OpenShift Container Platform 4.15

Distributed tracing

Distributed tracing installation, usage, and release notes
OpenShift Container Platform 4.15 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. RELEASE NOTES

1.1. RELEASE NOTES FOR RED HAT OPENSOURCE DISTRIBUTED TRACING PLATFORM 3.1

1.1.1. Distributed tracing overview

1.1.2. Component versions in the Red Hat OpenShift distributed tracing platform 3.1

1.1.3. Red Hat OpenShift distributed tracing platform (Tempo)

1.1.3.1. New features and enhancements

1.1.3.2. Bug fixes

1.1.3.3. Known issues

1.1.4. Red Hat OpenShift distributed tracing platform (Jaeger)

1.1.4.1. Support for OpenShift Elasticsearch Operator

1.1.4.2. Deprecated functionality

1.1.4.3. Bug fixes

1.1.4.4. Known issues

1.1.5. Getting support

1.1.6. Making open source more inclusive

1.2. RELEASE NOTES FOR PAST RELEASES OF RED HAT OPENSOURCE DISTRIBUTED TRACING PLATFORM

1.2.1. Distributed tracing overview

1.2.2. Release notes for Red Hat OpenShift distributed tracing platform 3.0

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

1.2.2.2. Red Hat OpenShift distributed tracing platform (Jaeger)

1.2.2.2.1. Deprecated functionality

1.2.2.2.2. New features and enhancements

1.2.2.2.3. Bug fixes

1.2.2.2.4. Known issues

1.2.2.3. Red Hat OpenShift distributed tracing platform (Tempo)

1.2.2.3.1. New features and enhancements

1.2.2.3.2. Bug fixes

1.2.2.3.3. Known issues

1.2.3. Release notes for Red Hat OpenShift distributed tracing platform 2.9.2

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

1.2.3.2. CVEs

1.2.3.3. Red Hat OpenShift distributed tracing platform (Jaeger)

1.2.3.3.1. Known issues

1.2.3.4. Red Hat OpenShift distributed tracing platform (Tempo)

1.2.3.4.1. Known issues

1.2.4. Release notes for Red Hat OpenShift distributed tracing platform 2.9.1

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

1.2.4.2. CVEs

1.2.4.3. Red Hat OpenShift distributed tracing platform (Jaeger)

1.2.4.3.1. Known issues

1.2.4.4. Red Hat OpenShift distributed tracing platform (Tempo)

1.2.4.4.1. Known issues

1.2.5. Release notes for Red Hat OpenShift distributed tracing platform 2.9

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

1.2.5.2. Red Hat OpenShift distributed tracing platform (Jaeger)

1.2.5.2.1. Bug fixes

1.2.5.2.2. Known issues

1.2.5.3. Red Hat OpenShift distributed tracing platform (Tempo)

1.2.5.3.1. New features and enhancements

1.2.5.3.2. Bug fixes

1.2.5.3.3. Known issues
1.2.6. Release notes for Red Hat OpenShift distributed tracing platform 2.8
   1.2.6.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.8
   1.2.6.2. Technology Preview features
   1.2.6.3. Bug fixes
1.2.7. Release notes for Red Hat OpenShift distributed tracing platform 2.7
   1.2.7.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.7
   1.2.7.2. Bug fixes
1.2.8. Release notes for Red Hat OpenShift distributed tracing platform 2.6
   1.2.8.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.6
   1.2.8.2. Bug fixes
1.2.9. Release notes for Red Hat OpenShift distributed tracing platform 2.5
   1.2.9.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.5
   1.2.9.2. New features and enhancements
   1.2.9.3. Bug fixes
1.2.10. Release notes for Red Hat OpenShift distributed tracing platform 2.4
   1.2.10.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.4
   1.2.10.2. New features and enhancements
   1.2.10.3. Technology Preview features
   1.2.10.4. Bug fixes
1.2.11. Release notes for Red Hat OpenShift distributed tracing platform 2.3
   1.2.11.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.3.1
   1.2.11.2. Component versions in the Red Hat OpenShift distributed tracing platform 2.3.0
   1.2.11.3. New features and enhancements
   1.2.11.4. Bug fixes
1.2.12. Release notes for Red Hat OpenShift distributed tracing platform 2.2
   1.2.12.1. Technology Preview features
   1.2.12.2. Bug fixes
1.2.13. Release notes for Red Hat OpenShift distributed tracing platform 2.1
   1.2.13.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.1
   1.2.13.2. Technology Preview features
   1.2.13.3. Bug fixes
1.2.14. Release notes for Red Hat OpenShift distributed tracing platform 2.0
   1.2.14.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.0
   1.2.14.2. New features and enhancements
   1.2.14.3. Technology Preview features
   1.2.14.4. Bug fixes
1.2.15. Getting support
1.2.16. Making open source more inclusive

CHAPTER 2. DISTRIBUTED TRACING ARCHITECTURE ......................................................... 25
  2.1. DISTRIBUTED TRACING ARCHITECTURE .................................................. 25
     2.1.1. Distributed tracing overview ................................................. 25
     2.1.2. Red Hat OpenShift distributed tracing platform features .......... 25
     2.1.3. Red Hat OpenShift distributed tracing platform architecture ..... 26
     2.1.4. Additional resources ...................................................... 27

CHAPTER 3. DISTRIBUTED TRACING PLATFORM (TEMPO) .............................................. 28
  3.1. INSTALLING THE DISTRIBUTED TRACING PLATFORM (TEMPO) .................... 28
     3.1.1. Object storage setup .................................................... 28
     3.1.2. Installing the distributed tracing platform (Tempo) from the web console 29
     3.1.3. Installing the distributed tracing platform (Tempo) by using the CLI 32
     3.1.4. Additional resources .................................................... 36
  3.2. CONFIGURING AND DEPLOYING THE DISTRIBUTED TRACING PLATFORM (TEMPO) 36
3.2.1. Customizing your deployment
   3.2.1.1. Distributed tracing default configuration options
   3.2.1.2. The distributed tracing platform (Tempo) storage configuration
   3.2.1.3. Query configuration options
      3.2.1.3.1. Additional resources
   3.2.1.4. Configuration of the monitor tab in Jaeger UI
      3.2.1.4.1. OpenTelemetry Collector configuration
      3.2.1.4.2. Tempo configuration
      3.2.1.4.3. Span RED metrics and alerting rules
      3.2.1.5. Multitenancy
   3.2.2. Setting up monitoring for the distributed tracing platform (Tempo)
      3.2.2.1. Configuring TempoStack metrics and alerts
      3.2.2.2. Configuring Tempo Operator metrics and alerts
3.3. UPDATING THE DISTRIBUTED TRACING PLATFORM (TEMPO)
   3.3.1. Additional resources
3.4. REMOVING THE RED HAT OPENShift DISTRIBUTED TRACING PLATFORM (TEMPO)
   3.4.1. Removing a TempoStack instance by using the web console
   3.4.2. Removing a TempoStack instance by using the CLI
   3.4.3. Additional resources
4. CHAPTER 4. DISTRIBUTED TRACING PLATFORM (JAEGER) .......................................................... 53
4.1. INSTALLING THE DISTRIBUTED TRACING PLATFORM JAEGER
   4.1.1. Prerequisites
   4.1.2. Red Hat OpenShift distributed tracing platform installation overview
   4.1.3. Installing the OpenShift Elasticsearch Operator
   4.1.4. Installing the Red Hat OpenShift distributed tracing platform (Jaeger) Operator
4.2. CONFIGURING AND DEPLOYING THE DISTRIBUTED TRACING PLATFORM JAEGER
   4.2.1. Supported deployment strategies
   4.2.2. Deploying the distributed tracing platform default strategy from the web console
      4.2.2.1. Deploying the distributed tracing platform default strategy from the CLI
      4.2.3. Deploying the distributed tracing platform production strategy from the web console
      4.2.3.1. Deploying the distributed tracing platform production strategy from the CLI
   4.2.4. Deploying the distributed tracing platform streaming strategy from the web console
      4.2.4.1. Deploying the distributed tracing platform streaming strategy from the CLI
   4.2.5. Validating your deployment
      4.2.5.1. Accessing the Jaeger console
   4.2.6. Customizing your deployment
      4.2.6.1. Deployment best practices
   4.2.6.2. Distributed tracing default configuration options
   4.2.6.3. Jaeger Collector configuration options
   4.2.6.4. Distributed tracing sampling configuration options
   4.2.6.5. Distributed tracing storage configuration options
      4.2.6.5.1. Auto-provisioning an Elasticsearch instance
      4.2.6.5.2. Connecting to an existing Elasticsearch instance
   4.2.6.6. Managing certificates with Elasticsearch
   4.2.6.7. Query configuration options
   4.2.6.8. Ingester configuration options
   4.2.7. Injecting sidecars
      4.2.7.1. Automatically injecting sidecars
      4.2.7.2. Manually injecting sidecars
4.3. UPDATING THE DISTRIBUTED TRACING PLATFORM JAEGER
   4.3.1. Additional resources
4.4. REMOVING THE DISTRIBUTED TRACING PLATFORM JAEGER
   4.4.1. Removing a Jaeger instance by using the web console
   4.4.2. Removing a Jaeger instance by using the CLI
   4.4.3. Additional resources
4.4.1. Removing a distributed tracing platform (Jaeger) instance by using the web console
4.4.2. Removing a distributed tracing platform (Jaeger) instance by using the CLI
4.4.3. Removing the Red Hat OpenShift distributed tracing platform Operators
CHAPTER 1. RELEASE NOTES

1.1. RELEASE NOTES FOR RED HAT OPENSHEET DISTRIBUTED TRACING PLATFORM 3.1

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

**IMPORTANT**

Jaeger does not use FIPS validated cryptographic modules.

1.1.2. Component versions in the Red Hat OpenShift distributed tracing platform 3.1

<table>
<thead>
<tr>
<th>Operator</th>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>2.3.1</td>
</tr>
<tr>
<td>Red Hat build of OpenTelemetry</td>
<td>OpenTelemetry</td>
<td>0.93.0</td>
</tr>
<tr>
<td>Red Hat OpenShift distributed tracing platform (Jaeger) (deprecated)</td>
<td>Jaeger</td>
<td>1.53.0</td>
</tr>
</tbody>
</table>

1.1.3. Red Hat OpenShift distributed tracing platform (Tempo)

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

- Support for cluster-wide proxy environments.
- Support for TraceQL to Gateway component.

### 1.1.3.2. Bug fixes

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

- Before this update, when a TempoStack instance was created with the `monitorTab` enabled in OpenShift Container Platform 4.15, the required `tempo-redmetrics-cluster-monitoring-view` ClusterRoleBinding was not created. This update resolves the issue by fixing the Operator RBAC for the monitor tab when the Operator is deployed in an arbitrary namespace. ([TRACING-3786](#))

- Before this update, when a TempoStack instance was created on an OpenShift Container Platform cluster with only an IPV6 networking stack, the compactor and ingestor pods ran in the `CrashLoopBackOff` state, resulting in multiple errors. This update provides support for IPv6 clusters. ([TRACING-3226](#))

### 1.1.3.3. Known issues

There are currently known issues:

- 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](#))

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

#### 1.1.4.1. Support for OpenShift Elasticsearch Operator

Red Hat OpenShift distributed tracing platform (Jaeger) 3.1 is supported for use with the OpenShift Elasticsearch Operator 5.6, 5.7, and 5.8.

#### 1.1.4.2. Deprecated functionality

In the Red Hat OpenShift distributed tracing platform 3.1, Jaeger and support for Elasticsearch remain 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 the Red Hat OpenShift distributed tracing platform 3.1, 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.

#### 1.1.4.3. Bug fixes

This update introduces the following bug fix for the distributed tracing platform (Jaeger):
Before this update, the connection target URL for the jaeger-agent container in the jager-query pod was overwritten with another namespace URL in OpenShift Container Platform 4.13. This was caused by a bug in the sidecar injection code in the jaeger-operator, causing nondeterministic jaeger-agent injection. With this update, the Operator prioritizes the Jaeger instance from the same namespace as the target deployment. (TRACING-3722)

1.1.4.4. Known issues

There are currently 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 architectures.

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. 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 PAST RELEASES OF RED HAT OPENSHIFT DISTRIBUTED TRACING PLATFORM

1.2.1. Distributed tracing overview

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

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

Optimize performance and latency

Perform root cause analysis

The distributed tracing platform consists of three components:

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

- **Red Hat build of OpenTelemetry** which is based on the open source OpenTelemetry project.

- **Red Hat OpenShift distributed tracing platform (Jaeger)** which is based on the open source Jaeger project.

**IMPORTANT**

Jaeger does not use FIPS validated cryptographic modules.

### 1.2.2. Release notes for Red Hat OpenShift distributed tracing platform 3.0

#### 1.2.2.1. 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 OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>2.3.0</td>
</tr>
</tbody>
</table>

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

##### 1.2.2.2.1. Deprecated functionality

In the Red Hat OpenShift distributed tracing platform 3.0, Jaeger and support for 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 the Red Hat OpenShift distributed tracing platform 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.

##### 1.2.2.2.2. 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.

1.2.2.3. Bug fixes

This update introduces the following bug fix for the distributed tracing platform (Jaeger):

• Before this update, the Red Hat OpenShift distributed tracing platform (Jaeger) operator used other images than relatedImages. This caused the ImagePullBackOff error in disconnected network environments when launching the jaeger pod because the oc adm catalog mirror command mirrors images specified in relatedImages. This update provides support for disconnected environments when using the oc adm catalog mirror CLI command. (TRACING-3546)

1.2.2.4. Known issues

There is currently a known issue:

• Currently, Apache Spark is not supported.

• Currently, the streaming deployment via AMQ/Kafka is not supported on the IBM Z and IBM Power architectures.

1.2.2.3. Red Hat OpenShift distributed tracing platform (Tempo)

1.2.2.3.1. 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.

1.2.2.3.2. Bug fixes

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

• Before this update, the TempoStack CRD was not accepting custom CA certificate despite the option to choose CA certificates. This update fixes support for the custom TLS CA option for connecting to object storage. (TRACING-3462)

• Before this update, when mirroring the Red Hat OpenShift distributed tracing platform operator images to a mirror registry for use in a disconnected cluster, the related operator images for tempo, tempo-gateway, opa-openshift, and tempo-query were not mirrored. This update fixes support for disconnected environments when using the oc adm catalog mirror CLI command. (TRACING-3523)

• Before this update, the query frontend service of the Red Hat OpenShift distributed tracing platform was using internal mTLS when gateway was not deployed. This caused endpoint failure errors. This update fixes mTLS when Gateway is not deployed. (TRACING-3510)

1.2.2.3.3. Known issues

There are currently known issues:
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)

1.2.3. Release notes for Red Hat OpenShift distributed tracing platform 2.9.2

1.2.3.1. 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 OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>2.1.1</td>
</tr>
</tbody>
</table>

1.2.3.2. CVEs

This release fixes CVE-2023-46234.

1.2.3.3. Red Hat OpenShift distributed tracing platform (Jaeger)

1.2.3.3.1. Known issues

There are currently known issues:

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

1.2.3.4. 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.

1.2.3.4.1. Known issues

There are currently 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:
```
1.2.4. Release notes for Red Hat OpenShift distributed tracing platform 2.9.1

1.2.4.1. 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 OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>2.1.1</td>
</tr>
</tbody>
</table>

1.2.4.2. CVEs

This release fixes [CVE-2023-44487](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44487).

1.2.4.3. Red Hat OpenShift distributed tracing platform (Jaeger)

1.2.4.3.1. Known issues

There are currently known issues:

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

1.2.4.4. 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.

1.2.4.4.1. Known issues

There are currently 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:

   ```
   $ 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:

   ```
   $ 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:e4295f837066eb05b8c5897f31eb2bd81684a8c59d6f9498d3590c62c12a
                  - name: registry.redhat.io/rhosdt/tempo-gateway-rhel8@sha256:b62f5cedf6eb597b638f14da6aaeae50f4162980a8a6f87b7061e88d90fac23
                  - name: registry.redhat.io/rhosdt/tempo-query-rhel8@sha256:8cd134deca47d6817b26566e272e63f75367653d589f5c90855c59b2f0aban0e9
      - name: tempo-product
        channels:
          - name: stable
            additionalImages:
              - name: registry.redhat.io/rhosdt/tempo-rhel8@sha256:e4295f837066eb05b8c5897f31eb2bd81684a8c59d6f9498d3590c62c12a
                - name: registry.redhat.io/rhosdt/tempo-gateway-rhel8@sha256:b62f5cedf6eb597b638f14da6aaeae50f4162980a8a6f87b7061e88d90fac23
                - name: registry.redhat.io/rhosdt/tempo-query-rhel8@sha256:8cd134deca47d6817b26566e272e63f75367653d589f5c90855c59b2f0aban0e9
```

1.2.5. Release notes for Red Hat OpenShift distributed tracing platform 2.9

1.2.5.1. 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 OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>2.11</td>
</tr>
</tbody>
</table>

1.2.5.2. Red Hat OpenShift distributed tracing platform (Jaeger)

1.2.5.2.1. 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)

1.2.5.2.2. Known issues

There are currently known issues:

- Apache Spark is not supported.

- The streaming deployment via AMQ/Kafka is unsupported on the IBM Z and IBM Power architectures.

1.2.5.3. 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.

1.2.5.3.1. 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 the 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.
1.2.5.3.2. 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)

1.2.5.3.3. Known issues

There are currently 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
```
• 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:e4295f837066e6fb05b5c5897f31eb2b9bd81684a82c59d6f9498dd3590c62c12a
                    - name: registry.redhat.io/rhosdt/tempo-gateway-rhel8@sha256:b62f5cedf8e05907b638f14ca6aee050f4f1642980a8af87b7061e88d90fac23
                    - name: registry.redhat.io/rhosdt/tempo-gateway-opa-rhel8@sha256:8cd134deca47d6817b2656d2e726c3f75367653d589f5c90855c59b2fab01e9
                    - name: registry.redhat.io/rhosdt/tempo-query-rhel8@sha256:0da43034f440b8258a48a0697ba643b5643d48b615c8b882ac7f4f1f80aad08e
```

### 1.2.6. Release notes for Red Hat OpenShift distributed tracing platform 2.8

#### 1.2.6.1. 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 OpenShift distributed tracing platform (Tempo)</td>
<td>Tempo</td>
<td>0.1.0</td>
</tr>
</tbody>
</table>

#### 1.2.6.2. 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.
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.

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

1.2.7. Release notes for Red Hat OpenShift distributed tracing platform 2.7

1.2.7.1. 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>
</tbody>
</table>

1.2.7.2. Bug fixes
This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.
1.2.8. Release notes for Red Hat OpenShift distributed tracing platform 2.6

1.2.8.1. 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>
</tbody>
</table>

1.2.8.2. Bug fixes

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

1.2.9. Release notes for Red Hat OpenShift distributed tracing platform 2.5

1.2.9.1. 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>
</tbody>
</table>

1.2.9.2. 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.

1.2.9.3. Bug fixes

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

1.2.10. Release notes for Red Hat OpenShift distributed tracing platform 2.4

1.2.10.1. 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>
</tbody>
</table>
1.2.10.2. New features and enhancements

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

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

1.2.10.3. 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.

1.2.10.4. Bug fixes

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

1.2.11. Release notes for Red Hat OpenShift distributed tracing platform 2.3

1.2.11.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.3.1

<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>1.30.2</td>
</tr>
</tbody>
</table>

1.2.11.2. 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>
</tbody>
</table>

1.2.11.3. 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.

1.2.11.4. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.
1.2.12. Release notes for Red Hat OpenShift distributed tracing platform 2.2

1.2.12.1. Technology Preview features

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

1.2.12.2. Bug fixes

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

1.2.13. Release notes for Red Hat OpenShift distributed tracing platform 2.1

1.2.13.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.1

<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>1.29.1</td>
</tr>
</tbody>
</table>

1.2.13.2. Technology Preview features

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

   **CA file configuration for OpenTelemetry version 0.33**

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

```

   **CA file configuration for OpenTelemetry version 0.41.1**

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

1.2.13.3. Bug fixes

This release addresses Common Vulnerabilities and Exposures (CVEs) and bug fixes.
1.2.14. Release notes for Red Hat OpenShift distributed tracing platform 2.0

1.2.14.1. Component versions in the Red Hat OpenShift distributed tracing platform 2.0

<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>
</tbody>
</table>

1.2.14.2. 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.

1.2.14.3. 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.

1.2.14.4. Bug fixes

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

1.2.15. Getting support

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

From the Customer Portal, you can:

- Search or browse through the Red Hat Knowledgebase of articles and solutions relating to Red Hat products.
- Submit a support case to Red Hat Support.
- Access other product documentation.
To identify issues with your cluster, you can use Insights in OpenShift Cluster Manager. Insights provides details about issues and, if available, information on how to solve a problem.

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

1.2.16. Making open source more inclusive

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright’s message.
CHAPTER 2. 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 (Tempo)** which is based on the open source Grafana Tempo project.
- **Red Hat build of OpenTelemetry** which is based on the open source OpenTelemetry project.
- **Red Hat OpenShift distributed tracing platform (Jaeger)** which is based on the open source Jaeger project.

**IMPORTANT**

Jaeger does not use FIPS validated cryptographic modules.

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 (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.

- **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. Red Hat OpenShift distributed tracing platform (Jaeger) supports the Elasticsearch storage.

- **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.

### 2.1.4. Additional resources

- [Red Hat build of OpenTelemetry](https://www.redhat.com)
CHAPTER 3. DISTRIBUTED TRACING PLATFORM (TEMPO)

3.1. 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.

3.1.1. Object storage setup

You can use the following configuration parameters when setting up a supported object storage.

Table 3.1. Required secret parameters

<table>
<thead>
<tr>
<th>Storage provider</th>
<th>Required 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                              | 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                          |
3.1.2. Installing the distributed tracing platform (Tempo) from the web console

You can install the distributed tracing platform (Tempo) from 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.
- 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**.

**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.

**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
kind: TempoStack
metadata:
  name: sample
namespace: <project_of_tempostack_instance>
```
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.

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.
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.

3.1.3. 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:

```
$ 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:

```
$ 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:

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

2. Run the following command to create a project of your choice for the TempoStack instance that you will create in a subsequent step:

```
$ 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 the following command:

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

**Example secret for Amazon S3 and MinIO storage**
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: 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
```

```yaml
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:
  storageSize: 1Gi
  storage:
    secret:
      name: <secret-name> ①
      type: <secret-provider> ②
template:
  queryFrontend:
    jaegerQuery:
      enabled: true
  ingress:
    route:
      termination: edge
      type: route
```

① The value of the **name** in the **metadata** of the secret.

② 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:
```
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:

   ```bash
   $ 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.
3.1.4. 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

3.2. 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.

3.2.1. 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.

3.2.1.1. 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
apiVersion: tempo.grafana.com/v1alpha1
kind: TempoStack
metadata:
  name: name
spec:
  storage: {}
  resources: {}
  storageSize: 200M
  replicationFactor: 1
  retention: {}
  template:
    distributor: {}
    ingester: {}
    compactor: {}
    querier: {}
    queryFrontend: {}
    gateway: {}
```

Table 3.2. 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>tempo.grafana.com/v1alpha1</td>
<td>tempo.grafana.com/v1alpha1</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></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>
</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>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 spec node. When the definition relates to an individual component, it is placed under the spec/template/&lt;component&gt; 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>
</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
description: TempoStack
metadata:
  name: simplest
spec:
  storage: |
    secret:
      name: minio
type: s3
resources: |
  total:
```
This section specifies the deployed object storage back end, which requires a created secret with credentials for access to the object storage.

### 3.2.1.2. 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>
<thead>
<tr>
<th>Table 3.3. General storage parameters used by the Tempo Operator to define distributed tracing storage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><code>spec:</code></td>
</tr>
<tr>
<td><code>storage:</code></td>
</tr>
<tr>
<td><code>secretname:</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 3.4. Required secret parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage provider</strong></td>
</tr>
</tbody>
</table>
### Storage provider

**Red Hat OpenShift Data Foundation**

<table>
<thead>
<tr>
<th>name</th>
<th>tempostack-dev-odf # example</th>
<th>bucket: <code>&lt;bucket_name&gt;</code> # requires an ObjectBucketClaim</th>
<th>endpoint: <code>https://s3.openshift-storage.svc</code></th>
<th>access_key_id: <code>&lt;data_foundation_access_key_id&gt;</code></th>
<th>access_key_secret: <code>&lt;data_foundation_access_key_secret&gt;</code></th>
</tr>
</thead>
</table>

**MinIO**

See [MinIO Operator](#).

<table>
<thead>
<tr>
<th>name</th>
<th>tempostack-dev-minio # example</th>
<th>bucket: <code>&lt;minio_bucket_name&gt;</code></th>
<th>endpoint: <code>&lt;minio_bucket_endpoint&gt;</code></th>
<th>access_key_id: <code>&lt;minio_access_key_id&gt;</code></th>
<th>access_key_secret: <code>&lt;minio_access_key_secret&gt;</code></th>
</tr>
</thead>
</table>

**Amazon S3**

<table>
<thead>
<tr>
<th>name</th>
<th>tempostack-dev-s3 # example</th>
<th>bucket: <code>&lt;s3_bucket_name&gt;</code></th>
<th>endpoint: <code>&lt;s3_bucket_endpoint&gt;</code></th>
<th>access_key_id: <code>&lt;s3_access_key_id&gt;</code></th>
<th>access_key_secret: <code>&lt;s3_access_key_secret&gt;</code></th>
</tr>
</thead>
</table>

**Microsoft Azure Blob Storage**

<table>
<thead>
<tr>
<th>name</th>
<th>tempostack-dev-azure # example</th>
<th>container: <code>&lt;azure_blob_storage_container_name&gt;</code></th>
<th>account_name: <code>&lt;azure_blob_storage_account_name&gt;</code></th>
<th>account_key: <code>&lt;azure_blob_storage_account_key&gt;</code></th>
</tr>
</thead>
</table>

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

- **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

### 3.2.1.3. Query configuration options

Two components of the distributed tracing platform (Tempo), the querier and query frontend, manage queries. You can configure both of these components.

The querier component finds the requested trace ID in the ingesters or back-end storage. Depending on the set parameters, the querier component can query both the ingesters and pull bloom or indexes from the back end to search blocks in object storage. The querier component exposes an HTTP endpoint at `GET /querier/api/traces/<trace_id>`, but it is not expected to be used directly. Queries must be sent to the query frontend.

#### Table 3.5. Configuration parameters for the querier component

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>nodeSelector</td>
<td>The simple form of the node-selection constraint.</td>
<td>type: object</td>
</tr>
<tr>
<td>replicas</td>
<td>The number of replicas to be created for the component.</td>
<td>type: integer; format: int32</td>
</tr>
<tr>
<td>tolerations</td>
<td>Component-specific pod tolerations.</td>
<td>type: array</td>
</tr>
</tbody>
</table>

The query frontend component is responsible for sharding the search space for an incoming query. The query frontend exposes traces via a simple HTTP endpoint: `GET /api/traces/<trace_id>`. Internally, the query frontend component splits the `blockID` space into a configurable number of shards and then queues these requests. The querier component connects to the query frontend component via a streaming gRPC connection to process these sharded queries.

#### Table 3.6. Configuration parameters for the query frontend component

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>component</td>
<td>Configuration of the query frontend component.</td>
<td>type: object</td>
</tr>
<tr>
<td>component.nodeSelector</td>
<td>The simple form of the node selection constraint.</td>
<td>type: object</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>component.replicas</td>
<td>The number of replicas to be created for the query frontend component.</td>
<td>type: integer; format: int32</td>
</tr>
<tr>
<td>component.tolerations</td>
<td>Pod tolerations specific to the query frontend component.</td>
<td>type: array</td>
</tr>
<tr>
<td>jaegerQuery</td>
<td>The options specific to the Jaeger Query component.</td>
<td>type: object</td>
</tr>
<tr>
<td>jaegerQuery.enabled</td>
<td>When enabled, creates the Jaeger Query component jaegerQuery.</td>
<td>type: boolean</td>
</tr>
<tr>
<td>jaegerQuery.ingress</td>
<td>The options for the Jaeger Query ingress.</td>
<td>type: object</td>
</tr>
<tr>
<td>jaegerQuery.ingress.annotations</td>
<td>The annotations of the ingress object.</td>
<td>type: object</td>
</tr>
<tr>
<td>jaegerQuery.ingress.host</td>
<td>The hostname of the ingress object.</td>
<td>type: string</td>
</tr>
<tr>
<td>jaegerQuery.ingress.ingressClassName</td>
<td>The name of an IngressClass cluster resource. Defines which ingress controller serves this ingress resource.</td>
<td>type: string</td>
</tr>
<tr>
<td>jaegerQuery.ingress.route</td>
<td>The options for the OpenShift route.</td>
<td>type: object</td>
</tr>
<tr>
<td>jaegerQuery.ingress.route.termination</td>
<td>The termination type. The default is edge.</td>
<td>type: string (enum: insecure, edge, passthrough, reencrypt)</td>
</tr>
<tr>
<td>jaegerQuery.ingress.type</td>
<td>The type of ingress for the Jaeger Query UI. The supported types are ingress, route, and none.</td>
<td>type: string (enum: ingress, route)</td>
</tr>
<tr>
<td>jaegerQuery.monitorTab</td>
<td>The monitor tab configuration.</td>
<td>type: object</td>
</tr>
<tr>
<td>jaegerQuery.monitorTab.enabled</td>
<td>Enables the monitor tab in the Jaeger console. The PrometheusEndpoint must be configured.</td>
<td>type: boolean</td>
</tr>
</tbody>
</table>
### Example configuration of the query frontend component in a TempoStack CR

```yaml
apiVersion: tempo.grafana.com/v1alpha1
type: string

kind: TempoStack

metadata:
  name: simplest

spec:
  storage:
    secret:
      name: minio
      type: s3
    storageSize: 200M
  resources:
    total:
      limits:
        memory: 2Gi
        cpu: 2000m
  template:
    queryFrontend:
      jaegerQuery:
        enabled: true
        ingress:
          route:
            termination: edge
            type: route
```

#### 3.2.1.3.1. Additional resources

- Understanding taints and tolerations

#### 3.2.1.4. Configuration of the monitor tab in Jaeger UI

Trace data contains rich information, and the data is normalized across instrumented languages and frameworks. Therefore, request rate, error, and duration (RED) metrics can be extracted from traces. The metrics can be visualized in Jaeger console in the Monitor tab.

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.

#### 3.2.1.4.1. OpenTelemetry Collector configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>jaegerQuery.monitorTab.prometheusEndpoint</td>
<td>The endpoint to the Prometheus instance that contains the span rate, error, and duration (RED) metrics. For example, <a href="https://thanos-quierer.openshift-monitoring.svc.cluster.local:9091">https://thanos-quierer.openshift-monitoring.svc.cluster.local:9091</a>.</td>
<td>type: string</td>
</tr>
</tbody>
</table>
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
        add_metric_suffixes: false
        resource_to_telemetry_conversion:
          enabled: true
          # by default resource attributes are dropped
        otlp:
          endpoint: "tempo-simplest-distributor:4317"
          tls:
            insecure: true
    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.
5. The Spanmetrics connector is configured as exporter in traces pipeline.
The Spanmetrics connector is configured as receiver in metrics pipeline.

3.2.1.4.2. 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.

3.2.1.4.3. Span RED metrics and alerting rules

The metrics generated by the spanmetrics connector are usable with alerting rules. For example, for alerts about a slow service or to define service level objectives (SLOs), the connector creates a duration_bucket histogram and the calls counter metric. These metrics have labels that identify the service, API name, operation type, and other attributes.

Table 3.7. Labels of the metrics created in the spanmetrics connector

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_name</td>
<td>Service name set by the otel_service_name environment variable.</td>
<td>frontend</td>
</tr>
<tr>
<td>span_name</td>
<td>Name of the operation.</td>
<td>/</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/customer</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
<td>Values</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
</tbody>
</table>
| span_kind | Identifies the server, client, messaging, or internal operation. | • SPAN_KIND_SERVER
• SPAN_KIND_CLIENT
• SPAN_KIND_PRODUCER
• SPAN_KIND_CONSUMER
• SPAN_KIND_INTERNAL |

**Example PrometheusRule CR that defines an alerting rule for SLO when not serving 95% of requests within 2000ms on the front-end service**

```yaml
apiVersion: monitoring.coreos.com/v1
kind: PrometheusRule
metadata:
  name: span-red
spec:
groups:
- name: server-side-latency
  rules:
  - alert: SpanREDFrontendAPIRequestLatency
    expr: histogram_quantile(0.95, sum(rate(duration_bucket{service_name="frontend", span_kind="SPAN_KIND_SERVER"}[5m])) by (le, service_name, span_name)) > 2000
    labels:
      severity: Warning
      annotations:
        summary: "High request latency on {{labels.service_name}} and {{labels.span_name}}"
        description: "{{labels.instance}} has 95th request latency above 2s (current value: {{value}})"

1 The expression for checking if 95% of the front-end server response time values are below 2000 ms. The time range ([5m]) must be at least four times the scrape interval and long enough to accommodate a change in the metric.

3.2.1.5. 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 http://<gateway-ingress>/api/traces/v1/<tenant-name>/search.

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

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: tempostack-traces-reader
rules:
  - apiGroups:
    - 'tempo.grafana.com'
    resources:
    - dev
    - prod
    resourceNames:
    - 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
kind: ClusterRole
name: tempostack-traces-reader
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: system:authenticated

1. Lists the tenants.

2. The **get** value enables the read operation.

3. 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
metadata:
  name: cluster-collector
  namespace: tracing-system
spec:
  mode: deployment
  serviceAccount: otel-collector
  config:
    extensions: |
      bearertokenauth:
        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: bearertokenauth
          headers:
            X-Scope-OrgID: "dev"
  service:
    extensions: [bearertokenauth]
    pipelines:
      traces:
        exporters: [otlp/dev]
```

3.2.2. 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.

3.2.2.1. 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`: 
To enable alerts for a TempoStack instance, set the `spec.observability.metrics.createPrometheusRules` field to `true`:

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

2. To enable alerts for a TempoStack instance, set the `spec.observability.metrics.createPrometheusRules` field to `true`:

```yaml
apiVersion: tempo.grafana.com/v1alpha1
kind: 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.

### 3.2.2.2. 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.
3.3. 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.

3.3.1. Additional resources

- Operator Lifecycle Manager concepts and resources
- Updating installed Operators

3.4. 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.

3.4.1. 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.

3.4.2. 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`:

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

Procedure

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

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

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

   ```shell
   $ 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:

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

3.4.3. Additional resources

- Deleting Operators from a cluster
- Getting started with the OpenShift CLI
4.1. INSTALLING THE DISTRIBUTED TRACING PLATFORM JAEGGER

**IMPORTANT**

The Red Hat OpenShift distributed tracing platform (Jaeger) is a deprecated feature. Deprecated functionality is still included in OpenShift Container Platform and continues to be supported; however, it will be removed in a future release of this product and is not recommended for new deployments.

For the most recent list of major functionality that has been deprecated or removed within OpenShift Container Platform, refer to the *Deprecated and removed features* section of the OpenShift Container Platform release notes.

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.

### 4.1.1. 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 4.15 overview.

- Install OpenShift Container Platform 4.15.
  - Install OpenShift Container Platform 4.15 on AWS
  - Install OpenShift Container Platform 4.15 on user-provisioned AWS
  - Install OpenShift Container Platform 4.15 on bare metal
  - Install OpenShift Container Platform 4.15 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.
4.1.2. 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.

4.1.3. 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.

### 4.1.4. 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.

4.2. CONFIGURING AND DEPLOYING THE DISTRIBUTED TRACING PLATFORM JAEGER

**IMPORTANT**

The Red Hat OpenShift distributed tracing platform (Jaeger) is a deprecated feature. Deprecated functionality is still included in OpenShift Container Platform and continues to be supported; however, it will be removed in a future release of this product and is not recommended for new deployments.

For the most recent list of major functionality that has been deprecated or removed within OpenShift Container Platform, refer to the Deprecated and removed features section of the OpenShift Container Platform release notes.

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**

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

1 Deployment strategy.

**4.2.1. 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®.

### 4.2.2. 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`.

   a. Go to Home → Projects.
   
   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 Details tab, under Provided APIs, the Operator provides a single link.

6. Under Jaeger, click Create Instance.

7. On the Create Jaeger page, to install using the defaults, click Create to create the distributed tracing platform (Jaeger) instance.

8. On the Jaegers page, click the name of the distributed tracing platform (Jaeger) instance, for example, *jaeger-all-in-one-inmemory*.

9. On the Jaeger Details page, click the Resources tab. Wait until the pod has a status of "Running" before continuing.

### 4.2.2.1. 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:

   ```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):

   ```bash
   $ oc create -n tracing-system -f jaeger.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, 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-cdff7897b-qhfdx</td>
<td>2/2</td>
<td>Running</td>
<td>0</td>
<td>24s</td>
</tr>
</tbody>
</table>

4.2.3. 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`.

   a. Navigate to **Home → Projects**.

   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.

### 4.2.3.1. 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:

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>elasticsearch-cdm-jaegersystemjaegerproduction-1-6676cf568gwhlw</td>
<td>2/2</td>
<td>Running</td>
<td>0</td>
<td>10m</td>
</tr>
</tbody>
</table>
4.2.4. 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`.
   - **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 streaming YAML configuration, for example:

   **Example jaeger-streaming.yaml file**

   ```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
   
   | ¹ | 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.

**4.2.4.1. 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:

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

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

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

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

4. Run the following command to deploy Jaeger:

   ```
   $ oc create -n tracing-system -f jaeger-streaming.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, you should see output similar to the following example:

```
NAME                                                                 READY STATUS  RESTARTS AGE
elasticsearch-cdm-jaegersystemjaegerstreaming-1-697b66d6f6cztccn   2/2     Running   0 5m40s
elasticsearch-cdm-jaegersystemjaegerstreaming-2-5f4b95c789gckz      2/2     Running   0 5m37s
elasticsearch-cdm-jaegersystemjaegerstreaming-3-7b6d964576nnznz97   2/2     Running   0 5m5s
jaeger-streaming-collector-6f6db799f-rtcfm                         1/1     Running   0 80s
jaeger-streaming-entity-operator-6b6d67cc99-4lm9q                  3/3     Running   2 2m18s
jaeger-streaming-ingester-7d479847f8-5h8kc                        1/1     Running   0 80s
jaeger-streaming-kafka-0                                           2/2     Running   0 3m1s
jaeger-streaming-query-65b5bb854-ncnc7                             3/3     Running   0 80s
jaeger-streaming-zookeeper-0                                        2/2     Running   0 3m39s
```
4.2.5. Validating your deployment

4.2.5.1. 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 JAEGGER_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.

4.2.6. Customizing your deployment

```bash
$ oc login --username=<NAMEOFUSER> https://<HOSTNAME>:6443
$ export JAEGER_URL=$(oc get route -n tracing-system jaeger -o jsonpath='{.spec.host}')
```
4.2.6.1. 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.

4.2.6.2. 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 4.1. Jaeger 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>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>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>
<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 <strong>spec</strong> node. When the definition relates to an individual component, it is placed under the <strong>spec/&lt;component&gt;</strong> 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>
</tbody>
</table>
## allInOne

Because the **allInOne** image deploys the Agent, Collector, Query, Ingester, and Jaeger UI in a single pod, configuration for this deployment must nest component configuration under the **allInOne** parameter.

### agent:
Configuration options that define the Agent.

### collector:
Configuration options that define the Jaeger Collector.

### sampling:
Configuration options that define the sampling strategies for tracing.

### 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>allInOne:</td>
<td>Because the <strong>allInOne</strong> image deploys the Agent, Collector, Query, Ingester, and Jaeger UI in a single pod, configuration for this deployment must nest component configuration under the <strong>allInOne</strong> parameter.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
kind: Jaeger
metadata:
  name: jaeger-all-in-one-inmemory
```
4.2.6.3. 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 4.2. Parameters used by the Operator to define the Jaeger Collector |
|-------------------------------------------------|------------------|------------------|
| Parameter                                      | Description           | Values          |
| collector:                                      | Specifies the number of Collector replicas to create. | Integer, for example, 5 |
| replicas:                                      |                                |                |

<p>| Table 4.3. Configuration parameters passed to the Collector |
|-------------------------------------------------|------------------|------------------|
| Parameter                                      | Description           | Values          |
| spec:                                          | Configuration options that define the Jaeger Collector. |                |
| collector:                                     |                                |                |
| options:                                       |                                |                |
| num-workers:                                   | The number of workers pulling from the queue. | Integer, for example, 50 |
| options:                                       |                                |                |
| collector:                                     |                                |                |
| queue-size:                                    | The size of the Collector queue. | Integer, for example, 2000 |
| options:                                       |                                |                |
| kafka:                                         | The <strong>topic</strong> parameter identifies the Kafka configuration used by the Collector to produce the messages, and the Ingester to consume the messages. | Label for the producer. |
| producer:                                      |                                |                |
| topic: jaeger-spans                            |                                |                |
| options:                                       |                                |                |
| kafka:                                         | 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. |                |
| producer:                                      |                                |                |
| brokers:                                       |                                |                |
| my-cluster-kafka-brokers.kafka:9092             |                                |                |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>log-level:</td>
<td>Logging level for the Collector.</td>
<td>Possible values: <strong>debug, info, warn, error, fatal, panic</strong>.</td>
</tr>
<tr>
<td>otlp: enabled: true</td>
<td>To accept OTLP/gRPC, explicitly enable the <strong>otlp</strong>. All the other options are optional.</td>
<td></td>
</tr>
<tr>
<td>grpc: host-port: 4317</td>
<td></td>
<td></td>
</tr>
<tr>
<td>max-connection-age: 0s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>max-connection-age-grace: 0s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>max-message-size: 4194304</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tls: enabled: false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cert: /path/to/cert.crt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cipher-suites: &quot;TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>client-ca: /path/to/cert.ca</td>
<td></td>
<td></td>
</tr>
<tr>
<td>reload-interval: 0s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>min-version: 1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>max-version: 1.3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
options:
  otlp:
    enabled: true
  http:
    cors:
      allowed-headers:
        [<header-name>, [ <header-name> ]]
      allowed-origins: *
      host-port: 4318
      max-connection-age: 0s
      max-connection-age-grace: 0s
      max-message-size: 4194304
      read-timeout: 0s
      read-header-timeout: 2s
      idle-timeout: 0s
      tls:
        enabled: false
        cert: /path/to/cert.crt
        cipher-suites:
        "TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256"
        client-ca:
        /path/to/cert.ca
        reload-interval: 0s
        min-version: 1.2
        max-version: 1.3

To accept OTLP/HTTP, explicitly enable the **otlp**. All the other options are optional.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.6.4. Distributed tracing sampling configuration options</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>While all traces are generated, only a few are sampled. Sampling a trace marks the trace for further processing and storage.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
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 4.4. Jaeger sampling options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec:</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>sampling:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>options: {}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default_strategy:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>service_strategy:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>type:</td>
<td>Sampling strategy to use. See descriptions above.</td>
<td>Valid values are probabilistic, and ratelimiting.</td>
<td>probabilistic</td>
</tr>
<tr>
<td>service_strategy:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>type:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default_strategy:</td>
<td>Parameters for the selected sampling strategy.</td>
<td>Decimal and integer values (0, 1, 10)</td>
<td>1</td>
</tr>
<tr>
<td>param:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>service_strategy:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>param:</td>
<td></td>
<td></td>
<td></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
```

CHAPTER 4. DISTRIBUTED TRACING PLATFORM (JAEGER)
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
```

### 4.2.6.5. 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 4.5. 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></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>storage:</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>type:</code></td>
<td>Type of storage to use for the deployment.</td>
<td><code>memory</code> or <code>elasticsearch</code>. 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><code>memory</code></td>
</tr>
</tbody>
</table>
### Table 4.6. 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>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>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>

#### 4.2.6.5.1. 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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>elasticsearch: properties: doNotProvision:</code></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><code>elasticsearch: properties: name:</code></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><code>string</code></td>
<td><code>elasticsearch</code></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>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>nodeCount:</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>resources:</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></td>
</tr>
<tr>
<td>requests:</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>cpu:</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>
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
      storage: persistent
```
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.

4.2.6.5.2. 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 4.8. General ES configuration parameters**

```yaml
storageClassName: gp2
size: 5Gi
resources:
  requests:
    cpu: 200m
    memory: 4Gi
  limits:
    memory: 4Gi
redundancyPolicy: ZeroRedundancy
```
<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 \texttt{es.max-doc-count} and \texttt{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>\textbf{[Deprecated – Will be removed in a future release, use } \texttt{es.max-doc-count} \textbf{instead.] } The maximum number of spans to fetch at a time, per query, in Elasticsearch. If you set both \texttt{es.max-num-spans} and \texttt{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>\texttt{true/false}</td>
<td>\texttt{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>\texttt{true/false}</td>
<td>\texttt{false}</td>
</tr>
</tbody>
</table>
### Table 4.9. 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: num-replicas</td>
<td>The number of replicas per index in Elasticsearch.</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>es: num-shards</td>
<td>The number of shards per index in Elasticsearch.</td>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>

### Table 4.10. 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: create-index-templates</td>
<td>Automatically create index templates at application startup when set to true. When templates are installed manually, set to false.</td>
<td>true/false</td>
<td>true</td>
</tr>
</tbody>
</table>
Optional prefix for distributed tracing platform (Jaeger) indices. For example, setting this to "production" creates indices named "production-tracing-*".

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>es: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>
</tbody>
</table>

Table 4.11. 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>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>1000</td>
<td></td>
</tr>
<tr>
<td>es:bulk:flush-interval</td>
<td>A time.Duration after which bulk requests are committed, regardless of other thresholds. To disable the bulk processor flush interval, set this to zero.</td>
<td>200ms</td>
<td></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>5000000</td>
<td></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>1</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.12. ES TLS configuration parameters

<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>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: 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 4.13. 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>es-archive: bulk: flush-interval:</td>
<td>A time.Duration 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>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: 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>true/ false</td>
<td>false</td>
</tr>
<tr>
<td>es-archive: enabled:</td>
<td>Enable extra storage.</td>
<td>true/ false</td>
<td>false</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>es-archive: max-num-spans:</td>
<td>[Deprecated - Will be removed in a future release, use <code>es-archive.max-doc-count</code> instead.] The maximum number of spans to fetch at a time, per query, in Elasticsearch.</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-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>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>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: 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>
<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**

apiVersion: jaegertracing.io/v1
kind: Jaeger
metadata:
  name: simple-prod
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:
    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
```

1. URL to Elasticsearch service running in default namespace.
2. TLS configuration. In this case only CA certificate, but it can also contain es.tls.key and es.tls.cert when using mutual TLS.
3. Secret which defines environment variables ES_PASSWORD and ES_USERNAME. Created by

   ```yaml
   # In the spec
   storage:
     type: elasticsearch
     options:
       es:
         index-prefix: my-prefix
         tls:
           ca: /es/certificates/ca.crt
           secretName: tracing-secret
   ```

   ```yaml
   spec:
     storage:
       type: elasticsearch
       options:
         es:
           index-prefix: my-prefix
           tls:
             ca: /es/certificates/ca.crt
             secretName: tracing-secret
   ```
Secret which defines environment variables ES_PASSWORD and ES_USERNAME. Created by kubectl create secret generic tracing-secret --from-literal=ES_PASSWORD=changeme --from-

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

4.2.6.6. 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:
```

OpenShift Container Platform 4.15 Distributed tracing
Prerequisites

- OpenShift Container Platform 4.7
- {logging-title} 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:
  strategy: production
  storage:
    type: elasticsearch
    elasticsearch:
      name: custom-es
      doNotProvision: true
      useCertManagement: true
```

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.

4.2.6.7. Query configuration options

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

Table 4.14. Parameters used by the Red Hat OpenShift distributed tracing platform (Jaeger) Operator to define Query
### 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
```

### 4.2.6.8. 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 4.16. 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>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, 1m0s. Default value is 0.</td>
</tr>
<tr>
<td>options:</td>
<td>The topic 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 consumer. For example, jaeger-spans.</td>
</tr>
<tr>
<td>deadlockInterval:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kafka:</td>
<td>Identifies the Kafka configuration used by the Ingester to consume the messages.</td>
<td>Label for the broker, for example, my-cluster-kafka-brokers.kafka:9092.</td>
</tr>
<tr>
<td>consumer:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>topic:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>brokers:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log-level:</td>
<td>Logging level for the Ingester.</td>
<td>Possible values: debug, info, warn, error, fatal, dpanic, panic.</td>
</tr>
</tbody>
</table>

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:
```

CHAPTER 4. DISTRIBUTED TRACING PLATFORM (JAEGER)
4.2.7. 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.

4.2.7.1. 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

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: myapp
  annotations:
    "sidecar.jaegertracing.io/inject": "true"  
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.

4.2.7.2. 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**

```yaml
apiVersion: apps/v1
kind: StatefulSet
metadata:
  name: example-statefulset
  namespace: example-ns
labels:
  app: example-app
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.
4.3. UPDATING THE DISTRIBUTED TRACING PLATFORM JAEGER

**IMPORTANT**

The Red Hat OpenShift distributed tracing platform (Jaeger) is a deprecated feature. Deprecated functionality is still included in OpenShift Container Platform and continues to be supported; however, it will be removed in a future release of this product and is not recommended for new deployments.

For the most recent list of major functionality that has been deprecated or removed within OpenShift Container Platform, refer to the * Deprecated and removed features* section of the OpenShift Container Platform release notes.

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.

4.3.1. Additional resources

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

4.4. REMOVING THE DISTRIBUTED TRACING PLATFORM JAEGER

**IMPORTANT**

The Red Hat OpenShift distributed tracing platform (Jaeger) is a deprecated feature. Deprecated functionality is still included in OpenShift Container Platform and continues to be supported; however, it will be removed in a future release of this product and is not recommended for new deployments.

For the most recent list of major functionality that has been deprecated or removed within OpenShift Container Platform, refer to the * Deprecated and removed features* section of the OpenShift Container Platform release notes.

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.

4.4.1. 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.

4.4.2. 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**:

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

Procedure

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

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

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

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

   For example,

   ```bash
   $ 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:
4.4.3. 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.