Troubleshooting

Understanding support for Red Hat OpenShift Service on AWS
Troubleshooting

Understanding support for Red Hat OpenShift Service on AWS
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 AWS account permissions for clusters without STS .......... 4
    2.1.3. Verify your AWS account and quota ........................................... 4
    2.1.4. AWS notification emails ............................................................ 4

CHAPTER 3. TROUBLESHOOTING IAM ROLES ..................................................... 6
  3.1. RESOLVING ISSUES WITH OCM-ROLES AND USER-ROLE IAM RESOURCES 6
    3.1.1. Creating an OpenShift Cluster Manager IAM role ............................. 6
    3.1.2. Creating an user-role IAM role .................................................. 8
    3.1.3. Linking your AWS account ....................................................... 9
    3.1.4. Associating multiple AWS accounts with your Red Hat organization 10

CHAPTER 4. TROUBLESHOOTING CLUSTER DEPLOYMENTS ................................ 11
  4.1. OBTAINING INFORMATION ON A FAILED CLUSTER ............................... 11
  4.2. FAILING TO CREATE A CLUSTER WITH AN OSDCCSADMIN ERROR .......... 11
  4.3. CREATING THE SERVICE ROLE FOR THE ELASTIC LOAD BALANCER (ELB) 11
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 AWS account permissions for clusters without STS

Run the following command to verify if your AWS account has the correct permissions. This command verifies permissions only for clusters that do not use the AWS Security Token Service (STS):

$ 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 IAM ROLES

3.1. RESOLVING ISSUES WITH OCM-ROLES AND USER-ROLE IAM RESOURCES

You may receive an error when trying to create a cluster using the rosa CLI.

Sample output

```
E: Failed to create cluster: The sts_user_role is not linked to account '1oNi'. Please create a user role and link it to the account.
```

This error means that the user-role IAM role is not linked to your AWS account. The most likely cause of this error is that another user in your Red Hat organization created the ocm-role IAM role. Your user-role IAM role needs to be created.

**NOTE**

After any user sets up an ocm-role IAM resource linked to a Red Hat account, any subsequent users wishing to create a cluster in that Red Hat organization must have a user-role IAM role to provision a cluster.

**Procedure**

- Assess the status of your ocm-role and user-role IAM roles with the following commands:

  ```
  $ rosa list ocm-role
  $ rosa list ocm-role
  ```

Sample output

```
I: Fetching ocm roles
ROLE NAME                         ROLE ARN                                          LINKED  ADMIN
ManagedOpenShift-OCM-Role-1158   arn:aws:iam::2066:role/ManagedOpenShift-OCM-Role-1158   No      No

I: Fetching user roles
ROLE NAME                                   ROLE ARN                                        LINKED
ManagedOpenShift-User.osdocs-Role  arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role  Yes
```

With the results of these commands, you can create and link the missing IAM resources.

3.1.1. Creating an OpenShift Cluster Manager IAM role

You create your OpenShift Cluster Manager IAM roles by using the command-line interface (CLI).
Prerequisites

- You have an AWS account.
- You have Red Hat Organization Administrator privileges in the OpenShift Cluster Manager organization.
- You have the permissions required to install AWS account-wide roles.
- You have installed and configured the latest AWS (aws) and ROSA (rosa) CLIs on your installation host.

Procedure

- To create an ocm-role IAM role with basic privileges, run the following command:
  
  ```
  $ rosa create ocm-role
  ```

- To create an ocm-role IAM role with admin privileges, run the following command:
  
  ```
  $ rosa create ocm-role --admin
  ```

  This command allows you to create the role by specifying specific attributes. The following example output shows the "auto mode" selected, which lets the rosa CLI to create your Operator roles and policies. See "Methods of account-wide role creation" in the Additional resources for more information.

Example output

```
I: Creating ocm role
? Role prefix: ManagedOpenShift 1
? Enable admin capabilities for the OCM role (optional): No 2
? Permissions boundary ARN (optional): 3
? Role creation mode: auto 4
I: Creating role using 'arn:aws:iam::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes 5
I: Created role 'ManagedOpenShift-OCM-Role-182' with ARN  'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182'
I: Linking OCM role
? OCM Role ARN: arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182 6
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with organization '<AWS ARN'? Yes 7
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' with organization account '<AWS ARN>'
```

1 A prefix value for all of the created AWS resources. In this example, ManagedOpenShift prepends all of the AWS resources.

2 Choose if you want this role to have the additional admin permissions.

---

**NOTE**

You do not see this prompt if you used the `--admin` option.
3. The Amazon Resource Name (ARN) of the policy to set permission boundaries.

4. Choose the method of how to create your AWS roles. Using auto, the rosa CLI tool generates and links the roles and policies. In the auto mode, you receive some different prompts to create the AWS roles.

5. The auto method asks if you want to create a specific ocm-role using your prefix.

6. Confirm that you want to associate your IAM role with your OpenShift Cluster Manager.

7. Links the created role with your AWS organization.

3.1.2. Creating an user-role IAM role

You can create your OpenShift Cluster Manager IAM roles by using the command-line interface (CLI).

Prerequisites

- You have an AWS account.
- You have installed and configured the latest AWS (aws) and ROSA (rosa) CLIs on your installation host.

Procedure

- To create an ocm-role IAM role with basic privileges, run the following command:

  ```bash
  $ rosa create user-role
  ```

  This command allows you create the role by specifying specific attributes. The following example output shows the “auto mode” selected, which lets the rosa CLI to create your Operator roles and policies. See “Understanding the auto and manual deployment modes” in the Additional resources for more information.

Example output

```
I: Creating User role
? Role prefix: ManagedOpenShift
? Permissions boundary ARN (optional): 
? Role creation mode: auto
I: Creating ocm user role using 'arn:aws:iam::2066:user'
? Create the 'ManagedOpenShift-User.osdocs-Role' role? Yes
I: Created role 'ManagedOpenShift-User.osdocs-Role' with ARN 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role'
I: Linking User role
? User Role ARN: arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role
? Link the 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' role with account '1AGE'? Yes
I: Successfully linked role ARN 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' with account '1AGE'
```

A prefix value for all of the created AWS resources. In this example, ManagedOpenShift prepends all of the AWS resources.
The Amazon Resource Name (ARN) of the policy to set permission boundaries.

Choose the method of how to create your AWS roles. Using auto, the rosa CLI tool generates and links the role to your AWS account. In the auto mode, you receive some different prompts to create the AWS roles.

The auto method asks if you want to create a specific user-role using your prefix.

Links the created role with your AWS organization.

3.1.3. Linking your AWS account

You link your AWS account using the rosa CLI.

Prerequisites

- You have an AWS account.
- You are using OpenShift Cluster Manager to create clusters.
- You have the permissions required to install AWS account-wide roles.
- You have installed and configured the latest AWS (aws) and ROSA (rosa) CLIs on your installation host.
- You have created your ocm-role and user-role IAM roles.

Procedure

1. From the CLI, link your ocm-role resource to your Red Hat organization by using your Amazon Resource Name (ARN):

```
NOTE
You must have Red Hat Organization Administrator privileges to run the rosa link command. After you link the ocm-role resource with your AWS account, it is visible for all users in the organization.
```

   $ rosa link ocm-role --role-arn <arn>

   Example output

   I: Linking OCM role
   ? Link the `<AWS ACCOUNT ID>` role with organization `<ORG ID>`? Yes
   I: Successfully linked role-arn `<AWS ACCOUNT ID>` with organization account `<ORG ID>`

2. From the CLI, link your user-role resource to your Red Hat user account by using your Amazon Resource Name (ARN):

   $ rosa link user-role --role-arn <arn>

   Example output
3.1.4. Associating multiple AWS accounts with your Red Hat organization

You can associate multiple AWS accounts with your Red Hat organization. Associating multiple accounts lets you create Red Hat OpenShift Service on AWS (ROSA) clusters on any of the associated AWS accounts from your Red Hat organization.

With this feature, you can create clusters in different AWS regions by using multiple AWS profiles as region-bound environments.

Prerequisites

- You have an AWS account.
- You are using OpenShift Cluster Manager to create clusters.
- You have the permissions required to install AWS account-wide roles.
- You have installed and configured the latest AWS (aws) and ROSA (rosa) CLIs on your installation host.
- You have created your ocm-role and user-role IAM roles.

Procedure

To associate an additional AWS account, first create a profile in your local AWS configuration. Then, associate the account with your Red Hat organization by creating the ocm-role, user, and account roles in the additional AWS account.

To create the roles in an additional region, specify the --profile <aws-profile> parameter when running the rosa create commands and replace <aws_profile> with the additional account profile name:

- To specify an AWS account profile when creating an OpenShift Cluster Manager role:

  $ rosa create --profile <aws_profile> ocm-role

- To specify an AWS account profile when creating a user role:

  $ rosa create --profile <aws_profile> user-role

- To specify an AWS account profile when creating the account roles:

  $ rosa create --profile <aws_profile> account-roles

**NOTE**

If you do not specify a profile, the default AWS profile is used.
CHAPTER 4. TROUBLESHOOTING CLUSTER DEPLOYMENTS

This document describes how to troubleshoot cluster deployment errors.

4.1. OBTAINING INFORMATION ON A FAILED CLUSTER

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

Procedure

Run the following command to get more information:

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

4.2. FAILING TO CREATE A CLUSTER 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.

Procedure

To fix this issue:

1. Delete the stack:

\$ rosa init --delete-stack

2. Reinitialize your account:

\$ rosa init

4.3. CREATING THE SERVICE ROLE FOR THE ELASTIC LOAD BALANCER (ELB)

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:

Error: Error creating network Load Balancer: AccessDenied: User: arn:aws:sts::xxxxxxxxxxxxx:assumed-role/ManagedOpenShift-Installer-Role/xxxxxxxxxxxxxxxx is not authorized to perform: iam:CreateServiceLinkedRole on resource:
arn:aws:iam::xxxxxxxxxxxx:role/aws-service-role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing

Procedure

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

This command only needs to be executed once per account.

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