Red Hat OpenShift Service on AWS 4 Troubleshooting

Understanding support for Red Hat OpenShift Service on AWS
Legal Notice

Copyright © 2022 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation’s permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

This document provides information about getting support for Red Hat OpenShift Service on AWS (ROSA).
Table of Contents

CHAPTER 1. TROUBLESHOOTING EXPIRED TOKENS .................................................. 3
  1.1. TROUBLESHOOTING EXPIRED OFFLINE ACCESS TOKENS .......................... 3

CHAPTER 2. TROUBLESHOOTING INSTALLATIONS ................................................. 4
  2.1. INSTALLATION TROUBLESHOOTING ......................................................... 4
    2.1.1. Inspect install or uninstall logs ...................................................... 4
    2.1.2. Verify your Amazon Web Services (AWS) account permissions .............. 4
    2.1.3. Verify your AWS account and quota .............................................. 4
    2.1.4. AWS notification emails ................................................................. 4

CHAPTER 3. TROUBLESHOOTING CLUSTER DEPLOYMENTS ...................................... 6
  3.1. TROUBLESHOOTING CLUSTER DEPLOYMENTS ............................................ 6
    3.1.1. General deployment failure ......................................................... 6
    3.1.2. Deployment failure with an osdCcsAdmin error .................................. 6
    3.1.3. Elastic load balancer (ELB) AccessDenied error ................................. 6
CHAPTER 1. TROUBLESHOOTING EXPIRED TOKENS

1.1. TROUBLESHOOTING EXPIRED OFFLINE ACCESS TOKENS

If you use the rosa CLI and your api.openshift.com offline access token expires, an error message appears. This happens when sso.redhat.com invalidates the token.

Example output

Can't get tokens ....
Can't get access tokens ....

Procedure

- Generate a new offline access token at the following URL. A new offline access token is generated every time you visit the URL.
  - Red Hat OpenShift Service on AWS (ROSA):
    - https://console.redhat.com/openshift/token/rosa
CHAPTER 2. TROUBLESHOOTING INSTALLATIONS

2.1. INSTALLATION TROUBLESHOOTING

2.1.1. Inspect install or uninstall logs

To display install logs:

- Run the following command, replacing `<cluster_name>` with the name of your cluster:
  
  `$ rosa logs install --cluster=<cluster_name>`

- To watch the logs, include the `--watch` flag:
  
  `$ rosa logs install --cluster=<cluster_name> --watch`

To display uninstall logs:

- Run the following command, replacing `<cluster_name>` with the name of your cluster:
  
  `$ rosa logs uninstall --cluster=<cluster_name>`

- To watch the logs, include the `--watch` flag:
  
  `$ rosa logs uninstall --cluster=<cluster_name> --watch`

2.1.2. Verify your Amazon Web Services (AWS) account permissions

Run the following command to verify your AWS account has the correct permissions:

```
$ rosa verify permissions
```

If you receive any errors, double check to ensure than an SCP is not applied to your AWS account. If you are required to use an SCP, see Red Hat Requirements for Customer Cloud Subscriptions for details on the minimum required SCP.

2.1.3. Verify your AWS account and quota

Run the following command to verify you have the available quota on your AWS account:

```
$ rosa verify quota
```

AWS quotas change based on region. Be sure you are verifying your quota for the correct AWS region. If you need to increase your quota, navigate to your AWS console, and request a quota increase for the service that failed.

2.1.4. AWS notification emails

When creating a cluster, the Red Hat OpenShift Service on AWS service creates small instances in all supported regions. This check ensures the AWS account being used can deploy to each supported region.
For AWS accounts that are not using all supported regions, AWS may send one or more emails confirming that "Your Request For Accessing AWS Resources Has Been Validated". Typically the sender of this email is aws-verification@amazon.com.

This is expected behavior as the Red Hat OpenShift Service on AWS service is validating your AWS account configuration.
CHAPTER 3. TROUBLESHOOTING CLUSTER DEPLOYMENTS

3.1. TROUBLESHOOTING CLUSTER DEPLOYMENTS

This document describes how to troubleshoot cluster deployment errors.

3.1.1. General deployment failure

If a cluster deployment fails, the cluster is put into an "error" state.

Run the following command to get more information:

```
$ rosa describe cluster -c <my_cluster_name> --debug
```

3.1.2. Deployment failure with an osdCcsAdmin error

If a cluster creation action fails, you can receive the following error message.

Example output

```
Failed to create cluster: Unable to create cluster spec: Failed to get access keys for user 'osdCcsAdmin': NoSuchEntity: The user with name osdCcsAdmin cannot be found.
```

To fix this issue:

1. Delete the stack:

   ```
   $ rosa init --delete-stack
   ```

2. Reinitialize your account:

   ```
   $ rosa init
   ```

3.1.3. Elastic load balancer (ELB) AccessDenied error

If you have not created a load balancer in your AWS account, it is possible that the service role for the elastic load balancer (ELB) might not exist yet. You may receive the following error:

```
```

To resolve this issue, ensure that the role exists on your AWS account. If not, create this role with the following command:

```
aws iam get-role --role-name "AWSServiceRoleForElasticLoadBalancing" || aws iam create-service-linked-role --aws-service-name "elasticloadbalancing.amazonaws.com"
```
NOTE

This command only needs to be executed once per account.