Red Hat OpenStack Platform 17.0

Service Telemetry Framework 1.5

Installing and deploying Service Telemetry Framework 1.5
Installing and deploying Service Telemetry Framework 1.5

OpenStack Team
rhos-docs@redhat.com
Abstract

Install the core components and deploy Service Telemetry Framework 1.5
# Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE .............................................. 4

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION .......................... 5

CHAPTER 1. INTRODUCTION TO SERVICE TELEMETRY FRAMEWORK 1.5 ............ 6
  1.1. SUPPORT FOR SERVICE TELEMETRY FRAMEWORK .......................... 6
  1.2. SERVICE TELEMETRY FRAMEWORK ARCHITECTURE ..................... 6
  1.3. INSTALLATION SIZE OF RED HAT OPENSİFT CONTAINER PLATFORM .... 9

CHAPTER 2. PREPARING YOUR RED HAT OPENSİFT CONTAINER PLATFORM ENVIRONMENT FOR SERVICE TELEMETRY FRAMEWORK ........................ 10
  2.1. OBSERVABILITY STRATEGY IN SERVICE TELEMETRY FRAMEWORK ........ 10
  2.2. PERSISTENT VOLUMES .................................................................. 10
    2.2.1. Ephemeral storage .................................................................. 11
  2.3. RESOURCE ALLOCATION .............................................................. 11
  2.4. NETWORK CONSIDERATIONS FOR SERVICE TELEMETRY FRAMEWORK .. 11

CHAPTER 3. INSTALLING THE CORE COMPONENTS OF SERVICE TELEMETRY FRAMEWORK ................................. 12
  3.1. DEPLOYING SERVICE TELEMETRY FRAMEWORK TO THE RED HAT OPENSİFT CONTAINER PLATFORM ENVIRONMENT ........................................... 12
  3.2. CREATING A SERVICETELEMETRY OBJECT IN RED HAT OPENSİFT CONTAINER PLATFORM ........................... 16
    3.2.1. Primary parameters of the ServiceTelemetry object .................... 19
      The backends parameter .............................................................. 20
      Enabling Prometheus as a storage back end for metrics ............... 20
      Configuring persistent storage for Prometheus .......................... 20
      Enabling Elasticsearch as a storage back end for events ............. 21
      Configuring persistent storage for Elasticsearch ....................... 21
      The clouds parameter .............................................................. 22
      The alerting parameter ............................................................ 23
      The graphing parameter .......................................................... 23
      The highAvailability parameter ............................................... 23
      The transports parameter ....................................................... 23
  3.3. ACCESSING USER INTERFACES FOR STF COMPONENTS ................. 23
  3.4. CONFIGURING AN ALTERNATE OBSERVABILITY STRATEGY .............. 24

CHAPTER 4. CONFIGURING RED HAT OPENSİFT PLATFORM FOR SERVICE TELEMETRY FRAMEWORK .................. 26
  4.1. DEPLOYING RED HAT OPENSİFT PLATFORM OVERCLOUD FOR SERVICE TELEMETRY FRAMEWORK .................. 26
    4.1.1. Getting CA certificate from Service Telemetry Framework for overcloud configuration .................. 27
    4.1.2. Retrieving the AMQ Interconnect route address ....................... 27
    4.1.3. Creating the base configuration for STF ................................. 27
    4.1.4. Configuring the STF connection for the overcloud .................... 29
    4.1.5. Deploying the overcloud ..................................................... 31
    4.1.6. Validating client-side installation ....................................... 32
  4.2. DISABLING RED HAT OPENSİFT PLATFORM SERVICES USED WITH SERVICE TELEMETRY FRAMEWORK ........ 35
  4.3. DEPLOYING TO NON-STANDARD NETWORK TOPOLOGIES ............... 36
  4.4. CONFIGURING MULTIPLE CLOUDS ............................................ 37
    4.4.1. Planning AMQ address prefixes .......................................... 38
    4.4.2. Deploying Smart Gateways ................................................ 38
    4.4.3. Deleting the default Smart Gateways .................................... 41
    4.4.4. Setting a unique cloud domain ........................................... 41
4.4.5. Creating the Red Hat OpenStack Platform environment file for multiple clouds
4.4.5.1. Ansible-based deployment of Service Telemetry Framework
4.4.6. Querying metrics data from multiple clouds

CHAPTER 5. USING OPERATIONAL FEATURES OF SERVICE TELEMETRY FRAMEWORK .................. 47
5.1. DASHBOARDS IN SERVICE TELEMETRY FRAMEWORK ........................................ 47
  5.1.1. Configuring Grafana to host the dashboard ........................................ 48
  5.1.2. Overriding the default Grafana container image ....................................... 49
  5.1.3. Importing dashboards ............................................................................. 50
  5.1.4. Retrieving and setting Grafana login credentials ...................................... 51
5.2. METRICS RETENTION TIME PERIOD IN SERVICE TELEMETRY FRAMEWORK ..... 52
  5.2.1. Editing the metrics retention time period in Service Telemetry Framework ... 52
5.3. ALERTS IN SERVICE TELEMETRY FRAMEWORK .............................................. 53
  5.3.1. Creating an alert rule in Prometheus ...................................................... 53
  5.3.2. Configuring custom alerts ....................................................................... 54
  5.3.3. Creating a standard alert route in Alertmanager ..................................... 55
  5.3.4. Creating an alert route with templating in Alertmanager ...................... 57
5.4. CONFIGURING SNMP TRAPS ............................................................................ 59
5.5. HIGH AVAILABILITY ......................................................................................... 60
  5.5.1. Configuring high availability .................................................................... 60
5.6. EPHEMERAL STORAGE ..................................................................................... 61
  5.6.1. Configuring ephemeral storage ............................................................... 61
5.7. OBSERVABILITY STRATEGY IN SERVICE TELEMETRY FRAMEWORK ................. 62
  5.7.1. Configuring an alternate observability strategy ...................................... 62
5.8. RESOURCE USAGE OF RED HAT OPENSTACK PLATFORM SERVICES ................. 63
  5.8.1. Disabling resource usage monitoring of Red Hat OpenStack Platform services 64
5.9. RED HAT OPENSTACK PLATFORM API STATUS AND CONTAINERIZED SERVICES HEALTH 64
  5.9.1. Disabling container health and API status monitoring ............................ 64

CHAPTER 6. RENEWING THE AMQ INTERCONNECT CERTIFICATE .................. 66
  6.1. CHECKING FOR AN EXPIRED AMQ INTERCONNECT CA CERTIFICATE .......... 66
  6.2. UPDATING THE AMQ INTERCONNECT CA CERTIFICATE ......................... 67

CHAPTER 7. REMOVING SERVICE TELEMETRY FRAMEWORK FROM THE RED HAT OPENSIFT CONTAINER PLATFORM ENVIRONMENT .............................. 68
  7.1. DELETING THE NAMESPACE ....................................................................... 68
  7.2. REMOVING THE CATALOGSOURCE ........................................................... 68
  7.3. REMOVING THE CERT-MANAGER OPERATOR .......................................... 68
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.
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Tell us how we can make it better.

Using the Direct Documentation Feedback (DDF) function

Use the Add Feedback DDF function for direct comments on specific sentences, paragraphs, or code blocks.

1. View the documentation in the Multi-page HTML format.
2. Ensure that you see the Feedback button in the upper right corner of the document.
3. Highlight the part of text that you want to comment on.
4. Click Add Feedback.
5. Complete the Add Feedback field with your comments.
6. Optional: Add your email address so that the documentation team can contact you for clarification on your issue.
7. Click Submit.
CHAPTER 1. INTRODUCTION TO SERVICE TELEMETRY FRAMEWORK 1.5

Service Telemetry Framework (STF) collects monitoring data from Red Hat OpenStack Platform (RHOSP) or third-party nodes. You can use STF to perform the following tasks:

- Store or archive the monitoring data for historical information.
- View the monitoring data graphically on the dashboard.
- Use the monitoring data to trigger alerts or warnings.

The monitoring data can be either metric or event:

**Metric**

A numeric measurement of an application or system.

**Event**

Irregular and discrete occurrences that happen in a system.

The components of STF use a message bus for data transport. Other modular components that receive and store data are deployed as containers on Red Hat OpenShift Container Platform.

**IMPORTANT**

STF is compatible with Red Hat OpenShift Container Platform version 4.10

Additional resources

- For more information about how to deploy Red Hat OpenShift Container Platform, see the Red Hat OpenShift Container Platform product documentation.
- You can install Red Hat OpenShift Container Platform on cloud platforms or on bare metal. For more information about STF performance and scaling, see https://access.redhat.com/articles/4907241.
- You can install Red Hat OpenShift Container Platform on bare metal or other supported cloud platforms. For more information about installing Red Hat OpenShift Container Platform, see OpenShift Container Platform 4.10 Documentation.

1.1. SUPPORT FOR SERVICE TELEMETRY FRAMEWORK

Red Hat supports the two most recent versions of Service Telemetry Framework (STF). Earlier versions are not supported. For more information, see the Service Telemetry Framework Supported Version Matrix.

Red Hat supports the core Operators and workloads, including AMQ Interconnect, Service Telemetry Operator, and Smart Gateway Operator. Red Hat does not support the community Operators or workload components, such as Elasticsearch, Prometheus, Alertmanager, Grafana, and their Operators.

You can only deploy STF in a fully connected network environment. You cannot deploy STF in Red Hat OpenShift Container Platform-disconnected environments or network proxy environments.

1.2. SERVICE TELEMETRY FRAMEWORK ARCHITECTURE
Service Telemetry Framework (STF) uses a client-server architecture, in which Red Hat OpenStack Platform (RHOSP) is the client and Red Hat OpenShift Container Platform is the server.

STF consists of the following components:

- **Data collection**
  - collectd: Collects infrastructure metrics and events.
  - Ceilometer: Collects RHOSP metrics and events.

- **Transport**
  - AMQ Interconnect: An AMQP 1.x compatible messaging bus that provides fast and reliable data transport to transfer the metrics to STF for storage.
  - Smart Gateway: A Golang application that takes metrics and events from the AMQP 1.x bus to deliver to Elasticsearch or Prometheus.

- **Data storage**
  - Prometheus: Time-series data storage that stores STF metrics received from the Smart Gateway.
  - Elasticsearch: Events data storage that stores STF events received from the Smart Gateway.

- **Observation**
  - Alertmanager: An alerting tool that uses Prometheus alert rules to manage alerts.
  - Grafana: A visualization and analytics application that you can use to query, visualize, and explore data.

The following table describes the application of the client and server components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>An AMQP 1.x compatible messaging bus</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Smart Gateway</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Prometheus</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>collectd</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Ceilometer</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>
IMPORTANT

To ensure that the monitoring platform can report operational problems with your cloud, do not install STF on the same infrastructure that you are monitoring.

Figure 1.1. Service Telemetry Framework architecture overview

For client side metrics, collectd provides infrastructure metrics without project data, and Ceilometer provides RHOSP platform data based on projects or user workload. Both Ceilometer and collectd deliver data to Prometheus by using the AMQ Interconnect transport, delivering the data through the message bus. On the server side, a Golang application called the Smart Gateway takes the data stream from the bus and exposes it as a local scrape endpoint for Prometheus.

If you plan to collect and store events, collectd and Ceilometer deliver event data to the server side by using the AMQ Interconnect transport. Another Smart Gateway writes the data to the Elasticsearch datastore.

Server-side STF monitoring infrastructure consists of the following layers:

- Service Telemetry Framework 1.5
- Red Hat OpenShift Container Platform 4.10
- Infrastructure platform
1.3. INSTALLATION SIZE OF RED HAT OPENSSHIFT CONTAINER PLATFORM

The size of your Red Hat OpenShift Container Platform installation depends on the following factors:

- The infrastructure that you select.
- The number of nodes that you want to monitor.
- The number of metrics that you want to collect.
- The resolution of metrics.
- The length of time that you want to store the data.

Installation of Service Telemetry Framework (STF) depends on an existing Red Hat OpenShift Container Platform environment.

For more information about minimum resources requirements when you install Red Hat OpenShift Container Platform on baremetal, see Minimum resource requirements in the Installing a cluster on bare metal guide. For installation requirements of the various public and private cloud platforms that you can install, see the corresponding installation documentation for your cloud platform of choice.
CHAPTER 2. PREPARING YOUR RED HAT OPENSİFT CONTAINER PLATFORM ENVIRONMENT FOR SERVICE TELEMETRY FRAMEWORK

To prepare your Red Hat OpenShift Container Platform environment for Service Telemetry Framework (STF), you must plan for persistent storage, adequate resources, event storage, and network considerations:

- Ensure that you have persistent storage available in your Red Hat OpenShift Container Platform cluster for a production-grade deployment. For more information, see Section 2.2, “Persistent volumes”.

- Ensure that enough resources are available to run the Operators and the application containers. For more information, see Section 2.3, “Resource allocation”.

- Ensure that you have a fully connected network environment. For more information, see Section 2.4, “Network considerations for Service Telemetry Framework”.

2.1. OBSERVABILITY STRATEGY IN SERVICE TELEMETRY FRAMEWORK

Service Telemetry Framework (STF) does not include storage backends and alerting tools. STF uses community operators to deploy Prometheus, Alertmanager, Grafana, and Elasticsearch. STF makes requests to these community operators to create instances of each application configured to work with STF.

Instead of having Service Telemetry Operator create custom resource requests, you can use your own deployments of these applications or other compatible applications, and scrape the metrics Smart Gateways for delivery to your own Prometheus-compatible system for telemetry storage. If you set the observability strategy to use alternative backends instead, persistent or ephemeral storage is not required for STF.

2.2. PERSISTENT VOLUMES

Service Telemetry Framework (STF) uses persistent storage in Red Hat OpenShift Container Platform to request persistent volumes so that Prometheus and Elasticsearch can store metrics and events.

When you enable persistent storage through the Service Telemetry Operator, the Persistent Volume Claims (PVC) requested in an STF deployment results in an access mode of RWO (ReadWriteOnce). If your environment contains pre-provisioned persistent volumes, ensure that volumes of RWO are available in the Red Hat OpenShift Container Platform default configured storageClass.

Additional resources

- For more information about configuring persistent storage for Red Hat OpenShift Container Platform, see Understanding persistent storage.

- For more information about recommended configurable storage technology in Red Hat OpenShift Container Platform, see Recommended configurable storage technology.

- For more information about configuring persistent storage for Prometheus in STF, see the section called “Configuring persistent storage for Prometheus”.

Red Hat OpenStack Platform 17.0 Service Telemetry Framework 1.5
For more information about configuring persistent storage for Elasticsearch in STF, see the section called “Configuring persistent storage for Elasticsearch”.

2.2.1. Ephemeral storage

You can use ephemeral storage to run Service Telemetry Framework (STF) without persistently storing data in your Red Hat OpenShift Container Platform cluster.

**WARNING**

If you use ephemeral storage, you might experience data loss if a pod is restarted, updated, or rescheduled onto another node. Use ephemeral storage only for development or testing, and not production environments.

2.3. RESOURCE ALLOCATION

To enable the scheduling of pods within the Red Hat OpenShift Container Platform infrastructure, you need resources for the components that are running. If you do not allocate enough resources, pods remain in a **Pending** state because they cannot be scheduled.

The amount of resources that you require to run Service Telemetry Framework (STF) depends on your environment and the number of nodes and clouds that you want to monitor.

**Additional resources**

- For recommendations about sizing for metrics collection, see Service Telemetry Framework Performance and Scaling.
- For information about sizing requirements for Elasticsearch, see https://www.elastic.co/guide/en/cloud-on-k8s/current/k8s-managing-compute-resources.html.

2.4. NETWORK CONSIDERATIONS FOR SERVICE TELEMETRY FRAMEWORK

You can only deploy Service Telemetry Framework (STF) in a fully connected network environment. You cannot deploy STF in Red Hat OpenShift Container Platform-disconnected environments or network proxy environments.
CHAPTER 3. INSTALLING THE CORE COMPONENTS OF SERVICE TELEMETRY FRAMEWORK

You can use Operators to load the Service Telemetry Framework (STF) components and objects. Operators manage each of the following STF core and community components:

- cert-manager
- AMQ Interconnect
- Smart Gateway
- Prometheus and AlertManager
- Elasticsearch
- Grafana

Prerequisites

- Red Hat OpenShift Container Platform version 4.10 is running.
- You have prepared your Red Hat OpenShift Container Platform environment and ensured that there is persistent storage and enough resources to run the STF components on top of the Red Hat OpenShift Container Platform environment. For more information, see Service Telemetry Framework Performance and Scaling.
- Your environment is fully connected. STF does not work in a Red Hat OpenShift Container Platform disconnected environments or network proxy environments.

IMPORTANT

STF is compatible with Red Hat OpenShift Container Platform version 4.10

Additional resources

- For more information about Operators, see the Understanding Operators guide.

3.1. DEPLOYING SERVICE TELEMETRY FRAMEWORK TO THE RED HAT OPENSSHIFT CONTAINER PLATFORM ENVIRONMENT

Deploy Service Telemetry Framework (STF) to collect, store, and monitor events:

Procedure

1. Create a namespace to contain the STF components, for example, `service-telemetry`:

   ```
   $ oc new-project service-telemetry
   ```

2. Create an OperatorGroup in the namespace so that you can schedule the Operator pods:

   ```
   $ oc create -f - <<EOF
   ```
3. Create a namespace for the cert-manager Operator:

```bash
$ oc create -f - <<EOF
apiVersion: project.openshift.io/v1
kind: Project
metadata:
  name: openshift-cert-manager-operator
spec:
  finalizers:
    - kubernetes
EOF
```

4. Create an OperatorGroup for the cert-manager Operator:

```bash
$ oc create -f - <<EOF
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: openshift-cert-manager-operator
namespace: openshift-cert-manager-operator
spec: {}
EOF
```

5. Subscribe to the cert-manager Operator by using the redhat-operators CatalogSource:

```bash
$ oc create -f - <<EOF
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: openshift-cert-manager-operator
namespace: openshift-cert-manager-operator
spec:
  channel: tech-preview
  installPlanApproval: Automatic
  name: openshift-cert-manager-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
EOF
```

6. Validate your ClusterServiceVersion. Ensure that cert-manager Operator displays a phase of **Succeeded**:

```
$ oc get csv --namespace openshift-cert-manager-operator --
```
7. Subscribe to the AMQ Interconnect Operator by using the redhat-operators CatalogSource:

```$ oc create -f - <<EOF
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: amq7-interconnect-operator
  namespace: service-telemetry
spec:
  channel: 1.10.x
  installPlanApproval: Automatic
  name: amq7-interconnect-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
EOF```

8. Validate your ClusterServiceVersion. Ensure that amq7-interconnect-operator.v1.10.10 displays a phase of **Succeeded**:

```$ oc get csv --selector=operators.coreos.com/amq7-interconnect-operator.service-telemetry
NAME                                 DISPLAY                                  VERSION   REPLACES     PHASE
amq7-interconnect-operator.v1.10.10  Red Hat Integration - AMQ Interconnect   1.10.10
amq7-interconnect-operator.v1.10.4   Succeeded```

9. Enable the OperatorHub.io Community Catalog Source to install data storage and visualization Operators:

```$ oc create -f - <<EOF
apiVersion: operators.coreos.com/v1alpha1
kind: CatalogSource
metadata:
  name: operatorhubio-operators
EOF```

**WARNING**

Red Hat supports the core Operators and workloads, including AMQ Interconnect, Service Telemetry Operator, and Smart Gateway Operator. Red Hat does not support the community Operators or workload components, inclusive of Elasticsearch, Prometheus, Alertmanager, Grafana, and their Operators.
If you plan to store metrics in Prometheus, you must enable the Prometheus Operator. To enable the Prometheus Operator, create the following manifest in your Red Hat OpenShift Container Platform environment:

```
namespace: openshift-marketplace
spec:
  sourceType: grpc
  image: quay.io/operatorhubio/catalog:latest
  displayName: OperatorHub.io Operators
  publisher: OperatorHub.io
EOF
```

$ oc create -f - <<EOF
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: prometheus
  namespace: service-telemetry
spec:
  channel: beta
  installPlanApproval: Automatic
  name: prometheus
  source: operatorhubio-operators
  sourceNamespace: openshift-marketplace
EOF

$ oc get csv --selector=operators.coreos.com/prometheus.service-telemetry

<table>
<thead>
<tr>
<th>NAME</th>
<th>DISPLAY</th>
<th>VERSION</th>
<th>REPLACES</th>
<th>PHASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>prometheusoperator.0.47.0</td>
<td>Prometheus Operator</td>
<td>0.47.0</td>
<td>prometheusoperator.0.37.0</td>
<td>Succeeded</td>
</tr>
</tbody>
</table>

If you plan to store events in Elasticsearch, you must enable the Elastic Cloud on Kubernetes (ECK) Operator. To enable the ECK Operator, create the following manifest in your Red Hat OpenShift Container Platform environment:

```
namespace: openshift-marketplace
spec:
  sourceType: grpc
  image: quay.io/operatorhubio/catalog:latest
  displayName: OperatorHub.io Operators
  publisher: OperatorHub.io
EOF
```

$ oc create -f - <<EOF
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: elasticsearch-eck-operator-certified
  namespace: service-telemetry
spec:
  channel: stable
  installPlanApproval: Automatic
  name: elasticsearch-eck-operator-certified
  source: certified-operators
  sourceNamespace: openshift-marketplace
EOF

$ oc get csv --selector=operators.coreos.com/elasticsearch-eck-operator-certified.service-telemetry

<table>
<thead>
<tr>
<th>NAME</th>
<th>DISPLAY</th>
<th>VERSION</th>
<th>REPLACES</th>
<th>PHASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>elasticsearch-eck-operator-certified.0.1.0</td>
<td>Elastic Cloud on Kubernetes Operator</td>
<td>0.1.0</td>
<td>elasticsearch-eck-operator-certified.0.0.0</td>
<td>Succeeded</td>
</tr>
</tbody>
</table>

10. Verify that the ClusterServiceVersion for Prometheus **Succeeded**:

11. Verify that the ClusterServiceVersion for Elastic Cloud on Kubernetes **Succeeded**:

12. If you plan to store events in Elasticsearch, you must enable the Elastic Cloud on Kubernetes (ECK) Operator. To enable the ECK Operator, create the following manifest in your Red Hat OpenShift Container Platform environment:

```
namespace: openshift-marketplace
spec:
  sourceType: grpc
  image: quay.io/operatorhubio/catalog:latest
  displayName: OperatorHub.io Operators
  publisher: OperatorHub.io
EOF
```

$ oc create -f - <<EOF
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: elasticsearch-eck-operator-certified
  namespace: service-telemetry
spec:
  channel: stable
  installPlanApproval: Automatic
  name: elasticsearch-eck-operator-certified
  source: certified-operators
  sourceNamespace: openshift-marketplace
EOF

$ oc get csv --selector=operators.coreos.com/elasticsearch-eck-operator-certified.service-telemetry

<table>
<thead>
<tr>
<th>NAME</th>
<th>DISPLAY</th>
<th>VERSION</th>
<th>REPLACES</th>
<th>PHASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>elasticsearch-eck-operator-certified.0.1.0</td>
<td>Elastic Cloud on Kubernetes Operator</td>
<td>0.1.0</td>
<td>elasticsearch-eck-operator-certified.0.0.0</td>
<td>Succeeded</td>
</tr>
</tbody>
</table>

13. Verify that the ClusterServiceVersion for Elastic Cloud on Kubernetes **Succeeded**:
14. Create the Service Telemetry Operator subscription to manage the STF instances:

```
$ oc create -f - <<EOF
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: service-telemetry-operator
  namespace: service-telemetry
spec:
  channel: stable-1.5
  installPlanApproval: Automatic
  name: service-telemetry-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
EOF
```

15. Validate the Service Telemetry Operator and the dependent operators:

```
$ oc get csv --namespace service-telemetry
```

### 3.2. CREATING A SERVICETELEMETRY OBJECT IN RED HAT OPENSIFT CONTAINER PLATFORM

Create a **ServiceTelemetry** object in Red Hat OpenShift Container Platform to result in the Service Telemetry Operator creating the supporting components for a Service Telemetry Framework (STF) deployment. For more information, see **Section 3.2.1, “Primary parameters of the ServiceTelemetry object”**.

**Procedure**
1. To create a `ServiceTelemetry` object that results in an STF deployment that uses the default values, create a `ServiceTelemetry` object with an empty `spec` parameter:

```sh
dir $ oc apply -f - <<EOF
apiVersion: infra.watch/v1beta1
kind: ServiceTelemetry
metadata:
  name: default
  namespace: service-telemetry
spec: {}
EOF
```

To override a default value, define the parameter that you want to override. In this example, enable Elasticsearch by setting `enabled` to `true`:

```sh
dir $ oc apply -f - <<EOF
apiVersion: infra.watch/v1beta1
kind: ServiceTelemetry
metadata:
  name: default
  namespace: service-telemetry
spec:
  backends:
    events:
      elasticsearch:
        enabled: true
EOF
```

Creating a `ServiceTelemetry` object with an empty `spec` parameter results in an STF deployment with the following default settings:

```yaml
apiVersion: infra.watch/v1beta1
kind: ServiceTelemetry
metadata:
  name: default
  namespace: service-telemetry
spec:
  alerting:
    alertmanager:
      receivers:
        snmpTraps:
          enabled: false
target: 192.168.24.254
storage:
  persistent:
    pvcStorageRequest: 20G
strategy: persistent
enabled: true
backends:
  events:
    elasticsearch:
      enabled: false
storage:
persistent:
  pvcStorageRequest: 20Gi
```
strategy: persistent
version: 7.16.1
logs:
  loki:
    enabled: false
  flavor: 1x.extra-small
  replicationFactor: 1
storage:
  objectStorageSecret: test
  storageClass: standard
metrics:
  prometheus:
    enabled: true
    scrapeInterval: 10s
storage:
  persistent:
    pvcStorageRequest: 20G
    retention: 24h
    strategy: persistent
clouds:
  - events:
      collectors:
        - collectorType: collectd
debugEnabled: false
        subscriptionAddress: collectd/cloud1-notify
        - collectorType: ceilometer
debugEnabled: false
        subscriptionAddress: anycast/ceilometer/cloud1-event.sample
metrics:
  collectors:
    - collectorType: collectd
debugEnabled: false
    subscriptionAddress: collectd/cloud1-telemetry
    - collectorType: ceilometer
debugEnabled: false
    subscriptionAddress: anycast/ceilometer/cloud1-metering.sample
    - collectorType: sensubility
debugEnabled: false
    subscriptionAddress: sensubility/cloud1-telemetry
name: cloud1
graphing:
  enabled: false
grafana:
  adminPassword: secret
  adminUser: root
  baseImage: docker.io/grafana/grafana:latest
disableSignoutMenu: false
  ingressEnabled: false
highAvailability:
  enabled: false
observabilityStrategy: use_community
transports:
  qdr:
    enabled: true
  web:
    enabled: false
To override these defaults, add the configuration to the `spec` parameter.

2. View the STF deployment logs in the Service Telemetry Operator:

   ```
   $ oc logs --selector name=service-telemetry-operator
   ...
   --------------------------- Ansible Task Status Event StdOut -----------------
   PLAY RECAP *********************************************************************
   localhost                  : ok=90   changed=0    unreachable=0    failed=0    skipped=26
   rescued=0    ignored=0
   $ oc get pods
   NAME                                                      READY   STATUS    RESTARTS   AGE
   alertmanager-default-0                                    2/2     Running   0          17m
   default-cloud1-ceil-meter-smartgateway-6484b98b68-vd48z   2/2     Running   0          17m
   default-cloud1-coll-meter-smartgateway-799f687658-4gxp  2/2     Running   0          17m
   default-cloud1-sens-meter-smartgateway-c7f4f7fc8-c57b4   2/2     Running   0          17m
   default-interconnect-54658f5d4-pzrpt                      1/1     Running   0          17m
   elastic-operator-66b7bc49c4-sxkc2                        1/1     Running   0          52m
   interconnect-operator-69df6b9cb6-7hhp9                    1/1     Running   0          50m
   prometheus-default-0                                      2/2     Running   0          17m
   prometheus-operator-6458b74d86-wbdqp                     1/1     Running   0          51m
   service-telemetry-operator-864646787c-hd9pm               1/1     Running   0          51m
   smart-gateway-operator-79778cf548-mz5z7                   1/1     Running   0          51m
   
   Verification
   
   - To determine that all workloads are operating correctly, view the pods and the status of each pod.

   **NOTE**

   If you set the `backends.events.elasticsearch.enabled` parameter to `true`, the notification Smart Gateways report `Error` and `CrashLoopBackOff` error messages for a period of time before Elasticsearch starts.

3.2.1. Primary parameters of the ServiceTelemetry object

The `ServiceTelemetry` object comprises the following primary configuration parameters:

- alerting
- backends
- clouds
- graphing
- highAvailability
- transports
You can configure each of these configuration parameters to provide different features in an STF deployment.

**IMPORTANT**

Support for `servicetelemetry.infra.watch/v1alpha1` was removed from STF 1.3.

**The backends parameter**

Use the `backends` parameter to control which storage back ends are available for storage of metrics and events, and to control the enablement of Smart Gateways that the `clouds` parameter defines. For more information, see the section called “The clouds parameter”.

Currently, you can use Prometheus as the metrics storage back end and Elasticsearch as the events storage back end.

**Enabling Prometheus as a storage back end for metrics**

To enable Prometheus as a storage back end for metrics, you must configure the `ServiceTelemetry` object.

**Procedure**

- Configure the `ServiceTelemetry` object:

```yaml
apiVersion: infra.watch/v1beta1
kind: ServiceTelemetry
metadata:
  name: default
  namespace: service-telemetry
spec:
  backends:
    metrics:
      prometheus:
        enabled: true
```

**Configuring persistent storage for Prometheus**

Use the additional parameters that are defined in `backends.metrics.prometheus.storage.persistent` to configure persistent storage options for Prometheus, such as storage class and volume size.

Use `storageClass` to define the back end storage class. If you do not set this parameter, the Service Telemetry Operator uses the default storage class for the Red Hat OpenShift Container Platform cluster.

Use the `pvcStorageRequest` parameter to define the minimum required volume size to satisfy the storage request. If volumes are statically defined, it is possible that a volume size larger than requested is used. By default, Service Telemetry Operator requests a volume size of **20G** (20 Gigabytes).

**Procedure**

- List the available storage classes:

  ```
  $ oc get storageclasses
  NAME                 PROVISIONER                RECLAIMPOLICY   VOLUMEBINDINGMODE ALLOWVOLUMEEXPANSION   AGE
  csi-manila-ceph      manila.csi.openstack.org   Delete          Immediate   false       20h
  ```
Configure the `ServiceTelemetry` object:

```yaml
apiVersion: infra.watch/v1beta1
class: ServiceTelemetry
metadata:
  name: default
  namespace: service-telemetry
spec:
  backends:
    metrics:
      prometheus:
        enabled: true
    storage:
      strategy: persistent
      persistent:
        storageClass: standard-csi
        pvcStorageRequest: 50G
```

Enabling Elasticsearch as a storage back end for events

To enable Elasticsearch as a storage back end for events, you must configure the `ServiceTelemetry` object.

Procedure

- Configure the `ServiceTelemetry` object:

  ```yaml
  apiVersion: infra.watch/v1beta1
class: ServiceTelemetry
metadata:
  name: default
  namespace: service-telemetry
spec:
  backends:
    events:
      elasticsearch:
        enabled: true
  ```

Configuring persistent storage for Elasticsearch

Use the additional parameters defined in `backends.events.elasticsearch.storage.persistent` to configure persistent storage options for Elasticsearch, such as storage class and volume size.

Use `storageClass` to define the back end storage class. If you do not set this parameter, the Service Telemetry Operator uses the default storage class for the Red Hat OpenShift Container Platform cluster.

Use the `pvcStorageRequest` parameter to define the minimum required volume size to satisfy the storage request. If volumes are statically defined, it is possible that a volume size larger than requested is used. By default, Service Telemetry Operator requests a volume size of 20Gi (20 Gibibytes).
- List the available storage classes:

```yaml
$ oc get storageclasses
NAME                  PROVISIONER                RECLAIMPOLICY   VOLUMEBINDINGMODE
ALLOWVOLUMEEXPANSION  AGE
csi-manila-ceph        manila.csi.openstack.org Delete Immediate false 20h
standard (default)    kubernetes.io/cinder   Delete   WaitForFirstConsumer true 20h
standard-csi          cinder.csi.openstack.org Delete   WaitForFirstConsumer true 20h
```

- Configure the **ServiceTelemetry** object:

```yaml
apiVersion: infra.watch/v1beta1
kind: ServiceTelemetry
metadata:
  name: default
  namespace: service-telemetry
spec:
  backends:
    events:
      elasticsearch:
        enabled: true
        version: 7.16.1
  storage:
    strategy: persistent
    persistent:
      storageClass: standard-csi
      pvcStorageRequest: 50G
```

**The clouds parameter**

Use the `clouds` parameter to define which Smart Gateway objects deploy, thereby providing the interface for multiple monitored cloud environments to connect to an instance of STF. If a supporting back end is available, then metrics and events Smart Gateways for the default cloud configuration are created. By default, the Service Telemetry Operator creates Smart Gateways for **cloud1**.

You can create a list of cloud objects to control which Smart Gateways are created for the defined clouds. Each cloud consists of data types and collectors. Data types are **metrics** or **events**. Each data type consists of a list of collectors, the message bus subscription address, and a parameter to enable debugging. Available collectors for metrics are **collectd**, **ceilometer**, and **sensubility**. Available collectors for events are **collectd** and **ceilometer**. Ensure that the subscription address for each of these collectors is unique for every cloud, data type, and collector combination.

The default **cloud1** configuration is represented by the following **ServiceTelemetry** object, which provides subscriptions and data storage of metrics and events for collectd, Ceilometer, and Sensubility data collectors for a particular cloud instance:

```yaml
apiVersion: infra.watch/v1beta1
kind: ServiceTelemetry
metadata:
  name: stf-default
  namespace: service-telemetry
spec:
  clouds:
```

Red Hat OpenStack Platform 17.0 Service Telemetry Framework 1.5
Each item of the **clouds** parameter represents a cloud instance. A cloud instance consists of three top-level parameters: **name**, **metrics**, and **events**. The **metrics** and **events** parameters represent the corresponding back end for storage of that data type. The **collectors** parameter specifies a list of objects made up of two required parameters, **collectorType** and **subscriptionAddress**, and these represent an instance of the Smart Gateway. The **collectorType** parameter specifies data collected by either collectd, Ceilometer, or Sensubility. The **subscriptionAddress** parameter provides the AMQ Interconnect address to which a Smart Gateway subscribes.

You can use the optional Boolean parameter **debugEnabled** within the **collectors** parameter to enable additional console debugging in the running Smart Gateway pod.

### Additional resources

- For more information about deleting default Smart Gateways, see Section 4.4.3, “Deleting the default Smart Gateways”.
- For more information about how to configure multiple clouds, see Section 4.4, “Configuring multiple clouds”.

#### The alerting parameter

Use the **alerting** parameter to control creation of an Alertmanager instance and the configuration of the storage back end. By default, **alerting** is enabled. For more information, see Section 5.3, “Alerts in Service Telemetry Framework”.

#### The graphing parameter

Use the **graphing** parameter to control the creation of a Grafana instance. By default, **graphing** is disabled. For more information, see Section 5.1, “Dashboards in Service Telemetry Framework”.

#### The highAvailability parameter

Use the **highAvailability** parameter to control the instantiation of multiple copies of STF components to reduce recovery time of components that fail or are rescheduled. By default, **highAvailability** is disabled. For more information, see Section 5.5, “High availability”.

#### The transports parameter

Use the **transports** parameter to control the enablement of the message bus for a STF deployment. The only transport currently supported is AMQ Interconnect. By default, the **qdr** transport is enabled.

### 3.3. ACCESSING USER INTERFACES FOR STF COMPONENTS

```yaml
- name: cloud1
  metrics:
    collectors:
      - collectorType: collectd
        subscriptionAddress: collectd/telemetry
      - collectorType: ceilometer
        subscriptionAddress: anycast/ceilometer/metering.sample
      - collectorType: sensubility
        subscriptionAddress: sensubility/telemetry
        debugEnabled: false
  events:
    collectors:
      - collectorType: collectd
        subscriptionAddress: collectd/notify
      - collectorType: ceilometer
        subscriptionAddress: anycast/ceilometer/event.sample
```
In Red Hat OpenShift Container Platform, applications are exposed to the external network through a route. For more information about routes, see Configuring ingress cluster traffic.

In Service Telemetry Framework (STF), HTTPS routes are exposed for each service that has a web-based interface. These routes are protected by Red Hat OpenShift Container Platform RBAC and any user that has a ClusterRoleBinding that enables them to view Red Hat OpenShift Container Platform Namespaces can log in. For more information about RBAC, see Using RBAC to define and apply permissions.

Procedure

1. Log in to Red Hat OpenShift Container Platform.
2. Change to the service-telemetry namespace:
   ```bash
   $ oc project service-telemetry
   ```
3. List the available web UI routes in the service-telemetry project:
   ```bash
   $ oc get routes | grep web
   default-alertmanager-proxy   default-alertmanager-proxy-service-telemetry.apps.infra.watch
   default-alertmanager-proxy   web  reencrypt/Redirect   None
   default-prometheus-proxy     default-prometheus-proxy-service-telemetry.apps.infra.watch
   default-prometheus-proxy     web  reencrypt/Redirect   None
   ```
4. In a web browser, navigate to https://<route_address> to access the web interface for the corresponding service.

3.4. CONFIGURING AN ALTERNATE OBSERVABILITY STRATEGY

To configure STF to skip the deployment of storage, visualization, and alerting backends, add observabilityStrategy: none to the ServiceTelemetry spec. In this mode, only AMQ Interconnect routers and metrics Smart Gateways are deployed, and you must configure an external Prometheus-compatible system to collect metrics from the STF Smart Gateways.

**NOTE**

Currently, only metrics are supported when you set observabilityStrategy to none. Events Smart Gateways are not deployed.

Procedure

1. Create a ServiceTelemetry object with the property observabilityStrategy: none in the spec parameter. The manifest shows results in a default deployment of STF that is suitable for receiving telemetry from a single cloud with all metrics collector types.
   ```bash
   $ oc apply -f - <<EOF
   apiVersion: infra.watch/v1beta1
   kind: ServiceTelemetry
   metadata:
     name: default
   namespace: service-telemetry
   EOF
   ```
spec:
  observabilityStrategy: none
EOF

2. To verify that all workloads are operating correctly, view the pods and the status of each pod:

```
$ oc get pods
NAME                                                      READY   STATUS    RESTARTS   AGE
default-cloud1-ceil-meter-smartgateway-59c845d65b-gzhcs   3/3     Running   0          132m
default-cloud1-coll-meter-smartgateway-75bbd948b9-d5phm   3/3     Running   0          132m
default-cloud1-sens-meter-smartgateway-7fddb57b6d-dh2g9   3/3     Running   0          132m
default-interconnect-668d5bbcd6-57b2l                   1/1     Running   0          132m
interconnect-operator-b8f5bb647-tlp5t                   1/1     Running   0          47h
service-telemetry-operator-566b9dd695-wkvjq              1/1     Running   0          156m
smart-gateway-operator-58d77dcf7-6xsq7                   1/1     Running   0          47h
```

Additional resources

For more information about configuring additional clouds or to change the set of supported collectors, see Section 4.4.2, "Deploying Smart Gateways"
CHAPTER 4. CONFIGURING RED HAT OPENSTACK PLATFORM FOR SERVICE TELEMETRY FRAMEWORK

To collect metrics, events, or both, and to send them to the Service Telemetry Framework (STF) storage domain, you must configure the Red Hat OpenStack Platform (RHOSP) overcloud to enable data collection and transport.

STF can support both single and multiple clouds. The default configuration in RHOSP and STF set up for a single cloud installation.

- For a single RHOSP overcloud deployment with default configuration, see Section 4.1, "Deploying Red Hat OpenStack Platform overcloud for Service Telemetry Framework".
- To plan your RHOSP installation and configuration STF for multiple clouds, see Section 4.4, "Configuring multiple clouds".
- As part of an RHOSP overcloud deployment, you might need to configure additional features in your environment:
  - To deploy data collection and transport to STF on RHOSP cloud nodes that employ routed L3 domains, such as distributed compute node (DCN) or spine-leaf, see Section 4.3, "Deploying to non-standard network topologies".
  - To disable the data collector services, see Section 4.2, "Disabling Red Hat OpenStack Platform services used with Service Telemetry Framework".

4.1. DEPLOYING RED HAT OPENSTACK PLATFORM OVERCLOUD FOR SERVICE TELEMETRY FRAMEWORK

As part of the Red Hat OpenStack Platform (RHOSP) overcloud deployment, you must configure the data collectors and the data transport to Service Telemetry Framework (STF).

Procedure

1. Section 4.1.1, "Getting CA certificate from Service Telemetry Framework for overcloud configuration"

2. Retrieving the AMQ Interconnect route address

3. Creating the base configuration for STF

4. Configuring the STF connection for the overcloud

5. Deploying the overcloud

6. Validating client-side installation

Additional resources

- To collect data through AMQ Interconnect, see the amqp1 plug-in.
4.1.1. Getting CA certificate from Service Telemetry Framework for overcloud configuration

To connect your Red Hat OpenStack Platform overcloud to Service Telemetry Framework (STF), retrieve the CA certificate of AMQ Interconnect that runs within Service Telemetry Framework and use the certificate in the Red Hat OpenStack Platform configuration.

Procedure

1. View a list of available certificates in Service Telemetry Framework:

   $ oc get secrets

2. Retrieve and note the content of the `default-interconnect-selfsigned` Secret:

   $ oc get secret/default-interconnect-selfsigned -o jsonpath='{.data.ca.crt}' | base64 -d

4.1.2. Retrieving the AMQ Interconnect route address

When you configure the Red Hat OpenStack Platform (RHOSP) overcloud for Service Telemetry Framework (STF), you must provide the AMQ Interconnect route address in the STF connection file.

Procedure

1. Log in to your Red Hat OpenShift Container Platform environment.

2. In the `service-telemetry` project, retrieve the AMQ Interconnect route address:

   $ oc get routes -ogo-template="{{ range .items }}{{printf "%s
" .spec.host }}{{ end }}" | grep "-5671"
   default-interconnect-5671-service-telemetry.apps.infra.watch

4.1.3. Creating the base configuration for STF

To configure the base parameters to provide a compatible data collection and transport for Service Telemetry Framework (STF), you must create a file that defines the default data collection values.

Procedure

1. Log in to the Red Hat OpenStack Platform (RHOSP) undercloud as the `stack` user.

2. Create a configuration file called `enable-stf.yaml` in the `/home/stack` directory.
IMPORTANT

Setting `EventPipelinePublishers` and `PipelinePublishers` to empty lists results in no event or metric data passing to RHOSP telemetry components, such as Gnocchi or Panko. If you need to send data to additional pipelines, the Ceilometer polling interval of 30 seconds, as specified in `ExtraConfig`, might overwhelm the RHOSP telemetry components, and you must increase the interval to a larger value, such as 300. Increasing the value to a longer polling interval results in less telemetry resolution in STF.

```
enable-stf.yaml
```

```
parameter_defaults:
  # only send to STF, not other publishers
  EventPipelinePublishers: []
  PipelinePublishers: []

  # manage the polling and pipeline configuration files for Ceilometer agents
  ManagePolling: true
  ManagePipeline: true

  # enable Ceilometer metrics and events
  CeilometerQdrPublishMetrics: true
  CeilometerQdrPublishEvents: true

  # enable collection of API status
  CollectdEnableSensubility: true
  CollectdSensubilityTransport: amqp1

  # enable collection of containerized service metrics
  CollectdEnableLibpodstats: true

  # set collectd overrides for higher telemetry resolution and extra plugins
  # to load
  CollectdConnectionType: amqp1
  CollectdAmqpInterval: 5
  CollectdDefaultPollingInterval: 5
  CollectdExtraPlugins:
    - vmem

  # set standard prefixes for where metrics and events are published to QDR
  MetricsQdrAddresses:
    - prefix: 'collectd'
      distribution: multicast
    - prefix: 'anycast/ceilometer'
      distribution: multicast

  ExtraConfig:
    ceilometer::agent::polling::polling_interval: 30
    ceilometer::agent::polling::polling_meters:
      - cpu
      - disk.*
      - ip.*
      - image.*
      - memory
```
4.1.4. Configuring the STF connection for the overcloud

To configure the Service Telemetry Framework (STF) connection, you must create a file that contains the connection configuration of the AMQ Interconnect for the overcloud to the STF deployment. Enable the collection of events and storage of the events in STF and deploy the overcloud. The default configuration is for a single cloud instance with the default message bus topics. For configuration of multiple cloud deployments, see Section 4.4, “Configuring multiple clouds”.

Prerequisites

- Retrieve the CA certificate from the AMQ Interconnect deployed by STF. For more information, see Section 4.1.1, “Getting CA certificate from Service Telemetry Framework for overcloud configuration”.
- Retrieve the AMQ Interconnect route address. For more information, see Section 4.1.2, “Retrieving the AMQ Interconnect route address”.

Procedure

1. Log in to the RHOSP undercloud as the stack user.
2. Create a configuration file called stf-connectors.yaml in the /home/stack directory.
3. In the stf-connectors.yaml file, configure the MetricsQdrConnectors address to connect the

```yaml
- memory.*
- network.*
- perf.*
- port
- port.*
- switch
- switch.*
- storage.*
- volume.*

# to avoid filling the memory buffers if disconnected from the message bus
# note: this may need an adjustment if there are many metrics to be sent.
collectd::plugin::amqp1::send_queue_limit: 5000

# receive extra information about virtual memory
collectd::plugin::vmem::verbose: true

# provide name and uuid in addition to hostname for better correlation
# to ceilometer data
collectd::plugin::virt::hostname_format: "name uuid hostname"

# provide the human-friendly name of the virtual instance
collectd::plugin::virt::plugin_instance_format: metadata

# set memcached collectd plugin to report its metrics by hostname
# rather than host IP, ensuring metrics in the dashboard remain uniform
collectd::plugin::memcached::instances:
  local:
    host: "%(hiera('fqdn_canonical'))"
    port: 11211
```

29
AMQ Interconnect on the overcloud to the STF deployment. You configure the topic addresses for Sensubility, Ceilometer, and collectd in this file to match the defaults in STF. For more information about customizing topics and cloud configuration, see Section 4.4, “Configuring multiple clouds”.

- The resource_registry configuration directly loads the collectd service because you do not include the collectd-write-qdr.yaml environment file for multiple cloud deployments.

- Replace the host parameter with the value of HOST/PORT that you retrieved in Section 4.1.2, “Retrieving the AMQ Interconnect route address”.

- Replace the caCertFileContent parameter with the contents retrieved in Section 4.1.1, “Getting CA certificate from Service Telemetry Framework for overcloud configuration”.

- Replace the host sub-parameter of MetricsQdrConnectors with the value of HOST/PORT that you retrieved in Section 4.1.2, “Retrieving the AMQ Interconnect route address”.

- Set CeilometerQdrEventsConfig.topic to define the topic for Ceilometer events. The format of this value is anycast/ceilometer/cloud1-event.sample.

- Set CeilometerQdrMetricsConfig.topic to define the topic for Ceilometer metrics. The format of this value is anycast/ceilometer/cloud1-metering.sample.

- Set CollectdAmqpInstances to define the topic for collectd events. The format of this value is collectd/cloud1-notify.

- Set CollectdAmqpInstances to define the topic for collectd metrics. The format of this value is collectd/cloud1-telemetry.

- Set CollectdSensubilityResultsChannel to define the topic for collectd-sensubility events. The format of this value is sensubility/cloud1-telemetry.

stf-connectors.yaml

```yaml
resource_registry:
  OS::TripleO::Services::Collectd: /usr/share/openstack-tripleo-heat-templates/deployment/metrics/collectd-container-puppet.yaml

parameter_defaults:
  MetricsQdrConnectors:
    - host: stf-default-interconnect-5671-service-telemetry.apps.infra.watch
      port: 443
      role: edge
      verifyHostname: false
      sslProfile: sslProfile

  MetricsQdrSSLProfiles:
    - name: sslProfile
      caCertFileContent: |
        -----BEGIN CERTIFICATE-----
        <snip>
        -----END CERTIFICATE-----

  CeilometerQdrEventsConfig:
    driver: amqp
    topic: cloud1-event
```
4.1.5. Deploying the overcloud

Deploy or update the overcloud with the required environment files so that data is collected and transmitted to Service Telemetry Framework (STF).

Procedure

1. Log in to the Red Hat OpenStack Platform (RHOSP) undercloud as the stack user.

2. Source the authentication file:

   ```
   [stack@undercloud-0 ~]$ source stackrc
   (undercloud) [stack@undercloud-0 ~]$
   ```

3. Add the following files to your RHOSP director deployment to configure data collection and AMQ Interconnect:

   - The `ceilometer-write-qdr.yaml` file to ensure that Ceilometer telemetry and events are sent to STF
   - The `qdr-edge-only.yaml` file to ensure that the message bus is enabled and connected to STF message bus routers
   - The `enable-stf.yaml` environment file to ensure defaults are configured correctly
   - The `stf-connectors.yaml` environment file to define the connection to STF

4. Deploy the RHOSP overcloud:

   ```
   (undercloud) [stack@undercloud-0 ~]$ openstack overcloud deploy <other_arguments> 
   --templates /usr/share/openstack-tripleo-heat-templates \\ 
   --environment-file <...other_environment_files...> \\ 
   --environment-file /usr/share/openstack-tripleo-heat-templates/environments/metrics/ceilometer-write-qdr.yaml \\ 
   --environment-file /usr/share/openstack-tripleo-heat-templates/environments/metrics/qdr-edge-only.yaml \\ 
   --environment-file /home/stack/enable-stf.yaml \\ 
   --environment-file /home/stack/stf-connectors.yaml
   ```
4.1.6. Validating client-side installation

To validate data collection from the Service Telemetry Framework (STF) storage domain, query the data sources for delivered data. To validate individual nodes in the Red Hat OpenStack Platform (RHOSP) deployment, use SSH to connect to the console.

**TIP**

Some telemetry data is available only when RHOSP has active workloads.

**Procedure**

1. Log in to an overcloud node, for example, controller-0.

2. Ensure that the `metrics_qdr` container is running on the node:

   ```
   $ sudo podman container inspect --format '{{.State.Status}}' metrics_qdr
   running
   
   $ sudo podman exec -it metrics_qdr cat /etc/qpid-dispatch/qdrouterd.conf
   ```

3. Return the internal network address on which AMQ Interconnect is running, for example, **172.17.1.44** listening on port **5666**:

   ```
   $ sudo podman exec -it metrics_qdr qdstat --bus=172.17.1.44:5666 --connections
   ```

4. Return a list of connections to the local AMQ Interconnect:

   ```
   $ sudo podman exec -it metrics_qdr qdstat --bus=172.17.1.44:5666 --connections
   ```

<table>
<thead>
<tr>
<th>id</th>
<th>host</th>
<th>container</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>role dir security</td>
<td>authentication tenant</td>
</tr>
<tr>
<td>1</td>
<td>default-interconnect-5671-service-telemetry.apps.infra.watch:443</td>
<td>default-interconnect-7458fd4d69-bgzf</td>
</tr>
<tr>
<td></td>
<td>TLSv1.2(DHE-RSA-AES256-GCM-SHA384) anonymous-user</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>172.17.1.44:60290</td>
<td>openstack.org/om/container/controller-0/ceilometer-agent-notification/25/5c02cee550f143ec9ea030db5cccb414</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>172.17.1.44:36408</td>
<td>metrics</td>
</tr>
</tbody>
</table>
There are four connections:

- Outbound connection to STF
- Inbound connection from ceilometer
- Inbound connection from collectd
- Inbound connection from our `qdstat` client

The outbound STF connection is provided to the `MetricsQdrConnectors` host parameter and is the route for the STF storage domain. The other hosts are internal network addresses of the client connections to this AMQ Interconnect.

5. To ensure that messages are delivered, list the links, and view the `_edge` address in the `deliv` column for delivery of messages:

```
$ sudo podman exec -it metrics_qdr qdstat --bus=172.17.1.44:5666 --links
```

<table>
<thead>
<tr>
<th>Router Links</th>
<th>Type</th>
<th>Dir</th>
<th>Conn ID</th>
<th>ID</th>
<th>Peer</th>
<th>Class</th>
<th>Addr</th>
<th>Phs</th>
<th>Cap</th>
<th>Pri</th>
<th>Undel</th>
<th>Unsett</th>
<th>Deliv</th>
<th>Presett</th>
<th>Psdrop</th>
<th>Acc</th>
<th>Rej</th>
<th>Rel</th>
<th>Mod</th>
<th>Delay</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. To list the addresses from RHOSP nodes to STF, connect to Red Hat OpenShift Container Platform to retrieve the AMQ Interconnect pod name and list the connections. List the available AMQ Interconnect pods:

```
$ oc get pods -l application=default-interconnect
```
Connect to the pod and list the known connections. In this example, there are three edge connections from the RHOSP nodes with connection id 22, 23, and 24:

```bash
$ oc exec -it default-interconnect-7458fd4d69-bgzfb -- qdstat --connections
```

2020-04-21 18:25:47.243852 UTC
default-interconnect-7458fd4d69-bgzfb

Connections

<table>
<thead>
<tr>
<th>id</th>
<th>host</th>
<th>container</th>
<th>role</th>
<th>dir</th>
<th>security</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>10.129.0.110:48498</td>
<td>bridge-3f5</td>
<td>edge</td>
<td>in</td>
<td>no-security</td>
</tr>
<tr>
<td></td>
<td>anonymous-user</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>000:00:00:02 000:17:36:29</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>10.129.0.111:43254</td>
<td>rcv[default-cloud1-ceil-meter-smartgateway-58f885c76d-xmxwn]</td>
<td>edge</td>
<td>in</td>
<td>no-security</td>
</tr>
<tr>
<td></td>
<td>anonymous-user</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>000:00:00:02 000:17:36:20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>10.130.0.109:50518</td>
<td>rcv[default-cloud1-coll-event-smartgateway-58fbbd4485-rl9bd]</td>
<td>normal</td>
<td>in</td>
<td>no-security</td>
</tr>
<tr>
<td></td>
<td>anonymous-user</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>000:17:36:11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>10.130.0.110:33802</td>
<td>rcv[default-cloud1-ceil-event-smartgateway-6cfb65478c-g5q82]</td>
<td>normal</td>
<td>in</td>
<td>no-security</td>
</tr>
<tr>
<td></td>
<td>anonymous-user</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>10.128.0.1:51948</td>
<td>Router.ceph-0.redhat.local</td>
<td>edge</td>
<td>in</td>
<td>TLSv1/SSLv3(DHE-RSA-AES256-GCM-SHA384) anonymous-user</td>
</tr>
<tr>
<td></td>
<td>anonymous-user</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>000:00:00:03 000:22:08:43</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>10.128.0.1:51950</td>
<td>Router.compute-0.redhat.local</td>
<td>edge</td>
<td>in</td>
<td>TLSv1/SSLv3(DHE-RSA-AES256-GCM-SHA384) anonymous-user</td>
</tr>
<tr>
<td></td>
<td>anonymous-user</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>000:00:00:03 000:22:08:43</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>10.128.0.1:52082</td>
<td>Router.controller-0.redhat.local</td>
<td>edge</td>
<td>in</td>
<td>TLSv1/SSLv3(DHE-RSA-AES256-GCM-SHA384) anonymous-user</td>
</tr>
<tr>
<td></td>
<td>anonymous-user</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>000:00:00:00 000:22:08:34</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>127.0.0.1:42202</td>
<td>c2f541c1-4c97-4b37-a189-a396c08fb079</td>
<td>normal</td>
<td>in</td>
<td>no-security</td>
</tr>
<tr>
<td></td>
<td>anonymous-user</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>000:00:00:00 000:00:00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8. To view the number of messages delivered by the network, use each address with the `oc exec` command:

```bash
$ oc exec -it default-interconnect-7458fd4d69-bgzfb -- qdstat --address
```

2020-04-21 18:20:10.293258 UTC
default-interconnect-7458fd4d69-bgzfb

Router Addresses

<table>
<thead>
<tr>
<th>class</th>
<th>addr</th>
<th>phs</th>
<th>distrib</th>
<th>pri</th>
<th>local</th>
<th>remote</th>
<th>in</th>
<th>out</th>
<th>thru</th>
<th>fallback</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mobile anycast/ceilometer/event.sample</td>
<td>0</td>
<td>balanced</td>
<td>-</td>
<td>1</td>
<td>0</td>
<td>970</td>
<td>970</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
4.2. DISABLING RED HAT OPENSTACK PLATFORM SERVICES USED WITH SERVICE TELEMETRY FRAMEWORK

Disable the services used when deploying Red Hat OpenStack Platform (RHOSP) and connecting it to Service Telemetry Framework (STF). There is no removal of logs or generated configuration files as part of the disablement of the services.

Procedure

1. Log in to the RHOSP undercloud as the stack user.
2. Source the authentication file:
   ```bash
   [stack@undercloud-0 ~]$ source stackrc
   (undercloud) [stack@undercloud-0 ~]$ 
   ```
3. Create the `disable-stf.yaml` environment file:
   ```bash
   (undercloud) [stack@undercloud-0]$ cat > $HOME/disable-stf.yaml <<EOF
   ---
   resource_registry:
   OS::TripleO::Services::CeilometerAgentCentral: OS::Heat::None
   OS::TripleO::Services::CeilometerAgentNotification: OS::Heat::None
   OS::TripleO::Services::CeilometerAgentIpmi: OS::Heat::None
   OS::TripleO::Services::ComputeCeilometerAgent: OS::Heat::None
   OS::TripleO::Services::Redis: OS::Heat::None
   OS::TripleO::Services::Collectd: OS::Heat::None
   OS::TripleO::Services::MetricsQdr: OS::Heat::None
   EOF
   ```
4. Remove the following files from your RHOSP director deployment:
   - `ceilometer-write-qdr.yaml`
   - `qdr-edge-only.yaml`
   - `enable-stf.yaml`
   - `stf-connectors.yaml`
5. Update the RHOSP overcloud. Ensure that you use the `disable-stf.yaml` file early in the list of environment files. By adding `disable-stf.yaml` early in the list, other environment files can override the configuration that would disable the service:
   ```bash
   (undercloud) [stack@undercloud-0 ~]$ openstack overcloud deploy <other_arguments>
   --templates /usr/share/openstack-tripleo-heat-templates \
   --environment-file /home/stack/disable-stf.yaml
   ```
DEPLOYING TO NON-STANDARD NETWORK TOPOLOGIES

If your nodes are on a separate network from the default InternalApi network, you must make configuration adjustments so that AMQ Interconnect can transport data to the Service Telemetry Framework (STF) server instance. This scenario is typical in a spine-leaf or a DCN topology. For more information about DCN configuration, see the Spine Leaf Networking guide.

If you use STF with Red Hat OpenStack Platform (RHOSP) 17.0 and plan to monitor your Ceph, Block, or Object Storage nodes, you must make configuration changes that are similar to the configuration changes that you make to the spine-leaf and DCN network configuration. To monitor Ceph nodes, use the CephStorageExtraConfig parameter to define which network interface to load into the AMQ Interconnect and collectd configuration files.

Similarly, you must specify BlockStorageExtraConfig and ObjectStorageExtraConfig parameters if your environment uses Block and Object Storage roles.

To deploy a spine-leaf topology, you must create roles and networks, then assign those networks to the available roles. When you configure data collection and transport for STF for an RHOSP deployment, the default network for roles is InternalApi. For Ceph, Block and Object storage roles, the default network is Storage. Because a spine-leaf configuration can result in different networks being assigned to different Leaf groupings and those names are typically unique, additional configuration is required in the parameter_defaults section of the RHOSP environment files.

**Procedure**

1. Document which networks are available for each of the Leaf roles. For examples of network name definitions, see Creating a network data file in the Spine Leaf Networking guide. For more information about the creation of the Leaf groupings (roles) and assignment of the networks to those groupings, see Creating a roles data file in the Spine Leaf Networking guide.

2. Add the following configuration example to the ExtraConfig section for each of the leaf roles. In this example, internal_api_subnet is the value defined in the name_lower parameter of your network definition (with _subnet appended to the name for Leaf 0), and is the network to which the ComputeLeaf0 leaf role is connected. In this case, the network identification of 0 corresponds to the Compute role for leaf 0, and represents a value that is different from the default internal API network name.

   For the ComputeLeaf0 leaf role, specify extra configuration to perform a hiera lookup to determine which network interface for a particular network to assign to the collectd AMQP host parameter. Perform the same configuration for the AMQ Interconnect listener address parameter.

   ```
   ComputeLeaf0ExtraConfig:
   tripleo::profile::base::metrics::collectd::amqp_host: "%(hiera('internal_api_subnet'))"
   tripleo::profile::base::metrics::qdr::listener_addr: "%(hiera('internal_api_subnet'))"
   ```

   Additional leaf roles typically replace _subnet with _leafN. N represents a unique identifier for the leaf.
This example configuration is on a CephStorage leaf role:

```
ComputeLeaf1ExtraConfig:
tripleo::profile::base::metrics::collectd::amqp_host: "%(hiera('internal_api_leaf1'))"
tripleo::profile::base::metrics::qdr::listener_addr: "%(hiera('internal_api_leaf1'))"
```

```
CephStorageLeaf0ExtraConfig:
tripleo::profile::base::metrics::collectd::amqp_host: "%(hiera('storage_subnet'))"
tripleo::profile::base::metrics::qdr::listener_addr: "%(hiera('storage_subnet'))"
```

### 4.4. CONFIGURING MULTIPLE CLOUDS

You can configure multiple Red Hat OpenStack Platform (RHOSP) clouds to target a single instance of Service Telemetry Framework (STF). When you configure multiple clouds, every cloud must send metrics and events on their own unique message bus topic. In the STF deployment, Smart Gateway instances listen on these topics to save information to the common data store. Data that is stored by the Smart Gateway in the data storage domain is filtered by using the metadata that each of Smart Gateways creates.

---

**Figure 4.1. Two RHOSP clouds connect to STF**

---

```
To configure the RHOSP overcloud for a multiple cloud scenario, complete the following tasks:

1. Plan the AMQP address prefixes that you want to use for each cloud. For more information, see Section 4.4.1, “Planning AMQP address prefixes”.

2. Deploy metrics and events consumer Smart Gateways for each cloud to listen on the corresponding address prefixes. For more information, see Section 4.4.2, “Deploying Smart Gateways”.

3. Configure each cloud with a unique domain name. For more information, see Section 4.4.4, “Setting a unique cloud domain”.

4. Create the base configuration for STF. For more information, see Section 4.1.3, “Creating the base configuration for STF”.

5. Configure each cloud to send its metrics and events to STF on the correct address. For more information, see Section 4.4.5, “Creating the Red Hat OpenStack Platform environment file for multiple clouds”.

### 4.4.1. Planning AMQP address prefixes

By default, Red Hat OpenStack Platform (RHOSP) nodes receive data through two data collectors; collectd and Ceilometer. The collectd-sensubility plugin requires a unique address. These components send telemetry data or notifications to the respective AMQP addresses, for example, `collectd/telemetry`. STF Smart Gateways listen on those AMQP addresses for data. To support multiple clouds and to identify which cloud generated the monitoring data, configure each cloud to send data to a unique address. Add a cloud identifier prefix to the second part of the address. The following list shows some example addresses and identifiers:

- `collectd/cloud1-telemetry`
- `collectd/cloud1-notify`
- `sensubility/cloud1-telemetry`
- `anycast/ceilometer/cloud1-metering.sample`
- `anycast/ceilometer/cloud1-event.sample`
- `collectd/cloud2-telemetry`
- `collectd/cloud2-notify`
- `sensubility/cloud2-telemetry`
- `anycast/ceilometer/cloud2-metering.sample`
- `anycast/ceilometer/cloud2-event.sample`
- `collectd/us-east-1-telemetry`
- `collectd/us-west-3-telemetry`

### 4.4.2. Deploying Smart Gateways

You must deploy a Smart Gateway for each of the data collection types for each cloud; one for collectd metrics, one for collectd events, one for Ceilometer metrics, one for Ceilometer events, and one for
collectd-sensubility metrics. Configure each of the Smart Gateways to listen on the AMQP address that you define for the corresponding cloud. To define Smart Gateways, configure the `clouds` parameter in the `ServiceTelemetry` manifest.

When you deploy STF for the first time, Smart Gateway manifests are created that define the initial Smart Gateways for a single cloud. When you deploy Smart Gateways for multiple cloud support, you deploy multiple Smart Gateways for each of the data collection types that handle the metrics and the events data for each cloud. The initial Smart Gateways are defined in `cloud1` with the following subscription addresses:

<table>
<thead>
<tr>
<th>collector</th>
<th>type</th>
<th>default subscription address</th>
</tr>
</thead>
<tbody>
<tr>
<td>collectd</td>
<td>metrics</td>
<td>collectd/telemetry</td>
</tr>
<tr>
<td>collectd</td>
<td>events</td>
<td>collectd/notify</td>
</tr>
<tr>
<td>collectd-sensubility</td>
<td>metrics</td>
<td>sensubility/telemetry</td>
</tr>
<tr>
<td>Ceilometer</td>
<td>metrics</td>
<td>anycast/ceilometer/metering.sample</td>
</tr>
<tr>
<td>Ceilometer</td>
<td>events</td>
<td>anycast/ceilometer/event.sample</td>
</tr>
</tbody>
</table>

**Prerequisites**

- You have determined your cloud naming scheme. For more information about determining your naming scheme, see Section 4.4.1, “Planning AMQP address prefixes”.
- You have created your list of clouds objects. For more information about creating the content for the `clouds` parameter, see the section called “The clouds parameter”.

**Procedure**

1. Log in to Red Hat OpenShift Container Platform.
2. Change to the `service-telemetry` namespace:
   ```sql
   $ oc project service-telemetry
   ```
3. Edit the `default` ServiceTelemetry object and add a `clouds` parameter with your configuration:
WARNING

Long cloud names might exceed the maximum pod name of 63 characters. Ensure that the combination of the ServiceTelemetry name default and the clouds.name does not exceed 19 characters. Cloud names cannot contain any special characters, such as -. Limit cloud names to alphanumeric (a-z, 0-9).

Topic addresses have no character limitation and can be different from the clouds.name value.

$ oc edit stf default

```yaml
apiVersion: infra.watch/v1beta1
kind: ServiceTelemetry
metadata:

spec:

clouds:

- name: cloud1
  events:
    collectors:
      - collectorType: collectd
        subscriptionAddress: collectd/cloud1-notify
      - collectorType: ceilometer
        subscriptionAddress: anycast/ceilometer/cloud1-event.sample

metrics:

    collectors:
      - collectorType: collectd
        subscriptionAddress: collectd/cloud1-telemetry
      - collectorType: sensubility
        subscriptionAddress: sensubility/cloud1-telemetry
      - collectorType: ceilometer
        subscriptionAddress: anycast/ceilometer/cloud1-metering.sample

- name: cloud2
  events:
```

4. Save the ServiceTelemetry object.

5. Verify that each Smart Gateway is running. This can take several minutes depending on the number of Smart Gateways:

```
$ oc get po -l app=smart-gateway

NAME                                                      READY   STATUS    RESTARTS   AGE
---                                                      -------- -------- -------- -----
default-cloud1-ceil-event-smartgateway-6cfb65478c-g5q82   2/2     Running   0          13h
default-cloud1-ceil-meter-smartgateway-58f885c76d-xmxwrn   2/2     Running   0          13h
```
4.4.3. Deleting the default Smart Gateways

After you configure Service Telemetry Framework (STF) for multiple clouds, you can delete the default Smart Gateways if they are no longer in use. The Service Telemetry Operator can remove SmartGateway objects that were created but are no longer listed in the ServiceTelemetry clouds list of objects. To enable the removal of SmartGateway objects that are not defined by the clouds parameter, you must set the cloudsRemoveOnMissing parameter to true in the ServiceTelemetry manifest.

TIP

If you do not want to deploy any Smart Gateways, define an empty clouds list by using the clouds: [] parameter.

WARNING

The cloudsRemoveOnMissing parameter is disabled by default. If you enable the cloudsRemoveOnMissing parameter, you remove any manually created SmartGateway objects in the current namespace without any possibility to restore.

Procedure

1. Define your clouds parameter with the list of cloud objects that you want the Service Telemetry Operator to manage. For more information, see the section called “The clouds parameter”.

2. Edit the ServiceTelemetry object and add the cloudsRemoveOnMissing parameter:

```yaml
apiVersion: infra.watch/v1beta1
kind: ServiceTelemetry
metadata:
  ...  
spec:
  ...
  cloudsRemoveOnMissing: true
  clouds:
  ...
```

3. Save the modifications.

4. Verify that the Operator deleted the Smart Gateways. This can take several minutes while the Operators reconcile the changes:

   ```bash
   $ oc get smartgateways
   ```

4.4.4. Setting a unique cloud domain
To ensure that AMQ Interconnect router connections from Red Hat OpenStack Platform (RHOSP) to Service Telemetry Framework (STF) are unique and do not conflict, configure the CloudDomain parameter.

Procedure

1. Create a new environment file, for example, hostnames.yaml.

2. Set the CloudDomain parameter in the environment file, as shown in the following example:

   ```yaml
   CloudDomain: newyork-west-04
   CephStorageHostnameFormat: 'ceph-%index%'
   ObjectStorageHostnameFormat: 'swift-%index%'
   ComputeHostnameFormat: 'compute-%index%'
   ```

3. Add the new environment file to your deployment.

Additional resources

- Section 4.4.5, “Creating the Red Hat OpenStack Platform environment file for multiple clouds”
- Core Overcloud Parameters in the Overcloud Parameters guide

4.4.5. Creating the Red Hat OpenStack Platform environment file for multiple clouds

To label traffic according to the cloud of origin, you must create a configuration with cloud-specific instance names. Create an stf-connectors.yaml file and adjust the values of CeilometerQdrEventsConfig, CeilometerQdrMetricsConfig and CollectdAmqpInstances to match the AMQP address prefix scheme.

NOTE

If you enabled container health and API status monitoring, you must also modify the CollectdSensubilityResultsChannel parameter. For more information, see Section 5.9, “Red Hat OpenStack Platform API status and containerized services health”.

Prerequisites

- You have retrieved the CA certificate from the AMQ Interconnect deployed by STF. For more information, see Section 4.1.1, “Getting CA certificate from Service Telemetry Framework for overcloud configuration”.

- You have created your list of clouds objects. For more information about creating the content for the clouds parameter, see the clouds configuration parameter.

- You have retrieved the AMQ Interconnect route address. For more information, see Section 4.1.2, “Retrieving the AMQ Interconnect route address”.

- You have created the base configuration for STF. For more information, see Section 4.1.3, “Creating the base configuration for STF”.

42
You have created a unique domain name environment file. For more information, see Section 4.4.4, “Setting a unique cloud domain”.

Procedure

1. Log in to the Red Hat OpenStack Platform undercloud as the stack user.
2. Create a configuration file called stf-connectors.yaml in the /home/stack directory.
3. In the stf-connectors.yaml file, configure the MetricsQdrConnectors address to connect to the AMQ interconnect on the overcloud deployment. Configure the CeilometerQdrEventsConfig, CeilometerQdrMetricsConfig, CollectdAmqpInstances, and CollectdSensubilityResultsChannel topic values to match the AMQP address that you want for this cloud deployment.

   - The resource_registry configuration directly loads the collectd service because you do not include the collectd-write-qdr.yaml environment file for multiple cloud deployments.
   - Replace the MetricsQdrConnectors.host parameter with the value of HOST/PORT that you retrieved in Section 4.1.2, “Retrieving the AMQ Interconnect route address”.
   - Replace the caCertFileContent parameter with the contents retrieved in Section 4.1.1, “Getting CA certificate from Service Telemetry Framework for overcloud configuration”.
   - Set the CeilometerQdrEventsConfig.topic to define the topic for Ceilometer events. This value is the address format of anycast/ceilometer/cloud1-event.sample.
   - Set the CeilometerQdrMetricsConfig.topic to define the topic for Ceilometer metrics. This value is the address format of anycast/ceilometer/cloud1-metering.sample.
   - Set the CollectdAmqpInstances to define the topic for collectd events. This value is the format of collectd/cloud1-notify.
   - Set the CollectdAmqpInstances to define the topic for collectd metrics. This value is the format of collectd/cloud1-telemetry.
   - Set the CollectdSensubilityResultsChannel to define the topic for collectd-sensubility events. This value is the format of sensubility/cloud1-telemetry.

```
resource_registry:
    OS::TripleO::Services::Collectd: /usr/share/openstack-tripleo-heat-templates/deployment/metrics/collectd-container-puppet.yaml

parameter_defaults:
    MetricsQdrConnectors:
        - host: stf-default-interconnect-5671-service-telemetry.apps.infra.watch
          port: 443
          role: edge
          verifyHostname: false
          sslProfile: sslProfile

    MetricsQdrSSLProfiles:
        - name: sslProfile
          caCertFileContent: |
```
4. Ensure that the naming convention in the `stf-connectors.yaml` file aligns with the `spec.bridge.amqpUrl` field in the Smart Gateway configuration. For example, configure the `CeilometerQdrEventsConfig.topic` field to a value of `cloud1-event`.

5. Source the authentication file:

   ```bash
   [stack@undercloud-0 ~]$ source stackrc
   (undercloud) [stack@undercloud-0 ~]$ openstack overcloud deploy <other_arguments>
   --templates /usr/share/openstack-tripleo-heat-templates \
   --environment-file <...other_environment_files...>
   --environment-file /usr/share/openstack-tripleo-heat-templates/environments/metrics/ceilometer-write-qdr.yaml
   ```

6. Include the `stf-connectors.yaml` file and unique domain name environment file `hostnames.yaml` in the `openstack overcloud deployment` command, with any other environment files relevant to your environment:

   ```yaml
   CeilometerQdrEventsConfig:
     driver: amqp
     topic: cloud1-event

   CeilometerQdrMetricsConfig:
     driver: amqp
     topic: cloud1-metering

   CollectdAmqpInstances:
     cloud1-notify:
       notify: true
       format: JSON
       presettle: false
     cloud1-telemetry:
       format: JSON
       presettle: false

   CollectdSensubilityResultsChannel: sensubility/cloud1-telemetry
   ```

   **WARNING**

   If you use the `collectd-write-qdr.yaml` file with a custom `CollectdAmqpInstances` parameter, data publishes to the custom and default topics. In a multiple cloud environment, the configuration of the `resource_registry` parameter in the `stf-connectors.yaml` file loads the collectd service.
7. Deploy the Red Hat OpenStack Platform overcloud.

### 4.4.5.1. Ansible-based deployment of Service Telemetry Framework

**WARNING**

The content for this feature is available in this release as a Documentation Preview, and therefore is not fully verified by Red Hat. Use it only for testing, and do not use in a production environment.

As of Red Hat OpenStack Platform 17.0, you can preview the use of Ansible instead of Puppet for deploying Service Telemetry Framework (STF) components. The use of Ansible has the following advantages:

- Consolidation of configuration under a single service-specific THT variable (MetricsQdrVars and CollectdVars)
- The ability to switch QDR modes from mesh-mode to edge-only and back
- Fewer technologies used in the deployment stack, resulting in a simpler debug process

To use the Ansible-based deployment, substitute the word “ansible” in place of “puppet” in the `resource_registry` section of your `stf-connectors.yaml` file:

```bash
--environment-file /usr/share/openstack-tripleo-heat-templates/environments/metrics/qdr-edge-only.yaml \  
--environment-file /home/stack/hostnames.yaml \  
--environment-file /home/stack/enable-stf.yaml \  
--environment-file /home/stack/stf-connectors.yaml
```

To set the configuration, use the new service-specific THT variables, as shown in the following example:

```yaml
parameter_defaults:
  MetricsQdrVars:
    tripleo_metrics_qdr_deployment_mode: edge-only
  CollectdVars:
    tripleo_collectd_amqp_host: stf.mycluster.example.com
```


Additional resources

- For information about how to validate the deployment, see Section 4.1.6, “Validating client-side installation”.

4.4.6. Querying metrics data from multiple clouds

Data stored in Prometheus has a **service** label according to the Smart Gateway it was scraped from. You can use this label to query data from a specific cloud.

To query data from a specific cloud, use a Prometheus **promql** query that matches the associated **service** label; for example: `collectd_uptime{service="default-cloud1-coll-meter"}`.
CHAPTER 5. USING OPERATIONAL FEATURES OF SERVICE TELEMETRY FRAMEWORK

You can use the following operational features to provide additional functionality to the Service Telemetry Framework (STF):

- Configuring dashboards
- Configuring the metrics retention time period
- Configuring alerts
- Configuring SNMP traps
- Configuring high availability
- Configuring ephemeral storage
- Configuring an alternate observability strategy
- Monitoring the resource use of OpenStack services
- Monitoring container health and API status

5.1. DASHBOARDS IN SERVICE TELEMETRY FRAMEWORK

Use the third-party application, Grafana, to visualize system-level metrics that the data collectors collectd and Ceilometer gather for each individual host node.

For more information about configuring data collectors, see Section 4.1, "Deploying Red Hat OpenStack Platform overcloud for Service Telemetry Framework".

You can use dashboards to monitor a cloud:

**Infrastructure dashboard**

Use the infrastructure dashboard to view metrics for a single node at a time. Select a node from the upper left corner of the dashboard.

**Cloud view dashboard**

Use the cloud view dashboard to view panels to monitor service resource usage, API stats, and cloud events. You must enable API health monitoring and service monitoring to provide the data for this dashboard. API health monitoring is enabled by default in the STF base configuration. For more information, see Section 4.1.3, "Creating the base configuration for STF".

- For more information about API health monitoring, see Section 5.9, "Red Hat OpenStack Platform API status and containerized services health".
- For more information about RHOSP service monitoring, see Section 5.8, "Resource usage of Red Hat OpenStack Platform services".

**Virtual machine view dashboard**

Use the virtual machine view dashboard to view panels to monitor virtual machine infrastructure usage. Select a cloud and project from the upper left corner of the dashboard.

**Memcached view dashboard**
Use the memcached view dashboard to view panels to monitor connections, availability, system metrics and cache performance. Select a cloud from the upper left corner of the dashboard.

5.1.1. Configuring Grafana to host the dashboard

Grafana is not included in the default Service Telemetry Framework (STF) deployment so you must deploy the Grafana Operator from OperatorHub.io. When you use the Service Telemetry Operator to deploy Grafana, it results in a Grafana instance and the configuration of the default data sources for the local STF deployment.

Procedure

1. Log in to Red Hat OpenShift Container Platform.

2. Change to the service-telemetry namespace:

   ```
   $ oc project service-telemetry
   ```

3. Deploy the Grafana operator:

   ```
   $ oc apply -f - <<EOF
   apiVersion: operators.coreos.com/v1alpha1
   kind: Subscription
   metadata:
     name: grafana-operator
     namespace: service-telemetry
   spec:
     channel: v4
     installPlanApproval: Automatic
     name: grafana-operator
     source: operatorhubio-operators
     sourceNamespace: openshift-marketplace
   EOF
   ```

4. Verify that the Operator launched successfully. In the command output, if the value of the PHASE column is Succeeded, the Operator launched successfully:

   ```
   $ oc get csv --selector operators.coreos.com/grafana-operator.service-telemetry
   NAME                       DISPLAY            VERSION   REPLACES                   PHASE
   grafana-operator.v4.6.0   Grafana Operator   4.6.0     grafana-operator.v4.5.1   Succeeded
   ```

5. To launch a Grafana instance, create or modify the ServiceTelemetry object. Set graphing.enabled and graphing.grafana.ingressEnabled to true. Optionally, set the value of graphing.grafana.baseImage to the Grafana workload container image that will be deployed:

   ```
   $ oc edit stf default
   ```

   ```yaml
   apiVersion: infra.watch/v1beta1
   kind: ServiceTelemetry
   ... 
   spec: 
     ... 
     graphing:
   ```
6. Verify that the Grafana instance deployed:

   $ oc get pod -l app=grafana

   NAME                                  READY   STATUS    RESTARTS   AGE
   grafana-deployment-7fc7848b56-sbkhv   1/1     Running   0          1m

7. Verify that the Grafana data sources installed correctly:

   $ oc get grafanadatasources

   NAME                AGE
   default-datasources 20h

8. Verify that the Grafana route exists:

   $ oc get route grafana-route

   NAME            HOST/PORT                                          PATH   SERVICES          PORT   TERMINATION   WILDCARD
   grafana-route   grafana-route-service-telemetry.apps.infra.watch          grafana-service 3000   edge          None

5.1.2. Overriding the default Grafana container image

The dashboards in Service Telemetry Framework (STF) require features that are available only in Grafana version 8.1.0 and later. By default, the Service Telemetry Operator installs a compatible version. You can override the base Grafana image by specifying the image path to an image registry with `graphing.grafana.baseImage`.

Procedure

1. Ensure that you have the correct version of Grafana:

   $ oc get pod -l "app=grafana" -o=jsonpath='{.items[0].spec.containers[0].image}''
   docker.io/grafana/grafana:7.3.10

2. If the running image is older than 8.1.0, patch the ServiceTelemetry object to update the image. Service Telemetry Operator updates the Grafana manifest, which restarts the Grafana deployment:

   $ oc patch stf/default --type merge -p "{"spec":{"graphing":{"grafana":{"baseImage":"docker.io/grafana/grafana:8.1.5"}}}"

3. Verify that a new Grafana pod exists and has a STATUS value of Running:
4. Verify that the new instance is running the updated image:

```
$ oc get pod -l "app=grafana" -ojsonpath='{.items[0].spec.containers[0].image}'
docker.io/grafana/grafana:8.1.0
```

5.1.3. Importing dashboards

The Grafana Operator can import and manage dashboards by creating `GrafanaDashboard` objects. You can view example dashboards at [https://github.com/infrawatch/dashboards](https://github.com/infrawatch/dashboards).

**PROCEDURE**

The paths and dashboards names refer to STF 1.3 which is the earliest version of STF the dashboards are compatible and can be used with STF versions 1.3 through 1.5.

1. Import the infrastructure dashboard:

```
grafanadashboard.integreatly.org/rhos-dashboard-1.3 created
```

2. Import the cloud dashboard:

```
grafanadashboard.integreatly.org/rhos-cloud-dashboard-1.3 created
```

**WARNING**

For some panels in the cloud dashboard, you must set the value of the `collectd` `virt` plugin parameter `hostname_format` to `name uuid hostname` in the `stf-connectors.yaml` file. If you do not configure this parameter, affected dashboards remain empty. For more information about the `virt` plugin, see [collectd plugins](https://github.com/infrawatch/dashboards).

3. Import the cloud events dashboard:

```
grafanadashboard.integreatly.org/rhos-cloudevents-dashboard created
```
4. Import the virtual machine dashboard:
   
   ```
   grafanadashboard.integreatly.org/virtual-machine-view-1.3 configured
   ```

5. Import the memcached dashboard:
   
   ```
   grafanadashboard.integreatly.org/memcached-dashboard-1.3 created
   ```

6. Verify that the dashboards are available:
   
   ```
   $ oc get grafanadashboards
   NAME               AGE
   memcached-dashboard-1.3       115s
   rhos-cloud-dashboard-1.3     2m12s
   rhos-cloudevents-dashboard   2m6s
   rhos-dashboard-1.3           2m17s
   virtual-machine-view-1.3     2m
   ```

7. Retrieve the Grafana route address:
   
   ```
   $ oc get route grafana-route -o jsonpath='{.spec.host}'
   grafana-route-service-telemetry.apps.infra.watch
   ```

8. In a web browser, navigate to https://<grafana_route_address>. Replace <grafana_route_address> with the value that you retrieved in the previous step.

9. To view the dashboard, click **Dashboards** and **Manage**.

5.1.4. Retrieving and setting Grafana login credentials

Service Telemetry Framework (STF) sets default login credentials when Grafana is enabled. You can override the credentials in the **ServiceTelemetry** object.

**Procedure**

1. Log in to Red Hat OpenShift Container Platform.

2. Change to the **service-telemetry** namespace:
   
   ```
   $ oc project service-telemetry
   ```

3. Retrieve the default username and password from the STF object:
   
   ```
   $ oc get stf default -o jsonpath="{.spec.graphing.grafana["adminUser","adminPassword"]}
   ```
4. To modify the default values of the Grafana administrator username and password through the ServiceTelemetry object, use the `graphing.grafana.adminUser` and `graphing.grafana.adminPassword` parameters.

5.2. METRICS RETENTION TIME PERIOD IN SERVICE TELEMETRY FRAMEWORK

The default retention time for metrics stored in Service Telemetry Framework (STF) is 24 hours, which provides enough data for trends to develop for the purposes of alerting.

For long-term storage, use systems designed for long-term data retention, for example, Thanos.

Additional resources

- To adjust STF for additional metrics retention time, see Section 5.2.1, “Editing the metrics retention time period in Service Telemetry Framework”.

- For recommendations about Prometheus data storage and estimating storage space, see https://prometheus.io/docs/prometheus/latest/storage/#operational-aspects

- For more information about Thanos, see https://thanos.io/

5.2.1. Editing the metrics retention time period in Service Telemetry Framework

You can adjust Service Telemetry Framework (STF) for additional metrics retention time.

Procedure

1. Log in to Red Hat OpenShift Container Platform.

2. Change to the service-telemetry namespace:

   ```
   $ oc project service-telemetry
   ```

3. Edit the ServiceTelemetry object:

   ```
   $ oc edit stf default
   ```

4. Add retention: 7d to the storage section of backends.metrics.prometheus.storage to increase the retention period to seven days:

   ```
   apiVersion: infradata/v1beta1
   kind: ServiceTelemetry
   metadata:
     name: stf-default
     namespace: service-telemetry
   spec:
   ... 
   ```

   **NOTE**

   If you set a long retention period, retrieving data from heavily populated Prometheus systems can result in queries returning results slowly.
5.3. ALERTS IN SERVICE TELEMETRY FRAMEWORK

You create alert rules in Prometheus and alert routes in Alertmanager. Alert rules in Prometheus servers send alerts to an Alertmanager, which manages the alerts. Alertmanager can silence, inhibit, or aggregate alerts, and send notifications by using email, on-call notification systems, or chat platforms.

To create an alert, complete the following tasks:

1. Create an alert rule in Prometheus. For more information, see Section 5.3.1, "Creating an alert rule in Prometheus".

2. Create an alert route in Alertmanager. There are two ways in which you can create an alert route:

   - Creating a standard alert route in Alertmanager.
   - Creating an alert route with templating in Alertmanager.

Additional resources

For more information about alerts or notifications with Prometheus and Alertmanager, see https://prometheus.io/docs/alerting/overview/

To view an example set of alerts that you can use with Service Telemetry Framework (STF), see https://github.com/infrawatch/service-telemetry-operator/tree/master/deploy/alerts

5.3.1. Creating an alert rule in Prometheus

Prometheus evaluates alert rules to trigger notifications. If the rule condition returns an empty result set, the condition is false. Otherwise, the rule is true and it triggers an alert.

Procedure

1. Log in to Red Hat OpenShift Container Platform.

2. Change to the service-telemetry namespace:

   $ oc project service-telemetry
3. Create a `PrometheusRule` object that contains the alert rule. The Prometheus Operator loads the rule into Prometheus:

```yaml
$ oc apply -f - <<EOF
apiVersion: monitoring.coreos.com/v1
kind: PrometheusRule
metadata:
  creationTimestamp: null
labels:
  prometheus: default
  role: alert-rules
name: prometheus-alarm-rules
namespace: service-telemetry
spec:
groups:
  - name: ./openstack.rules
    rules:
      - alert: Collectd metrics receive rate is zero
        expr: rate(sg_total_collectd_msg_received_count[1m]) == 0
EOF
```

To change the rule, edit the value of the `expr` parameter.

4. To verify that the Operator loaded the rules into Prometheus, run the `curl` command against the default-prometheus-proxy route with basic authentication:

```bash
$ curl -k --user "internal:$(oc get secret default-prometheus-htpasswd -ogo-template='{{ .data.password | base64decode }}')" https://$(oc get route default-prometheus-proxy -ogo-template='{{ .spec.host }}')/api/v1/rules
```

Additional resources

- For more information on alerting, see [https://github.com/coreos/prometheus-operator/blob/master/Documentation/user-guides/alerting.md](https://github.com/coreos/prometheus-operator/blob/master/Documentation/user-guides/alerting.md)

5.3.2. Configuring custom alerts

You can add custom alerts to the `PrometheusRule` object that you created in Section 5.3.1, “Creating an alert rule in Prometheus”.

Procedure

1. Use the `oc edit` command:

   ```bash
   $ oc edit prometheusrules prometheus-alarm-rules
   ```
2. Edit the PrometheusRules manifest.

3. Save and close the manifest.

Additional resources

- For more information about how to configure alerting rules, see https://prometheus.io/docs/prometheus/latest/configuration/alerting_rules/.
- For more information about PrometheusRules objects, see https://github.com/coreos/prometheus-operator/blob/master/Documentation/user-guides/alerting.md

5.3.3. Creating a standard alert route in Alertmanager

Use Alertmanager to deliver alerts to an external system, such as email, IRC, or other notification channel. The Prometheus Operator manages the Alertmanager configuration as a Red Hat OpenShift Container Platform secret. By default, Service Telemetry Framework (STF) deploys a basic configuration that results in no receivers:

```yaml
alertmanager.yaml: |
  global:
    resolve_timeout: 5m
  route:
    group_by: ['job']
    group_wait: 30s
    group_interval: 5m
    repeat_interval: 12h
    receiver: 'null'
  receivers:
    - name: 'null'
```

To deploy a custom Alertmanager route with STF, you must pass an `alertmanagerConfigManifest` parameter to the Service Telemetry Operator that results in an updated secret, managed by the Prometheus Operator.

**NOTE**

If your `alertmanagerConfigManifest` contains a custom template to construct the title and text of the sent alert, deploy the contents of the `alertmanagerConfigManifest` using a base64-encoded configuration. For more information, see Section 5.3.4, “Creating an alert route with templating in Alertmanager”.

Procedure

1. Log in to Red Hat OpenShift Container Platform.

2. Change to the `service-telemetry` namespace:

   $ oc project service-telemetry

3. Edit the ServiceTelemetry object for your STF deployment:
4. Add the new parameter `alertmanagerConfigManifest` and the `Secret` object contents to define the `alertmanager.yaml` configuration for Alertmanager:

    NOTE
    This step loads the default template that the Service Telemetry Operator manages. To verify that the changes are populating correctly, change a value, return the `alertmanager-default` secret, and verify that the new value is loaded into memory. For example, change the value of the parameter `global.resolve_timeout` from 5m to 10m.

    $ oc edit stf default

```yaml
apiVersion: infra.watch/v1beta1
kind: ServiceTelemetry
metadata:
  name: default
  namespace: service-telemetry
spec:
  backends:
    metrics:
      prometheus:
        enabled: true
    alertmanagerConfigManifest:
      apiVersion: v1
      kind: Secret
      metadata:
        name: 'alertmanager-default'
        namespace: 'service-telemetry'
      type: Opaque
      stringData:
        alertmanager.yaml: |
        global:
          resolve_timeout: 10m
        route:
          group_by: ['job']
          group_wait: 30s
          group_interval: 5m
          repeat_interval: 12h
          receiver: 'null'
        receivers:
          - name: 'null'

$ oc get secret alertmanager-default -o go-template=('{{index .data "alertmanager.yaml" | base64decode }}')
```

5. Verify that the configuration has been applied to the secret:

    $ oc get secret alertmanager-default -o go-template=('{{index .data "alertmanager.yaml" | base64decode }}')

    global:
      resolve_timeout: 10m
    route:
      group_by: ['job']
      group_wait: 30s
      group_interval: 5m
6. Run the `curl` command against the `alertmanager-proxy` service to retrieve the status and `configYAML` contents, and verify that the supplied configuration matches the configuration in Alertmanager:

```bash
```

```yaml
{"status":"success","data":{"configYAML":"...","...}}
```

7. Verify that the `configYAML` field contains the changes you expect.

8. To clean up the environment, delete the `curl` pod:

```bash
$ oc delete pod curl
```

```
pod "curl" deleted
```

### Additional resources

- For more information about the Red Hat OpenShift Container Platform secret and the Prometheus operator, see [Prometheus user guide on alerting](#).

#### 5.3.4. Creating an alert route with templating in Alertmanager

Use Alertmanager to deliver alerts to an external system, such as email, IRC, or other notification channel. The Prometheus Operator manages the Alertmanager configuration as a Red Hat OpenShift Container Platform secret. By default, Service Telemetry Framework (STF) deploys a basic configuration that results in no receivers:

```yaml
repeat_interval: 12h
receiver: 'null'
receivers:
  - name: 'null'
```

If the `alertmanagerConfigManifest` parameter contains a custom template, for example, to construct the title and text of the sent alert, deploy the contents of the `alertmanagerConfigManifest` by using a base64-encoded configuration.

### Procedure
1. Log in to Red Hat OpenShift Container Platform.

2. Change to the `service-telemetry` namespace:
   ```bash
   $ oc project service-telemetry
   ```

3. Edit the `ServiceTelemetry` object for your STF deployment:
   ```bash
   $ oc edit stf default
   ```

4. To deploy a custom Alertmanager route with STF, you must pass an `alertmanagerConfigManifest` parameter to the Service Telemetry Operator that results in an updated secret that is managed by the Prometheus Operator:

   ```yaml
   apiVersion: infra.watch/v1beta1
   kind: ServiceTelemetry
   metadata:
     name: default
     namespace: service-telemetry
   spec:
     backends:
       metrics:
         prometheus:
           enabled: true
     alertmanagerConfigManifest: |
     # Rest of the manifest
   ```

5. Verify that the configuration has been applied to the secret:
   ```bash
   $ oc get secret alertmanager-default -o go-template="{{index .data "alertmanager.yaml" | base64decode }}"
   ```

   ```yaml
   global:
     resolve_timeout: 10m
     slack_api_url: <slack_api_url>
   receivers:
     - name: slack
       slack_configs:
         - channel: #stf-alerts
           title: |- 
           text: >-
   ```
Run the `curl` command against the alertmanager-proxy service to retrieve the status and `configYAML` contents, and verify that the supplied configuration matches the configuration in Alertmanager:

```
{
"status":"success","data":{"configYAML":"...",...}}
```

7. Verify that the `configYAML` field contains the changes you expect.

8. To clean up the environment, delete the `curl` pod:

```
$ oc delete pod curl
pod "curl" deleted
```

Additional resources

- For more information about the Red Hat OpenShift Container Platform secret and the Prometheus operator, see Prometheus user guide on alerting.

## 5.4. CONFIGURING SNMP TRAPS

You can integrate Service Telemetry Framework (STF) with an existing infrastructure monitoring platform that receives notifications through SNMP traps. To enable SNMP traps, modify the `ServiceTelemetry` object and configure the `snmpTraps` parameters.

For more information about configuring alerts, see Section 5.3, “Alerts in Service Telemetry Framework”.

### Prerequisites

- Know the IP address or hostname of the SNMP trap receiver where you want to send the alerts

### Procedure

1. To enable SNMP traps, modify the `ServiceTelemetry` object:

```
$ oc edit stf default
```

2. Set the `alerting.alertmanager.receivers.snmpTraps` parameters:

```
apiVersion: infra.watch/v1beta1
```
3. Ensure that you set the value of target to the IP address or hostname of the SNMP trap receiver.

5.5. HIGH AVAILABILITY

With high availability, Service Telemetry Framework (STF) can rapidly recover from failures in its component services. Although Red Hat OpenShift Container Platform restarts a failed pod if nodes are available to schedule the workload, this recovery process might take more than one minute, during which time events and metrics are lost. A high availability configuration includes multiple copies of STF components, which reduces recovery time to approximately 2 seconds. To protect against failure of an Red Hat OpenShift Container Platform node, deploy STF to an Red Hat OpenShift Container Platform cluster with three or more nodes.

WARNING

STF is not yet a fully fault tolerant system. Delivery of metrics and events during the recovery period is not guaranteed.

Enabling high availability has the following effects:

- Three Elasticsearch pods run instead of the default one.
- The following components run two pods instead of the default one:
  - AMQ Interconnect
  - Alertmanager
  - Prometheus
  - Events Smart Gateway
  - Metrics Smart Gateway
- Recovery time from a lost pod in any of these services reduces to approximately 2 seconds.

5.5.1. Configuring high availability

```yaml
kind: ServiceTelemetry
...  
spec:
...
  alerting:
    alertmanager:
      receivers:
        snmpTraps:
          enabled: true
          target: 10.10.10.10
```

```yaml
spec:
  alerting:
    alertmanager:
      receivers:
        snmpTraps:
          enabled: true
          target: 10.10.10.10
```
To configure Service Telemetry Framework (STF) for high availability, add `highAvailability.enabled: true` to the ServiceTelemetry object in Red Hat OpenShift Container Platform. You can set this parameter at installation time or, if you already deployed STF, complete the following steps:

**Procedure**

1. Log in to Red Hat OpenShift Container Platform.
2. Change to the `service-telemetry` namespace:
   ```bash
   $ oc project service-telemetry
   ```
3. Use the `oc` command to edit the ServiceTelemetry object:
   ```bash
   $ oc edit stf default
   ```
4. Add `highAvailability.enabled: true` to the `spec` section:
   ```yaml
   apiVersion: infra.watch/v1beta1
   kind: ServiceTelemetry
   ...  
   spec:  
   ...  
   highAvailability:  
   enabled: true
   ```
5. Save your changes and close the object.

### 5.6. EPHEMERAL STORAGE

You can use ephemeral storage to run Service Telemetry Framework (STF) without persistently storing data in your Red Hat OpenShift Container Platform cluster.

**WARNING**

If you use ephemeral storage, you might experience data loss if a pod is restarted, updated, or rescheduled onto another node. Use ephemeral storage only for development or testing, and not production environments.

#### 5.6.1. Configuring ephemeral storage

To configure STF components for ephemeral storage, add `..storage.strategy: ephemeral` to the corresponding parameter. For example, to enable ephemeral storage for the Prometheus back end, set `backends.metrics.prometheus.storage.strategy: ephemeral`. Components that support configuration of ephemeral storage include `alerting.alertmanager`, `backends.metrics.prometheus`, and `backends.events.elasticsearch`. You can add ephemeral storage configuration at installation time or, if you already deployed STF, complete the following steps:

**Procedure**
1. Log in to Red Hat OpenShift Container Platform.

2. Change to the `service-telemetry` namespace:

   ```bash
   $ oc project service-telemetry
   ```

3. Edit the ServiceTelemetry object:

   ```bash
   $ oc edit stf default
   ```

4. Add the `...storage.strategy: ephemeral` parameter to the `spec` section of the relevant component:

   ```json
   apiVersion: infra.watch/v1beta1
   kind: ServiceTelemetry
   metadata:
     name: stf-default
     namespace: service-telemetry
   spec:
     alerting:
       enabled: true
     alertmanager:
       storage:
         strategy: ephemeral
     backends:
       metrics:
         prometheus:
           enabled: true
           storage:
             strategy: ephemeral
       events:
         elasticsearch:
           enabled: true
           storage:
             strategy: ephemeral
   ```

5. Save your changes and close the object.

## 5.7. OBSERVABILITY STRATEGY IN SERVICE TELEMETRY FRAMEWORK

Service Telemetry Framework (STF) does not include storage backends and alerting tools. STF uses community operators to deploy Prometheus, Alertmanager, Grafana, and Elasticsearch. STF makes requests to these community operators to create instances of each application configured to work with STF.

Instead of having Service Telemetry Operator create custom resource requests, you can use your own deployments of these applications or other compatible applications, and scrape the metrics Smart Gateways for delivery to your own Prometheus-compatible system for telemetry storage. If you set the observability strategy to use alternative backends instead, persistent or ephemeral storage is not required for STF.

### 5.7.1. Configuring an alternate observability strategy
To configure STF to skip the deployment of storage, visualization, and alerting backends, add `observabilityStrategy: none` to the ServiceTelemetry spec. In this mode, only AMQ Interconnect routers and metrics Smart Gateways are deployed, and you must configure an external Prometheus-compatible system to collect metrics from the STF Smart Gateways.

**NOTE**
Currently, only metrics are supported when you set `observabilityStrategy` to `none`. Events Smart Gateways are not deployed.

**Procedure**

1. Create a ServiceTelemetry object with the property `observabilityStrategy: none` in the `spec` parameter. The manifest shows results in a default deployment of STF that is suitable for receiving telemetry from a single cloud with all metrics collector types.

   ```bash
   $ oc apply -f - <<EOF
   apiVersion: infra.watch/v1beta1
   kind: ServiceTelemetry
   metadata:
     name: default
     namespace: service-telemetry
   spec:
     observabilityStrategy: none
   EOF
   
   $ oc get pods
   NAME                                                      READY   STATUS    RESTARTS   AGE
   default-cloud1-ceil-meter-smartgateway-59c845d65b-gzhcs   3/3     Running   0          132m
   default-cloud1-coll-meter-smartgateway-75bbd948b9-d5phm   3/3     Running   0          132m
   default-cloud1-sens-meter-smartgateway-7fdbb57b6d-dh2g9   3/3     Running   0          132m
   default-interconnect-668d5bbcd6-57b21                     1/1     Running   0          132m
   interconnect-operator-b8f5bb647-tlp5t                     1/1     Running   0          47h
   service-telemetry-operator-566b9dd695-wkvjq               1/1     Running   0          156m
   smart-gateway-operator-58d77dcf7-6xsq7                    1/1     Running   0          47h
   
2. To verify that all workloads are operating correctly, view the pods and the status of each pod:

**Additional resources**

For more information about configuring additional clouds or to change the set of supported collectors, see Section 4.4.2, ”Deploying Smart Gateways”

### 5.8. RESOURCE USAGE OF RED HAT OPENSTACK PLATFORM SERVICES

You can monitor the resource usage of the Red Hat OpenStack Platform (RHOSP) services, such as the APIs and other infrastructure processes, to identify bottlenecks in the overcloud by showing services that run out of compute power. Resource usage monitoring is enabled by default.

**Additional resources**

- To disable resource usage monitoring, see Section 5.8.1, ”Disabling resource usage monitoring of Red Hat OpenStack Platform services”. 
5.8.1. Disabling resource usage monitoring of Red Hat OpenStack Platform services

To disable the monitoring of RHOSP containerized service resource usage, you must set the `CollectdEnableLibpodstats` parameter to `false`.

Prerequisites

- You have created the `stf-connectors.yaml` file. For more information, see Section 4.1, “Deploying Red Hat OpenStack Platform overcloud for Service Telemetry Framework”.
- You are using the most current version of Red Hat OpenStack Platform (RHOSP) 17.0.

Procedure

1. Open the `stf-connectors.yaml` file and add the `CollectdEnableLibpodstats` parameter to override the setting in `enable-stf.yaml`. Ensure that `stf-connectors.yaml` is called from the `openstack overcloud deploy` command after `enable-stf.yaml`:

   ```yaml
   CollectdEnableLibpodstats: false
   ```

2. Continue with the overcloud deployment procedure. For more information, see Section 4.1.5, “Deploying the overcloud”.

5.9. RED HAT OPENSTACK PLATFORM API STATUS AND CONTAINERIZED SERVICES HEALTH

You can use the OCI (Open Container Initiative) standard to assess the container health status of each Red Hat OpenStack Platform (RHOSP) service by periodically running a health check script. Most RHOSP services implement a health check that logs issues and returns a binary status. For the RHOSP APIs, the health checks query the root endpoint and determine the health based on the response time.

Monitoring of RHOSP container health and API status is enabled by default.

Additional resources

- To disable RHOSP container health and API status monitoring, see Section 5.9.1, “Disabling container health and API status monitoring”.

5.9.1. Disabling container health and API status monitoring

To disable RHOSP containerized service health and API status monitoring, you must set the `CollectdEnableSensubility` parameter to `false`.

Prerequisites

- You have created the `stf-connectors.yaml` file in your templates directory. For more information, see Section 4.1, “Deploying Red Hat OpenStack Platform overcloud for Service Telemetry Framework”.
- You are using the most current version of Red Hat OpenStack Platform (RHOSP) 17.0.
1. Open the `stf-connectors.yaml` and add the `CollectdEnableSensubility` parameter to override the setting in `enable-stf.yaml`. Ensure that `stf-connectors.yaml` is called from the `openstack overcloud deploy` command after `enable-stf.yaml`:

   ```yaml
   CollectdEnableSensubility: false
   ```

2. Continue with the overcloud deployment procedure. For more information, see Section 4.1.5, “Deploying the overcloud”.

Additional resources

- For more information about multiple cloud addresses, see Section 4.4, “Configuring multiple clouds”.
CHAPTER 6. RENEWING THE AMQ INTERCONNECT CERTIFICATE

Periodically, you must renew the CA certificate that secures the AMQ Interconnect connection between Red Hat OpenStack Platform (RHOSP) and Service Telemetry Framework (STF) when the certificate expires. The renewal is handled automatically by the cert-manager component in Red Hat OpenShift Container Platform, but you must manually copy the renewed certificate to your RHOSP nodes.

6.1. CHECKING FOR AN EXPIRED AMQ INTERCONNECT CA CERTIFICATE

When the CA certificate expires the AMQ Interconnect connections will remain up, but will be unable to reconnect if they are interrupted. Eventually you will find that some or all of the connections from your Red Hat OpenStack Platform (RHOSP) Routers have failed, showing errors on both sides, and the expiry (or "Not After") field in your CA certificate will be in the past.

Procedure

1. Log in to Red Hat OpenShift Container Platform.
2. Change to the service-telemetry namespace:
   ```bash
   $ oc project service-telemetry
   ```
3. Check that some or all Router connections have failed:
   ```bash
   $ oc exec -it $(oc get po -l application=default-interconnect -o jsonpath='{.items[0].metadata.name}') -- qdstat --connections | grep Router | wc
   0 0 0
   ```
4. Check for this error in the Red Hat OpenShift Container Platform-hosted AMQ Interconnect logs:
   ```bash
   $ oc logs -l application=default-interconnect | tail
   [
   2022-11-10 20:51:22.863466 +0000 SERVER (info) [C261] Connection from 10.10.10.10:34570 (to 0.0.0.0:5671) failed: amqp:connection:framing-error SSL Failure: error:140940E5:SSL routines:ssl3_read_bytes:ssl handshake failure
   ```
5. Log into your RHOSP undercloud.
6. Check for this error in the RHOSP-hosted AMQ Interconnect logs of a node where the connection has failed:
   ```bash
   $ ssh controller-0.ctlplane -- sudo tail /var/log/containers/metrics_qdr/metrics_qdr.log
   [
   ```
7. Confirm that the CA certificate has expired by examining the file on an RHOSP node:

```bash
$ ssh controller-0.ctlplane -- cat /var/lib/config-data/puppet-generated/metrics_qdr/etc/pki/tls/certs/CA_sslProfile.pem | openssl x509 -text | grep "Not After"
Not After : Nov 10 20:31:16 2022 GMT
$ date
Mon Nov 14 11:10:40 EST 2022
```

### 6.2. UPDATING THE AMQ INTERCONNECT CA CERTIFICATE

To update the AMQ Interconnect certificate, you will need to export it from Red Hat OpenShift Container Platform and copy it to your Red Hat OpenStack Platform (RHOSP) nodes.

**Procedure**

1. Log in to Red Hat OpenShift Container Platform.

2. Change to the `service-telemetry` namespace:

   ```bash
   $ oc project service-telemetry
   ```

3. Export the CA certificate to `STFCA.pem`:

   ```bash
   $ oc get secret/default-interconnect-selfsigned -o jsonpath='{.data.ca.crt}' | base64 -d > STFCA.pem
   ```

4. Copy `STFCA.pem` to your RHOSP undercloud.

5. Log into your RHOSP undercloud.

6. Edit the `stf-connectors.yaml` file to contain the new `caCertFileContent` (For more information, see Section 4.1.4, “Configuring the STF connection for the overcloud”)

   **NOTE**

   You do not need to perform an overcloud deploy after performing the steps below. We edit the `stf-connectors.yaml` file only to make sure that future deployments will not overwrite the new CA certificate.

7. Copy the `STFCA.pem` file to each RHOSP overcloud node:

   ```bash
   [stack@undercloud-0 ~]$ ansible -i overcloud-deploy/overcloud/tripleo-ansible-inventory.yaml allovercloud -b -m copy -a "src=STFCA.pem dest=/var/lib/config-data/puppet-generated/metrics_qdr/etc/pki/tls/certs/CA_sslProfile.pem"
   ```

8. Restart the `metrics_qdr` container on each RHOSP overcloud node:

   ```bash
   [stack@undercloud-0 ~]$ ansible -i overcloud-deploy/overcloud/tripleo-ansible-inventory.yaml allovercloud -m shell -a "sudo podman restart metrics_qdr"
   ```
CHAPTER 7. REMOVING SERVICE TELEMETRY FRAMEWORK FROM THE RED HAT OCP CONTAINER PLATFORM ENVIRONMENT

Remove Service Telemetry Framework (STF) from an Red Hat OpenShift Container Platform environment if you no longer require the STF functionality.

To remove STF from the Red Hat OpenShift Container Platform environment, you must perform the following tasks:

1. Delete the namespace.
2. Remove the catalog source.
3. Remove the cert-manager Operator.

7.1. DELETING THE NAMESPACE

To remove the operational resources for STF from Red Hat OpenShift Container Platform, delete the namespace.

Procedure

1. Run the oc delete command:

   $ oc delete project service-telemetry

2. Verify that the resources have been deleted from the namespace:

   $ oc get all
   No resources found.

7.2. REMOVING THE CATALOGSOURCE

If you do not expect to install Service Telemetry Framework (STF) again, delete the CatalogSource. When you remove the CatalogSource, PackageManifests related to STF are automatically removed from the Operator Lifecycle Manager catalog.

Procedure

1. If you enabled the OperatorHub.io Community Catalog Source during the installation process and you no longer need this catalog source, delete it:

   $ oc delete --namespace=openshift-marketplace catalogsource operatorhubio-operators
catalogsource.operators.coreos.com "operatorhubio-operators" deleted

Additional resources

For more information about the OperatorHub.io Community Catalog Source, see Section 3.1, “Deploying Service Telemetry Framework to the Red Hat OpenShift Container Platform environment”.

7.3. REMOVING THE CERT-MANAGER OPERATOR
If you are not using the cert-manager Operator for any other applications, delete the Subscription, ClusterServiceVersion, and CustomResourceDefinitions.

**Procedure**

1. Delete the Subscription from the `openshift-cert-manager-operator` namespace:

   ```
   $ oc delete --namespace=openshift-cert-manager-operator subscription openshift-cert-manager-operator
   subscription.operators.coreos.com "openshift-cert-manager-operator" deleted
   ```

2. Retrieve the version number of your installed ClusterServiceVersion:

   ```
   $ oc get --namespace=openshift-cert-manager-operator subscription openshift-cert-manager-operator -oyaml | grep currentCSV
   Example output:
   currentCSV: openshift-cert-manager.v1.7.1
   ```

3. Delete the ClusterServiceVersion from the `openshift-cert-manager-operator` namespace:

   ```
   $ oc delete --namespace=openshift-cert-manager-operator csv openshift-cert-manager.v1.7.1
   clusterserviceversion.operators.coreos.com "openshift-cert-manager.v1.7.1" deleted
   ```

4. Get the current list of CustomResourceDefinitions provided by the Operator so they can be deleted after removal of the ClusterServiceVersion:

   ```
   $ oc get csv -n openshift-cert-manager-operator openshift-cert-manager.v1.7.1 -oyaml | grep "kind: CustomResourceDefinition" -A2 | grep name | awk '{print $2}'
   Example output:
   certificaterequests.cert-manager.io
   certificates.cert-manager.io
   certmanagers.config.openshift.io
   certmanagers.operator.openshift.io
   challenges.acme.cert-manager.io
   clusterissuers.cert-manager.io
   issuers.cert-manager.io
   orders.acme.cert-manager.io
   ```

5. Delete the CustomResourceDefinitions related to the cert-manager Operator:

   ```
   $ oc delete crd certificaterequests.cert-manager.io certificates.cert-manager.io
   ```
Example output:

```bash
$ oc delete project openshift-cert-manager openshift-cert-manager-operator
```

Example output:

```bash
project.project.openshift.io "openshift-cert-manager" deleted
project.project.openshift.io "openshift-cert-manager-operator" deleted
```

Additional information

- Deleting Operators from a cluster.