Red Hat OpenShift Service on AWS 4

Troubleshooting

Understanding support for Red Hat OpenShift Service on AWS
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. REMOTE HEALTH MONITORING WITH CONNECTED CLUSTERS ........................................... 3
  1.1. SHOWING DATA COLLECTED BY REMOTE HEALTH MONITORING ................................. 3
    1.1.1. Showing data collected by Telemetry ............................................................................ 3
    1.1.2. Showing data collected by the Insights Operator ......................................................... 6

CHAPTER 2. TROUBLESHOOTING EXPIRED TOKENS ................................................................. 8
  2.1. TROUBLESHOOTING EXPIRED OFFLINE ACCESS TOKENS ................................................ 8

CHAPTER 3. TROUBLESHOOTING INSTALLATIONS .................................................................... 9
  3.1. INSTALLATION TROUBLESHOOTING ............................................................................... 9
    3.1.1. Inspect install or uninstall logs ..................................................................................... 9
    3.1.2. Verify your AWS account permissions for clusters without STS ............................... 9
    3.1.3. Verify your AWS account and quota .......................................................................... 9
    3.1.4. AWS notification emails ............................................................................................ 9

CHAPTER 4. TROUBLESHOOTING IAM ROLES ......................................................................... 11
  4.1. RESOLVING ISSUES WITH OCM-ROLES AND USER-ROLE IAM RESOURCES .............. 11
    4.1.1. Creating an OpenShift Cluster Manager IAM role ...................................................... 11
    4.1.2. Creating an user-role IAM role ................................................................................. 13
    4.1.3. Linking your AWS account ....................................................................................... 14
    4.1.4. Associating multiple AWS accounts with your Red Hat organization .................... 15

CHAPTER 5. TROUBLESHOOTING CLUSTER DEPLOYMENTS .................................................. 17
  5.1. OBTAINING INFORMATION ON A FAILED CLUSTER....................................................... 17
  5.2. FAILING TO CREATE A CLUSTER WITH AN OSDCCSADMIN ERROR ......................... 17
  5.3. CREATING THE ELASTIC LOAD BALANCING (ELB) SERVICE-LINKED ROLE .............. 17
  5.4. REPAIRING A CLUSTER THAT CANNOT BE DELETED .................................................... 18

CHAPTER 6. RED HAT OPENS东海 SHIFT SERVICE ON AWS MANAGED RESOURCES .......... 19
  6.1. OVERVIEW ...................................................................................................................... 19
  6.2. HIVE MANAGED RESOURCES ....................................................................................... 19
  6.3. RED HAT OPENS东海 SHIFT SERVICE ON AWS ADD-ON NAMESPACES .................. 35
  6.4. RED HAT OPENS东海 SHIFT SERVICE ON AWS VALIDATING WEBHOOKS ............... 36
1.1. SHOWING DATA COLLECTED BY REMOTE HEALTH MONITORING

As an administrator, you can review the metrics collected by Telemetry and the Insights Operator.

1.1.1. Showing data collected by Telemetry

You can view the cluster and components time series data captured by Telemetry.

Prerequisites

- You have installed the OpenShift Container Platform CLI (oc).
- You have access to the cluster as a user with the `cluster-admin` role or the `cluster-monitoring-view` role.

Procedure

1. Log in to a cluster.
2. Run the following command, which queries a cluster’s Prometheus service and returns the full set of time series data captured by Telemetry:

```
```
CHAPTER 1. REMOTE HEALTH MONITORING WITH CONNECTED CLUSTERS

--data-urlencode 'match[]=\{
  __name__="cluster:alertmanager_integrations:max"
\}'
--data-urlencode 'match[]=\{
  __name__="cluster:telemetry_selected_series:count"
\}'
--data-urlencode 'match[]=\{
  __name__="openshift:prometheus_tsdb_head_series:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="openshift:prometheus_tsdb_head_samples_appended_total:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="monitoring:container_memory_working_set_bytes:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="namespace_job:scrape_series_added:topk3_sum1h"
\}'
--data-urlencode 'match[]=\{
  __name__="namespace_job:scrape_samples_post_metric_relabeling:topk3"
\}'
--data-urlencode 'match[]=\{
  __name__="monitoring:haproxy_server_http_responses_total:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="rhm_status"
\}'
--data-urlencode 'match[]=\{
  __name__="status:upgrading:version:rhoam_state:max"
\}'
--data-urlencode 'match[]=\{
  __name__="state:rhoam_critical_alerts:max"
\}'
--data-urlencode 'match[]=\{
  __name__="state:rhoam_warning_alerts:max"
\}'
--data-urlencode 'match[]=\{
  __name__="rhoam_7d_slo_percentile:max"
\}'
--data-urlencode 'match[]=\{
  __name__="cluster:vsphere_vcenter_info:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="cluster:kube_persistentvolume_plugin_type_counts:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="visual_web_terminal_sessions_total"
\}'
--data-urlencode 'match[]=\{
  __name__="cluster:vsphere_esxi_version_total:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="cluster:vsphere_node_hw_version_total:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="openshift:build_by_strategy:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="rhods_aggregate_availability"
\}'
--data-urlencode 'match[]=\{
  __name__="rhods_total_users"
\}'
--data-urlencode 'match[]=\{
  __name__="instance:etcd_disk_wal_fsync_duration_seconds:histogram_quantile",quantile="0.99"
\}'
--data-urlencode 'match[]=\{
  __name__="instance:etcd_mvcc_db_total_size_in_bytes:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="instance:etcd_network_peer_round_trip_time_seconds:histogram_quantile",quantile="0.99"
\}'
--data-urlencode 'match[]=\{
  __name__="instance:etcd_mvcc_db_total_size_in_use_in_bytes:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="instance:etcd_disk_backend_commit_duration_seconds:histogram_quantile",quantile="0.99"
\}'
--data-urlencode 'match[]=\{
  __name__="jaeger_operator_instances_storage_types"
\}'
--data-urlencode 'match[]=\{
  __name__="jaeger_operator_instances_strategies"
\}'
--data-urlencode 'match[]=\{
  __name__="jaeger_operator_instances_agent_strategies"
\}'
--data-urlencode 'match[]=\{
  __name__="appsvcs:cores_by_product:sum"
\}'
--data-urlencode 'match[]=\{
  __name__="nto_custom_profiles:count"
\}'
--data-urlencode 'match[]=\{
  __name__="openshift_csi_share_configmap"
\}'
--data-urlencode 'match[]=\{
  __name__="openshift_csi_share_secret"
\}'


1.1.2. Showing data collected by the Insights Operator

You can review the data that is collected by the Insights Operator.

**Prerequisites**

- Access to the cluster as a user with the `cluster-admin` role.

**Procedure**

1. Find the name of the currently running pod for the Insights Operator:

   ```bash
   $ INSIGHTS_OPERATOR_POD=$(oc get pods --namespace=openshift-insights -o custom-columns=:metadata.name --no-headers --field-selector=status.phase=Running)
   ```
2. Copy the recent data archives collected by the Insights Operator:

```bash
$ oc cp openshift-insights/$INSIGHTS_OPERATOR_POD:/var/lib/insights-operator ./insights-data
```

The recent Insights Operator archives are now available in the `insights-data` directory.
CHAPTER 2. TROUBLESHOOTING EXPIRED TOKENS

2.1. 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 3. TROUBLESHOOTING INSTALLATIONS

3.1. INSTALLATION TROUBLESHOOTING

3.1.1. Inspect install or uninstall logs

To display install logs:

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

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

To display uninstall logs:

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

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

3.1.2. 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):

$$\text{}\text{rosa verify permissions}\text{}$$

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.

3.1.3. Verify your AWS account and quota

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

$$\text{}\text{rosa verify quota}\text{}$$

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.

3.1.4. 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 4. TROUBLESHOOTING IAM ROLES

4.1. 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
  
  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
  
  $ rosa list user-role
  
  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.

4.1.1. 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 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
? Enable admin capabilities for the OCM role (optional): No
? Permissions boundary ARN (optional):
? Role creation mode: auto
I: Creating role using 'arn:aws:iam::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes
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
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with organization '<AWS ARN>'? Yes
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.
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 roles and policies. 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 **ocm-role** using your prefix.

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

Links the created role with your AWS organization.

### 4.1.2. 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:

  ```
  $ 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'
```

1. 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.

### 4.1.3. Linking your AWS account

You can link your AWS account to existing IAM roles by using the **rosa** CLI.

**Prerequisites**

- You have an AWS account.
- You are using **OpenShift Cluster Manager Hybrid Cloud Console** to create clusters.
- You have the permissions required to install AWS account-wide roles. See the "Additional resources" of this section for more information.
- 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, but have not yet linked them to your AWS account. You can check whether your IAM roles are already linked by running the following commands:

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

If **Yes** is displayed in the **Linked** column for both roles, you have already linked the roles to an AWS account.

**Procedure**

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

   ```
   $ rosa link ocm-role --role-arn <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**
2. From the CLI, link your **user-role** resource to your Red Hat user account by using your Amazon Resource Name (ARN):

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

**Example output**

```bash
I: Linking User role
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125' role with organization '<AWS ID>'? Yes
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125' with organization account '<AWS ID>'
```

### 4.1.4. 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 Hybrid Cloud Console* 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:

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

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

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

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

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

**NOTE**

If you do not specify a profile, the default AWS profile is used.
CHAPTER 5. TROUBLESHOOTING CLUSTER DEPLOYMENTS

This document describes how to troubleshoot cluster deployment errors.

5.1. 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:

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

5.2. 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
   ```
2. Reinitialize your account:
   ```
   $ rosa init
   ```

5.3. CREATING THE ELASTIC LOAD BALANCING (ELB) SERVICE-LINKED ROLE

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

```
```

**Procedure**

To resolve this issue, ensure that the role exists on your AWS account. If not, create this role with the following command:
5.4. REPAIRING A CLUSTER THAT CANNOT BE DELETED

In specific cases, the following error appears in OpenShift Cluster Manager Hybrid Cloud Console if you attempt to delete your cluster.

Error deleting cluster
CLUSTERS-MGMT-400: Failed to delete cluster <hash>: sts_user_role is not linked to your account. sts_ocm_role is linked to your organization <org number> which requires sts_user_role to be linked to your Red Hat account <account ID>. Please create a user role and link it to the account: User Account <account ID> is not authorized to perform STS cluster operations

Operation ID: b0572d6e-fe54-499b-8c97-46bf6890011c

If you try to delete your cluster from the CLI, the following error appears.

E: Failed to delete cluster <hash>: sts_user_role is not linked to your account. sts_ocm_role is linked to your organization <org number> which requires sts_user_role to be linked to your Red Hat account <account ID>. Please create a user role and link it to the account: User Account <account ID> is not authorized to perform STS cluster operations

This error occurs when the **user-role** is unlinked or deleted.

**Procedure**

1. Run the following command to create the **user-role** IAM resource:

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

2. After you see that the role has been created, you can delete the cluster. The following confirms that the role was created and linked:

   ```bash
   I: Successfully linked role ARN <user role ARN> with account <account ID>
   ```
CHAPTER 6. RED HAT OPENSHIFT SERVICE ON AWS MANAGED RESOURCES

6.1. OVERVIEW

The following covers all resources managed or protected by the Service Reliability Engineering Platform (SRE-P) Team. Customers should not attempt to modify these resources because doing so can lead to cluster instability.

6.2. HIVE MANAGED RESOURCES

The following list displays the Red Hat OpenShift Service on AWS resources managed by OpenShift Hive, the centralized fleet configuration management system. These resources are in addition to the OpenShift Container Platform resources created during installation. OpenShift Hive continually attempts to maintain consistency across all Red Hat OpenShift Service on AWS clusters. Changes to Red Hat OpenShift Service on AWS resources should be made through OpenShift Cluster Manager so that OpenShift Cluster Manager and Hive are synchronized. Contact ocm-feedback@redhat.com if OpenShift Cluster Manager does not support modifying the resources in question.

Example 6.1. List of Hive managed resources

Resources:
- ConfigMap:
  - namespace: openshift-deployment-validation-operator
    name: deployment-validation-operator-config
  - namespace: openshift-managed-upgrade-operator
    name: managed-upgrade-operator-config
  - namespace: openshift-monitoring
    name: cluster-monitoring-config
  - namespace: openshift-monitoring
    name: managed-namespaces
  - namespace: openshift-monitoring
    name: ocp-namespaces
  - namespace: openshift-monitoring
    name: osd-rebalance-infra-nodes
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter-code
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter-trusted-ca-bundle
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter-code
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter-trusted-ca-bundle
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols-code
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols-trusted-ca-bundle
  - namespace: openshift-monitoring
    name: token-refresher-trusted-ca-bundle
  - namespace: openshift-security
    name: osd-audit-policy
Endpoints:
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-metrics
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
- namespace: openshift-monitoring
  name: token-refresher
- namespace: openshift-validation-webhook
  name: validation-webhook
Namespace:
- name: dedicated-admin
- name: openshift-addon-operator
- name: openshift-aqua
- name: openshift-aws-vpce-operator
- name: openshift-backplane
- name: openshift-backplane-cee
- name: openshift-backplane-csa
- name: openshift-backplane-cse
- name: openshift-backplane-csm
- name: openshift-backplane-managed-scripts
- name: openshift-backplane-mobb
- name: openshift-backplane-srep
- name: openshift-backplane-tam
- name: openshift-build-test
- name: openshift-cloud-ingress-operator
- name: openshift-codeready-workspaces
- name: openshift-custom-domains-operator
- name: openshift-customer-monitoring
- name: openshift-deployment-validation-operator
- name: openshift-managed-node-metadata-operator
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-observability-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-strimzi
- name: openshift-validation-webhook
- name: openshift-velero
- name: openshift-monitoring
- name: openshift
- name: openshift-cluster-version
ReplicationController:
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-1
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-1
CHAPTER 6. RED HAT OPENSHIFT SERVICE ON AWS MANAGED RESOURCES

Secret:
- namespace: openshift-authentication
  name: v4-0-config-user-idp-0-file-data
- namespace: openshift-authentication
  name: v4-0-config-user-template-error
- namespace: openshift-authentication
  name: v4-0-config-user-template-login
- namespace: openshift-authentication
  name: v4-0-config-user-template-provider-selection
- namespace: openshift-config
  name: htpasswd-secret
- namespace: openshift-config
  name: osd-oauth-templates-errors
- namespace: openshift-config
  name: osd-oauth-templates-login
- namespace: openshift-config
  name: osd-oauth-templates-providers
- namespace: openshift-config
  name: sbasabat-mc-primary-cert-bundle-secret
- namespace: openshift-config
  name: support
- namespace: openshift-ingress
  name: sbasabat-mc-primary-cert-bundle-secret
- namespace: openshift-kube-apiserver
  name: user-serving-cert-000
- namespace: openshift-kube-apiserver
  name: user-serving-cert-001
- namespace: openshift-monitoring
  name: dms-secret
- namespace: openshift-monitoring
  name: observatorium-credentials
- namespace: openshift-monitoring
  name: pd-secret
- namespace: openshift-security
  name: splunk-auth
ServiceAccount:
- namespace: openshift-backplane-managed-scripts
  name: osd-backplane
- namespace: openshift-backplane-srep
  name: osd-delete-ownerrefs-serviceaccounts
- namespace: openshift-backplane
  name: osd-delete-backplane-serviceaccounts
- namespace: openshift-build-test
  name: sre-build-test
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-marketplace
  name: osd-patch-subscription-source
- namespace: openshift-monitoring
  name: configure-alertmanager-operator
- namespace: openshift-monitoring
  name: osd-cluster-ready
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
- namespace: openshift-network-diagnostics
  name: sre-pod-network-connectivity-check-pruner
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator
- namespace: openshift-sre-pruning
  name: bz1980755
- namespace: openshift-sre-pruning
  name: sre-pruner-sa
- namespace: openshift-validation-webhook
  name: validation-webhook
- namespace: openshift-velero
  name: managed-velero-operator
- namespace: openshift-velero
  name: velero
- namespace: openshift-backplane-srep
  name: UNIQUE_BACKPLANE_SERVICEACCOUNT_ID
Service:
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-metrics
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
- namespace: openshift-monitoring
  name: token-refresher
- namespace: openshift-validation-webhook
  name: validation-webhook
AddonOperator:
- name: addon-operator
ValidatingWebhookConfiguration:
- name: sre-hiveownership-validation
- name: sre-namespace-validation
- name: sre-pod-validation
- name: sre-prometheusrule-validation
- name: sre-regular-user-validation
- name: sre-scc-validation
- name: sre-techpreviewnoupgrade-validation
DaemonSet:
- namespace: openshift-monitoring
  name: audit-exporter
- namespace: openshift-validation-webhook
  name: validation-webhook

Deployment:
- namespace: openshift-monitoring
  name: token-refresher

DeploymentConfig:
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols

ClusterRoleBinding:
- name: aqua-scanner-binding
- name: backplane-impersonate-cluster-admin
- name: backplane-impersonate-cluster-admin
- name: bzu980755
- name: dedicated-admins-cluster
- name: dedicated-admins-registry-cas-cluster
- name: openshift-backplane-managed-scripts-reader
- name: osd-cluster-ready
- name: osd-delete-backplane-script-resources
- name: osd-delete-ownerrefs-serviceaccounts
- name: osd-patch-subscription-source
- name: osd-rebalance-infra-nodes
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: splunk-forwarder-operator-clusterrolebinding
- name: sre-build-test
- name: sre-pod-network-connectivity-check-pruner
- name: sre-pruner-buildsdepl Baby
- name: velero
- name: webhook-validation

ClusterRole:
- name: backplane-cee-readers-cluster
- name: backplane-impersonate-cluster-admin
- name: backplane-readers-cluster
- name: backplane-srep-admins-cluster
- name: backplane-srep-admins-project
- name: bzu980755
- name: dedicated-admins-aggregate-cluster
- name: dedicated-admins-aggregate-project
- name: dedicated-admins-cluster
- name: dedicated-admins-manage-operators
- name: dedicated-admins-project
- name: dedicated-admins-registry-cas-cluster
- name: dedicated-readers
- name: image-scanner
- name: openshift-backplane-managed-scripts-reader
- name: openshift-splunk-forwarder-operator
- name: osd-cluster-ready
- name: osd-custom-domains-dedicated-admin-cluster
- name: osd-delete-backplane-script-resources
- name: osd-delete-backplane-serviceaccounts
- name: osd-delete-ownerrefs-serviceaccounts
- name: osd-get-namespace
- name: osd-netnamespaces-dedicated-admin-cluster
- name: osd-patchsubscription-source
- name: osd-readers-aggregate
- name: osd-rebalance-infrastructure-nodes
- name: osd-rebalance-infrastructure-nodes-openshift-pod-rebalance
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: sre-allow-read-machine-info
- name: sre-build-test
- name: sre-pruner-buildsdeploys-cr
- name: webhook-validation-cr

RoleBinding:
- namespace: kube-system
  name: cloud-ingress-operator-cluster-config-v1-reader
- namespace: openshift-aqua
  name: dedicated-admins-openshift-aqua
- namespace: openshift-backplane-managed-scripts
  name: osd-delete-backplane-script-resources
- namespace: openshift-build-test
  name: sre-build-test
- namespace: openshift-cloud-ingress-operator
  name: osd-rebalance-infrastructure-nodes-openshift-pod-rebalance
- namespace: openshift-codeready-workspaces
  name: dedicated-admins-openshift-codeready-workspaces
- namespace: openshift-config
  name: dedicated-admins-project-request
- namespace: openshift-config
  name: dedicated-admins-registry-cas-project
- namespace: openshift-image-registry
  name: osd-rebalance-infrastructure-nodes-openshift-pod-rebalance
- namespace: openshift-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-machine-api
  name: cloud-ingress-operator
- namespace: openshift-machine-api
  name: cloud-ingress-operator
name: osd-cluster-ready
- namespace: openshift-machine-api
  name: sre-ebs-iops-reporter-read-machine-info
- namespace: openshift-machine-api
  name: sre-stuck-ebs-vols-read-machine-info
- namespace: openshift-managed-node-metadata-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-marketplace
  name: dedicated-admins-openshift-marketplace
- namespace: openshift-monitoring
  name: backplane-cee
- namespace: openshift-monitoring
  name: muo-monitoring-reader
- namespace: openshift-monitoring
  name: oao-monitoring-manager
- namespace: openshift-monitoring
  name: osd-cluster-ready
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes-openshift-monitoring
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
- namespace: openshift-must-gather-operator
  name: backplane-cee-mustgather
- namespace: openshift-must-gather-operator
  name: backplane-srep-mustgather
- namespace: openshift-must-gather-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-network-diagnostics
  name: sre-pod-network-connectivity-check-pruner
- namespace: openshift-network-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-ocm-agent-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-operators-redhat
  name: admin-dedicated-admins
- namespace: openshift-operators-redhat
  name: admin-system:serviceaccounts:distributed-admin
- namespace: openshift-operators-redhat
  name: openshift-operators-redhat-distributed-admins
- namespace: openshift-operators-redhat
  name: openshift-operators-redhat:serviceaccounts:distributed-admin
- namespace: openshift-operators
  name: dedicated-admins-openshift-operators
- namespace: openshift-osd-metrics
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-osd-metrics
  name: prometheus-k8s
- namespace: openshift-rbac-permissions
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-rbac-permissions
name: prometheus-k8s
- namespace: openshift-route-monitor-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-security
  name: osd-rebalance-infra-nodes-openshift-security
- namespace: openshift-splunk-forwarder-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-strimzi
  name: dedicated-admins-openshift-strimzi
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-uwm-config-create
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-uwm-config-edit
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-uwm-managed-am-secret
- namespace: openshift-user-workload-monitoring
  name: osd-rebalance-infra-nodes-openshift-user-workload-monitoring
- namespace: openshift-velero
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-velero
  name: prometheus-k8s
Role:
- namespace: kube-system
  name: cluster-config-v1-reader
- namespace: kube-system
  name: cluster-config-v1-reader-cio
- namespace: openshift-aqua
  name: dedicated-admins-openshift-aqua
- namespace: openshift-backplane-managed-scripts
  name: osd-delete-backplane-script-resources
- namespace: openshift-build-test
  name: sre-build-test
- namespace: openshift-codeready-workspaces
  name: dedicated-admins-openshift-codeready-workspaces
- namespace: openshift-config
  name: dedicated-admins-project-request
- namespace: openshift-config
  name: dedicated-admins-registry-cas-project
- namespace: openshift-config
  name: muo-pullsecret-reader
- namespace: openshift-config
  name: oao-openshiftconfig-reader
- namespace: openshift-config
  name: osd-cluster-ready
- namespace: openshift-customer-monitoring
  name: dedicated-admins-openshift-customer-monitoring
- namespace: openshift-customer-monitoring
  name: prometheus-k8s-openshift-customer-monitoring
- namespace: openshift-dns
  name: dedicated-admins-openshift-dns
- namespace: openshift-dns
  name: osd-rebalance-infra-nodes-openshift-dns
- namespace: openshift-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-ingress
  name: cloud-ingress-operator

Red Hat OpenShift Service on AWS 4 Troubleshooting
CHAPTER 6. RED HAT OPENShift SERVICE ON AWS MANAGED RESOURCES

- namespace: openshift-kube-apiserver
  name: cloud-ingress-operator
- namespace: openshift-machine-api
  name: cloud-ingress-operator
- namespace: openshift-machine-api
  name: osd-cluster-ready
- namespace: openshift-marketplace
  name: dedicated-admins-openshift-marketplace
- namespace: openshift-monitoring
  name: backplane-cee
- namespace: openshift-monitoring
  name: muo-monitoring-reader
- namespace: openshift-monitoring
  name: oao-monitoring-manager
- namespace: openshift-monitoring
  name: osd-cluster-ready
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes-openshift-monitoring
- namespace: openshift-must-gather-operator
  name: backplane-cee-mustgather
- namespace: openshift-must-gather-operator
  name: backplane-srep-mustgather
- namespace: openshift-network-diagnostics
  name: sre-pod-network-connectivity-check-pruner
- namespace: openshift-operators
  name: dedicated-admins-openshift-operators
- namespace: openshift-osd-metrics
  name: prometheus-k8s
- namespace: openshift-rbac-permissions
  name: prometheus-k8s
- namespace: openshift-security
  name: osd-rebalance-infra-nodes-openshift-security
- namespace: openshift-strimzi
  name: dedicated-admins-openshift-strimzi
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-user-workload-monitoring-create-cm
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-user-workload-monitoring-manage-am-secret
- namespace: openshift-user-workload-monitoring
  name: prometheus-k8s
CronJob:
- namespace: openshift-backplane-managed-scripts
  name: osd-delete-backplane-script-resources
- namespace: openshift-backplane-srep
  name: osd-delete-ownerrefs-serviceaccounts
- namespace: openshift-backplane
  name: osd-delete-backplane-serviceaccounts
- namespace: openshift-build-test
  name: sre-build-test
- namespace: openshift-marketplace
  name: osd-patch-subscription-source
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes
- namespace: openshift-network-diagnostics
name: sre-pod-network-connectivity-check-pruner
- namespace: openshift-sre-pruning
  name: builds-pruner
- namespace: openshift-sre-pruning
  name: bz1980755
- namespace: openshift-sre-pruning
  name: deployments-pruner
Job:
- namespace: openshift-monitoring
  name: osd-cluster-ready
CredentialsRequest:
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-credentials-aws
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-credentials-gcp
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-aws-credentials
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-aws-credentials
- namespace: openshift-velero
  name: managed-velero-operator-iam-credentials-aws
- namespace: openshift-velero
  name: managed-velero-operator-iam-credentials-gcp
APIScheme:
- namespace: openshift-cloud-ingress-operator
  name: rh-api
PublishingStrategy:
- namespace: openshift-cloud-ingress-operator
  name: publishingstrategy
EndpointSlice:
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-metrics-rhtwg
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter-4cw9r
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-6tx5g
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-gmdhs
- namespace: openshift-monitoring
  name: token-refresher-v5cpg
- namespace: openshift-validation-webhook
  name: validation-webhook-bl99t
MachineHealthCheck:
- namespace: openshift-machine-api
  name: srep-infra-healthcheck
- namespace: openshift-machine-api
  name: srep-metal-worker-healthcheck
- namespace: openshift-machine-api
  name: srep-worker-healthcheck
MachineSet:
- namespace: openshift-machine-api
  name: sbasabat-mc-qhqkn-infra-us-east-1a
- namespace: openshift-machine-api
  name: sbasabat-mc-qhqkn-worker-us-east-1a
ContainerRuntimeConfig:
- name: custom-crio
KubeletConfig:
- name: custom-kubelet

SubjectPermission:
- namespace: openshift-rbac-permissions
  name: backplane-ceed
- namespace: openshift-rbac-permissions
  name: backplane-csa
- namespace: openshift-rbac-permissions
  name: backplane-cse
- namespace: openshift-rbac-permissions
  name: backplane-csm
- namespace: openshift-rbac-permissions
  name: backplane-mobb
- namespace: openshift-rbac-permissions
  name: backplane-srep
- namespace: openshift-rbac-permissions
  name: backplane-tam
- namespace: openshift-rbac-permissions
  name: dedicated-admin-serviceaccounts
- namespace: openshift-rbac-permissions
  name: dedicated-admin-serviceaccounts-core-ns
- namespace: openshift-rbac-permissions
  name: dedicated-admins
- namespace: openshift-rbac-permissions
  name: dedicated-admins-alert-routing-edit
- namespace: openshift-rbac-permissions
  name: dedicated-admins-core-ns
- namespace: openshift-rbac-permissions
  name: dedicated-admins-customer-monitoring
- namespace: openshift-rbac-permissions
  name: osd-delete-backplane-serviceaccounts
- namespace: openshift-rbac-permissions
  name: sre-build-test

VeleroInstall:
- namespace: openshift-velero
  name: cluster

PrometheusRule:
- namespace: openshift-monitoring
  name: rhmi-sre-cluster-admins
- namespace: openshift-monitoring
  name: rhoam-sre-cluster-admins
- namespace: openshift-monitoring
  name: sre-alertmanager-silences-active
- namespace: openshift-monitoring
  name: sre-alerts-stuck-builds
- namespace: openshift-monitoring
  name: sre-alerts-stuck-volumes
- namespace: openshift-monitoring
  name: sre-cloud-ingress-operator-offline-alerts
- namespace: openshift-monitoring
  name: sre-configure-alertmanager-operator-offline-alerts
- namespace: openshift-monitoring
  name: sre-control-plane-resizing-alerts
- namespace: openshift-monitoring
  name: sre-dns-alerts
- namespace: openshift-monitoring
name: sre-ebs-iops-burstbalance
- namespace: openshift-monitoring
  name: sre-elasticsearch-jobs
- namespace: openshift-monitoring
  name: sre-elasticsearch-managed-notification-alerts
- namespace: openshift-monitoring
  name: sre-excessive-memory
- namespace: openshift-monitoring
  name: sre-haproxy-reload-fail
- namespace: openshift-monitoring
  name: sre-internal-slo-recording-rules
- namespace: openshift-monitoring
  name: sre-kubekubequoteexceeded
- namespace: openshift-monitoring
  name: sre-leader-election-master-status-alerts
- namespace: openshift-monitoring
  name: sre-managed-node-metadata-operator-alerts
- namespace: openshift-monitoring
  name: sre-managed-notification-alerts
- namespace: openshift-monitoring
  name: sre-managed-upgrade-operator-alerts
- namespace: openshift-monitoring
  name: sre-managed-velero-operator-alerts
- namespace: openshift-monitoring
  name: sre-node-unschedulable
- namespace: openshift-monitoring
  name: sre-oauth-server
- namespace: openshift-monitoring
  name: sre-pending-csr-alert
- namespace: openshift-monitoring
  name: sre-proxy-managed-notification-alerts
- namespace: openshift-monitoring
  name: sre-pruning
- namespace: openshift-monitoring
  name: sre-pv
- namespace: openshift-monitoring
  name: sre-router-health
- namespace: openshift-monitoring
  name: sre-runaway-sdn-preventing-container-creation
- namespace: openshift-monitoring
  name: sre-slo-recording-rules
- namespace: openshift-monitoring
  name: sre-telemetry-managed-labels-recording-rules
- namespace: openshift-monitoring
  name: sre-telemeter-client
- namespace: openshift-monitoring
  name: sre-telemetry-managed-labels-recording-rules
- namespace: openshift-monitoring
  name: sre-telemetry-managed-labels-recording-rules
- namespace: openshift-monitoring
  name: sre-upgrade-send-managed-notification-alerts
- namespace: openshift-monitoring
  name: sre-upgrade-send-managed-notification-alerts
- namespace: openshift-monitoring
  name: sre-uptime-sla
  ServiceMonitor:
    - namespace: openshift-monitoring
      name: sre-dns-latency-exporter
    - namespace: openshift-monitoring
      name: sre-ebs-iops-reporter
    - namespace: openshift-monitoring
      name: sre-stuck-ebs-vols
ClusterUrlMonitor:
- namespace: openshift-route-monitor-operator
  name: api
RouteMonitor:
- namespace: openshift-route-monitor-operator
  name: console
NetworkPolicy:
- namespace: openshift-deployment-validation-operator
  name: allow-from-openshift-insights
- namespace: openshift-deployment-validation-operator
  name: allow-from-openshift-olm
- namespace: openshift-monitoring
  name: token-refresher
ManagedNotification:
- namespace: openshift-ocm-agent-operator
  name: sre-elasticsearch-managed-notifications
- namespace: openshift-ocm-agent-operator
  name: sre-managed-notifications
- namespace: openshift-ocm-agent-operator
  name: sre-proxy-managed-notifications
- namespace: openshift-ocm-agent-operator
  name: sre-upload-managed-notifications
OcmAgent:
- namespace: openshift-ocm-agent-operator
  name: ocmagent
CatalogSource:
- namespace: openshift-addon-operator
  name: addon-operator-catalog
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-registry
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator-registry
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-catalog
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator-registry
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator-catalog
- namespace: openshift-monitoring
  name: configure-alertmanager-operator-registry
- namespace: openshift-must-gather-operator
  name: must-gather-operator-registry
- namespace: openshift-observability-operator
  name: observability-operator-catalog
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator-registry
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter-registry
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator-registry
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator-registry
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator-catalog
- namespace: openshift-velero
  name: managed-velero-operator-registry
OperatorGroup:
- namespace: openshift-addon-operator
  name: addon-operator-og
- namespace: openshift-aqua
  name: openshift-aqua
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-codeready-workspaces
  name: openshift-codeready-workspaces
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator
- namespace: openshift-customer-monitoring
  name: openshift-customer-monitoring
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-og
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator-og
- namespace: openshift-must-gather-operator
  name: must-gather-operator
- namespace: openshift-observability-operator
  name: observability-operator-og
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator-og
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator-og
- namespace: openshift-strimzi
  name: openshift-strimzi
- namespace: openshift-velero
  name: managed-velero-operator
Subscription:
- namespace: openshift-addon-operator
  name: addon-operator
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-monitoring
  name: configure-alertmanager-operator
- namespace: openshift-must-gather-operator
  name: must-gather-operator
- namespace: openshift-observability-operator
  name: observability-operator
CHAPTER 6. RED HAT OPENShift SERVICE ON AWS MANAGED RESOURCES

- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator
- namespace: openshift-splunk-forwarder-operator
  name: openshift-splunk-forwarder-operator
- namespace: openshift-velero
  name: managed-velero-operator

PackageManifest:
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator
- namespace: openshift-addon-operator
  name: addon-operator
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator
- namespace: openshift-velero
  name: managed-velero-operator
- namespace: openshift-deployment-validation-operator
  name: managed-upgrade-operator
- namespace: openshift-custom-domains-operator
  name: managed-node-metadata-operator
- namespace: openshift-route-monitor-operator
  name: custom-domains-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator
- namespace: openshift-observability-operator
  name: observability-operator
- namespace: openshift-monitoring
  name: configure-alertmanager-operator
- namespace: openshift-must-gather-operator
  name: deployment-validation-operator
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter

Status:
- {}

Project:
- name: dedicated-admin
- name: openshift-addon-operator
- name: openshift-aqua
- name: openshift-backplane
- name: openshift-backplane-cee
- name: openshift-backplane-csa
- name: openshift-backplane-cse
- name: openshift-backplane-csm
- name: openshift-backplane-managed-scripts
- name: openshift-backplane-mobb
- name: openshift-backplane-srep
- name: openshift-backplane-tam
- name: openshift-build-test
- name: openshift-cloud-ingress-operator
- name: openshift-codeready-workspaces
- name: openshift-custom-domains-operator
- name: openshift-customer-monitoring
- name: openshift-deployment-validation-operator
- name: openshift-managed-node-metadata-operator
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-observability-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-strimzi
- name: openshift-validation-webhook
- name: openshift-velero

ClusterResourceQuota:
- name: loadbalancer-quota
- name: persistent-volume-quota

SecurityContextConstraints:
- name: pcap-dedicated-admins
- name: splunkforwarder

SplunkForwarder:
- namespace: openshift-security
  name: splunkforwarder

Group:
- name: dedicated-admins

User:
- name: backplane-cluster-admin

Backup:
- namespace: openshift-velero
  name: daily-full-backup-20221123112305
- namespace: openshift-velero
  name: daily-full-backup-20221125042537
- namespace: openshift-velero
  name: daily-full-backup-20221126010038
- namespace: openshift-velero
  name: daily-full-backup-20221127010039
- namespace: openshift-velero
  name: daily-full-backup-20221128010040
- namespace: openshift-velero
  name: daily-full-backup-20221129050847
- namespace: openshift-velero
  name: hourly-object-backup-20221128051740
- namespace: openshift-velero
  name: hourly-object-backup-20221128061740
- namespace: openshift-velero
  name: hourly-object-backup-20221128071740
- namespace: openshift-velero
6.3. RED HAT OPENSHIFT SERVICE ON AWS ADD-ON NAMESPACES

Red Hat OpenShift Service on AWS add-ons are services available for installation after cluster installation. These additional services include Red Hat OpenShift Dev Spaces, Red Hat OpenShift API Management, and Cluster Logging Operator. Any changes to resources within the following namespaces can be overridden by the add-on during upgrades, which can lead to unsupported configurations for the add-on functionality.

Example 6.2. List of add-on managed namespaces

```yaml
addon-namespaces:
  ocs-converged-dev: openshift-storage
  managed-api-service-internal: redhat-rhoami-operator
  codeready-workspaces-operator: codeready-workspaces-operator
  managed-odh: redhat-ods-operator
  codeready-workspaces-operator-qe: codeready-workspaces-operator-qe
  integreatly-operator: redhat-rhmi-operator
  nvidia-gpu-addon: redhat-nvidia-gpu-addon
  integreatly-operator-internal: redhat-rhmi-operator
  rhosak-qe: redhat-managed-kafka-operator-qe
  rhoams: redhat-rhoam-operator
  ocs-converged: openshift-storage
  addon-operator: redhat-addon-operator
  rhosak: redhat-managed-kafka-operator
  kas-fleetshard-operator-qe: redhat-kas-fleetshard-operator-qe
  prow-operator: prow
  cluster-logging-operator: openshift-logging
  advanced-cluster-management: redhat-open-cluster-management
  cert-manager-operator: redhat-cert-manager-operator
  dba-operator: addon-dba-operator
  reference-addon: redhat-reference-addon
```
6.4. RED HAT OPENSShift SERVICE ON AWS VALIDATING WEBHOOks

Red Hat OpenShift Service on AWS validating webhooks are a set of dynamic admission controls maintained by the OpenShift SRE team. These HTTP callbacks, also known as webhooks, are called for various types of requests to ensure cluster stability. The following list describes the various webhooks with rules containing the registered operations and resources that are controlled. Any attempt to circumvent these validating webhooks could affect the stability and supportability of the cluster.

Example 6.3. List of validating webhooks

```json
[
  {
    "webhookName": "clusterlogging-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE"
        ],
        "apiGroups": [
          "logging.openshift.io"
        ],
        "apiVersions": ["v1"],
        "resources": [
          "clusterloggings"
        ],
        "scope": "Namespaced"
      }
    ],
    "documentString": "Managed OpenShift Customers may set log retention outside the allowed range of 0-7 days"
  },
  {
    "webhookName": "hiveownership-validation",
    "rules": [
      {
        "operations": [
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          "quota.openshift.io"
        ],
        "apiVersions": ["*"],
        "resources": [
          "clusterresourcequotas"
        ]
      }
    ],
    "documentString": "Managed OpenShift Customers may set quota limits outside the allowed ranges"
  }
]
```
Managed OpenShift customers may not edit certain managed resources. A managed resource has a "hive.openshift.io/managed": "true" label.

Managed OpenShift Customers may not modify namespaces specified in the [openshift-monitoring/addons-namespaces openshift-monitoring/managed-namespaces openshift-monitoring/ocp-namespaces] ConfigMaps because customer workloads should be placed in customer-created namespaces. Customers may not create namespaces identified by this regular expression (com$|io$|in$) because it could interfere with critical DNS resolution. Additionally, customers may not set or change the values of these Namespace labels [managed.openshift.io/storage-pv-quota-exempt managed.openshift.io/service-lb-quota-exempt].
"documentString": "Managed OpenShift Customers may use tolerations on Pods that could cause those Pods to be scheduled on infra or master nodes."
},

{  
  "webhookName": "regular-user-validation",
  "rules": [
    
      {  
          "operations": [  
          "*"
        ],
        "apiGroups": [  
          "cloudcredential.openshift.io",
          "machine.openshift.io",
          "admissionregistration.k8s.io",
          "addons.managed.openshift.io",
          "cloudingress.managed.openshift.io",
          "managed.openshift.io",
          "ocmagent.managed.openshift.io",
          "splunkforwarder.managed.openshift.io",
          "upgrade.managed.openshift.io"
        ],
        "apiVersions": [  
          "*"
        ],
        "resources": [  
          "*/*"
        ],
        "scope": "*"
      },
      
      {  
          "operations": [  
          "*"
        ],
        "apiGroups": [  
          "autoscaling.openshift.io"
        ],
        "apiVersions": [  
          "*"
        ],
        "resources": [  
          "clusterautoscalers",
          "machineautoscalers"
        ],
        "scope": "*"
      },
      
      {  
          "operations": [  
          "*"
        ],
        "apiGroups": [  
          "config.openshift.io"
        ],
        "apiVersions": [  
          "*"
        ],
        "resources": [  
          "clusterautoscalers",
          "machineautoscalers"
        ],
        "scope": "*"
      }
  ]
}
"apiVersions": [ 
  "*"
],
"resources": [
  "clusterversions",
  "clusterversions/status",
  "Schedulers",
  "apiservers"
],
"scope": "*"
},
{
  "operations": [ 
    "*"
  ],
  "apiGroups": [ 
    "operator.openshift.io"
  ],
  "apiVersions": [ 
    "*"
  ],
  "resources": [
    "kubeapiservers",
    "openshiftapiservers"
  ],
  "scope": "*"
},
{
  "operations": [ 
    "*"
  ],
  "apiGroups": [ 
    ""
  ],
  "apiVersions": [ 
    "*"
  ],
  "resources": [
    "nodes",
    "nodes/*"
  ],
  "scope": "*"
},
{
  "operations": [ 
    "*"
  ],
  "apiGroups": [ 
    "managed.openshift.io"
  ],
  "apiVersions": [ 
    "*"
  ],
  "resources": [
    "subjectpermissions",
    "subjectpermissions/*"
  ]
}
Managed OpenShift customers may not manage any objects in the following API groups:

- network.openshift.io
- cloudcredential.openshift.io
- managed.openshift.io
- ocmmagent.managed.openshift.io
- upgrade.managed.openshift.io
- config.openshift.io
- operator.openshift.io
- machine.openshift.io
- admissionregistration.k8s.io
- addons.managed.openshift.io
- cloudingress.managed.openshift.io
- splunkforwarder.managed.openshift.io
- autoscaling.openshift.io

nor may Managed OpenShift customers alter the APIServer, KubeAPIServer, OpenShiftAPIServer, ClusterVersion, Node or SubjectPermission objects.

Managed OpenShift Customers may not modify the following default SCCs:

- anyuid
- hostaccess
- hostmount-anyuid
- hostnetwork
- node-exporter
- nonroot
- privileged
- restricted

Managed OpenShift Customers may not upgrade the following API groups:

- network.openshift.io
- cloudcredential.openshift.io
- managed.openshift.io
- ocmmagent.managed.openshift.io
- upgrade.managed.openshift.io
- config.openshift.io
- operator.openshift.io
- machine.openshift.io
- admissionregistration.k8s.io
- addons.managed.openshift.io
- cloudingress.managed.openshift.io
- splunkforwarder.managed.openshift.io
- autoscaling.openshift.io
"operations": [
"CREATE",
"UPDATE"
],
"apiGroups": [
"config.openshift.io"
],
"apiVersions": [
"*"
],
"resources": [
"featuregates"
],
"scope": "Cluster"
}

"documentString": "Managed OpenShift Customers may not use TechPreviewNoUpgrade FeatureGate that could prevent any future ability to do a y-stream upgrade to their clusters."
}