



OpenShift Dedicated 4

Troubleshooting

Understanding support for OpenShift Dedicated

OpenShift Dedicated 4 Troubleshooting

Understanding support for OpenShift Dedicated

Legal Notice

Copyright © 2022 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

Abstract

This document provides information about getting support for OpenShift Dedicated.

Table of Contents

CHAPTER 1. REMOTE HEALTH MONITORING WITH CONNECTED CLUSTERS	3
1.1. ABOUT REMOTE HEALTH MONITORING	3
1.1.1. About Telemetry	3
1.1.1.1. Information collected by Telemetry	4
1.1.2. About the Insights Operator	5
1.1.2.1. Information collected by the Insights Operator	5
1.1.3. Understanding Telemetry and Insights Operator data flow	5
1.1.4. Additional details about how remote health monitoring data is used	6
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	8
1.3. OPTING OUT OF REMOTE HEALTH REPORTING	8
1.4. USING INSIGHTS TO IDENTIFY ISSUES WITH YOUR CLUSTER	8
1.4.1. About Red Hat Insights Advisor for OpenShift Dedicated	8
1.4.2. Understanding Insights Advisor recommendations	9
1.4.3. Displaying potential issues with your cluster	9
1.4.4. Displaying all Insights Advisor recommendations	10
1.4.5. Disabling Insights Advisor recommendations	10
1.4.6. Enabling a previously disabled Insights Advisor recommendation	11
1.4.7. Displaying the Insights status in the web console	11
CHAPTER 2. SUMMARIZING CLUSTER SPECIFICATIONS	13
2.1. SUMMARIZING CLUSTER SPECIFICATIONS THROUGH CLUSTERVERSION	13
CHAPTER 3. OPENSIFT DEDICATED MANAGED RESOURCES	14
3.1. OVERVIEW	14
3.2. HIVE MANAGED RESOURCES	14
3.3. OPENSIFT DEDICATED ADD-ON NAMESPACES	22
3.4. OPENSIFT DEDICATED VALIDATING WEBHOOKS	23

CHAPTER 1. REMOTE HEALTH MONITORING WITH CONNECTED CLUSTERS

1.1. ABOUT REMOTE HEALTH MONITORING

OpenShift Dedicated 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 OpenShift Dedicated 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 OpenShift Dedicated 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](#).

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 Bugzilla.
- **Advanced release management.** OpenShift Dedicated 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 OpenShift Dedicated 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](#) 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 OpenShift Dedicated 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 OpenShift Dedicated 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 OpenShift Dedicated better and more intuitive to use.

1.1.1.1. Information collected by Telemetry

The following information is collected by Telemetry:

- The unique random identifier that is generated during an installation
- Version information, including the OpenShift Dedicated 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 name of the provider platform that OpenShift Dedicated is deployed on and the data center location
- 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
- The OpenShift Dedicated framework components installed in a cluster and their condition and status
- Usage information about components, features, and extensions
- Usage details about Technology Previews and unsupported configurations
- Information about degraded software
- Information about nodes that are marked as **NotReady**
- Events for all namespaces listed as "related objects" for a degraded Operator
- 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
- Information about the validity of certificates

Telemetry does not collect identifying information such as user names 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.

1.1.2. 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 OpenShift Dedicated can display the report of each cluster in [OpenShift Cluster Manager](#). 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:

- Proactively identify potential cluster issues and provide a solution and preventive actions in [OpenShift Cluster Manager](#)
- Improve OpenShift Dedicated by providing aggregated and critical information to product and support teams
- Make OpenShift Dedicated more intuitive

Additional resources

- The Insights Operator is installed and enabled by default. If you need to opt out of remote health reporting, see [Opting out of remote health reporting](#).

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 OpenShift Dedicated 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 OpenShift Dedicated is deployed on, such as Amazon Web Services, and the region that the cluster is located in
- If an Operator reports an issue, information is collected about core OpenShift Dedicated 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

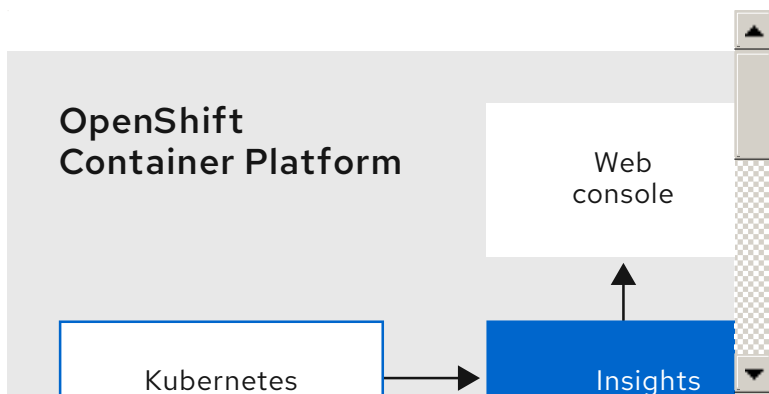
The Telemeter Client collects selected time series data from the Prometheus API. The time series data is uploaded to api.openshift.com every four minutes and thirty seconds for processing.

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](#) every two hours for processing. The Insights Operator also downloads the latest Insights analysis from [OpenShift Cluster Manager](#). This is used to populate the **Insights status** pop-up that is included in the **Overview** page in the OpenShift Dedicated 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.

User control / enabling and disabling telemetry and configuration data collection

You may disable OpenShift Dedicated Telemetry and the Insights Operator by following the instructions in [Opting out of remote health reporting](#).

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 see the cluster and components time series data captured by Telemetry.

Prerequisites

- Install the OpenShift CLI (**oc**).
- You must log in to the cluster with a user that has either the **cluster-admin** role or the **cluster-monitoring-view** role.

Procedure

1. Find the URL for the Prometheus service that runs in the OpenShift Dedicated cluster:

```
$ oc get route prometheus-k8s -n openshift-monitoring -o jsonpath="{.spec.host}"
```

2. Navigate to the URL.
3. Enter this query in the **Expression** input box and press **Execute**:

```
{__name__=~"cluster:usage:.*|count:up0|count:up1|cluster_version|cluster_version_available_updates|cluster_operator_up|cluster_operator_conditions|cluster_version_payload|cluster_installer|cluster_infrastructure_provider|cluster_feature_set|instance:etcd_object_counts:sum|ALERTS|code:apiserver_request_total:rate:sum|cluster:capacity_cpu_cores:sum|cluster:capacity_memory_bytes:sum|cluster:cpu_usage_cores:sum|cluster:memory_usage_bytes:sum|openshift:cpu_usage_cores:sum|openshift:memory_usage_bytes:sum|workload:cpu_usage_cores:sum|workload:memory_usage_bytes:sum|cluster:virt_platform_nodes:sum|cluster:node_instance_type_count:sum|cnv:vmi_status_running:count|cluster:vmi_request_cpu_cores:sum|node_role_os_version_machine:cpu_capacity_cores:sum|node_role_os_version_machine:cpu_capacity_sockets:sum|subscription_sync_total|olm_resolution_duration_seconds|csv_succeeded|csv_abnormal|cluster:kube_persistentvolumeclaim_resource_requests_storage_bytes:provisioner:sum|cluster:kubelet_volume_stats_used_bytes:provisioner:sum|ceph_cluster_total_bytes|ceph_cluster_total_used_raw_bytes|ceph_health_status|job:ceph_osd_metadata:count|job:kube_pv:count|job:ceph_pools_iops:total|job:ceph_pools_iops_bytes:total|job:ceph_versions_running:count|job:noobaa_total_unhealthy_buckets:sum|job:noobaa_bucket_count:sum|job:noobaa_total_object_count:sum|noobaa_accounts_num|noobaa_total_usage|console_url|cluster:network_attachment_definition_instances:max|cluster:network_attachment_definition_enabled_instance_up:max|cluster:ingress_controller_aws_nlb_active:sum|insightsclient_request_send_total|cam_app_workload_migrations|cluster:apiserver_current_inflight_requests:sum:max_over_time:2m|cluster:alertmanager_integrations:max|cluster:telemetry_selected_series:count|openshift:prometheus_tsdb_head_series:sum|openshift:prometheus_tsdb_head_samples_appended_total:sum|monitoring:container_memory_working_set_bytes:sum|namespace_job:scrape_series_added:topk3_sum1h|namespace_job:scrape_samples_post_metric_relabeling:topk3|monitoring:haproxy_server_http_responses_total:sum|rhmi_status|cluster_legacy_scheduler_policy|cluster_master_schedulable|che_workspace_status|che_workspace_started_total|che_workspace_failure_total|che_workspace_start_time
```

```
e_seconds_sum|che_workspace_start_time_seconds_count|cco_credentials_mode|cluster:kube
_persistentvolume_plugin_type_counts:sum|visual_web_terminal_sessions_total|acm_manage
_cluster_info|cluster:vsphere_vcenter_info:sum|cluster:vsphere_esxi_version_total:sum|cluster:
sphere_node_hw_version_total:sum|openshift:build_by_strategy:sum|rhods_aggregate_availab
lity|rhods_total_users|instance:etcd_disk_wal_fsync_duration_seconds:histogram_quantile|insta
nce:etcd_mvcc_db_total_size_in_bytes:sum|instance:etcd_network_peer_round_trip_time_secc
nds:histogram_quantile|instance:etcd_mvcc_db_total_size_in_use_in_bytes:sum|instance:etcd_
disk_backend_commit_duration_seconds:histogram_quantile|jaeger_operator_instances_storag
e_types|jaeger_operator_instances_strategies|jaeger_operator_instances_agent_strategies|ap
psvcs:cores_by_product:sum|nto_custom_profiles:count|openshift_csi_share_configmap|opens
hift_csi_share_secret|openshift_csi_share_mount_failures_total|openshift_csi_share_mount_re
quests_total",alertstate=~"firing"}
```

This query replicates the request that Telemetry makes against a running OpenShift Dedicated cluster's Prometheus service and returns the full set of time series captured by Telemetry.

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. OPTING OUT OF REMOTE HEALTH REPORTING

On OpenShift Dedicated, remote health reporting is always enabled. You cannot opt out.

1.4. USING INSIGHTS TO IDENTIFY ISSUES WITH YOUR CLUSTER

Insights repeatedly analyzes the data Insights Operator sends. Users of OpenShift Dedicated can display the report in the **Insights** tab of each cluster on [OpenShift Cluster Manager](#).

1.4.1. About Red Hat Insights Advisor for OpenShift Dedicated

You can use Insights Advisor to assess and monitor the health of your OpenShift Dedicated 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 OpenShift Dedicated 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.

1.4.2. 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

1.4.3. Displaying potential issues with your cluster

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

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](#).
- Remote health reporting is enabled, which is the default.
- You are logged in to [OpenShift Cluster Manager](#).

Procedure

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

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.

1.4.4. 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](#).

Procedure

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

1.4.5. 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](#).
- You are logged in to [OpenShift Cluster Manager](#).

Procedure

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

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**.


1.4.6. 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](#).
- You are logged in to [OpenShift Cluster Manager](#).

Procedure

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

1.4.7. 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 OpenShift Dedicated 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](#).

Prerequisites

- Your cluster is registered in [OpenShift Cluster Manager](#).
- Remote health reporting is enabled, which is the default.
- You are logged in to the OpenShift Dedicated web console.

Procedure

1. Navigate to **Home** → **Overview** in the OpenShift Dedicated 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. SUMMARIZING CLUSTER SPECIFICATIONS

2.1. SUMMARIZING CLUSTER SPECIFICATIONS THROUGH CLUSTERVERSION

You can obtain a summary of OpenShift Dedicated cluster specifications by querying the **clusterversion** resource.

Prerequisites

- You have access to the cluster as a user with the **cluster-admin** role.
- You have installed the OpenShift CLI (**oc**).

Procedure

1. Query cluster version, availability, uptime, and general status:

```
┆ $ oc get clusterversion
```

2. Obtain a detailed summary of cluster specifications, update availability, and update history:

```
┆ $ oc describe clusterversion
```

CHAPTER 3. OPENSIFT DEDICATED MANAGED RESOURCES

3.1. 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.

3.2. HIVE MANAGED RESOURCES

The following list displays the OpenShift Dedicated 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 OpenShift Dedicated clusters. Changes to OpenShift Dedicated 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 3.1. List of Hive managed resources

Resources:

ConfigMap:

- 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

Endpoints:

- namespace: openshift-monitoring
name: sre-dns-latency-exporter
- namespace: openshift-monitoring

```

name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
- namespace: openshift-monitoring
  name: token-refresher
- namespace: openshift-validation-webhook
  name: validation-webhook
Namespace:
- name: dedicated-admin
- name: openshift-addon-operator
- name: openshift-aqua
- name: openshift-aws-vpce-operator
- name: openshift-backplane
- name: openshift-backplane-cee
- name: openshift-backplane-managed-scripts
- name: openshift-backplane-srep
- name: openshift-build-test
- name: openshift-cloud-ingress-operator
- name: openshift-codeready-workspaces
- name: openshift-custom-domains-operator
- name: openshift-customer-monitoring
- name: openshift-managed-node-metadata-operator
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-strimzi
- name: openshift-validation-webhook
- name: openshift-velero
- name: openshift-monitoring
- name: openshift
- name: openshift-cluster-version
ReplicationController:
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-1
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-1
ServiceAccount:
- namespace: openshift-backplane-managed-scripts
  name: osd-backplane
- namespace: openshift-backplane-srep
  name: osd-delete-ownerrefs-serviceaccounts
- namespace: openshift-backplane
  name: osd-delete-backplane-serviceaccounts
- namespace: openshift-build-test
  name: sre-build-test
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator

```

- namespace: openshift-managed-upgrade-operator
name: managed-upgrade-operator
- namespace: openshift-marketplace
name: osd-patch-subscription-source
- namespace: openshift-monitoring
name: configure-alertmanager-operator
- namespace: openshift-monitoring
name: osd-cluster-ready
- namespace: openshift-monitoring
name: osd-rebalance-infra-nodes
- namespace: openshift-monitoring
name: sre-dns-latency-exporter
- namespace: openshift-monitoring
name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
name: sre-stuck-ebs-vols
- namespace: openshift-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: sre-pruner-sa
- namespace: openshift-validation-webhook
name: validation-webhook
- namespace: openshift-velero
name: managed-velero-operator
- namespace: openshift-velero
name: velero
- namespace: openshift-backplane-srep
name: UNIQUE_BACKPLANE_SERVICEACCOUNT_ID

Service:

- namespace: openshift-monitoring
name: sre-dns-latency-exporter
- namespace: openshift-monitoring
name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
name: sre-stuck-ebs-vols
- namespace: openshift-monitoring
name: token-refresher
- namespace: openshift-validation-webhook
name: validation-webhook

AddonOperator:

- name: addon-operator

ValidatingWebhookConfiguration:

- name: sre-hiveownership-validation
- name: sre-namespace-validation
- name: sre-pod-validation
- name: sre-regular-user-validation
- name: sre-scc-validation
- name: sre-techpreviewnoupgrade-validation

DaemonSet:

- namespace: openshift-monitoring
name: sre-dns-latency-exporter
- namespace: openshift-security

```

name: audit-exporter
- namespace: openshift-validation-webhook
  name: validation-webhook
Deployment:
- namespace: openshift-monitoring
  name: token-refresher
DeploymentConfig:
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
ClusterRoleBinding:
- name: aqua-scanner-binding
- name: backplane-cee-cluster-rolebinding
- name: backplane-cee-readers
- name: backplane-cluster-admin
- name: backplane-impersonate-cluster-admin
- name: backplane-srep-admins-cluster
- name: backplane-srep-readers-cluster
- name: configure-alertmanager-operator-prom
- name: dedicated-admins-cluster
- name: dedicated-admins-registry-cas-cluster
- name: openshift-backplane-managed-scripts-reader
- name: osd-cluster-ready
- name: osd-delete-backplane-script-resources
- name: osd-delete-ownerrefs-serviceaccounts
- name: osd-patch-subscription-source
- name: osd-rebalance-infra-nodes
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: splunk-forwarder-operator-clusterrolebinding
- name: sre-build-test
- name: sre-pruner-buildsdeploys-pruning
- name: velero
- name: webhook-validation
ClusterRole:
- name: backplane-cee-cluster-readers
- name: backplane-cee-readers-cluster
- name: backplane-impersonate-cluster-admin
- name: backplane-srep-admins-cluster
- name: backplane-srep-admins-project
- name: backplane-srep-readers-cluster
- name: dedicated-admins-aggregate-cluster
- name: dedicated-admins-aggregate-project
- name: dedicated-admins-cluster
- name: dedicated-admins-manage-operators
- name: dedicated-admins-project
- name: dedicated-admins-registry-cas-cluster
- name: dedicated-readers
- name: image-scanner
- name: openshift-backplane-managed-scripts-reader
- name: openshift-splunk-forwarder-operator
- name: osd-cluster-ready
- name: osd-custom-domains-dedicated-admin-cluster
- name: osd-delete-backplane-script-resources
- name: osd-delete-backplane-serviceaccounts

```

- name: osd-delete-ownerrefs-serviceaccounts
- name: osd-get-namespace
- name: osd-netnamespaces-dedicated-admin-cluster
- name: osd-patch-subscription-source
- name: osd-readers-aggregate
- name: osd-rebalance-infra-nodes
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: sre-allow-read-machine-info
- name: sre-build-test
- name: sre-pruner-buildsdeploys-cr
- name: webhook-validation-cr

CronJob:

- namespace: openshift-backplane-managed-scripts
name: osd-delete-backplane-script-resources
- namespace: openshift-backplane-srep
name: osd-delete-ownerrefs-serviceaccounts
- namespace: openshift-backplane
name: osd-delete-backplane-serviceaccounts
- namespace: openshift-build-test
name: sre-build-test
- namespace: openshift-marketplace
name: osd-patch-subscription-source
- namespace: openshift-monitoring
name: osd-rebalance-infra-nodes
- namespace: openshift-sre-pruning
name: builds-pruner
- namespace: openshift-sre-pruning
name: deployments-pruner

Job:

- namespace: openshift-monitoring
name: osd-cluster-ready

APIScheme:

- namespace: openshift-cloud-ingress-operator
name: rh-api

PublishingStrategy:

- namespace: openshift-cloud-ingress-operator
name: publishingstrategy

EndpointSlice:

- namespace: openshift-monitoring
name: sre-dns-latency-exporter-c2pcv
- namespace: openshift-monitoring
name: sre-ebs-iops-reporter-cl89c
- namespace: openshift-monitoring
name: sre-stuck-ebs-vols-lxjdv
- namespace: openshift-monitoring
name: token-refresher-5mv6s
- namespace: openshift-validation-webhook
name: validation-webhook-6v98z

MachineHealthCheck:

- namespace: openshift-machine-api
name: srep-infra-healthcheck
- namespace: openshift-machine-api
name: srep-worker-healthcheck

MachineSet:

- namespace: openshift-machine-api

```

name: pebrown-mcc-kq6gt-infra-ap-southeast-2a
- namespace: openshift-machine-api
  name: pebrown-mcc-kq6gt-worker-ap-southeast-2a
ContainerRuntimeConfig:
- name: custom-crio
KubeletConfig:
- name: custom-kubelet
SubjectPermission:
- namespace: openshift-rbac-permissions
  name: backplane-srep
- 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-core-ns
- namespace: openshift-rbac-permissions
  name: dedicated-admins-customer-monitoring
- namespace: openshift-rbac-permissions
  name: osd-delete-backplane-serviceaccounts
- namespace: openshift-rbac-permissions
  name: sre-build-test
VelerolInstall:
- namespace: openshift-velero
  name: cluster
ClusterUrlMonitor:
- namespace: openshift-route-monitor-operator
  name: api
RouteMonitor:
- namespace: openshift-route-monitor-operator
  name: console
NetworkPolicy:
- 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
OcmAgent:
- namespace: openshift-ocm-agent-operator
  name: ocmagent
CatalogSource:
- namespace: openshift-addon-operator
  name: addon-operator-catalog
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-registry
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator-registry
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator-registry
- namespace: openshift-managed-upgrade-operator

```

```
name: managed-upgrade-operator-catalog
- namespace: openshift-monitoring
  name: configure-alertmanager-operator-registry
- namespace: openshift-must-gather-operator
  name: must-gather-operator-registry
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator-registry
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter-registry
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator-registry
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator-registry
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator-catalog
- namespace: openshift-velero
  name: managed-velero-operator-registry
OperatorGroup:
- namespace: openshift-addon-operator
  name: addon-operator-og
- namespace: openshift-aqua
  name: openshift-aqua
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-codeready-workspaces
  name: openshift-codeready-workspaces
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator
- namespace: openshift-customer-monitoring
  name: openshift-customer-monitoring
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator-og
- namespace: openshift-must-gather-operator
  name: must-gather-operator
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator-og
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator-og
- namespace: openshift-strimzi
  name: openshift-strimzi
- namespace: openshift-velero
  name: managed-velero-operator
Subscription:
- namespace: openshift-addon-operator
  name: addon-operator
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-custom-domains-operator
```


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

Status:

- {}

Project:

- name: dedicated-admin
- name: openshift-addon-operator
- name: openshift-aqua
- name: openshift-backplane
- name: openshift-backplane-cee

```

- name: openshift-backplane-managed-scripts
- name: openshift-backplane-srep
- name: openshift-build-test
- name: openshift-cloud-ingress-operator
- name: openshift-codeready-workspaces
- name: openshift-custom-domains-operator
- name: openshift-customer-monitoring
- name: openshift-managed-node-metadata-operator
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-strimzi
- name: openshift-validation-webhook
- name: openshift-velero
ClusterResourceQuota:
- name: loadbalancer-quota
- name: persistent-volume-quota
SecurityContextConstraints:
- name: pcap-dedicated-admins
- name: splunkforwarder
SplunkForwarder:
- namespace: openshift-security
  name: splunkforwarder
Group:
- name: dedicated-admins
User:
- name: backplane-cluster-admin

```

3.3. OPENSIFT DEDICATED ADD-ON NAMESPACES

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

Example 3.2. 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
  gpu-operator: redhat-gpu-operator
  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
acm-operator: acm
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

```

3.4. OPENSIFT DEDICATED VALIDATING WEBHOOKS

OpenShift Dedicated 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. Upon request the webhooks accept or reject the request. 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 3.3. 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": "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": "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": "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"
  ],
  "scope": "*"
},
{
  "operations": [
    "*"
  ],
  "apiGroups": [
    "operator.openshift.io"
  ],
  "apiVersions": [
    "*"
  ],
  "resources": [
    "kubeapiservers",
    "openshiftapiservers"
  ],
  "scope": "*"
},
{
  "operations": [
    "*"
  ],
  "apiGroups": [
    ""
  ],
  "apiVersions": [
    "*"
  ],
  "resources": [
    "nodes",
    "nodes/*"
  ],
  "scope": "*"
},
{

```

```

"operations": [
  "*"
],
"apiGroups": [
  "managed.openshift.io"
],
"apiVersions": [
  "*"
],
"resources": [
  "subjectpermissions",
  "subjectpermissions/*"
],
"scope": "*"
},
{
  "operations": [
    "*"
  ],
  "apiGroups": [
    "network.openshift.io"
  ],
  "apiVersions": [
    "*"
  ],
  "resources": [
    "netnamespaces",
    "netnamespaces/*"
  ],
  "scope": "*"
}
],
"documentString": "Managed OpenShift customers may not manage any objects in the
following APIgroups [network.openshift.io cloudcredential.openshift.io managed.openshift.io
ocmagent.managed.openshift.io upgrade.managed.openshift.io config.openshift.io
operator.openshift.io machine.openshift.io admissionregistration.k8s.io
addons.managed.openshift.io cloudingress.managed.openshift.io
splunkforwarder.managed.openshift.io autoscaling.openshift.io], nor may Managed OpenShift
customers alter the APIServer, KubeAPIServer, OpenShiftAPIServer, ClusterVersion, Node or
SubjectPermission objects."
},
{
  "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 node-exporter nonroot privileged restricted]"
},
{
  "webhookName": "techpreviewnougrade-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."
}
]
```