



Red Hat OpenShift Service on AWS 4

Troubleshooting

Understanding support for Red Hat OpenShift Service on AWS

Red Hat OpenShift Service on AWS 4 Troubleshooting

Understanding support for Red Hat OpenShift Service on AWS

Legal Notice

Copyright © 2023 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. REMOTE HEALTH MONITORING WITH CONNECTED CLUSTERS	3
1.1. ABOUT REMOTE HEALTH MONITORING	3
1.1.1. About Telemetry	4
1.1.1.1. Information collected by Telemetry	4
1.1.1.1.1. System information	4
1.1.1.1.2. Sizing Information	4
1.1.1.1.3. Usage information	5
1.1.1.2. User Telemetry	5
1.1.2. About the Insights Operator	5
1.1.2.1. Information collected by the Insights Operator	6
1.1.3. Understanding Telemetry and Insights Operator data flow	6
1.1.4. Additional details about how remote health monitoring data is used	7
1.2. SHOWING DATA COLLECTED BY REMOTE HEALTH MONITORING	7
1.2.1. Showing data collected by Telemetry	7
1.2.2. Showing data collected by the Insights Operator	11
1.3. USING INSIGHTS TO IDENTIFY ISSUES WITH YOUR CLUSTER	11
1.3.1. About Red Hat Insights Advisor for Red Hat OpenShift Service on AWS	11
1.3.2. Understanding Insights Advisor recommendations	12
1.3.3. Displaying potential issues with your cluster	12
1.3.4. Displaying all Insights Advisor recommendations	13
1.3.5. Disabling Insights Advisor recommendations	13
1.3.6. Enabling a previously disabled Insights Advisor recommendation	14
1.3.7. Displaying the Insights status in the web console	14
CHAPTER 2. TROUBLESHOOTING EXPIRED TOKENS	16
2.1. TROUBLESHOOTING EXPIRED OFFLINE ACCESS TOKENS	16
CHAPTER 3. TROUBLESHOOTING INSTALLATIONS	17
3.1. INSTALLATION TROUBLESHOOTING	17
3.1.1. Inspect install or uninstall logs	17
3.1.2. Verify your AWS account permissions for clusters without STS	17
3.1.3. Verify your AWS account and quota	17
3.1.4. AWS notification emails	17
CHAPTER 4. TROUBLESHOOTING IAM ROLES	19
4.1. RESOLVING ISSUES WITH OCM-ROLES AND USER-ROLE IAM RESOURCES	19
4.1.1. Creating an ocm-role IAM role	19
4.1.2. Creating a user-role IAM role	21
4.1.3. Linking your AWS account	22
4.1.4. Associating multiple AWS accounts with your Red Hat organization	23
CHAPTER 5. TROUBLESHOOTING CLUSTER DEPLOYMENTS	25
5.1. OBTAINING INFORMATION ON A FAILED CLUSTER	25
5.2. FAILING TO CREATE A CLUSTER WITH AN OSDCCSADMIN ERROR	25
5.3. CREATING THE ELASTIC LOAD BALANCING (ELB) SERVICE-LINKED ROLE	25
5.4. REPAIRING A CLUSTER THAT CANNOT BE DELETED	26
CHAPTER 6. RED HAT OPENSIFT SERVICE ON AWS MANAGED RESOURCES	27
6.1. OVERVIEW	27
6.2. HIVE MANAGED RESOURCES	27
6.3. RED HAT OPENSIFT SERVICE ON AWS ADD-ON NAMESPACES	46
6.4. RED HAT OPENSIFT SERVICE ON AWS VALIDATING WEBHOOKS	46

CHAPTER 1. REMOTE HEALTH MONITORING WITH CONNECTED CLUSTERS

1.1. ABOUT REMOTE HEALTH MONITORING

Red Hat OpenShift Service on AWS collects telemetry and configuration data about your cluster and reports it to Red Hat by using the Telemeter Client and the Insights Operator. The data that is provided to Red Hat enables the benefits outlined in this document.

A cluster that reports data to Red Hat through Telemetry and the Insights Operator is considered a *connected cluster*.

Telemetry is the term that Red Hat uses to describe the information being sent to Red Hat by the Red Hat OpenShift Service on AWS Telemeter Client. Lightweight attributes are sent from connected clusters to Red Hat to enable subscription management automation, monitor the health of clusters, assist with support, and improve customer experience.

The **Insights Operator** gathers Red Hat OpenShift Service on AWS configuration data and sends it to Red Hat. The data is used to produce insights about potential issues that a cluster might be exposed to. These insights are communicated to cluster administrators on [OpenShift Cluster Manager Hybrid Cloud Console](#).

More information is provided in this document about these two processes.

Telemetry and Insights Operator benefits

Telemetry and the Insights Operator enable the following benefits for end-users:

- **Enhanced identification and resolution of issues** Events that might seem normal to an end-user can be observed by Red Hat from a broader perspective across a fleet of clusters. Some issues can be more rapidly identified from this point of view and resolved without an end-user needing to open a support case or file a [Jira issue](#).
- **Advanced release management.** Red Hat OpenShift Service on AWS offers the **candidate**, **fast**, and **stable** release channels, which enable you to choose an update strategy. The graduation of a release from **fast** to **stable** is dependent on the success rate of updates and on the events seen during upgrades. With the information provided by connected clusters, Red Hat can improve the quality of releases to **stable** channels and react more rapidly to issues found in the **fast** channels.
- **Targeted prioritization of new features and functionality** The data collected provides insights about which areas of Red Hat OpenShift Service on AWS are used most. With this information, Red Hat can focus on developing the new features and functionality that have the greatest impact for our customers.
- **A streamlined support experience.** You can provide a cluster ID for a connected cluster when creating a support ticket on the [Red Hat Customer Portal](#). This enables Red Hat to deliver a streamlined support experience that is specific to your cluster, by using the connected information. This document provides more information about that enhanced support experience.
- **Predictive analytics.** The insights displayed for your cluster on [OpenShift Cluster Manager Hybrid Cloud Console](#) are enabled by the information collected from connected clusters. Red Hat is investing in applying deep learning, machine learning, and artificial intelligence

automation to help identify issues that Red Hat OpenShift Service on AWS clusters are exposed to.

1.1.1. About Telemetry

Telemetry sends a carefully chosen subset of the cluster monitoring metrics to Red Hat. The Telemeter Client fetches the metrics values every four minutes and thirty seconds and uploads the data to Red Hat. These metrics are described in this document.

This stream of data is used by Red Hat to monitor the clusters in real-time and to react as necessary to problems that impact our customers. It also allows Red Hat to roll out Red Hat OpenShift Service on AWS upgrades to customers to minimize service impact and continuously improve the upgrade experience.

This debugging information is available to Red Hat Support and Engineering teams with the same restrictions as accessing data reported through support cases. All connected cluster information is used by Red Hat to help make Red Hat OpenShift Service on AWS better and more intuitive to use.

1.1.1.1. Information collected by Telemetry

The following information is collected by Telemetry:

1.1.1.1.1. System information

- Version information, including the Red Hat OpenShift Service on AWS cluster version and installed update details that are used to determine update version availability
- Update information, including the number of updates available per cluster, the channel and image repository used for an update, update progress information, and the number of errors that occur in an update
- The unique random identifier that is generated during an installation
- Configuration details that help Red Hat Support to provide beneficial support for customers, including node configuration at the cloud infrastructure level, hostnames, IP addresses, Kubernetes pod names, namespaces, and services
- The Red Hat OpenShift Service on AWS framework components installed in a cluster and their condition and status
- Events for all namespaces listed as "related objects" for a degraded Operator
- Information about degraded software
- Information about the validity of certificates
- The name of the provider platform that Red Hat OpenShift Service on AWS is deployed on and the data center location

1.1.1.1.2. Sizing Information

- Sizing information about clusters, machine types, and machines, including the number of CPU cores and the amount of RAM used for each
- The number of etcd members and the number of objects stored in the etcd cluster

- Number of application builds by build strategy type

1.1.1.1.3. Usage information

- Usage information about components, features, and extensions
- Usage details about Technology Previews and unsupported configurations

Telemetry does not collect identifying information such as usernames or passwords. Red Hat does not intend to collect personal information. If Red Hat discovers that personal information has been inadvertently received, Red Hat will delete such information. To the extent that any telemetry data constitutes personal data, please refer to the [Red Hat Privacy Statement](#) for more information about Red Hat's privacy practices.

1.1.1.2. User Telemetry

Red Hat collects anonymized user data from your browser. This anonymized data includes what pages, features, and resource types that the user of all clusters with enabled telemetry uses.

Other considerations:

- User events are grouped as a SHA-1 hash.
- User's IP address is saved as **0.0.0.0**.
- User names and IP addresses are never saved as separate values.

1.1.2. About the Insights Operator

The Insights Operator periodically gathers configuration and component failure status and, by default, reports that data every two hours to Red Hat. This information enables Red Hat to assess configuration and deeper failure data than is reported through Telemetry.

Users of Red Hat OpenShift Service on AWS can display the report of each cluster in the [Insights Advisor](#) service on Red Hat Hybrid Cloud Console. If any issues have been identified, Insights provides further details and, if available, steps on how to solve a problem.

The Insights Operator does not collect identifying information, such as user names, passwords, or certificates. See [Red Hat Insights Data & Application Security](#) for information about Red Hat Insights data collection and controls.

Red Hat uses all connected cluster information to:

- Identify potential cluster issues and provide a solution and preventive actions in the [Insights Advisor](#) service on Red Hat Hybrid Cloud Console
- Improve Red Hat OpenShift Service on AWS by providing aggregated and critical information to product and support teams
- Make Red Hat OpenShift Service on AWS more intuitive

Additional resources

- The Insights Operator is installed and enabled by default.

1.1.2.1. Information collected by the Insights Operator

The following information is collected by the Insights Operator:

- General information about your cluster and its components to identify issues that are specific to your Red Hat OpenShift Service on AWS version and environment
- Configuration files, such as the image registry configuration, of your cluster to determine incorrect settings and issues that are specific to parameters you set
- Errors that occur in the cluster components
- Progress information of running updates, and the status of any component upgrades
- Details of the platform that Red Hat OpenShift Service on AWS is deployed on, such as Amazon Web Services, and the region that the cluster is located in
- Cluster workload information transformed into discreet Secure Hash Algorithm (SHA) values, which allows Red Hat to assess workloads for security and version vulnerabilities without disclosing sensitive details
- If an Operator reports an issue, information is collected about core Red Hat OpenShift Service on AWS pods in the **openshift-*** and **kube-*** projects. This includes state, resource, security context, volume information, and more.

Additional resources

- The Insights Operator source code is available for review and contribution. See the [Insights Operator upstream project](#) for a list of the items collected by the Insights Operator.

1.1.3. Understanding Telemetry and Insights Operator data flow

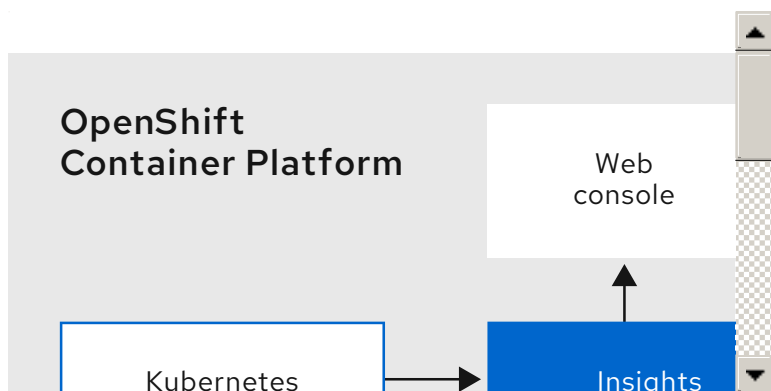
The Telemeter Client collects selected time series data from the Prometheus API. The time series data is uploaded to [api.openshift.com](#) every four minutes and thirty seconds for processing.

The Insights Operator gathers selected data from the Kubernetes API and the Prometheus API into an archive. The archive is uploaded to [OpenShift Cluster Manager Hybrid Cloud Console](#) every two hours for processing. The Insights Operator also downloads the latest Insights analysis from [OpenShift Cluster Manager Hybrid Cloud Console](#). This is used to populate the **Insights status** pop-up that is included in the **Overview** page in the Red Hat OpenShift Service on AWS web console.

All of the communication with Red Hat occurs over encrypted channels by using Transport Layer Security (TLS) and mutual certificate authentication. All of the data is encrypted in transit and at rest.

Access to the systems that handle customer data is controlled through multi-factor authentication and strict authorization controls. Access is granted on a need-to-know basis and is limited to required operations.

Telemetry and Insights Operator data flow



1.1.4. Additional details about how remote health monitoring data is used

The information collected to enable remote health monitoring is detailed in [Information collected by Telemetry](#) and [Information collected by the Insights Operator](#).

As further described in the preceding sections of this document, Red Hat collects data about your use of the Red Hat Product(s) for purposes such as providing support and upgrades, optimizing performance or configuration, minimizing service impacts, identifying and remediating threats, troubleshooting, improving the offerings and user experience, responding to issues, and for billing purposes if applicable.

Collection safeguards

Red Hat employs technical and organizational measures designed to protect the telemetry and configuration data.

Sharing

Red Hat may share the data collected through Telemetry and the Insights Operator internally within Red Hat to improve your user experience. Red Hat may share telemetry and configuration data with its business partners in an aggregated form that does not identify customers to help the partners better understand their markets and their customers' use of Red Hat offerings or to ensure the successful integration of products jointly supported by those partners.

Third parties

Red Hat may engage certain third parties to assist in the collection, analysis, and storage of the Telemetry and configuration data.

1.2. SHOWING DATA COLLECTED BY REMOTE HEALTH MONITORING

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

1.2.1. 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:

```
$ curl -G -k -H "Authorization: Bearer $(oc whoami -t)" \
https://$(oc get route prometheus-k8s-federate -n \
openshift-monitoring -o jsonpath="{.spec.host}"/federate \
--data-urlencode 'match[]={__name__=~"cluster:usage:.*"}' \
--data-urlencode 'match[]={__name__="count:up0"}' \
--data-urlencode 'match[]={__name__="count:up1"}' \
--data-urlencode 'match[]={__name__="cluster_version"}' \
--data-urlencode 'match[]={__name__="cluster_version_available_updates"}' \
--data-urlencode 'match[]={__name__="cluster_version_capability"}' \
--data-urlencode 'match[]={__name__="cluster_operator_up"}' \
--data-urlencode 'match[]={__name__="cluster_operator_conditions"}' \
--data-urlencode 'match[]={__name__="cluster_version_payload"}' \
--data-urlencode 'match[]={__name__="cluster_installer"}' \
--data-urlencode 'match[]={__name__="cluster_infrastructure_provider"}' \
--data-urlencode 'match[]={__name__="cluster_feature_set"}' \
--data-urlencode 'match[]={__name__="instance:etcd_object_counts:sum"}' \
--data-urlencode 'match[]={__name__="ALERTS",alertstate="firing"}' \
--data-urlencode 'match[]={__name__="code:apiserver_request_total:rate:sum"}' \
--data-urlencode 'match[]={__name__="cluster:capacity_cpu_cores:sum"}' \
--data-urlencode 'match[]={__name__="cluster:capacity_memory_bytes:sum"}' \
--data-urlencode 'match[]={__name__="cluster:cpu_usage_cores:sum"}' \
--data-urlencode 'match[]={__name__="cluster:memory_usage_bytes:sum"}' \
--data-urlencode 'match[]={__name__="openshift:cpu_usage_cores:sum"}' \
--data-urlencode 'match[]={__name__="openshift:memory_usage_bytes:sum"}' \
--data-urlencode 'match[]={__name__="workload:cpu_usage_cores:sum"}' \
--data-urlencode 'match[]={__name__="workload:memory_usage_bytes:sum"}' \
--data-urlencode 'match[]={__name__="cluster:virt_platform_nodes:sum"}' \
--data-urlencode 'match[]={__name__="cluster:node_instance_type_count:sum"}' \
--data-urlencode 'match[]={__name__="cnv:vmi_status_running:count"}' \
--data-urlencode 'match[]={__name__="cluster:vmi_request_cpu_cores:sum"}' \
--data-urlencode 'match[]={__name__="node_role_os_version_machine:cpu_capacity_cores:sum"}' \
--data-urlencode 'match[]={__name__="node_role_os_version_machine:cpu_capacity_sockets:sum"}' \
--data-urlencode 'match[]={__name__="subscription_sync_total"}' \
--data-urlencode 'match[]={__name__="olm_resolution_duration_seconds"}' \
--data-urlencode 'match[]={__name__="csv_succeeded"}' \
--data-urlencode 'match[]={__name__="csv_abnormal"}' \
--data-urlencode 'match[]={__name__="cluster:kube_persistentvolumeclaim_resource_requests_storage_bytes:provisioner:sum"}' \
--data-urlencode 'match[]={__name__="cluster:kubelet_volume_stats_used_bytes:provisioner:sum"}' \
--data-urlencode 'match[]={__name__="ceph_cluster_total_bytes"}' \
--data-urlencode 'match[]={__name__="ceph_cluster_total_used_raw_bytes"}' \
--data-urlencode 'match[]={__name__="ceph_health_status"}' \
--data-urlencode 'match[]={__name__="odf_system_raw_capacity_total_bytes"}' \
--data-urlencode 'match[]={__name__="odf_system_raw_capacity_used_bytes"}' \
--data-urlencode 'match[]={__name__="odf_system_health_status"}' \
--data-urlencode 'match[]={__name__="job:ceph_osd_metadata:count"}' \
--data-urlencode 'match[]={__name__="job:kube_pv:count"}'
```

```

--data-urlencode 'match[]={__name__="job:odf_system_pvs:count"}' \
--data-urlencode 'match[]={__name__="job:ceph_pools_iops:total"}' \
--data-urlencode 'match[]={__name__="job:ceph_pools_iops_bytes:total"}' \
--data-urlencode 'match[]={__name__="job:ceph_versions_running:count"}' \
--data-urlencode 'match[]={__name__="job:noobaa_total_unhealthy_buckets:sum"}' \
--data-urlencode 'match[]={__name__="job:noobaa_bucket_count:sum"}' \
--data-urlencode 'match[]={__name__="job:noobaa_total_object_count:sum"}' \
--data-urlencode 'match[]={__name__="odf_system_bucket_count", system_type="OCS",
system_vendor="Red Hat"}' \
--data-urlencode 'match[]={__name__="odf_system_objects_total", system_type="OCS",
system_vendor="Red Hat"}' \
--data-urlencode 'match[]={__name__="noobaa_accounts_num"}' \
--data-urlencode 'match[]={__name__="noobaa_total_usage"}' \
--data-urlencode 'match[]={__name__="console_url"}' \
--data-urlencode 'match[]=
{__name__="cluster:ovnkube_master_egress_routing_via_host:max"}' \
--data-urlencode 'match[]=
{__name__="cluster:network_attachment_definition_instances:max"}' \
--data-urlencode 'match[]=
{__name__="cluster:network_attachment_definition_enabled_instance_up:max"}' \
--data-urlencode 'match[]={__name__="cluster:ingress_controller_aws_nlb_active:sum"}' \
--data-urlencode 'match[]=
{__name__="cluster:route_metrics_controller_routes_per_shard:min"}' \
--data-urlencode 'match[]=
{__name__="cluster:route_metrics_controller_routes_per_shard:max"}' \
--data-urlencode 'match[]=
{__name__="cluster:route_metrics_controller_routes_per_shard:avg"}' \
--data-urlencode 'match[]=
{__name__="cluster:route_metrics_controller_routes_per_shard:median"}' \
--data-urlencode 'match[]={__name__="cluster:openshift_route_info:tls_termination:sum"}' \
--data-urlencode 'match[]={__name__="insightsclient_request_send_total"}' \
--data-urlencode 'match[]={__name__="cam_app_workload_migrations"}' \
--data-urlencode 'match[]=
{__name__="cluster:apiserver_current_inflight_requests:sum:max_over_time:2m"}' \
--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__="rhmi_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__="rhoam_7d_slo_remaining_error_budget:max"}' \
--data-urlencode 'match[]={__name__="cluster_legacy_scheduler_policy"}' \
--data-urlencode 'match[]={__name__="cluster_master_schedulable"}' \
--data-urlencode 'match[]={__name__="che_workspace_status"}' \

```

```

--data-urlencode 'match[]={__name__="che_workspace_started_total"}' \
--data-urlencode 'match[]={__name__="che_workspace_failure_total"}' \
--data-urlencode 'match[]={__name__="che_workspace_start_time_seconds_sum"}' \
--data-urlencode 'match[]={__name__="che_workspace_start_time_seconds_count"}' \
--data-urlencode 'match[]={__name__="cco_credentials_mode"}' \
--data-urlencode 'match[]={
{__name__="cluster:kube_persistentvolume_plugin_type_counts:sum"}' \
--data-urlencode 'match[]={__name__="visual_web_terminal_sessions_total"}' \
--data-urlencode 'match[]={__name__="acm_managed_cluster_info"}' \
--data-urlencode 'match[]={__name__="cluster:vsphere_vcenter_info:sum"}' \
--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_fsycn_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"}' \
--data-urlencode 'match[]={__name__="openshift_csi_share_mount_failures_total"}' \
--data-urlencode 'match[]={__name__="openshift_csi_share_mount_requests_total"}' \
--data-urlencode 'match[]={__name__="cluster:velero_backup_total:max"}' \
--data-urlencode 'match[]={__name__="cluster:velero_restore_total:max"}' \
--data-urlencode 'match[]={__name__="eo_es_storage_info"}' \
--data-urlencode 'match[]={__name__="eo_es_redundancy_policy_info"}' \
--data-urlencode 'match[]={__name__="eo_es_defined_delete_namespaces_total"}' \
--data-urlencode 'match[]={__name__="eo_es_misconfigured_memory_resources_info"}' \
--data-urlencode 'match[]={__name__="cluster:eo_es_data_nodes_total:max"}' \
--data-urlencode 'match[]={__name__="cluster:eo_es_documents_created_total:sum"}' \
--data-urlencode 'match[]={__name__="cluster:eo_es_documents_deleted_total:sum"}' \
--data-urlencode 'match[]={__name__="pod:eo_es_shards_total:max"}' \
--data-urlencode 'match[]={__name__="eo_es_cluster_management_state_info"}' \
--data-urlencode 'match[]={__name__="imageregistry:imagestreamtags_count:sum"}' \
--data-urlencode 'match[]={__name__="imageregistry:operations_count:sum"}' \
--data-urlencode 'match[]={__name__="log_logging_info"}' \
--data-urlencode 'match[]={__name__="log_collector_error_count_total"}' \
--data-urlencode 'match[]={__name__="log_forwarder_pipeline_info"}' \
--data-urlencode 'match[]={__name__="log_forwarder_input_info"}' \
--data-urlencode 'match[]={__name__="log_forwarder_output_info"}' \
--data-urlencode 'match[]={__name__="cluster:log_collected_bytes_total:sum"}' \
--data-urlencode 'match[]={__name__="cluster:log_logged_bytes_total:sum"}' \

```

```

--data-urlencode 'match[]={__name__="cluster:kata_monitor_running_shim_count:sum"}' \
--data-urlencode 'match[]={__name__="platform:hypershift_hostedclusters:max"}' \
--data-urlencode 'match[]={__name__="platform:hypershift_nodepools:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_unhealthy_bucket_claims:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_buckets_claims:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_unhealthy_namespace_resources:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_namespace_resources:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_unhealthy_namespace_buckets:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_namespace_buckets:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_accounts:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_usage:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_system_health_status:max"}' \
--data-urlencode 'match[]={__name__="ocs_advanced_feature_usage"}' \
--data-urlencode 'match[]={__name__="os_image_url_override:sum"}'

```

1.2.2. 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:

```

$ 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:

```

$ 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.

1.3. USING INSIGHTS TO IDENTIFY ISSUES WITH YOUR CLUSTER

Insights repeatedly analyzes the data Insights Operator sends. Users of Red Hat OpenShift Service on AWS can display the report in the **Insights** tab of each cluster on [OpenShift Cluster Manager Hybrid Cloud Console](#).

1.3.1. About Red Hat Insights Advisor for Red Hat OpenShift Service on AWS

You can use Insights Advisor to assess and monitor the health of your Red Hat OpenShift Service on AWS clusters. Whether you are concerned about individual clusters, or with your whole infrastructure, it is important to be aware of your exposure to issues that can affect service availability, fault tolerance, performance, or security.

Insights repeatedly analyzes the data that Insights Operator sends using a database of *recommendations*, which are sets of conditions that can leave your Red Hat OpenShift Service on AWS clusters at risk. Your data is then uploaded to the Insights Advisor service on Red Hat Hybrid Cloud Console where you can perform the following actions:

- See clusters impacted by a specific recommendation.
- Use robust filtering capabilities to refine your results to those recommendations.
- Learn more about individual recommendations, details about the risks they present, and get resolutions tailored to your individual clusters.
- Share results with other stakeholders.

1.3.2. Understanding Insights Advisor recommendations

Insights Advisor bundles information about various cluster states and component configurations that can negatively affect the service availability, fault tolerance, performance, or security of your clusters. This information set is called a recommendation in Insights Advisor and includes the following information:

- **Name:** A concise description of the recommendation
- **Added:** When the recommendation was published to the Insights Advisor archive
- **Category:** Whether the issue has the potential to negatively affect service availability, fault tolerance, performance, or security
- **Total risk:** A value derived from the *likelihood* that the condition will negatively affect your infrastructure, and the *impact* on operations if that were to happen
- **Clusters:** A list of clusters on which a recommendation is detected
- **Description:** A brief synopsis of the issue, including how it affects your clusters
- **Link to associated topics:** More information from Red Hat about the issue

1.3.3. Displaying potential issues with your cluster

This section describes how to display the Insights report in **Insights Advisor** on [OpenShift Cluster Manager Hybrid Cloud Console](#).

Note that Insights repeatedly analyzes your cluster and shows the latest results. These results can change, for example, if you fix an issue or a new issue has been detected.

Prerequisites

- Your cluster is registered on [OpenShift Cluster Manager Hybrid Cloud Console](#).
- Remote health reporting is enabled, which is the default.
- You are logged in to [OpenShift Cluster Manager Hybrid Cloud Console](#).

Procedure

1. Navigate to **Advisor** → **Recommendations** on [OpenShift Cluster Manager Hybrid Cloud Console](#).

Depending on the result, Insights Advisor displays one of the following:

- **No matching recommendations found**, if Insights did not identify any issues.
 - A list of issues Insights has detected, grouped by risk (low, moderate, important, and critical).
 - **No clusters yet**, if Insights has not yet analyzed the cluster. The analysis starts shortly after the cluster has been installed, registered, and connected to the internet.
2. If any issues are displayed, click the > icon in front of the entry for more details. Depending on the issue, the details can also contain a link to more information from Red Hat about the issue.

1.3.4. Displaying all Insights Advisor recommendations

The Recommendations view, by default, only displays the recommendations that are detected on your clusters. However, you can view all of the recommendations in the advisor archive.

Prerequisites

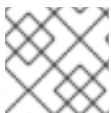
- Remote health reporting is enabled, which is the default.
- Your cluster is [registered](#) on Red Hat Hybrid Cloud Console.
- You are logged in to [OpenShift Cluster Manager Hybrid Cloud Console](#).

Procedure

1. Navigate to **Advisor** → **Recommendations** on [OpenShift Cluster Manager Hybrid Cloud Console](#).
2. Click the **X** icons next to the **Clusters Impacted** and **Status** filters. You can now browse through all of the potential recommendations for your cluster.

1.3.5. Disabling Insights Advisor recommendations

You can disable specific recommendations that affect your clusters, so that they no longer appear in your reports. It is possible to disable a recommendation for a single cluster or all of your clusters.



NOTE


Disabling a recommendation for all of your clusters also applies to any future clusters.

Prerequisites

- Remote health reporting is enabled, which is the default.
- Your cluster is registered on [OpenShift Cluster Manager Hybrid Cloud Console](#).
- You are logged in to [OpenShift Cluster Manager Hybrid Cloud Console](#).

Procedure

1. Navigate to **Advisor** → **Recommendations** on [OpenShift Cluster Manager Hybrid Cloud Console](#).
2. Click the name of the recommendation to disable. You are directed to the single recommendation page.
3. To disable the recommendation for a single cluster:

a. Click the **Options** menu  for that cluster, and then click **Disable recommendation for cluster**.

b. Enter a justification note and click **Save**.

4. To disable the recommendation for all of your clusters:
 - a. Click **Actions** → **Disable recommendation**.
 - b. Enter a justification note and click **Save**.


1.3.6. Enabling a previously disabled Insights Advisor recommendation

When a recommendation is disabled for all clusters, you will no longer see the recommendation in Insights Advisor. You can change this behavior.

Prerequisites

- Remote health reporting is enabled, which is the default.
- Your cluster is registered on [OpenShift Cluster Manager Hybrid Cloud Console](#).
- You are logged in to [OpenShift Cluster Manager Hybrid Cloud Console](#).

Procedure

1. Navigate to **Advisor** → **Recommendations** on [OpenShift Cluster Manager Hybrid Cloud Console](#).
2. Filter the recommendations by **Status** → **Disabled**.
3. Locate the recommendation to enable.
4. Click the **Options** menu , and then click **Enable recommendation**.

1.3.7. Displaying the Insights status in the web console

Insights repeatedly analyzes your cluster and you can display the status of identified potential issues of your cluster in the Red Hat OpenShift Service on AWS web console. This status shows the number of issues in the different categories and, for further details, links to the reports in [OpenShift Cluster Manager Hybrid Cloud Console](#).

Prerequisites

- Your cluster is registered in [OpenShift Cluster Manager Hybrid Cloud Console](#).
- Remote health reporting is enabled, which is the default.
- You are logged in to the Red Hat OpenShift Service on AWS web console.

Procedure

1. Navigate to **Home** → **Overview** in the Red Hat OpenShift Service on AWS web console.
2. Click **Insights** on the **Status** card.
The pop-up window lists potential issues grouped by risk. Click the individual categories or **View all recommendations in Insights Advisor** to display more details.

CHAPTER 2. TROUBLESHOOTING EXPIRED TOKENS

2.1. TROUBLESHOOTING EXPIRED OFFLINE ACCESS TOKENS

If you use the Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa**, 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:

```
$ 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
```

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):

```
$ 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.

3.1.3. 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.

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 Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa**.

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
```

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
```

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

Sample output

```
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 ocm-role IAM role

You create your **ocm-role** 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 Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa**, 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 (**rosa**) 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 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.

4.1.2. Creating a user-role IAM role

You can create your **user-role** IAM roles by using the command-line interface (CLI).

Prerequisites

- You have an AWS account.
- You have installed and configured the latest Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa**, on your installation host.

Procedure

- To create a **user-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 (**rosa**) 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 1
? Permissions boundary ARN (optional): 2
? Role creation mode: auto 3
I: Creating ocm user role using 'arn:aws:iam::2066:user'
? Create the 'ManagedOpenShift-User.osdocs-Role' role? Yes 4
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 5
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.

- 2 The Amazon Resource Name (ARN) of the policy to set permission boundaries.
- 3 Choose the method of how to create your AWS roles. Using **auto**, the ROSA CLI generates and links the role to your AWS account. In the **auto** mode, you receive some different prompts to create the AWS roles.
- 4 The auto method asks if you want to create a specific **user-role** using your prefix.
- 5 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 Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa**.

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):



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>'
```

- 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

```
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:

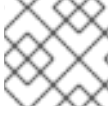
```
$ rosa create --profile <aws_profile> ocm-role
```

- 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 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:

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

5.2. FAILING TO CREATE A CLUSTER WITH ANOSDCCSADMIN 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

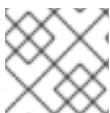
If you have not created a load balancer in your AWS account, it is possible that the service-linked role for Elastic Load Balancing (ELB) might not exist yet. You may receive the following error:

```
Error: Error creating network Load Balancer: AccessDenied: User: arn:aws:sts::xxxxxxxxxxxx:assumed-role/ManagedOpenShift-Installer-Role/xxxxxxxxxxxxxxxxxxxx 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:

```
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.

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:

```
$ 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:

```
I: Successfully linked role ARN <user role ARN> with account <account ID>
```

CHAPTER 6. RED HAT OPENSIFT 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-config
name: rosa-brand-logo
- namespace: openshift-console
name: custom-logo
- namespace: openshift-deployment-validation-operator
name: deployment-validation-operator-config
- namespace: openshift-file-integrity
name: fr-aide-conf
- 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
 - namespace: openshift-validation-webhook
name: webhook-cert
 - namespace: openshift
name: motd
- 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-scanning
name: loggerservice
 - namespace: openshift-security
name: audit-exporter
 - 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-cloud-ingress-operator
 - name: openshift-codeready-workspaces
 - name: openshift-compliance
 - name: openshift-container-security
 - name: openshift-custom-domains-operator
 - name: openshift-customer-monitoring
 - name: openshift-deployment-validation-operator
 - name: openshift-managed-node-metadata-operator
 - name: openshift-file-integrity
 - name: openshift-logging
 - 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-scanning
 - name: openshift-security
 - name: openshift-splunk-forwarder-operator
 - name: openshift-sre-pruning
 - name: openshift-strimzi
 - name: openshift-suricata
 - 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
- 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: rosa-oauth-templates-errors
 - namespace: openshift-config
name: rosa-oauth-templates-login
 - namespace: openshift-config
name: rosa-oauth-templates-providers
 - namespace: openshift-config
name: support
 - namespace: openshift-config
name: tony-devlab-primary-cert-bundle-secret
 - namespace: openshift-ingress
name: tony-devlab-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-scanning
name: clam-secrets
 - namespace: openshift-scanning
name: logger-secrets
 - namespace: openshift-security
name: splunk-auth
- ServiceAccount:
- namespace: openshift-backplane-managed-scripts
name: osd-backplane
 - namespace: openshift-backplane-srep
name: 6804d07fb268b8285b023bcf65392f0e
 - namespace: openshift-backplane-srep
name: osd-delete-ownerrefs-serviceaccounts
 - namespace: openshift-backplane
name: osd-delete-backplane-serviceaccounts
 - 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-machine-api
name: osd-disable-cpms
 - 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-scanning
name: logger-sa
 - namespace: openshift-scanning
name: scanner-sa
 - namespace: openshift-sre-pruning
name: sre-pruner-sa
 - namespace: openshift-suricata
name: ids-test
 - namespace: openshift-suricata

```

name: suricata-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-scanning
  name: loggerservice
- namespace: openshift-security
  name: audit-exporter
- 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: sre-dns-latency-exporter
- namespace: openshift-scanning
  name: logger
- namespace: openshift-scanning
  name: scanner
- namespace: openshift-security
  name: audit-exporter
- namespace: openshift-suricata
  name: suricata
- 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-cluster-admin
- name: backplane-impersonate-cluster-admin
- name: bz1980755
- name: configure-alertmanager-operator-prom
- name: dedicated-admins-cluster
- name: dedicated-admins-registry-cas-cluster
- name: logger-clusterrolebinding
- name: openshift-backplane-managed-scripts-reader
- name: osd-cluster-admin
- 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-pod-network-connectivity-check-pruner
- name: sre-pruner-buildsdeploys-pruning
- 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: bz1980755
- 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: logger-clusterrole
- 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-patch-subscription-source
- name: osd-readers-aggregate
- name: osd-rebalance-infra-nodes
- name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: sre-allow-read-machine-info
```

- name: sre-pruner-buildsdeploys-cr
- name: webhook-validation-cr
- RoleBinding:
 - namespace: kube-system
 - name: cloud-ingress-operator-cluster-config-v1-reader
 - namespace: kube-system
 - name: managed-velero-operator-cluster-config-v1-reader
 - namespace: openshift-aqua
 - name: dedicated-admins-openshift-aqua
 - namespace: openshift-backplane-managed-scripts
 - name: backplane-cee-mustgather
 - namespace: openshift-backplane-managed-scripts
 - name: backplane-srep-mustgather
 - namespace: openshift-backplane-managed-scripts
 - name: osd-delete-backplane-script-resources
 - namespace: openshift-cloud-ingress-operator
 - name: osd-rebalance-infra-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-config
 - name: muo-pullsecret-reader
 - namespace: openshift-config
 - name: oao-openshiftconfig-reader
 - namespace: openshift-config
 - name: osd-cluster-ready
 - namespace: openshift-custom-domains-operator
 - name: osd-rebalance-infra-nodes-openshift-pod-rebalance
 - 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-image-registry
 - name: osd-rebalance-infra-nodes-openshift-pod-rebalance
 - namespace: openshift-ingress-operator
 - name: cloud-ingress-operator
 - namespace: openshift-ingress
 - name: cloud-ingress-operator
 - namespace: openshift-kube-apiserver
 - name: cloud-ingress-operator
 - namespace: openshift-machine-api
 - name: cloud-ingress-operator
 - namespace: openshift-logging
 - name: admin-dedicated-admins
 - namespace: openshift-logging
 - name: admin-system:serviceaccounts:dedicated-admin
 - namespace: openshift-logging
 - name: openshift-logging-dedicated-admins
 - namespace: openshift-logging

```
name: openshift-logging:serviceaccounts:dedicated-admin
- namespace: openshift-machine-api
  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-machine-api
  name: osd-disable-cpms
- 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:dedicated-admin
- namespace: openshift-operators-redhat
  name: openshift-operators-redhat-dedicated-admins
- namespace: openshift-operators-redhat
  name: openshift-operators-redhat:serviceaccounts:dedicated-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-scanning
  name: scanner-rolebinding
- namespace: openshift-security
  name: osd-rebalance-infra-nodes-openshift-security
- namespace: openshift-security
  name: prometheus-k8s
- namespace: openshift-splunk-forwarder-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-strimzi
  name: dedicated-admins-openshift-strimzi
- namespace: openshift-suricata
  name: suricata-rolebinding
- 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: backplane-cee-pcap-collector
- namespace: openshift-backplane-managed-scripts
  name: backplane-srep-pcap-collector
- namespace: openshift-backplane-managed-scripts
  name: osd-delete-backplane-script-resources
- 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
- namespace: openshift-kube-apiserver
name: cloud-ingress-operator
- namespace: openshift-machine-api
name: cloud-ingress-operator
- namespace: openshift-logging
name: dedicated-admins-openshift-logging
- namespace: openshift-machine-api
name: osd-cluster-ready
- namespace: openshift-machine-api
name: osd-disable-cpms
- 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-scanning
name: scanner-role
- namespace: openshift-security
name: osd-rebalance-infra-nodes-openshift-security
- namespace: openshift-security
name: prometheus-k8s
- namespace: openshift-strimzi
name: dedicated-admins-openshift-strimzi
- namespace: openshift-suricata
name: suricata-role

- 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: osd-rebalance-infra-nodes-openshift-user-workload-monitoring
- namespace: openshift-velero
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-machine-api
name: osd-disable-cpms
- 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
- namespace: openshift-suricata
name: ids-tester

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

ScanSettingBinding:

- namespace: openshift-compliance
name: fedramp-high-ocp

- namespace: openshift-compliance
name: fedramp-high-rhcos

ScanSetting:

- namespace: openshift-compliance
name: osd

TailoredProfile:

- namespace: openshift-compliance
name: rhcos4-high-rosa

OAuth:

- name: cluster

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-scanning
name: loggerservice-zprbq
- namespace: openshift-security
name: audit-exporter-nqfdk
- namespace: openshift-validation-webhook
name: validation-webhook-97b8t

FileIntegrity:

- namespace: openshift-file-integrity
name: osd-fileintegrity

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

MachineConfig:

- name: 00-master-chrony
- name: 00-worker-chrony

SubjectPermission:

- namespace: openshift-rbac-permissions
name: backplane-cee
- 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
- 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-avo-pendingacceptance
 - 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-fr-alerts-low-disk-space

- namespace: openshift-monitoring
name: sre-haproxy-reload-fail
 - namespace: openshift-monitoring
name: sre-internal-slo-recording-rules
 - namespace: openshift-monitoring
name: sre-kubequotaexceeded
 - namespace: openshift-monitoring
name: sre-leader-election-master-status-alerts
 - namespace: openshift-monitoring
name: sre-managed-kube-apiserver-missing-on-node
 - namespace: openshift-monitoring
name: sre-managed-kube-controller-manager-missing-on-node
 - namespace: openshift-monitoring
name: sre-managed-kube-scheduler-missing-on-node
 - 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-telemeter-client
 - 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-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-upgrade-managed-notifications
OcmAgent:
- namespace: openshift-ocm-agent-operator
name: ocmagent
- namespace: openshift-security
name: audit-exporter
Console:
- name: cluster
CatalogSource:
- namespace: openshift-addon-operator
name: addon-operator-catalog
- namespace: openshift-cloud-ingress-operator
name: cloud-ingress-operator-registry
- namespace: openshift-compliance
name: compliance-operator-registry
- namespace: openshift-container-security
name: container-security-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-file-integrity
name: file-integrity-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-compliance
  name: compliance-operator
- namespace: openshift-container-security
  name: container-security-operator
- 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-file-integrity
  name: file-integrity-operator
- namespace: openshift-logging
  name: openshift-logging
- 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-compliance
  name: compliance-operator-sub
- namespace: openshift-container-security
  name: container-security-operator-sub
- 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-file-integrity
  name: file-integrity-operator-sub
- 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
- 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-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-container-security
  name: container-security-operator
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator

```

- namespace: openshift-file-integrity
name: file-integrity-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
 - namespace: openshift-compliance
name: compliance-operator
 - namespace: openshift-rbac-permissions
name: rbac-permissions-operator
- 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-cloud-ingress-operator
 - name: openshift-codeready-workspaces
 - name: openshift-compliance
 - name: openshift-container-security
 - name: openshift-custom-domains-operator
 - name: openshift-customer-monitoring
 - name: openshift-deployment-validation-operator
 - name: openshift-managed-node-metadata-operator
 - name: openshift-file-integrity
 - name: openshift-logging
 - 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-scanning

- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-strimzi
- name: openshift-suricata
- name: openshift-validation-webhook
- name: openshift-velero

ClusterResourceQuota:

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

SecurityContextConstraints:

- name: osd-scanning-scc
- name: osd-suricata-scc
- name: pcap-dedicated-admins
- name: splunkforwarder

SplunkForwarder:

- namespace: openshift-security
- name: splunkforwarder

Group:

- name: cluster-admins
- 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
- name: hourly-object-backup-20221128081740
- namespace: openshift-velero
- name: hourly-object-backup-20221128091740
- namespace: openshift-velero
- name: hourly-object-backup-20221129050852
- namespace: openshift-velero
- name: hourly-object-backup-20221129051747
- namespace: openshift-velero
- name: weekly-full-backup-20221116184315
- namespace: openshift-velero
- name: weekly-full-backup-20221121033854
- namespace: openshift-velero
- name: weekly-full-backup-20221128020040

Schedule:

- namespace: openshift-velero
name: daily-full-backup
- namespace: openshift-velero
name: hourly-object-backup
- namespace: openshift-velero
name: weekly-full-backup

6.3. RED HAT OPENSIFT 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

```

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
  ocm-addon-test-operator: redhat-ocm-addon-test-operator
  kas-fleetshard-operator: redhat-kas-fleetshard-operator
  connectors-operator: redhat-openshift-connectors

```

6.4. RED HAT OPENSIFT 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

```
[
  {
    "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": "clusterrolebindings-validation",
    "rules": [
      {
        "operations": [
          "DELETE"
        ],
        "apiGroups": [
          "rbac.authorization.k8s.io"
        ],
        "apiVersions": [
          "v1"
        ],
        "resources": [
          "clusterrolebindings"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift Customers may not delete the cluster role bindings
under the managed namespaces: (^openshift-.*|kube-system)"
  },
  {
    "webhookName": "hiveownership-validation",
    "rules": [
      {
        "operations": [
          "UPDATE",
          "DELETE"
        ],

```

```

    "apiGroups": [
      "quota.openshift.io"
    ],
    "apiVersions": [
      "*"
    ],
    "resources": [
      "clusterresourcequotas"
    ],
    "scope": "Cluster"
  }
],
"webhookObjectSelector": {
  "matchLabels": {
    "hive.openshift.io/managed": "true"
  }
},
"documentString": "Managed OpenShift customers may not edit certain managed resources. A
managed resource has a \"hive.openshift.io/managed\": \"true\" label."
},
{
  "webhookName": "imagecontentpolicies-validation",
  "rules": [
    {
      "operations": [
        "CREATE",
        "UPDATE"
      ],
      "apiGroups": [
        "config.openshift.io"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "imagedigestmirrorsets",
        "imagetagmirrorsets"
      ],
      "scope": "Cluster"
    },
    {
      "operations": [
        "CREATE",
        "UPDATE"
      ],
      "apiGroups": [
        "operator.openshift.io"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "imagecontentsourcepolicies"
      ],
      "scope": "Cluster"
    }
  ]
}

```

```

    ],
    "documentString": "Managed OpenShift customers may not create ImageContentSourcePolicy,
ImageDigestMirrorSet, or ImageTagMirrorSet resources that configure mirrors for the entirety of
quay.io, registry.redhat.io, nor registry.access.redhat.com. If needed, specific repositories can
have mirrors configured, such as quay.io/example."
  },
  {
    "webhookName": "ingresscontroller-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE"
        ],
        "apiGroups": [
          "operator.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "ingresscontroller",
          "ingresscontrollers"
        ],
        "scope": "Namespaced"
      }
    ],
    "documentString": "Managed OpenShift Customer may create IngressControllers without
necessary taints. This can cause those workloads to be provisioned on infra or master nodes."
  },
  {
    "webhookName": "namespace-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          ""
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "namespaces"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "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]."

```

    },
    {
      "webhookName": "pod-validation",
      "rules": [
        {
          "operations": [
            "*"
          ],
          "apiGroups": [
            "v1"
          ],
          "apiVersions": [
            "*"
          ],
          "resources": [
            "pods"
          ],
          "scope": "Namespaced"
        }
      ],
      "documentString": "Managed OpenShift Customers may use tolerations on Pods that could cause those Pods to be scheduled on infra or master nodes."
    },
    {
      "webhookName": "prometheusrule-validation",
      "rules": [
        {
          "operations": [
            "CREATE",
            "UPDATE",
            "DELETE"
          ],
          "apiGroups": [
            "monitoring.coreos.com"
          ],
          "apiVersions": [
            "*"
          ],
          "resources": [
            "prometheusrules"
          ],
          "scope": "Namespaced"
        }
      ],
      "documentString": "Managed OpenShift Customers may not create PrometheusRule in namespaces managed by Red Hat."
    },
    {
      "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": [
    "clusterversions",
    "clusterversions/status",
    "schedulers",
    "apiservers",
    "proxies"
  ],
  "scope": "*"
},
{
  "operations": [

```

```
"CREATE",
"UPDATE",
"DELETE"
],
"apiGroups": [
""
],
"apiVersions": [
"*"
],
"resources": [
"configmaps"
],
"scope": "*"
},
{
"operations": [
"*"
],
"apiGroups": [
"machineconfiguration.openshift.io"
],
"apiVersions": [
"*"
],
"resources": [
"machineconfigs",
"machineconfigpools"
],
"scope": "*"
},
{
"operations": [
"*"
],
"apiGroups": [
"operator.openshift.io"
],
"apiVersions": [
"*"
],
"resources": [
"kubeapiservers",
"openshiftapiservers"
],
"scope": "*"
},
{
"operations": [
"*"
],
"apiGroups": [
"managed.openshift.io"
],
"apiVersions": [
"*"
]
```



```

    ],
    "resources": [
      "subjectpermissions",
      "subjectpermissions/*"
    ],
    "scope": "*"
  },
  {
    "operations": [
      "*"
    ],
    "apiGroups": [
      "network.openshift.io"
    ],
    "apiVersions": [
      "*"
    ],
    "resources": [
      "netnamespaces",
      "netnamespaces/*"
    ],
    "scope": "*"
  }
],
"documentString": "Managed OpenShift customers may not manage any objects in the
following APIgroups [operator.openshift.io splunkforwarder.managed.openshift.io
config.openshift.io upgrade.managed.openshift.io autoscaling.openshift.io
machineconfiguration.openshift.io network.openshift.io cloudcredential.openshift.io
managed.openshift.io addons.managed.openshift.io cloudingress.managed.openshift.io
ocmagent.managed.openshift.io machine.openshift.io admissionregistration.k8s.io], nor may
Managed OpenShift customers alter the APIServer, KubeAPIServer, OpenShiftAPIServer,
ClusterVersion, Proxy or SubjectPermission objects."
},
{
  "webhookName": "regular-user-validation-osd",
  "rules": [
    {
      "operations": [
        "*"
      ],
      "apiGroups": [
        ""
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "nodes",
        "nodes/*"
      ],
      "scope": "*"
    }
  ],
  "documentString": "Managed OpenShift customers may not manage any objects in the
following APIgroups [], nor may Managed OpenShift customers alter the Node objects."
},

```

```

{
  "webhookName": "scc-validation",
  "rules": [
    {
      "operations": [
        "UPDATE",
        "DELETE"
      ],
      "apiGroups": [
        "security.openshift.io"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "securitycontextconstraints"
      ],
      "scope": "Cluster"
    }
  ],
  "documentString": "Managed OpenShift Customers may not modify the following default SCCs:
[anyuid hostaccess hostmount-anyuid hostnetwork hostnetwork-v2 node-exporter nonroot
nonroot-v2 privileged restricted restricted-v2]"
},
{
  "webhookName": "serviceaccount-validation",
  "rules": [
    {
      "operations": [
        "DELETE"
      ],
      "apiGroups": [
        ""
      ],
      "apiVersions": [
        "v1"
      ],
      "resources": [
        "serviceaccounts"
      ],
      "scope": "Namespaced"
    }
  ],
  "documentString": "Managed OpenShift Customers may not delete the service accounts under
the managed namespaces. "
},
{
  "webhookName": "techpreviewnoupgrade-validation",
  "rules": [
    {
      "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."
}
]
```