpenShift distributed tracing platform (Jaeger) Operator has been installed.

You have reviewed the instructions for how to customize the deployment.

You have access to the OpenShift CLI (`oc`) that matches your OpenShift Container Platform version.

You have access to the cluster as a user with the `cluster-admin` role.

**Procedure**

1. Log in to the OpenShift CLI (`oc`) as a user with the `cluster-admin` role by running the following command:

   ```bash
   $ oc login --username=<NAMEOFUSER> https://<HOSTNAME>:8443
   ```

2. Create a new project named `tracing-system` by running the following command:

   ```bash
   $ oc new-project tracing-system
   ```

3. Create a custom resource file named `jaeger-production.yaml` that contains the text of the example file in the previous procedure.

4. Run the following command to deploy distributed tracing platform (Jaeger):

   ```bash
   $ oc create -n tracing-system -f jaeger-production.yaml
   ```

5. Run the following command to watch the progress of the pods during the installation process:

   ```bash
   $ oc get pods -n tracing-system -w
   ```

   After the installation process has completed, you will see output similar to the following example:

   ```
   NAME                                                              READY   STATUS    RESTARTS   AGE
   elasticsearch-cdm-jaegersystemjaegerproduction-1-6676cf568gwhlw   2/2     Running   0          10m
   elasticsearch-cdm-jaegersystemjaegerproduction-2-bcd4c8bf5l6g6w   2/2     Running   0          10m
   elasticsearch-cdm-jaegersystemjaegerproduction-3-844d6d9694hhst   2/2     Running   0          10m
   jaeger-production-collector-94cd847d-jwjlj                        1/1     Running   3          8m32s
   jaeger-production-query-5cbfbd499d-tv8zf                          3/3     Running   3          8m32s
   ```

**3.2.4. Deploying the distributed tracing platform streaming strategy from the web console**

The **streaming** deployment strategy is intended for production environments that require a more scalable and highly available architecture, and where long-term storage of trace data is important.

The **streaming** strategy provides a streaming capability that sits between the Collector and the Elasticsearch storage. This reduces the pressure on the storage under high load situations, and enables other trace post-processing capabilities to tap into the real-time span data directly from the Kafka streaming platform.
NOTE

The streaming strategy requires an additional Red Hat subscription for AMQ Streams. If you do not have an AMQ Streams subscription, contact your sales representative for more information.

NOTE

The streaming deployment strategy is currently unsupported on IBM Z.

Prerequisites

- The AMQ Streams Operator has been installed. If using version 1.4.0 or higher you can use self-provisioning. Otherwise you must create the Kafka instance.
- The Red Hat OpenShift distributed tracing platform (Jaeger) Operator has been installed.
- You have reviewed the instructions for how to customize the deployment.
- You have access to the cluster as a user with the `cluster-admin` role.

Procedure

1. Log in to the OpenShift Container Platform web console as a user with the `cluster-admin` role.

2. Create a new project, for example `tracing-system`.

   b. Click `Create Project`.
   c. Enter `tracing-system` in the `Name` field.
   d. Click `Create`.

3. Navigate to `Operators` → `Installed Operators`.

4. If necessary, select `tracing-system` from the `Project` menu. You may have to wait a few moments for the Operators to be copied to the new project.

5. Click the Red Hat OpenShift distributed tracing platform (Jaeger) Operator. On the `Overview` tab, under `Provided APIs`, the Operator provides a single link.

6. Under `Jaeger`, click `Create Instance`.

7. On the `Create Jaeger` page, replace the default `all-in-one` YAML text with your streaming YAML configuration, for example:

   Example jaeger-streaming.yaml file
   
   ```yaml
   ```
If the brokers are not defined, AMQ Streams 1.4.0+ self-provisions Kafka.

8. Click **Create** to create the distributed tracing platform (Jaeger) instance.

9. On the **Jaegers** page, click the name of the distributed tracing platform (Jaeger) instance, for example, **jaeger-streaming**.

10. On the **Jaeger Details** page, click the **Resources** tab. Wait until all the pods have a status of "Running" before continuing.

### 3.2.4.1. Deploying the distributed tracing platform streaming strategy from the CLI

Follow this procedure to create an instance of distributed tracing platform (Jaeger) from the command line.

**Prerequisites**

- The AMQ Streams Operator has been installed. If using version 1.4.0 or higher you can use self-provisioning. Otherwise you must create the Kafka instance.

- The Red Hat OpenShift distributed tracing platform (Jaeger) Operator has been installed.

- You have reviewed the instructions for how to customize the deployment.

- You have access to the OpenShift CLI (**oc**) that matches your OpenShift Container Platform version.

- You have access to the cluster as a user with the **cluster-admin** role.

**Procedure**

1. Log in to the OpenShift CLI (**oc**) as a user with the **cluster-admin** role by running the following command:

   ```yaml
   apiVersion: jaegertracing.io/v1
   kind: Jaeger
   metadata:
     name: jaeger-streaming
   spec:
     strategy: streaming
     collector:
       options:
         kafka:
           producer:
             topic: jaeger-spans
             brokers: my-cluster-kafka-brokers.kafka:9092
           storage:
             type: elasticsearch
             ingester:
               options:
                 kafka:
                   consumer:
                     topic: jaeger-spans
                     brokers: my-cluster-kafka-brokers.kafka:9092
   ```

   If the brokers are not defined, AMQ Streams 1.4.0+ self-provisions Kafka.
3.2.5. Validating your deployment

3.2.5.1. Accessing the Jaeger console

To access the Jaeger console you must have either Red Hat OpenShift Service Mesh or Red Hat OpenShift distributed tracing platform installed, and Red Hat OpenShift distributed tracing platform (Jaeger) installed, configured, and deployed.

The installation process creates a route to access the Jaeger console.

If you know the URL for the Jaeger console, you can access it directly. If you do not know the URL, use the following directions.

Procedure from the web console

1. Log in to the OpenShift Container Platform web console as a user with cluster-admin rights. If you use Red Hat OpenShift Dedicated, you must have an account with the dedicated-admin role.
2. Navigate to Networking → Routes.

3. On the Routes page, select the control plane project, for example, tracing-system, from the Namespace menu. The Location column displays the linked address for each route.

4. If necessary, use the filter to find the jaeger route. Click the route Location to launch the console.

5. Click Log In With OpenShift

**Procedure from the CLI**

1. Log in to the OpenShift Container Platform CLI as a user with the **cluster-admin** role by running the following command. If you use Red Hat OpenShift Dedicated, you must have an account with the **dedicated-admin** role.

   ```bash
   $ oc login --username=<NAMEOFUSER> https://<HOSTNAME>:6443
   ```

2. To query for details of the route using the command line, enter the following command. In this example, tracing-system is the control plane namespace.

   ```bash
   $ export JAEGER_URL=$(oc get route -n tracing-system jaeger -o jsonpath='{.spec.host}')
   ```

3. Launch a browser and navigate to https://<JAEGER_URL>, where <JAEGER_URL> is the route that you discovered in the previous step.

4. Log in using the same user name and password that you use to access the OpenShift Container Platform console.

5. If you have added services to the service mesh and have generated traces, you can use the filters and Find Traces button to search your trace data. If you are validating the console installation, there is no trace data to display.

**3.2.6. Customizing your deployment**

**3.2.6.1. Deployment best practices**

- Red Hat OpenShift distributed tracing platform instance names must be unique. If you want to have multiple Red Hat OpenShift distributed tracing platform (Jaeger) instances and are using sidecar injected agents, then the Red Hat OpenShift distributed tracing platform (Jaeger) instances should have unique names, and the injection annotation should explicitly specify the Red Hat OpenShift distributed tracing platform (Jaeger) instance name the tracing data should be reported to.

- If you have a multitenant implementation and tenants are separated by namespaces, deploy a Red Hat OpenShift distributed tracing platform (Jaeger) instance to each tenant namespace.

For information about configuring persistent storage, see Understanding persistent storage and the appropriate configuration topic for your chosen storage option.

**3.2.6.2. Distributed tracing default configuration options**
The Jaeger custom resource (CR) defines the architecture and settings to be used when creating the distributed tracing platform (Jaeger) resources. You can modify these parameters to customize your distributed tracing platform (Jaeger) implementation to your business needs.

**Generic YAML example of the Jaeger CR**

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: name
spec:
  strategy: <deployment_strategy>
    allInOne:
      options: {}
      resources: {}
  agent:
    options: {}
    resources: {}
  collector:
    options: {}
    resources: {}
  sampling:
    options: {}
    resources: {}
  storage:
    type:
      options: {}
  query:
    options: {}
    resources: {}
  ingester:
    options: {}
    resources: {}
  options: {};
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>apiVersion</td>
<td>API version to use when creating the object.</td>
<td>jaegertracing.io/v1</td>
<td>jaegertracing.io/v1</td>
</tr>
<tr>
<td>kind</td>
<td>Defines the kind of Kubernetes object to create.</td>
<td>jaeger</td>
<td></td>
</tr>
<tr>
<td>metadata</td>
<td>Data that helps uniquely identify the object, including a <strong>name</strong> string, <strong>UID</strong>, and optional <strong>namespace</strong>.</td>
<td></td>
<td>OpenShift Container Platform automatically generates the <strong>UID</strong> and completes the <strong>namespace</strong> with the name of the project where the object is created.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Default value</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>--------</td>
<td>---------------</td>
</tr>
<tr>
<td>name:</td>
<td>Name for the object.</td>
<td>The name of your distributed tracing platform (Jaeger) instance.</td>
<td>jaeger-all-in-one-inmemory</td>
</tr>
<tr>
<td>spec:</td>
<td>Specification for the object to be created.</td>
<td>Contains all of the configuration parameters for your distributed tracing platform (Jaeger) instance. When a common definition for all Jaeger components is required, it is defined under the <code>spec</code> node. When the definition relates to an individual component, it is placed under the <code>spec/&lt;component&gt;</code> node.</td>
<td>N/A</td>
</tr>
<tr>
<td>strategy:</td>
<td>Jaeger deployment strategy</td>
<td>allInOne, production, or streaming</td>
<td>allInOne</td>
</tr>
<tr>
<td>allInOne:</td>
<td>Because the <code>allInOne</code> image deploys the Agent, Collector, Query, Ingester, and Jaeger UI in a single pod, configuration for this deployment must nest component configuration under the <code>allInOne</code> parameter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>agent:</td>
<td>Configuration options that define the Agent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>collector:</td>
<td>Configuration options that define the Jaeger Collector.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sampling:</td>
<td>Configuration options that define the sampling strategies for tracing.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
storage:
Configuration options that define the storage. All storage-related options must be placed under `storage`, rather than under the `allInOne` or other component options.

query:
Configuration options that define the Query service.

ingester:
Configuration options that define the Ingester service.

The following example YAML is the minimum required to create a Red Hat OpenShift distributed tracing platform (Jaeger) deployment using the default settings.

**Example minimum required dist-tracing-all-in-one.yaml**

```yaml
apiVersion: jaegertracing.io/v1
type: Jaeger
metadata: name: jaeger-all-in-one-inmemory
```

### 3.2.6.3. Jaeger Collector configuration options

The Jaeger Collector is the component responsible for receiving the spans that were captured by the tracer and writing them to persistent Elasticsearch storage when using the `production` strategy, or to AMQ Streams when using the `streaming` strategy.

The Collectors are stateless and thus many instances of Jaeger Collector can be run in parallel. Collectors require almost no configuration, except for the location of the Elasticsearch cluster.

**Table 3.2. Parameters used by the Operator to define the Jaeger Collector**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>collector: replicas:</td>
<td>Specifies the number of Collector replicas to create.</td>
<td>Integer, for example, 5</td>
</tr>
</tbody>
</table>

**Table 3.3. Configuration parameters passed to the Collector**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec:</td>
<td>Configuration options that define the Jaeger Collector.</td>
<td></td>
</tr>
<tr>
<td>collector:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>collector:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>num-workers:</td>
<td>The number of workers pulling from the queue.</td>
<td>Integer, for example, <strong>50</strong></td>
</tr>
<tr>
<td>options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>collector:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>queue-size:</td>
<td>The size of the Collector queue.</td>
<td>Integer, for example, <strong>2000</strong></td>
</tr>
<tr>
<td>options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kafka:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>producer:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>topic: jaeger-spans</td>
<td>The <strong>topic</strong> parameter identifies the Kafka configuration used by the Collector to produce the messages, and the Ingester to consume the messages.</td>
<td>Label for the producer.</td>
</tr>
<tr>
<td>options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kafka:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>producer:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>brokers: my-cluster-kafka-brokers.kafka:9092</td>
<td>Identifies the Kafka configuration used by the Collector to produce the messages. If brokers are not specified, and you have AMQ Streams 1.4.0+ installed, the Red Hat OpenShift distributed tracing platform (Jaeger) Operator will self-provision Kafka.</td>
<td></td>
</tr>
<tr>
<td>options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log-level:</td>
<td></td>
<td>Possible values: <strong>debug, info, warn, error, fatal, panic.</strong></td>
</tr>
</tbody>
</table>
3.2.6.4. Distributed tracing sampling configuration options

The Red Hat OpenShift distributed tracing platform (Jaeger) Operator can be used to define sampling strategies that will be supplied to tracers that have been configured to use a remote sampler.

While all traces are generated, only a few are sampled. Sampling a trace marks the trace for further processing and storage.

**NOTE**

This is not relevant if a trace was started by the Envoy proxy, as the sampling decision is made there. The Jaeger sampling decision is only relevant when the trace is started by an application using the client.

When a service receives a request that contains no trace context, the client starts a new trace, assigns it a random trace ID, and makes a sampling decision based on the currently installed sampling strategy. The sampling decision propagates to all subsequent requests in the trace so that other services are not making the sampling decision again.

distributed tracing platform (Jaeger) libraries support the following samplers:

- **Probabilistic** - The sampler makes a random sampling decision with the probability of sampling equal to the value of the `sampling.param` property. For example, using `sampling.param=0.1` samples approximately 1 in 10 traces.
• **Rate Limiting** - The sampler uses a leaky bucket rate limiter to ensure that traces are sampled with a certain constant rate. For example, using `sampling.param=2.0` samples requests with the rate of 2 traces per second.

**Table 3.4. Jaeger sampling options**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>spec: sampling: options:</code></td>
<td>Configuration options that define the sampling strategies for tracing.</td>
<td></td>
<td>If you do not provide configuration, the Collectors will return the default probabilistic sampling policy with 0.001 (0.1%) probability for all services.</td>
</tr>
<tr>
<td><code>default_strategy:</code></td>
<td>Sampling strategy to use. See descriptions above.</td>
<td>Valid values are <code>probabilistic</code>, and <code>ratelimiting</code>.</td>
<td><code>probabilistic</code></td>
</tr>
<tr>
<td><code>param:</code></td>
<td>Parameters for the selected sampling strategy.</td>
<td>Decimal and integer values (0, .1, 1, 10)</td>
<td>1</td>
</tr>
</tbody>
</table>

This example defines a default sampling strategy that is probabilistic, with a 50% chance of the trace instances being sampled.

**Probabilistic sampling example**

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: with-sampling
spec:
  sampling:
    options:
      default_strategy:
        type: probabilistic
        param: 0.5
    service_strategies:
      - service: alpha
        type: probabilistic
        param: 0.8
      operation_strategies:
        - operation: op1
          type: probabilistic
          param: 0.2
        - operation: op2
          type: probabilistic
```
If there are no user-supplied configurations, the distributed tracing platform (Jaeger) uses the following settings:

**Default sampling**

```yaml
spec:
  sampling:
    options:
      default_strategy:
        type: probabilistic
        param: 1
```

### 3.2.6.5. Distributed tracing storage configuration options

You configure storage for the Collector, Ingester, and Query services under `spec.storage`. Multiple instances of each of these components can be provisioned as required for performance and resilience purposes.

**Table 3.5. General storage parameters used by the Red Hat OpenShift distributed tracing platform (Jaeger) Operator to define distributed tracing storage**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>spec:</code></td>
<td>Type of storage to use for the deployment.</td>
<td><code>memory</code> or <code>elasticsearch</code>.</td>
<td><code>memory</code></td>
</tr>
<tr>
<td><code>storage:</code></td>
<td>Memory storage is only appropriate for development, testing, demonstrations, and proof of concept environments as the data does not persist if the pod is shut down. For production environments distributed tracing platform (Jaeger) supports Elasticsearch for persistent storage.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>type:</code></td>
<td>Name of the secret, for example <code>tracing-secret</code>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>secretname:</td>
<td>Configuration options that define the storage.</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td><code>options:</code></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3.6. Elasticsearch index cleaner parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage: esIndexCleaner: enabled:</td>
<td>When using Elasticsearch storage, by default a job is created to clean old traces from the index. This parameter enables or disables the index cleaner job.</td>
<td>true/ false</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>storage: esIndexCleaner: numberOfDays:</td>
<td>Number of days to wait before deleting an index.</td>
<td>Integer value</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>storage: esIndexCleaner: schedule:</td>
<td>Defines the schedule for how often to clean the Elasticsearch index.</td>
<td>Cron expression</td>
<td>&quot;55 23 * * *&quot;</td>
</tr>
</tbody>
</table>

3.2.6.5.1. Auto-provisioning an Elasticsearch instance

When you deploy a Jaeger custom resource, the Red Hat OpenShift distributed tracing platform (Jaeger) Operator uses the OpenShift Elasticsearch Operator to create an Elasticsearch cluster based on the configuration provided in the `storage` section of the custom resource file. The Red Hat OpenShift distributed tracing platform (Jaeger) Operator will provision Elasticsearch if the following configurations are set:

- `spec.storage:type` is set to `elasticsearch`
- `spec.storage.elasticsearch.doNotProvision` set to `false`
- `spec.storage.options.es.server-urls` is not defined, that is, there is no connection to an Elasticsearch instance that was not provisioned by the Red Hat Elasticsearch Operator.

When provisioning Elasticsearch, the Red Hat OpenShift distributed tracing platform (Jaeger) Operator sets the Elasticsearch custom resource name to the value of `spec.storage.elasticsearch.name` from the Jaeger custom resource. If you do not specify a value for `spec.storage.elasticsearch.name`, the Operator uses `elasticsearch`.

Restrictions

- You can have only one distributed tracing platform (Jaeger) with self-provisioned Elasticsearch instance per namespace. The Elasticsearch cluster is meant to be dedicated for a single distributed tracing platform (Jaeger) instance.
- There can be only one Elasticsearch per namespace.
NOTE

If you already have installed Elasticsearch as part of OpenShift Logging, the Red Hat OpenShift distributed tracing platform (Jaeger) Operator can use the installed OpenShift Elasticsearch Operator to provision storage.

The following configuration parameters are for a `self-provisioned` Elasticsearch instance, that is an instance created by the Red Hat OpenShift distributed tracing platform (Jaeger) Operator using the OpenShift Elasticsearch Operator. You specify configuration options for self-provisioned Elasticsearch under `spec:storage:elasticsearch` in your configuration file.

Table 3.7. Elasticsearch resource configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>elasticsearch:</td>
<td>Use to specify whether or not an Elasticsearch instance should be provisioned by the Red Hat OpenShift distributed tracing platform (Jaeger) Operator.</td>
<td><code>true/false</code></td>
<td><code>true</code></td>
</tr>
<tr>
<td>properties:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>doNotProvision:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>name:</td>
<td>Name of the Elasticsearch instance. The Red Hat OpenShift distributed tracing platform (Jaeger) Operator uses the Elasticsearch instance specified in this parameter to connect to Elasticsearch.</td>
<td>string</td>
<td><code>elasticsearch</code></td>
</tr>
<tr>
<td>nodeCount:</td>
<td>Number of Elasticsearch nodes. For high availability use at least 3 nodes. Do not use 2 nodes as “split brain” problem can happen.</td>
<td>Integer value. For example, Proof of concept = 1, Minimum deployment =3</td>
<td>3</td>
</tr>
<tr>
<td>resources:</td>
<td>Number of central processing units for requests, based on your environment's configuration.</td>
<td>Specified in cores or millicores, for example, 200m, 0.5, 1. For example, Proof of concept = 500m, Minimum deployment =1</td>
<td>1</td>
</tr>
<tr>
<td>requests: cpu:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Default value</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>elasticsearch:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>resources:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>requests:</td>
<td>Available memory for requests, based on your environment’s configuration.</td>
<td>Specified in bytes, for example, 200Ki, 50Mi, 5Gi. For example, Proof of concept = 1Gi, Minimum deployment = 16Gi*</td>
<td>16Gi</td>
</tr>
<tr>
<td>memory:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>limits:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cpu:</td>
<td>Limit on number of central processing units, based on your environment’s configuration.</td>
<td>Specified in cores or millicores, for example, 200m, 0.5, 1. For example, Proof of concept = 500m, Minimum deployment = 1</td>
<td></td>
</tr>
<tr>
<td>memory:</td>
<td>Available memory limit based on your environment’s configuration.</td>
<td>Specified in bytes, for example, 200Ki, 50Mi, 5Gi. For example, Proof of concept = 1Gi, Minimum deployment = 16Gi*</td>
<td></td>
</tr>
<tr>
<td>redundancyPolicy:</td>
<td>Data replication policy defines how Elasticsearch shards are replicated across data nodes in the cluster. If not specified, the Red Hat OpenShift distributed tracing platform (Jaeger) Operator automatically determines the most appropriate replication based on number of nodes.</td>
<td>ZeroRedundancy (no replica shards), SingleRedundancy (one replica shard), MultipleRedundancy (each index is spread over half of the Data nodes), FullRedundancy (each index is fully replicated on every Data node in the cluster).</td>
<td></td>
</tr>
</tbody>
</table>
elasticsearch:
useCertManagement:

Use to specify whether or not distributed tracing platform (Jaeger) should use the certificate management feature of the Red Hat Elasticsearch Operator. This feature was added to logging subsystem for Red Hat OpenShift 5.2 in OpenShift Container Platform 4.7 and is the preferred setting for new Jaeger deployments.

default value: true

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use to specify whether or not distributed tracing platform (Jaeger) should use the certificate management feature of the Red Hat Elasticsearch Operator. This feature was added to logging subsystem for Red Hat OpenShift 5.2 in OpenShift Container Platform 4.7 and is the preferred setting for new Jaeger deployments.</td>
<td>true/false</td>
<td>true</td>
</tr>
</tbody>
</table>

Each Elasticsearch node can operate with a lower memory setting though this is NOT recommended for production deployments. For production use, you must have no less than 16 Gi allocated to each pod by default, but preferably allocate as much as you can, up to 64 Gi per pod.

Production storage example:

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: simple-prod
spec:
  strategy: production
  storage:
    type: elasticsearch
    elasticsearch:
      nodeCount: 3
      resources:
        requests:
          cpu: 1
          memory: 16Gi
        limits:
          memory: 16Gi
```

Storage example with persistent storage:

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: simple-prod
spec:
  strategy: production
  storage:
    type: elasticsearch
    elasticsearch:
      nodeCount: 1
```
Persistent storage configuration. In this case AWS gp2 with 5Gi size. When no value is specified, distributed tracing platform (Jaeger) uses emptyDir. The OpenShift Elasticsearch Operator provisions PersistentVolumeClaim and PersistentVolume which are not removed with distributed tracing platform (Jaeger) instance. You can mount the same volumes if you create a distributed tracing platform (Jaeger) instance with the same name and namespace.

3.2.6.5.2. Connecting to an existing Elasticsearch instance

You can use an existing Elasticsearch cluster for storage with distributed tracing platform. An existing Elasticsearch cluster, also known as an external Elasticsearch instance, is an instance that was not installed by the Red Hat OpenShift distributed tracing platform (Jaeger) Operator or by the Red Hat Elasticsearch Operator.

When you deploy a Jaeger custom resource, the Red Hat OpenShift distributed tracing platform (Jaeger) Operator will not provision Elasticsearch if the following configurations are set:

- `spec.storage.elasticsearch.doNotProvision` set to `true`
- `spec.storage.options.es.server-urls` has a value
- `spec.storage.elasticsearch.name` has a value, or if the Elasticsearch instance name is `elasticsearch`.

The Red Hat OpenShift distributed tracing platform (Jaeger) Operator uses the Elasticsearch instance specified in `spec.storage.elasticsearch.name` to connect to Elasticsearch.

Restrictions

- You cannot share or reuse a OpenShift Container Platform logging Elasticsearch instance with distributed tracing platform (Jaeger). The Elasticsearch cluster is meant to be dedicated for a single distributed tracing platform (Jaeger) instance.

**NOTE**

Red Hat does not provide support for your external Elasticsearch instance. You can review the tested integrations matrix on the Customer Portal.

The following configuration parameters are for an already existing Elasticsearch instance, also known as an external Elasticsearch instance. In this case, you specify configuration options for Elasticsearch under `spec:storage:options:es` in your custom resource file.

Table 3.8. General ES configuration parameters
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>es:max-doc-count:</td>
<td>The maximum document count to return from an Elasticsearch query. This will also apply to aggregations. If you set both es:max-doc-count and es:max-num-spans, Elasticsearch will use the smaller value of the two.</td>
<td></td>
<td>10000</td>
</tr>
<tr>
<td>es:max-num-spans:</td>
<td>[Deprecated - Will be removed in a future release, use es:max-doc-count instead.] The maximum number of spans to fetch at a time, per query, in Elasticsearch. If you set both es:max-num-spans and es:max-doc-count, Elasticsearch will use the smaller value of the two.</td>
<td></td>
<td>10000</td>
</tr>
<tr>
<td>es:max-span-age:</td>
<td>The maximum lookback for spans in Elasticsearch.</td>
<td></td>
<td>72h0m0s</td>
</tr>
<tr>
<td>es:sniffer:</td>
<td>The sniffer configuration for Elasticsearch. The client uses the sniffing process to find all nodes automatically. Disabled by default.</td>
<td>true/false</td>
<td>false</td>
</tr>
<tr>
<td>es:sniffer-tls-enabled:</td>
<td>Option to enable TLS when sniffing an Elasticsearch Cluster. The client uses the sniffing process to find all nodes automatically. Disabled by default</td>
<td>true/false</td>
<td>false</td>
</tr>
</tbody>
</table>
### Table 3.9. ES data replication parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>es: timeout:</td>
<td>Timeout used for queries. When set to zero there is no timeout.</td>
<td></td>
<td>0s</td>
</tr>
<tr>
<td>es: username:</td>
<td>The username required by Elasticsearch. The basic authentication also loads CA if it is specified. See also es.password.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es: password:</td>
<td>The password required by Elasticsearch. See also, es.username.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es: version:</td>
<td>The major Elasticsearch version. If not specified, the value will be auto-detected from Elasticsearch.</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

### Table 3.10. ES index configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>es: num-replicas:</td>
<td>The number of replicas per index in Elasticsearch.</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>es: num-shards:</td>
<td>The number of shards per index in Elasticsearch.</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

| es: create-index-templates:   | Automatically create index templates at application startup when set to true. When templates are installed manually, set to false. | true/false | true          |
### Table 3.11. ES bulk processor configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>es:</strong>&lt;br&gt;index-prefix:</td>
<td>Optional prefix for distributed tracing platform (Jaeger) indices. For example, setting this to &quot;production&quot; creates indices named &quot;production-tracing-*&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es: bulk: actions:</td>
<td>The number of requests that can be added to the queue before the bulk processor decides to commit updates to disk.</td>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>es: bulk: flush-interval:</td>
<td>A <code>time.Duration</code> after which bulk requests are committed, regardless of other thresholds. To disable the bulk processor flush interval, set this to zero.</td>
<td></td>
<td>200ms</td>
</tr>
<tr>
<td>es: bulk: size:</td>
<td>The number of bytes that the bulk requests can take up before the bulk processor decides to commit updates to disk.</td>
<td></td>
<td>5000000</td>
</tr>
<tr>
<td>es: bulk: workers:</td>
<td>The number of workers that are able to receive and commit bulk requests to Elasticsearch.</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

### Table 3.12. ES TLS configuration parameters

81

---

OpenShift Container Platform 4.11 Distributed tracing

66
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>es: tls: ca:</td>
<td>Path to a TLS Certification Authority (CA) file used to verify the remote servers.</td>
<td></td>
<td>Will use the system truststore by default.</td>
</tr>
<tr>
<td>es: tls: cert:</td>
<td>Path to a TLS Certificate file, used to identify this process to the remote servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es: tls: enabled:</td>
<td>Enable transport layer security (TLS) when talking to the remote servers. Disabled by default.</td>
<td>true/ false</td>
<td>false</td>
</tr>
<tr>
<td>es: tls: key:</td>
<td>Path to a TLS Private Key file, used to identify this process to the remote servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es: tls: server-name:</td>
<td>Override the expected TLS server name in the certificate of the remote servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es: token-file:</td>
<td>Path to a file containing the bearer token. This flag also loads the Certification Authority (CA) file if it is specified.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3.13. ES archive configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>es-archive: bulk: actions:</td>
<td>The number of requests that can be added to the queue before the bulk processor decides to commit updates to disk.</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Default value</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------</td>
</tr>
<tr>
<td>es-archive: bulk: flush-interval:</td>
<td>A <code>time.Duration</code> after which bulk requests are committed, regardless of other thresholds. To disable the bulk processor flush interval, set this to zero.</td>
<td></td>
<td>0s</td>
</tr>
<tr>
<td>es-archive: bulk: size:</td>
<td>The number of bytes that the bulk requests can take up before the bulk processor decides to commit updates to disk.</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>es-archive: bulk: workers:</td>
<td>The number of workers that are able to receive and commit bulk requests to Elasticsearch.</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>es-archive: create-index-templates:</td>
<td>Automatically create index templates at application startup when set to <code>true</code>. When templates are installed manually, set to <code>false</code>.</td>
<td><code>true/ false</code></td>
<td><code>false</code></td>
</tr>
<tr>
<td>es-archive: enabled:</td>
<td>Enable extra storage.</td>
<td><code>true/ false</code></td>
<td><code>false</code></td>
</tr>
<tr>
<td>es-archive: index-prefix:</td>
<td>Optional prefix for distributed tracing platform (Jaeger) indices. For example, setting this to &quot;production&quot; creates indices named &quot;production-tracing-*&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es-archive: max-doc-count:</td>
<td>The maximum document count to return from an Elasticsearch query. This will also apply to aggregations.</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Default value</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>---------------</td>
</tr>
<tr>
<td>es-archive: max-num-spans:</td>
<td>[Deprecated - Will be removed in a future release, use es-archive:max-doc-count instead.] The maximum number of spans to fetch at a time, per query, in Elasticsearch.</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>es-archive: max-span-age:</td>
<td>The maximum lookback for spans in Elasticsearch.</td>
<td></td>
<td>0s</td>
</tr>
<tr>
<td>es-archive: num-replicas:</td>
<td>The number of replicas per index in Elasticsearch.</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>es-archive: num-shards:</td>
<td>The number of shards per index in Elasticsearch.</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>es-archive: password:</td>
<td>The password required by Elasticsearch. See also, es.username.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es-archive: server-urls:</td>
<td>The comma-separated list of Elasticsearch servers. Must be specified as fully qualified URLs, for example, <a href="http://localhost:9200">http://localhost:9200</a>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es-archive: sniffer:</td>
<td>The sniffer configuration for Elasticsearch. The client uses the sniffing process to find all nodes automatically. Disabled by default.</td>
<td>true/false</td>
<td>false</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Default value</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>es-archive: sniffer-tls-enabled:</td>
<td>Option to enable TLS when sniffing an Elasticsearch Cluster. The client uses the sniffing process to find all nodes automatically. Disabled by default.</td>
<td>true/false</td>
<td>false</td>
</tr>
<tr>
<td>es-archive: timeout:</td>
<td>Timeout used for queries. When set to zero there is no timeout.</td>
<td></td>
<td>0s</td>
</tr>
<tr>
<td>es-archive: tls: ca:</td>
<td>Path to a TLS Certification Authority (CA) file used to verify the remote servers.</td>
<td></td>
<td>Will use the system truststore by default.</td>
</tr>
<tr>
<td>es-archive: tls: cert:</td>
<td>Path to a TLS Certificate file, used to identify this process to the remote servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es-archive: tls: enabled:</td>
<td>Enable transport layer security (TLS) when talking to the remote servers. Disabled by default.</td>
<td>true/false</td>
<td>false</td>
</tr>
<tr>
<td>es-archive: tls: key:</td>
<td>Path to a TLS Private Key file, used to identify this process to the remote servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es-archive: tls: server-name:</td>
<td>Override the expected TLS server name in the certificate of the remote servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es-archive: token-file:</td>
<td>Path to a file containing the bearer token. This flag also loads the Certification Authority (CA) file if it is specified.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>es-archive.username</td>
<td>The username required by Elasticsearch. The basic authentication also loads CA if it is specified. See also es-archive.password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>es-archive.version</td>
<td>The major Elasticsearch version. If not specified, the value will be auto-detected from Elasticsearch.</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

#### Storage example with volume mounts

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: simple-prod
spec:
  strategy: production
  storage:
    type: elasticsearch
    options:
      es:
        index-prefix: my-prefix
        tls:
          ca: /es/certificates/ca.crt
      secretName: tracing-secret
  volumeMounts:
  - name: certificates
    mountPath: /es/certificates/
    readOnly: true
  volumes:
  - name: certificates
    secret:
      secretName: quickstart-es-http-certs-public
```

The following example shows a Jaeger CR using an external Elasticsearch cluster with TLS CA certificate mounted from a volume and user/password stored in a secret.

#### External Elasticsearch example

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: simple-prod
spec:
  strategy: production
  storage:
```
URL to Elasticsearch service running in default namespace.

TLS configuration. In this case only CA certificate, but it can also contain es.tls.key and es.tls.cert when using mutual TLS.

Secret which defines environment variables ES_PASSWORD and ES_USERNAME. Created by kubectl create secret generic tracing-secret --from-literal=ES_PASSWORD=changeme --from-literal=ES_USERNAME=elastic

Volume mounts and volumes which are mounted into all storage components.

### 3.2.6.6. Managing certificates with Elasticsearch

You can create and manage certificates using the Red Hat Elasticsearch Operator. Managing certificates using the Red Hat Elasticsearch Operator also lets you use a single Elasticsearch cluster with multiple Jaeger Collectors.

**IMPORTANT**

Managing certificates with Elasticsearch 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](#).

Starting with version 2.4, the Red Hat OpenShift distributed tracing platform (Jaeger) Operator delegates certificate creation to the Red Hat Elasticsearch Operator by using the following annotations in the Elasticsearch custom resource:

- **logging.openshift.io/elasticsearch-cert-management: "true"**
- **logging.openshift.io/elasticsearch-cert.jaeger-<shared-es-node-name>: "user.jaeger"**
logging.openshift.io/elasticsearch-cert.curator-<shared-es-node-name>:
"system.logging.curator"

Where the `<shared-es-node-name>` is the name of the Elasticsearch node. For example, if you create an Elasticsearch node named `custom-es`, your custom resource might look like the following example.

Example Elasticsearch CR showing annotations

```yaml
apiVersion: logging.openshift.io/v1
kind: Elasticsearch
metadata:
  annotations:
    logging.openshift.io/elasticsearch-cert-management: "true"
    logging.openshift.io/elasticsearch-cert.jaeger-custom-es: "user.jaeger"
    logging.openshift.io/elasticsearch-cert.curator-custom-es: "system.logging.curator"
name: custom-es
spec:
  managementState: Managed
  nodeSpec:
    resources:
      limits:
        memory: 16Gi
      requests:
        cpu: 1
        memory: 16Gi
    nodes:
      - nodeCount: 3
        proxyResources: {}
        resources: {}
        roles:
          - master
          - client
          - data
        storage: {}
  redundancyPolicy: ZeroRedundancy
```

Prerequisites

- OpenShift Container Platform 4.7
- logging subsystem for Red Hat OpenShift 5.2
- The Elasticsearch node and the Jaeger instances must be deployed in the same namespace. For example, `tracing-system`.

You enable certificate management by setting `spec.storage.elasticsearch.useCertManagement` to `true` in the Jaeger custom resource.

Example showing `useCertManagement`

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: jaeger-prod
spec:
```
The Red Hat OpenShift distributed tracing platform (Jaeger) Operator sets the Elasticsearch custom resource name to the value of `spec.storage.elasticsearch.name` from the Jaeger custom resource when provisioning Elasticsearch.

The certificates are provisioned by the Red Hat Elasticsearch Operator and the Red Hat OpenShift distributed tracing platform (Jaeger) Operator injects the certificates.

### 3.2.6.7. Query configuration options

Query is a service that retrieves traces from storage and hosts the user interface to display them.

**Table 3.14. Parameters used by the Red Hat OpenShift distributed tracing platform (Jaeger) Operator to define Query**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>query:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>replicas:</td>
<td>Specifies the number of Query replicas to create.</td>
<td>Integer, for example, 2</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3.15. Configuration parameters passed to Query**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>query:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>options:</td>
<td>Configuration options that define the Query service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log-level:</td>
<td>Logging level for Query.</td>
<td>Possible values: <code>debug</code>, <code>info</code>, <code>warn</code>, <code>error</code>, <code>fatal</code>, <code>panic</code></td>
<td></td>
</tr>
</tbody>
</table>
The base path for all jaeger-query HTTP routes can be set to a non-root value, for example, `/jaeger` would cause all UI URLs to start with `/jaeger`. This can be useful when running jaeger-query behind a reverse proxy.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>options:</td>
<td>The base path for all jaeger-query HTTP routes can be set to a non-root value, for example, <code>/jaeger</code> would cause all UI URLs to start with <code>/jaeger</code>. This can be useful when running jaeger-query behind a reverse proxy.</td>
<td><code>/&lt;path&gt;</code></td>
</tr>
</tbody>
</table>

Sample Query configuration

```yaml
apiVersion: jaegertracing.io/v1
kind: "Jaeger"
metadata:
  name: "my-jaeger"
spec:
  strategy: allInOne
  allInOne:
    options:
      log-level: debug
      query:
        base-path: /jaeger
```

3.2.6.8. Ingester configuration options

Ingester is a service that reads from a Kafka topic and writes to the Elasticsearch storage backend. If you are using the `allInOne` or `production` deployment strategies, you do not need to configure the Ingester service.

Table 3.16. Jaeger parameters passed to the Ingester

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec:</td>
<td>Configuration options that define the Ingester service.</td>
<td></td>
</tr>
<tr>
<td>ingester:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>spec:</td>
<td>Specifies the interval, in seconds or minutes, that the Ingester must wait for a message before terminating. The deadlock interval is disabled by default (set to 0), to avoid terminating the Ingester when no messages arrive during system initialization.</td>
<td>Minutes and seconds, for example, <code>1m0s</code>. Default value is 0.</td>
</tr>
<tr>
<td>deadlockInterval:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The **topic** parameter identifies the Kafka configuration used by the collector to produce the messages, and the Ingester to consume the messages.

Label for the consumer. For example, **jaeger-spans**.

Identifies the Kafka configuration used by the Ingester to consume the messages.

Label for the broker, for example, **my-cluster-kafka-brokers.kafka:9092**.

Logging level for the Ingester.

Possible values: **debug, info, warn, error, fatal, dpanic, panic**.

### Streaming Collector and Ingester example

```yaml
apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: simple-streaming
spec:
  strategy: streaming
  collector:
    options:
      kafka:
        producer:
          topic: jaeger-spans
          brokers: my-cluster-kafka-brokers.kafka:9092
    ingester:
      options:
        kafka:
          consumer:
            topic: jaeger-spans
            brokers: my-cluster-kafka-brokers.kafka:9092
          ingester:
            deadlockInterval: 5
  storage:
    type: elasticsearch
    options:
      es:
        server-urls: http://elasticsearch:9200
```

### 3.2.7. Injecting sidecars

The Red Hat OpenShift distributed tracing platform (Jaeger) relies on a proxy sidecar within the application’s pod to provide the Agent. The Red Hat OpenShift distributed tracing platform (Jaeger)
Operator can inject Agent sidecars into deployment workloads. You can enable automatic sidecar injection or manage it manually.

3.2.7.1. Automatically injecting sidecars

The Red Hat OpenShift distributed tracing platform (Jaeger) Operator can inject Jaeger Agent sidecars into deployment workloads. To enable automatic injection of sidecars, add the `sidecar.jaegertracing.io/inject` annotation set to either the string `true` or to the distributed tracing platform (Jaeger) instance name that is returned by running `$ oc get jaegers`. When you specify `true`, there must be only a single distributed tracing platform (Jaeger) instance for the same namespace as the deployment. Otherwise, the Operator is unable to determine which distributed tracing platform (Jaeger) instance to use. A specific distributed tracing platform (Jaeger) instance name on a deployment has a higher precedence than `true` applied on its namespace.

The following snippet shows a simple application that will inject a sidecar, with the agent pointing to the single distributed tracing platform (Jaeger) instance available in the same namespace:

**Automatic sidecar injection example**

```yaml
apiVersion: apps/v1
class: Deployment
metadata:
  name: myapp
  annotations:
    "sidecar.jaegertracing.io/inject": "true" 1
spec:
  selector:
    matchLabels:
      app: myapp
template:
    metadata:
      labels:
        app: myapp
    spec:
      containers:
      - name: myapp
        image: acme/myapp:myversion
```

1 Set to either the string `true` or to the Jaeger instance name.

When the sidecar is injected, the agent can then be accessed at its default location on `localhost`.

3.2.7.2. Manually injecting sidecars

The Red Hat OpenShift distributed tracing platform (Jaeger) Operator can only automatically inject Jaeger Agent sidecars into Deployment workloads. For controller types other than `Deployments`, such as `StatefulSets` and `DaemonSets`, you can manually define the Jaeger agent sidecar in your specification.

The following snippet shows the manual definition you can include in your containers section for a Jaeger agent sidecar:

**Sidecar definition example for a StatefulSet**
The agent can then be accessed at its default location on localhost.

3.3. UPDATING THE DISTRIBUTED TRACING PLATFORM JAEGER

```
apiVersion: apps/v1
kind: StatefulSet
metadata:
  name: example-statefulset
  namespace: example-ns
labels:
  app: example-app
spec:

  spec:
    containers:
    - name: example-app
      image: acme/myapp:myversion
      ports:
        - containerPort: 8080
          protocol: TCP
    - name: jaeger-agent
      image: registry.redhat.io/distributed-tracing/jaeger-agent-rhel7:<version>
      # The agent version must match the Operator version
      imagePullPolicy: IfNotPresent
      ports:
        - containerPort: 5775
          name: zk-compact-trft
          protocol: UDP
        - containerPort: 5778
          name: config-rest
          protocol: TCP
        - containerPort: 6831
          name: jg-compact-trft
          protocol: UDP
        - containerPort: 6832
          name: jg-binary-trft
          protocol: UDP
        - containerPort: 14271
          name: admin-http
          protocol: TCP
      args:
        - --reporter.grpc.host-port=dns:///jaeger-collector-headless.example-ns:14250
        - --reporter.type=grpc
```

The agent can then be accessed at its default location on localhost.

WARNING

Jaeger is deprecated in Red Hat OpenShift distributed tracing 3.0.
Operator Lifecycle Manager (OLM) controls the installation, upgrade, and role-based access control (RBAC) of Operators in a cluster. The OLM runs by default in OpenShift Container Platform. OLM queries for available Operators as well as upgrades for installed Operators.

During an update, the Red Hat OpenShift distributed tracing platform Operators upgrade the managed distributed tracing platform instances to the version associated with the Operator. Whenever a new version of the Red Hat OpenShift distributed tracing platform (Jaeger) Operator is installed, all the distributed tracing platform (Jaeger) application instances managed by the Operator are upgraded to the Operator’s version. For example, after upgrading the Operator from 1.10 installed to 1.11, the Operator scans for running distributed tracing platform (Jaeger) instances and upgrades them to 1.11 as well.

**IMPORTANT**

If you have not already updated your OpenShift Elasticsearch Operator as described in *Updating OpenShift Logging*, complete that update before updating your Red Hat OpenShift distributed tracing platform (Jaeger) Operator.

### 3.3.1. Additional resources

- Operator Lifecycle Manager concepts and resources
- Updating installed Operators
- Updating OpenShift Logging

### 3.4. REMOVING THE DISTRIBUTED TRACING PLATFORM JAEGER

The steps for removing Red Hat OpenShift distributed tracing platform from an OpenShift Container Platform cluster are as follows:

1. Shut down any Red Hat OpenShift distributed tracing platform pods.
2. Remove any Red Hat OpenShift distributed tracing platform instances.
4. Remove the Red Hat build of OpenTelemetry Operator.

#### 3.4.1. Removing a distributed tracing platform (Jaeger) instance by using the web console

You can remove a distributed tracing platform (Jaeger) instance in the Administrator view of the web console.

**WARNING**

When deleting an instance that uses in-memory storage, all data is irretrievably lost. Data stored in persistent storage such as Elasticsearch is not deleted when a Red Hat OpenShift distributed tracing platform (Jaeger) instance is removed.
Prerequisites

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

Procedure

1. Log in to the OpenShift Container Platform web console.
2. Navigate to Operators → Installed Operators.
3. Select the name of the project where the Operators are installed from the Project menu, for example, `openshift-operators`.
4. Click the Red Hat OpenShift distributed tracing platform (Jaeger) Operator.
5. Click the Jaeger tab.
6. Click the Options menu next to the instance you want to delete and select Delete Jaeger.
7. In the confirmation message, click Delete.

3.4.2. Removing a distributed tracing platform (Jaeger) instance by using the CLI

You can remove a distributed tracing platform (Jaeger) 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>
  $ oc login --username=<NAMEOFUSER>
  ```

Procedure

1. Log in with the OpenShift CLI (`oc`) by running the following command:

   ```
   $ oc login --username=<NAMEOFUSER>
   ```

2. To display the distributed tracing platform (Jaeger) instances, run the following command:

   ```
   $ oc get deployments -n <jaeger-project>
   ```

   For example,

   ```
   $ oc get deployments -n openshift-operators
   ```
The names of Operators have the suffix `-operator`. The following example shows two Red Hat OpenShift distributed tracing platform (Jaeger) Operators and four distributed tracing platform (Jaeger) instances:

```bash
$ oc get deployments -n openshift-operators
```

You will see output similar to the following:

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>UP-TO-DATE</th>
<th>AVAILABLE</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>elasticsearch-operator</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>93m</td>
</tr>
<tr>
<td>jaeger-operator</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>49m</td>
</tr>
<tr>
<td>jaeger-test</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>7m23s</td>
</tr>
<tr>
<td>jaeger-test2</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>6m48s</td>
</tr>
<tr>
<td>tracing1</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>7m8s</td>
</tr>
<tr>
<td>tracing2</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>35m</td>
</tr>
</tbody>
</table>

3. To remove an instance of distributed tracing platform (Jaeger), run the following command:

```bash
$ oc delete jaeger <deployment-name> -n <jaeger-project>
```

For example:

```bash
$ oc delete jaeger tracing2 -n openshift-operators
```

4. To verify the deletion, run the `oc get deployments` command again:

```bash
$ oc get deployments -n <jaeger-project>
```

For example:

```bash
$ oc get deployments -n openshift-operators
```

You will see generated output that is similar to the following example:

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>UP-TO-DATE</th>
<th>AVAILABLE</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>elasticsearch-operator</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>94m</td>
</tr>
<tr>
<td>jaeger-operator</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>50m</td>
</tr>
<tr>
<td>jaeger-test</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>8m14s</td>
</tr>
<tr>
<td>jaeger-test2</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>7m39s</td>
</tr>
<tr>
<td>tracing1</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>7m59s</td>
</tr>
</tbody>
</table>

### 3.4.3. Removing the Red Hat OpenShift distributed tracing platform Operators

**Procedure**

1. Follow the instructions in [Deleting Operators from a cluster](#) to remove the Red Hat OpenShift distributed tracing platform (Jaeger) Operator.

2. Optional: After the Red Hat OpenShift distributed tracing platform (Jaeger) Operator has been removed, remove the OpenShift Elasticsearch Operator.
CHAPTER 4. DISTRIBUTED TRACING PLATFORM (TEMPO)

4.1. INSTALLING THE DISTRIBUTED TRACING PLATFORM (TEMPO)

Installing the distributed tracing platform (Tempo) involves the following steps:

1. Setting up supported object storage.
2. Installing the Tempo Operator.
3. Creating a secret for the object storage credentials.
4. Creating a namespace for a TempoStack instance.
5. Creating a TempoStack custom resource to deploy at least one TempoStack instance.

4.1.1. Installing the distributed tracing platform (Tempo) from the web console

You can install the distributed tracing platform (Tempo) from the web console.

Prerequisites

- You are logged in to the OpenShift Container Platform 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.
- You are using a supported provider of object storage: Red Hat OpenShift Data Foundation, MinIO, Amazon S3, Azure Blob Storage, Google Cloud Storage.

Procedure

1. Install the Tempo Operator:
   a. Go to Operators → OperatorHub and search for Tempo Operator.
   b. Select the Tempo Operator that is OpenShift Operator for Tempo → 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-tempo-operator
   - Update approval → Automatic
c. In the **Details** tab of the page of the installed Operator, under **ClusterServiceVersion details**, verify that the installation **Status** is **Succeeded**.

2. Create a project of your choice for the **TempoStack** instance that you will create in a subsequent step: go to **Home → Projects → Create Project**.

3. In the project that you created for the **TempoStack** instance, create a secret for your object storage bucket: go to **Workloads → Secrets → Create → From YAML**.

**Table 4.1. Required secret parameters**

<table>
<thead>
<tr>
<th>Storage provider</th>
<th>Secret parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Red Hat OpenShift Data Foundation</strong></td>
<td><strong>name</strong>: tempostack-dev-odf # example</td>
</tr>
<tr>
<td></td>
<td><strong>bucket</strong>: &lt;bucket_name&gt; # requires an ObjectBucketClaim</td>
</tr>
<tr>
<td></td>
<td><strong>endpoint</strong>: <a href="https://s3.openshift-storage.svc">https://s3.openshift-storage.svc</a></td>
</tr>
<tr>
<td></td>
<td><strong>access_key_id</strong>: &lt;data_foundation_access_key_id&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>access_key_secret</strong>: &lt;data_foundation_access_key_secret&gt;</td>
</tr>
<tr>
<td><strong>MinIO</strong></td>
<td><strong>name</strong>: tempostack-dev-minio # example</td>
</tr>
<tr>
<td></td>
<td><strong>bucket</strong>: &lt;minio_bucket_name&gt; # MinIO documentation</td>
</tr>
<tr>
<td></td>
<td><strong>endpoint</strong>: &lt;minio_bucket_endpoint&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>access_key_id</strong>: &lt;minio_access_key_id&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>access_key_secret</strong>: &lt;minio_access_key_secret&gt;</td>
</tr>
<tr>
<td><strong>Amazon S3</strong></td>
<td><strong>name</strong>: tempostack-dev-s3 # example</td>
</tr>
<tr>
<td></td>
<td><strong>bucket</strong>: &lt;s3_bucket_name&gt; # Amazon S3 documentation</td>
</tr>
<tr>
<td></td>
<td><strong>endpoint</strong>: &lt;s3_bucket_endpoint&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>access_key_id</strong>: &lt;s3_access_key_id&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>access_key_secret</strong>: &lt;s3_access_key_secret&gt;</td>
</tr>
<tr>
<td><strong>Microsoft Azure Blob Storage</strong></td>
<td></td>
</tr>
<tr>
<td>Storage provider</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>name: tempostack-dev-azure # example</td>
<td></td>
</tr>
<tr>
<td>container: &lt;azure_blob_storage_container_name&gt; # Microsoft Azure documentation</td>
<td></td>
</tr>
<tr>
<td>account_name: &lt;azure_blob_storage_account_name&gt;</td>
<td></td>
</tr>
<tr>
<td>account_key: &lt;azure_blob_storage_account_key&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Google Cloud Storage on Google Cloud Platform (GCP)

| name: tempostack-dev-gcs # example |
| bucketname: <google_cloud_storage_bucket_name> # requires a bucket created in a GCP project |
| key.json: <path/to/key.json> # requires a service account in the bucket’s GCP project for GCP authentication |

Example secret for Amazon S3 and MinIO storage

```yaml
apiVersion: v1
class: Secret
metadata:
  name: minio-test
stringData:
  endpoint: http://minio.minio.svc:9000
  bucket: tempo
  access_key_id: tempo
  access_key_secret: <secret>
type: Opaque
```

4. Create a TempoStack instance.

**NOTE**

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

a. Go to Operators → Installed Operators.

b. Select TempoStack → Create TempoStack → YAML view.

c. In the YAML view, customize the TempoStack custom resource (CR):

```yaml
apiVersion: tempo.grafana.com/v1alpha1
class: TempoStack
metadata:
  name: sample
  namespace: <project_of_tempostack_instance>
spec:
```
The value of the **name** in the **metadata** of the secret.

1. The accepted values are **azure** for Azure Blob Storage; **gcs** for Google Cloud Storage; and **s3** for Amazon S3, MinIO, or Red Hat OpenShift Data Foundation.

**Example of a TempoStack CR for AWS S3 and MinIO storage**

```yaml
apiVersion: tempo.grafana.com/v1alpha1
kind: TempoStack
metadata:
  name: simplest
  namespace: <project_of_tempostack_instance>
spec:
  storageSize: 1Gi
  storage:
    secret:
      name: minio-test
      type: s3
  resources:
    total:
      limits:
        memory: 2Gi
        cpu: 2000m
  template:
    queryFrontend:
      jaegerQuery:
        enabled: true
        ingress:
          route:
            termination: edge
            type: route
```

The stack deployed in this example is configured to receive Jaeger Thrift over HTTP and OpenTelemetry Protocol (OTLP), which permits visualizing the data with the Jaeger UI.

d. Select **Create**.

**Verification**

1. Use the **Project:** dropdown list to select the project of the **TempoStack** instance.
2. Go to **Operators → Installed Operators** to verify that the **Status** of the **TempoStack** instance is **Condition: Ready**.

3. Go to **Workloads → Pods** to verify that all the component pods of the **TempoStack** instance are running.

4. Access the Tempo console:
   a. Go to **Networking → Routes** and **Ctrl+F** to search for **tempo**.
   b. In the **Location** column, open the URL to access the Tempo console.
   c. Select **Log In With OpenShift** to use your cluster administrator credentials for the web console.

   **NOTE**
   The Tempo console initially shows no trace data following the Tempo console installation.

4.1.2. Installing the distributed tracing platform (Tempo) by using the CLI

You can install the distributed tracing platform (Tempo) 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**:

  ```bash
  $ oc login --username=<your_username>
  ```

- You are using a supported provider of object storage: **Red Hat OpenShift Data Foundation**, **MinIO**, **Amazon S3**, **Azure Blob Storage**, **Google Cloud Storage**.

**Procedure**

1. Install the Tempo Operator:
   a. Create a project for the Tempo Operator by running the following command:

   ```bash
   $ oc apply -f - << EOF
   apiVersion: project.openshift.io/v1
   kind: Project
   metadata:
     labels:
       kubernetes.io/metadata.name: openshift-tempo-operator
   EOF
   ```
b. Create an Operator group by running the following command:

```bash
$ oc apply -f - << EOF
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: openshift-tempo-operator
namespace: openshift-tempo-operator
spec:
  upgradeStrategy: Default
EOF
```

c. Create a subscription by running the following command:

```bash
$ oc apply -f - << EOF
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: tempo-product
namespace: openshift-tempo-operator
spec:
  channel: stable
  installPlanApproval: Automatic
  name: tempo-product
  source: redhat-operators
  sourceNamespace: openshift-marketplace
EOF
```

d. Check the operator status by running the following command:

```bash
$ oc get csv -n openshift-tempo-operator
```

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

   - To create a project from standard input without metadata:

     ```bash
     $ oc new-project <project_of_tempostack_instance>
     ```

   - To create a project from standard input with metadata:

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

3. In the project that you created for the TempoStack instance, create a secret for your object storage bucket by running one of the following commands:
To create a secret from a YAML file:

```
$ oc apply -f <secret_file>.yaml
```

To create a secret from standard input:

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

### Table 4.2. Required secret parameters

<table>
<thead>
<tr>
<th>Storage provider</th>
<th>Secret parameters</th>
</tr>
</thead>
</table>
| **Red Hat OpenShift Data Foundation** | **name**: tempostack-dev-odf # example  
bucket: <bucket_name> # requires an ObjectBucketClaim  
endpoint: https://s3.openshift-storage.svc  
access_key_id: <data_foundation_access_key_id>  
access_key_secret: <data_foundation_access_key_secret> |
| **MinIO**                         | **name**: tempostack-dev-minio # example  
bucket: <minio_bucket_name> # MinIO documentation  
endpoint: <minio_bucket_endpoint>  
access_key_id: <minio_access_key_id>  
access_key_secret: <minio_access_key_secret> |
| **Amazon S3**                     | **name**: tempostack-dev-s3 # example  
bucket: <s3_bucket_name> # Amazon S3 documentation  
endpoint: <s3_bucket_endpoint>  
access_key_id: <s3_access_key_id>  
access_key_secret: <s3_access_key_secret> |
### Storage provider

**Microsoft Azure Blob Storage**

name: `tempostack-dev-azure` # example

container: `<azure_blob_storage_container_name>` # Microsoft Azure documentation

account_name: `<azure_blob_storage_account_name>`

account_key: `<azure_blob_storage_account_key>`

**Google Cloud Storage on Google Cloud Platform (GCP)**

name: `tempostack-dev-gcs` # example

bucketname: `<google_cloud_storage_bucket_name>` # requires a bucket created in a GCP project

key.json: `<path/to/key.json>` # requires a service account in the bucket’s GCP project for GCP authentication

### Example secret for Amazon S3 and MinIO storage

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: minio-test
stringData:
  endpoint: http://minio.minio.svc:9000
  bucket: tempo
  access_key_id: tempo
  access_key_secret: <secret>
  type: Opaque
```

4. Create a TempoStack instance in the project that you created for the TempoStack instance.

**NOTE**

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

a. Customize the **TempoStack** custom resource (CR):

```yaml
apiVersion: tempo.grafana.com/v1alpha1
kind: TempoStack
metadata:
  name: sample
  namespace: `<project_of_tempostack_instance>`
spec:
```
The value of the `name` in the `metadata` of the secret.

The accepted values are `azure` for Azure Blob Storage; `gcs` for Google Cloud Storage; and `s3` for Amazon S3, MinIO, or Red Hat OpenShift Data Foundation.

**TempoStack CR for AWS S3 and MinIO storage**

```
apiVersion: tempo.grafana.com/v1alpha1
kind: TempoStack
metadata:
  name: simplest
  namespace: project_of_tempstack_instance
spec:
  storageSize: 1Gi
  storage:
    secret:
      name: minio-test
      type: s3
  resources:
    total:
      limits:
        memory: 2Gi
        cpu: 2000m
  template:
    queryFrontend:
      jaegerQuery:
        enabled: true
        ingress:
          route:
            termination: edge
            type: route
```

The stack deployed in this example is configured to receive Jaeger Thrift over HTTP and OpenTelemetry Protocol (OTLP), which permits visualizing the data with the Jaeger UI.

b. Apply the customized CR by running the following command.

```
$ oc apply -f - << EOF
<TempoStack_custom_resource>
EOF
```
Verification

1. Verify that the status of all TempoStack components is Running and the conditions are type: Ready by running the following command:

   ```
   $ oc get tempostacks.tempo.grafana.com simplest -o yaml
   ```

2. Verify that all the TempoStack component pods are running by running the following command:

   ```
   $ oc get pods
   ```

3. Access the Tempo console:

   a. Query the route details by running the following command:

   ```
   $ export TEMPO_URL=$(oc get route -n <control_plane_namespace> tempo -o jsonpath='{.spec.host}')
   ```

   b. Open https://<route_from_previous_step> in a web browser.

   c. Log in using your cluster administrator credentials for the web console.

   **NOTE**

   The Tempo console initially shows no trace data following the Tempo console installation.

4.1.3. 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

4.2. CONFIGURING AND DEPLOYING THE DISTRIBUTED TRACING PLATFORM (TEMPO)

The Tempo Operator uses a custom resource definition (CRD) file that defines the architecture and configuration settings to be used when creating and deploying the distributed tracing platform (Tempo) resources. You can install the default configuration or modify the file.

4.2.1. Customizing your deployment

For information about configuring the back-end storage, see Understanding persistent storage and the appropriate configuration topic for your chosen storage option.
4.2.1.1. Distributed tracing default configuration options

The Tempo custom resource (CR) defines the architecture and settings to be used when creating the distributed tracing platform (Tempo) resources. You can modify these parameters to customize your distributed tracing platform (Tempo) implementation to your business needs.

Example of a generic Tempo YAML file

```yaml
cr: TempoStack
    metadata:
        name: tempo-all-in-one
    spec:
        storage: {}
        resources: {}
        storageSize: 200M
        replicationFactor: 1
        retention: {}
        template:
            distributor: {}
            ingester: {}
            compactor: {}
            querier: {}
            queryFrontend: {}
            gateway: {}
```

Table 4.3. Tempo parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>apiVersion</td>
<td>API version to use when creating the object.</td>
<td>tempotrace.io/v1</td>
<td>tempotrace.io/v1</td>
</tr>
<tr>
<td>kind:</td>
<td>Defines the kind of Kubernetes object to create.</td>
<td>tempo</td>
<td></td>
</tr>
<tr>
<td>metadata:</td>
<td>Data that uniquely identifies the object, including a name string, UID, and optional namespace.</td>
<td>OpenShift Container Platform automatically generates the UID and completes the namespace with the name of the project where the object is created.</td>
<td></td>
</tr>
<tr>
<td>name:</td>
<td>Name for the object.</td>
<td>Name of your TempoStack instance.</td>
<td>tempo-all-in-one-inmemory</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Default value</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>spec:</td>
<td>Specification for the object to be created.</td>
<td>Contains all of the configuration parameters for your TempoStack instance. When a common definition for all Tempo components is required, it is defined under the <code>spec</code> node. When the definition relates to an individual component, it is placed under the <code>spec/template/&lt;component&gt;</code> node.</td>
<td>N/A</td>
</tr>
<tr>
<td>resources:</td>
<td>Resources assigned to the TempoStack.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>storageSize:</td>
<td>Storage size for ingester PVCs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>replicationFactor:</td>
<td>Configuration for the replication factor.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>retention:</td>
<td>Configuration options for retention of traces.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>storage:</td>
<td>Configuration options that define the storage. All storage-related options must be placed under <code>storage</code> and not under the <code>allInOne</code> or other component options.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>template.distributor:</td>
<td>Configuration options for the Tempo distributor.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>template.ingester:</td>
<td>Configuration options for the Tempo ingester.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>template.compactor:</td>
<td>Configuration options for the Tempo compactor.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Minimum required configuration

The following is the required minimum for creating a distributed tracing platform (Tempo) deployment with the default settings:

```yaml
apiVersion: tempo.grafana.com/v1alpha1
kind: TempoStack
metadata:
  name: simplest
spec:
  storage: 1
    secret:
      name: minio
      type: s3
  resources:
    total:
      limits:
        memory: 2Gi
        cpu: 2000m
  template:
    queryFrontend:
      jaegerQuery:
        enabled: true
      ingress:
        type: route
```

This section specifies the deployed object storage back end, which requires a created secret with credentials for access to the object storage.

### 4.2.1.2. The distributed tracing platform (Tempo) storage configuration

You can configure object storage for the distributed tracing platform (Tempo) in the **TempoStack** custom resource under **spec.storage**. You can choose from among several storage providers that are supported.

**Table 4.4. General storage parameters used by the Tempo Operator to define distributed tracing storage**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec:</td>
<td>Type of storage to use for the deployment.</td>
<td>memory</td>
<td>memory</td>
</tr>
<tr>
<td>storage:</td>
<td>Name of the secret that contains the credentials for the set object storage type.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>secret</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>type:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| storage:  | CA is the name of a ConfigMap object containing a CA certificate. |        | |
| secretname: | | N/A | |
| tls: | | | |
| caName: | | | |

Table 4.5. Required secret parameters

**Storage provider**

<table>
<thead>
<tr>
<th>Secret parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Red Hat OpenShift Data Foundation</strong></td>
</tr>
<tr>
<td>name: tempostack-dev-odf # example</td>
</tr>
<tr>
<td>bucket: &lt;bucket_name&gt; # requires an ObjectBucketClaim</td>
</tr>
<tr>
<td>endpoint: <a href="https://s3.openshift-storage.svc">https://s3.openshift-storage.svc</a></td>
</tr>
<tr>
<td>access_key_id: &lt;data_foundation_access_key_id&gt;</td>
</tr>
<tr>
<td>access_key_secret: &lt;data_foundation_access_key_secret&gt;</td>
</tr>
</tbody>
</table>

**MinIO**
### Storage provider

See MinIO Operator.

**name**: tempostack-dev-minio # example

**bucket**: `<minio_bucket_name>` # MinIO documentation

**endpoint**: `<minio_bucket_endpoint>`

**access_key_id**: `<minio_access_key_id>`

**access_key_secret**: `<minio_access_key_secret>`

Amazon S3

**name**: tempostack-dev-s3 # example

**bucket**: `<s3_bucket_name>` # Amazon S3 documentation

**endpoint**: `<s3_bucket_endpoint>`

**access_key_id**: `<s3_access_key_id>`

**access_key_secret**: `<s3_access_key_secret>`

Microsoft Azure Blob Storage

**name**: tempostack-dev-azure # example

**container**: `<azure_blob_storage_container_name>` # Microsoft Azure documentation

**account_name**: `<azure_blob_storage_account_name>`

**account_key**: `<azure_blob_storage_account_key>`

Google Cloud Storage on Google Cloud Platform (GCP)

**name**: tempostack-dev-gcs # example

**bucketname**: `<google_cloud_storage_bucket_name>` # requires a `bucket` created in a GCP project

**key.json**: `<path/to/key.json>` # requires a `service account` in the bucket’s GCP project for GCP authentication

### 4.2.1.3. Query configuration options

Query is a service that retrieves traces from storage and hosts the user interface to display them.

Table 4.6. Parameters used by the Tempo Operator to define Query
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>query:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>replicas:</td>
<td>Specifies the number of Query replicas to create.</td>
<td>Positive integer</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.7. Configuration parameters passed to Query

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>query:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>options:</td>
<td>Configuration options that define the Query service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log-level:</td>
<td>Logging level for Query.</td>
<td>debug, info, warn, error, fatal, panic</td>
<td></td>
</tr>
<tr>
<td>base-path:</td>
<td>You can set the base path for all tempo-query HTTP routes to a non-root value: for example, /tempo will cause all UI URLs to start with /tempo. This can be useful when running tempo-query behind a reverse proxy.</td>
<td>/&lt;path&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Sample Query configuration

```yaml
apiVersion: tempotracing.io/v1
class: "Tempo"
metadata:
  name: "my-tempo"
spec:
  strategy: allInOne
  allInOne:
    options:
      log-level: debug
      query:
        base-path: /tempo
```

4.2.1.4. Configuration of the monitor tab in Jaeger UI

Trace data contains rich information, and the data is normalized across instrumented languages and frameworks. Therefore, additional metrics can be extracted from traces. These metrics are request count, duration, and error count (RED). The metrics can be visualized in Jaeger console in the Monitor.
The metrics are derived from spans in the OpenTelemetry Collector that are scraped from the Collector by the Prometheus deployed in the user-workload monitoring stack. The Jaeger UI queries these metrics from the Prometheus endpoint and visualizes them.

### 4.2.1.4.1. OpenTelemetry Collector configuration

The OpenTelemetry Collector requires configuration of the spanmetrics connector that derives metrics from traces and exports the metrics in the Prometheus format.

**OpenTelemetry Collector custom resource for span RED**

```yaml
kind: OpenTelemetryCollector
apiVersion: opentelemetry.io/v1alpha1
metadata:
  name: otel
spec:
  mode: deployment
  observability:
    metrics:
      enableMetrics: true
  config: |
    connectors:
      spanmetrics:
        metrics_flush_interval: 15s
    receivers:
      otlp:
        protocols:
          grpc:
          http:
    exporters:
      prometheus:
        endpoint: 0.0.0.0:8889
  service:
    pipelines:
      traces:
        receivers: [otlp]
        exporters: [otlp, spanmetrics]
      metrics:
        receivers: [spanmetrics]
        exporters: [prometheus]
```

1. Creates the **ServiceMonitor** custom resource to enable scraping of the Prometheus exporter.
2. The Spanmetrics connector receives traces and exports metrics.
3. The OTLP receiver to receive spans in the OpenTelemetry protocol.
4. The Prometheus exporter is used to export metrics in the Prometheus format.
The Spanmetrics connector is configured as exporter in traces pipeline.

The Spanmetrics connector is configured as receiver in metrics pipeline.

4.2.1.4.2. Tempo configuration

The **TempoStack** custom resource must specify the following: the **Monitor** tab is enabled, and the Prometheus endpoint is set to the Thanos querier service to query the data from the user-defined monitoring stack.

**TempoStack custom resource with the enabled Monitor tab**

```yaml
kind: TempoStack
apiVersion: tempo.grafana.com/v1alpha1
metadata:
  name: simplest
spec:
  template:
    queryFrontend:
      jaegerQuery:
        enabled: true
      monitorTab:
        enabled: true
      prometheusEndpoint: https://thanos-querier.openshift-monitoring.svc.cluster.local:9091
    ingress:
      type: route
```

1. Enables the monitoring tab in the Jaeger console.
2. The service name for Thanos Querier from user-workload monitoring.

4.2.1.5. Multitenancy

Multitenancy with authentication and authorization is provided in the Tempo Gateway service. The authentication uses OpenShift OAuth and the Kubernetes **TokenReview** API. The authorization uses the Kubernetes **SubjectAccessReview** API.

**Sample Tempo CR with two tenants, dev and prod**

```yaml
apiVersion: tempo.grafana.com/v1alpha1
kind: TempoStack
metadata:
  name: simplest
spec:
  tenants:
    mode: openshift
    authentication:
      - tenantName: dev
        tenantId: "1610b0c3-c509-4592-a256-a1871353dbfa"
      - tenantName: prod
        tenantId: "1610b0c3-c509-4592-a256-a1871353dbfb"
    template:
```
gateway:
  enabled: true
queryFrontend:
  jaegerQuery:
    enabled: true

1. Must be set to **openshift**.
2. The list of tenants.
3. The tenant name. Must be provided in the **X-Scope-OrgId** header when ingesting the data.
4. A unique tenant ID.
5. Enables a gateway that performs authentication and authorization. The Jaeger UI is exposed at

The authorization configuration uses the **ClusterRole** and **ClusterRoleBinding** of the Kubernetes
Role-Based Access Control (RBAC). By default, no users have read or write permissions.

**Sample of the read RBAC configuration that allows authenticated users to read the trace
data of the dev and prod tenants**

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: tempostack-traces-reader
rules:
  - apiGroups:
      - 'tempo.grafana.com'
    resources: 1
      - dev
      - prod
    resourceNames: 2
      - traces
    verbs:
      - 'get'
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: tempostack-traces-reader
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: tempostack-traces-reader
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: system:authenticated 3
```

1. Lists the tenants.
2. The **get** value enables the read operation.
Grants all authenticated users the read permissions for trace data.

Sample of the write RBAC configuration that allows the `otel-collector` service account to write the trace data for the `dev` tenant

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: otel-collector
  namespace: otel
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: tempostack-traces-write
rules:
- apiGroups:
  - 'tempo.grafana.com'
  resources:
  - dev
  resourceNames:
  - traces
  verbs:
  - 'create'
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: tempostack-traces
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: tempostack-traces-write
subjects:
- kind: ServiceAccount
  name: otel-collector
  namespace: otel
```

1. The service account name for the client to use when exporting trace data. The client must send the service account token, `/var/run/secrets/kubernetes.io/serviceaccount/token`, as the bearer token header.

2. Lists the tenants.

3. The `create` value enables the write operation.

Trace data can be sent to the Tempo instance from the OpenTelemetry Collector that uses the service account with RBAC for writing the data.

Sample OpenTelemetry CR configuration

```yaml
apiVersion: opentelemetry.io/v1alpha1
kind: OpenTelemetryCollector
```
4.2.2. Setting up monitoring for the distributed tracing platform (Tempo)

The Tempo Operator supports monitoring and alerting of each TempoStack component such as distributor, ingester, and so on, and exposes upgrade and operational metrics about the Operator itself.

4.2.2.1. Configuring TempoStack metrics and alerts

You can enable metrics and alerts of TempoStack instances.

Prerequisites

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

Procedure

1. To enable metrics of a TempoStack instance, set the `spec.observability.metrics.createServiceMonitors` field to `true`:

```yaml
metadata:
  name: cluster-collector
  namespace: tracing-system
spec:
  mode: deployment
  serviceAccount: otel-collector
config: |
  extensions:
  - beartertokenauth:
    filename: "/var/run/secrets/kubernetes.io/serviceaccount/token"
  exporters:
    - otlp/dev:
      endpoint: tempo-simplest-gateway.tempo.svc.cluster.local:8090
      tls:
        insecure: false
        ca_file: "/var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt"
      auth:
        authenticator: beartertokenauth
      headers:
        X-Scope-OrgID: "dev"
service:
  extensions: [beartertokenauth]
pipelines:
  traces:
    exporters: [otlp/dev]
```
2. To enable alerts for a TempoStack instance, set the `spec.observability.metrics.createPrometheusRules` field to `true`:

```yaml
apiVersion: tempo.grafana.com/v1alpha1
class: TempoStack
metadata:
  name: <name>
spec:
  observability:
    metrics:
      createPrometheusRules: true
```

**Verification**

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

1. Go to **Observe → Targets**, filter for **Source: User**, and check that **ServiceMonitors** in the format `tempo-<instance_name>-<component>` have the **Up** status.

2. To verify that alerts are set up correctly, go to **Observe → Alerting → Alerting rules**, filter for **Source: User**, and check that the **Alert rules** for the TempoStack instance components are available.

### 4.2.2.2. Configuring Tempo Operator metrics and alerts

When installing the Tempo Operator from the web console, you can select the **Enable Operator recommended cluster monitoring on this Namespace** checkbox, which enables creating metrics and alerts of the Tempo Operator.

If the checkbox was not selected during installation, you can manually enable metrics and alerts even after installing the Tempo Operator.

**Procedure**

- Add the `openshift.io/cluster-monitoring: "true"` label in the project where the Tempo Operator is installed, which is `openshift-tempo-operator` by default.

**Verification**

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

1. Go to **Observe → Targets**, filter for **Source: Platform**, and search for `tempo-operator`, which must have the **Up** status.

2. To verify that alerts are set up correctly, go to **Observe → Alerting → Alerting rules**, filter for **Source: Platform**, and locate the **Alert rules** for the **Tempo Operator**.

### 4.3. UPDATING THE DISTRIBUTED TRACING PLATFORM (TEMPO)

For version upgrades, the Tempo 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 Tempo Operator is upgraded to the new version, it scans for running TempoStack instances that it manages and upgrades them to the version corresponding to the Operator’s new version.

4.3.1. Additional resources

- Operator Lifecycle Manager concepts and resources
- Updating installed Operators

4.4. REMOVING THE RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM (TEMPO)

The steps for removing the Red Hat OpenShift distributed tracing platform (Tempo) from an OpenShift Container Platform cluster are as follows:

1. Shut down all distributed tracing platform (Tempo) pods.
2. Remove any TempoStack instances.
3. Remove the Tempo Operator.

4.4.1. Removing a TempoStack instance by using the web console

You can remove a TempoStack instance in the Administrator view of the web console.

Prerequisites

- You are logged in to the OpenShift Container Platform 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 → Tempo Operator → TempoStack.
2. To remove the TempoStack instance, select → Delete TempoStack → Delete.
3. Optional: Remove the Tempo Operator.

4.4.2. Removing a TempoStack instance by using the CLI

You can remove a TempoStack 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`:

  ```bash
  $ oc login --username=<your_username>
  ```

Procedure
1. Get the name of the TempoStack instance by running the following command:

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

2. Remove the TempoStack instance by running the following command:

  ```bash
  $ oc delete tempo <tempostack_instance_name> -n <project_of_tempostack_instance>
  ```

3. Optional: Remove the Tempo Operator.

Verification
1. Run the following command to verify that the TempoStack instance is not found in the output, which indicates its successful removal:

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

4.4.3. Additional resources
- Deleting Operators from a cluster
- Getting started with the OpenShift CLI