Red Hat OpenShift Service on AWS 4

Logging

Configuring cluster logging in Red Hat OpenShift Service on AWS 4
Configuring cluster logging in Red Hat OpenShift Service on AWS
Abstract
This document provides instructions for installing, configuring, and using cluster logging, which aggregates logs for a range of Red Hat OpenShift Service on AWS.
## Table of Contents

<table>
<thead>
<tr>
<th>CHAPTER 1. INSTALLING LOGGING ADD-ON SERVICES</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1. INSTALL THE LOGGING ADD-ON SERVICE</td>
<td>3</td>
</tr>
<tr>
<td>1.2. ADDITIONAL RESOURCES</td>
<td>5</td>
</tr>
<tr>
<td>CHAPTER 2. VIEWING CLUSTER LOGS</td>
<td>6</td>
</tr>
<tr>
<td>2.1. VIEWING FORWARDED LOGS</td>
<td>6</td>
</tr>
</tbody>
</table>
CHAPTER 1. INSTALLING LOGGING ADD-ON SERVICES

This section describes how to install the logging add-on and Amazon Web Services (AWS) CloudWatch log forwarding add-on services on Red Hat OpenShift Service on AWS (ROSA).

The AWS CloudWatch log forwarding service on ROSA has the following approximate log throughput rates. Message rates greater than these can result in dropped log messages.

Table 1.1. Approximate log throughput rates

<table>
<thead>
<tr>
<th>Message size (bytes)</th>
<th>Maximum expected rate (messages/second/node)</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>1,000</td>
</tr>
<tr>
<td>1,024</td>
<td>650</td>
</tr>
<tr>
<td>2,048</td>
<td>450</td>
</tr>
</tbody>
</table>

1.1. INSTALL THE LOGGING ADD-ON SERVICE

Red Hat OpenShift Service on AWS (ROSA) provides logging through the `cluster-logging-operator` add-on. This add-on service offers an optional application log forwarding solution based on AWS CloudWatch. This logging solution can be installed after the ROSA cluster is provisioned.

Procedure

1. Enter the following command:

   ```
   $ rosa install addon cluster-logging-operator --cluster=<cluster_name> --interactive
   ```

   For `<cluster_name>`, enter the name of your cluster.

2. When prompted, accept the default `yes` to install the `cluster-logging-operator`.

3. When prompted, accept the default `yes` to install the optional Amazon CloudWatch log forwarding add-on or enter `no` to decline the installation of this add-on.

   **NOTE**

   It is not necessary to install the AWS CloudWatch service when you install the `cluster-logging-operator`. You can install the AWS CloudWatch service at any time through the OpenShift Cluster Manager (OCM) console from the cluster’s Add-ons tab.

4. For the collection of applications, infrastructure, and audit logs, accept the default values or change them as needed:

   - **Applications logs**: Lets the Operator collect application logs, which includes everything that is *not* deployed in the openshift-, kube-, and default namespaces. Default: `yes`
   - **Infrastructure logs**: Lets the Operator collect logs from OpenShift Container Platform, Kubernetes, and some nodes. Default: `yes`
Audit logs: Type **yes** to let the Operator collect node logs related to security audits. By default, Red Hat stores audit logs outside the cluster through a separate mechanism that does not rely on the Cluster Logging Operator. For more information about default audit logging, see the ROSA Service Definition. Default: **no**

5. For the Amazon CloudWatch region, use the default cluster region, leave the **Cloudwatch region** value empty.

Example output

```
? Are you sure you want to install add-on 'cluster-logging-operator' on cluster '<cluster_name>'? Yes
? Use AWS CloudWatch (optional): Yes
? Collect Applications logs (optional): Yes
? Collect Infrastructure logs (optional): Yes
? Collect Audit logs (optional): No
? CloudWatch region (optional):
I: Add-on 'cluster-logging-operator' is now installing. To check the status run 'rosa list addons --cluster=<cluster_name>'
```

### NOTE

The installation can take approximately 10 minutes to complete.

**Verification steps**

1. To verify the logging installation status, enter the following command:

   ```
   $ rosa list addons --cluster=<cluster_name>
   ```

2. To verify which pods are deployed by **cluster-logging-operator** and their state of readiness:

   a. Log in to the **oc** CLI using **cluster-admin** credentials:

   ```
   $ oc login https://api.mycluster.abwp.s1.example.org:6443 \
   --username cluster-admin \
   --password <password>
   ```

   b. Enter the following command to get information about the pods for the default project. Alternatively, you can specify a different project.

   ```
   $ oc get pods -n openshift-logging
   ```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-logging-operator-&lt;pod_ID&gt;</td>
<td>2/2</td>
<td>Running</td>
<td>0</td>
<td>7m1s</td>
</tr>
<tr>
<td>fluentd-4mnwp</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>6m3s</td>
</tr>
<tr>
<td>fluentd-6xt25</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>6m3s</td>
</tr>
<tr>
<td>fluentd-fqjhv</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>6m3s</td>
</tr>
<tr>
<td>fluentd-gcvrg</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>6m3s</td>
</tr>
<tr>
<td>fluentd-vpwrt</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>6m3s</td>
</tr>
</tbody>
</table>
3. Optional: To get information about the `clusterlogging` instance, enter the following command:

   ```
   $ oc get clusterlogging -n openshift-logging
   ```

4. Optional: To get information about `clusterlogforwarders` instances, enter the following command:

   ```
   $ oc get clusterlogforwarders -n openshift-logging
   ```

### 1.2. ADDITIONAL RESOURCES

- Adding services to your cluster
CHAPTER 2. VIEWING CLUSTER LOGS

View forwarded cluster logs in the AWS console.

2.1. VIEWING FORWARDED LOGS

Logs that are being forwarded from Red Hat OpenShift Service on AWS are viewed in the Amazon Web Services (AWS) console.

Prerequisites

- The `cluster-logging-operator` add-on service is installed and Cloudwatch is enabled.

Procedure

1. Log in to the AWS console.
2. Select the region the cluster is deployed in.
3. Select the CloudWatch service.
4. Select Logs from the left column, and select Log Groups.
5. Select a log group to explore. You can view application, infrastructure, or audit logs, depending on which types were enabled during the add-on service installation. See the Amazon CloudWatch User Guide for more information.