Red Hat OpenShift Service on AWS 4

故障排除

了解对 Red Hat OpenShift Service on AWS 的支持

Last Updated: 2023-03-25

Red Hat OpenShift Service on AWS 4 故障排除

了解对 Red Hat OpenShift Service on AWS 的支持

法律通告

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.

摘要

本文档提供有关获取对 Red Hat OpenShift Service on AWS (ROSA) 的支持的信息。

目录

第 1 章 通过连接集群进行远程健康监控

1.1. 显示远程健康监控收集的数据

作为管理员，您可以查看 Telemetry 和 Insights Operator 收集的指标。

1.1.1. 显示 Telemetry 收集的数据

您可以查看 Telemetry 收集的集群和组件的时间序列数据。

前提条件

- 已安装 OpenShift Container Platform CLI (**oc**)。
- 您可以使用具有 **cluster-admin** 角色或 **cluster-monitoring-view** 角色的用户访问集群。

流程

1. 登录到集群。
2. 运行以下命令，它会查询集群的 Prometheus 服务并返回由 Telemetry 收集的完整时间序列数据集合：

```
$ 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:provisione
r: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_fsync_duration_seconds:histogram_quantile",quantile="0.
99"}' \
--data-urlencode 'match[]={__name__="instance:etcd_mvcc_db_total_size_in_bytes:sum"}' \
--data-urlencode 'match[]=
{__name__="instance:etcd_network_peer_round_trip_time_seconds:histogram_quantile",quant
ile="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",quan
tile="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"}'
```

1.1.2. 显示 Insights Operator 收集的数据

您可以查看 Insights Operator 收集的数据。

前提条件

- 使用具有 **cluster-admin** 角色的用户访问集群。

流程

1. 为 Insights Operator 查找当前正在运行的 pod 的名称：

```
$ INSIGHTS_OPERATOR_POD=$(oc get pods --namespace=openshift-insights -o custom-
columns=:metadata.name --no-headers  --field-selector=status.phase=Running)
```

2. 复制 Insights Operator 收集的最近数据存档：

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

Insights Operator 最近存档可在 **insights-data** 目录中找到。

第 2 章 已过期令牌故障排除

2.1. 过期的离线访问令牌故障排除

如果使用 **rosa** CLI 和 api.openshift.com 离线访问令牌过期，则会出现错误消息。当 sso.redhat.com 无效令牌时会出现这种情况。

输出示例

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

流程

- 通过以下 URL 生成一个新的离线访问令牌：每次访问 URL 时都会生成一个新的离线访问令牌。
  - Red Hat OpenShift Service on AWS (ROSA):
    https://console.redhat.com/openshift/token/rosa

第 3 章 安装故障排除

3.1. 安装故障排除

3.1.1. 检查安装或卸载日志

显示安装日志：

- 运行以下命令，使用您的集群名替换 **<cluster_name>**：

```
$ rosa logs install --cluster=<cluster_name>
```

- 要监视日志，请包含 **--watch** 标志：

```
$ rosa logs install --cluster=<cluster_name> --watch
```

显示卸载日志：

- 运行以下命令，使用您的集群名替换 **<cluster_name>**：

```
$ rosa logs uninstall --cluster=<cluster_name>
```

- 要监视日志，请包含 **--watch** 标志：

```
$ rosa logs uninstall --cluster=<cluster_name> --watch
```

3.1.2. 为没有 STS 的集群验证 AWS 帐户权限

运行以下命令，以验证 AWS 帐户是否有正确的权限。此命令只验证没有使用 AWS 安全令牌服务 (STS) 的集群的权限：

```
$ rosa verify permissions
```

如果您收到任何错误，请重复检查以确保没有将 SCP 应用到 AWS 帐户。如果需要使用 SCP，请参阅 Red Hat Requirements for Customer Cloud Subscriptions 以了解有关最低 SCP 要求的信息。

3.1.3. 验证 AWS 帐户和配额

运行以下命令，验证您在 AWS 帐户上有可用的配额：

```
$ rosa verify quota
```

AWS 配额根据区域进行更改。确保您为正确的 AWS 区域验证配额。如果需要提高配额，进入 AWS 控制台，并为失败的服务请求配额增加。

3.1.4. AWS 通知电子邮件

在创建集群时，Red Hat OpenShift Service on AWS 服务在所有支持的区域中创建小实例。此检查可确保使用的 AWS 帐户可以部署到每个支持的区域。

对于不使用所有支持的区域的 AWS 帐户，AWS 可能会发送一个或多个电子邮件确认"Your Request For Access AWS Resources Has Been Validated"。此电子邮件的发送者通常是 aws-verification@amazon.com。

这是预期的行为，因为 Red Hat OpenShift Service on AWS 服务正在验证 AWS 帐户配置。

第 4 章 IAM 角色故障排除

4.1. 解决 OCM-ROLES 和 USER-ROLE IAM 资源的问题

当尝试使用 **rosa** CLI 创建集群时，您可能会收到错误。

输出示例

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

此错误意味着 **user-role** IAM 角色没有链接到 AWS 帐户。此错误的最常见原因是红帽机构中的其他用户创建了 **ocm-role** IAM 角色。需要创建您的 **user-role** IAM 角色。

注意

在任何用户设置链接到红帽帐户的 **ocm-role** IAM 资源后，任何希望在该红帽机构中创建集群的后续用户都必须具有 **user-role** IAM 角色来置备集群。

流程

- 使用以下命令评估 **ocm-role** 和 **user-role** IAM 角色的状态：

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

输出示例

```
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
```

输出示例

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

在这些命令的结果中，您可以创建并链接缺少的 IAM 资源。

4.1.1. 创建 OpenShift Cluster Manager IAM 角色

您可以使用命令行界面 (CLI) 创建 OpenShift Cluster Manager IAM 角色。

前提条件

- 您有一个 AWS 帐户。

- 在 OpenShift Cluster Manager 组织中具有红帽机构管理员权限。
- 您有安装 AWS 范围的角色所需的权限。
- 您已在安装主机上安装和配置了最新的 AWS (**aws**) 和 ROSA (**rosa**) CLI。

流程

- 要使用基本权限创建 ocm-role IAM 角色，请运行以下命令：

```
$ rosa create ocm-role
```

- 要使用 admin 权限创建 ocm-role IAM 角色，请运行以下命令：

```
$ rosa create ocm-role --admin
```

此命令允许您通过指定特定属性来创建角色。以下示例输出显示选择了"自动模式"，它允许 **rosa** CLI 创建 Operator 角色和策略。如需更多信息，请参阅附加资源中的"集群范围的角色创建"。

输出示例

```
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. 所有创建的 AWS 资源的前缀值。在本例中，**ManagedOpenShift** 会预先填充所有 AWS 资源。
2. 如果您希望此角色具有额外的 admin 权限，请选择。

注意

如果使用 **--admin** 选项，则不会显示此提示。

3. 用于设置权限边界的策略的 Amazon 资源名称 (ARN)。
4. 选择如何创建 AWS 角色的方法。使用 **auto**，（**ros** CLI 工具）生成并链接角色和策略。在 **自动** 模式中，您收到一些不同的提示来创建 AWS 角色。
5. auto 方法询问您是否要使用您的前缀创建特定的 **ocm-role**。
6. 确认您要将 IAM 角色与 OpenShift Cluster Manager 关联。

7 将创建的角色与 AWS 组织相关联。

4.1.2. 创建 user-role IAM 角色

您可以使用命令行界面 (CLI) 创建 OpenShift Cluster Manager IAM 角色。

前提条件

- 您有一个 AWS 帐户。
- 您已在安装主机上安装和配置了最新的 AWS (**aws**) 和 ROSA (**rosa**) CLI。

流程

- 要使用基本权限创建 ocm-role IAM 角色，请运行以下命令：

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

此命令允许您通过指定特定属性来创建角色。以下示例输出显示选择了"自动模式"，它允许 **rosa** CLI 创建 Operator 角色和策略。如需更多信息，请参阅附加资源中的"了解自动和手动部署模式"。

输出示例

```
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 所有创建的 AWS 资源的前缀值。在本例中，**ManagedOpenShift** 会预先填充所有 AWS 资源。

2 用于设置权限边界的策略的 Amazon 资源名称 (ARN)。

3 选择如何创建 AWS 角色的方法。使用 **auto**，**rosa** CLI 工具会生成角色，并将角色链接到 AWS 帐户。在 **auto** 模式中，您收到一些不同的提示来创建 AWS 角色。

4 auto 方法询问您是否要使用您的前缀创建特定的 **user-role**。

5 将创建的角色与 AWS 组织相关联。

4.1.3. 链接 AWS 帐户

您可以使用 **rosa** CLI 将 AWS 帐户链接到现有的 IAM 角色。

前提条件

- 您有一个 AWS 帐户。
- 您可以使用 OpenShift Cluster Manager Hybrid Cloud Console 创建集群。
- 您有安装 AWS 范围的角色所需的权限。如需更多信息，请参阅本节的"附加资源"。
- 您已在安装主机上安装和配置了最新的 AWS (**aws**) 和 ROSA (**rosa**) CLI。
- 您已创建了 **ocm-role** 和 **user-role** IAM 角色，但还没有将它们链接到 AWS 帐户。您可以运行以下命令来检查您的 IAM 角色是否已链接：

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

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

如果这两个角色的 **Linked** 列中显示了 **Yes**，您已将角色链接到 AWS 帐户。

流程

1. 在 CLI 中，使用 Amazon Resource Name (ARN) 将 **ocm-role** 资源链接到红帽机构：

注意

您必须具有红帽机构管理员权限才能运行 **rosa link** 命令。将 **ocm-role** 资源与 AWS 帐户链接后，对机构的所有用户可见。

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

输出示例

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

2. 在 CLI 中，使用您的 Amazon 资源名称 (ARN) 将您的 **user-role** 资源链接到您的红帽用户帐户：

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

输出示例

```
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. 将多个 AWS 帐户与红帽机构相关联

您可以将多个 AWS 帐户与红帽机构相关联。通过关联多个帐户，您可以从您的红帽机构在 AWS (ROSA) 集群上创建 Red Hat OpenShift 服务。

使用此功能，您可以使用多个 AWS 配置集作为区域密集型环境在不同的 AWS 区域中创建集群。

前提条件

- 您有一个 AWS 帐户。
- 您可以使用 OpenShift Cluster Manager Hybrid Cloud Console 创建集群。
- 您有安装 AWS 范围的角色所需的权限。
- 您已在安装主机上安装和配置了最新的 AWS (**aws**) 和 ROSA (**rosa**) CLI。
- 您已创建了 **ocm-role** 和 **user-role** IAM 角色。

流程

要关联一个额外的 AWS 帐户，首先在本地 AWS 配置中创建配置集。然后，通过在其他 AWS 帐户中创建 **ocm-role**、用户帐户角色，将该帐户与您的红帽机构相关联。

要在附加区域中创建角色，在运行 **rosa create** 命令时指定 **--profile <aws-profile>** 参数，将 **<aws_profile>** 替换为附加帐户配置集名称：

- 在创建 OpenShift Cluster Manager 角色时指定 AWS 帐户配置集：

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

- 在创建用户角色时指定 AWS 帐户配置集：

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

- 在创建帐户角色时指定 AWS 帐户配置集：

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

注意

如果没有指定配置集，则使用默认 AWS 配置集。

第 5 章 集群部署故障排除

本文档论述了如何对集群部署错误进行故障排除。

5.1. 获取失败集群的信息

如果集群部署失败，集群将进入"错误"状态。

流程

运行以下命令来获取更多信息：

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

5.2. 无法创建具有 OSDCCSADMIN 错误的集群

如果集群创建操作失败，您可以收到以下出错信息。

输出示例

```
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.
```

流程

解决此问题的步骤：

1. 删除堆栈：

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

2. 重新初始化您的帐户：

```
$ rosa init
```

5.3. 创建 ELASTIC LOAD BALANCING (ELB)服务链接的角色

如果您还没有在 AWS 帐户中创建负载均衡器，则 Elastic Load Balancing (ELB)的服务链接角色可能尚不存在。您可能会收到以下错误：

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

流程

要解决这个问题，请确保您的 AWS 帐户中存在角色。如果没有，使用以下命令创建此角色：

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

注意

此命令只需要为每个帐户执行一次。

5.4. 修复无法删除的集群

在某些情况下，如果您尝试删除集群，OpenShift Cluster Manager Hybrid Cloud Console 中会出现以下错误。

> 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

如果您尝试从 CLI 删除集群，则会出现以下错误。

> 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

当 **user-role** 被取消链接或删除，会发生此错误。

流程

1. 运行以下命令来创建 **user-role** IAM 资源：

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

2. 在可以看到创建的角色后，您可以删除集群。以下确认，角色已创建并被链接：

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

第 6 章 RED HAT OPENSHIFT SERVICE ON AWS 受管资源

6.1. 概述

以下涵盖了由服务可靠性工程平台(SRE-P)团队管理或保护的所有资源。客户不应该尝试修改这些资源，因为这样做可能会导致集群不稳定。

6.2. HIVE 管理的资源

以下列表显示了由 OpenShift Hive 管理的 Red Hat OpenShift Service on AWS 资源，这是集中团队配置管理系统。这些资源除了在安装过程中创建的 OpenShift Container Platform 资源外。OpenShift Hive 不断尝试在所有 Red Hat OpenShift Service on AWS 间保持一致性。应该通过 OpenShift Cluster Manager 对 Red Hat OpenShift Service on AWS 进行修改，以便 OpenShift Cluster Manager 和 Hive 同步。如果 OpenShift Cluster Manager 不支持修改问题中的资源，请联系 ocm-feedback@redhat.com。

例 6.1. Hive 管理的资源列表

```
Resources:
  ConfigMap:
  - namespace: openshift-deployment-validation-operator
    name: deployment-validation-operator-config
  - namespace: openshift-managed-upgrade-operator
    name: managed-upgrade-operator-config
  - namespace: openshift-monitoring
    name: cluster-monitoring-config
  - namespace: openshift-monitoring
    name: managed-namespaces
  - namespace: openshift-monitoring
    name: ocp-namespaces
  - namespace: openshift-monitoring
    name: osd-rebalance-infra-nodes
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter-code
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter-trusted-ca-bundle
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter-code
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter-trusted-ca-bundle
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols-code
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols-trusted-ca-bundle
  - namespace: openshift-monitoring
    name: token-refresher-trusted-ca-bundle
  - namespace: openshift-security
    name: osd-audit-policy
  - namespace: openshift-validation-webhook
    name: webhook-cert
  Endpoints:
  - namespace: openshift-deployment-validation-operator
    name: deployment-validation-operator-metrics
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter
```

```
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
- namespace: openshift-monitoring
  name: token-refresher
- namespace: openshift-validation-webhook
  name: validation-webhook
Namespace:
- name: dedicated-admin
- name: openshift-addon-operator
- name: openshift-aqua
- name: openshift-aws-vpce-operator
- name: openshift-backplane
- name: openshift-backplane-cee
- name: openshift-backplane-csa
- name: openshift-backplane-cse
- name: openshift-backplane-csm
- name: openshift-backplane-managed-scripts
- name: openshift-backplane-mobb
- name: openshift-backplane-srep
- name: openshift-backplane-tam
- name: openshift-build-test
- name: openshift-cloud-ingress-operator
- name: openshift-codeready-workspaces
- name: openshift-custom-domains-operator
- name: openshift-customer-monitoring
- name: openshift-deployment-validation-operator
- name: openshift-managed-node-metadata-operator
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-observability-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-strimzi
- name: openshift-validation-webhook
- name: openshift-velero
- name: openshift-monitoring
- name: openshift
- name: openshift-cluster-version
ReplicationController:
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-1
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-1
Secret:
- namespace: openshift-authentication
  name: v4-0-config-user-idp-0-file-data
- namespace: openshift-authentication
  name: v4-0-config-user-template-error
```

```
  - namespace: openshift-authentication
    name: v4-0-config-user-template-login
  - namespace: openshift-authentication
    name: v4-0-config-user-template-provider-selection
  - namespace: openshift-config
    name: htpasswd-secret
  - namespace: openshift-config
    name: osd-oauth-templates-errors
  - namespace: openshift-config
    name: osd-oauth-templates-login
  - namespace: openshift-config
    name: osd-oauth-templates-providers
  - namespace: openshift-config
    name: sbasabat-mc-primary-cert-bundle-secret
  - namespace: openshift-config
    name: support
  - namespace: openshift-ingress
    name: sbasabat-mc-primary-cert-bundle-secret
  - namespace: openshift-kube-apiserver
    name: user-serving-cert-000
  - namespace: openshift-kube-apiserver
    name: user-serving-cert-001
  - namespace: openshift-monitoring
    name: dms-secret
  - namespace: openshift-monitoring
    name: observatorium-credentials
  - namespace: openshift-monitoring
    name: pd-secret
  - namespace: openshift-security
    name: splunk-auth
ServiceAccount:
  - namespace: openshift-backplane-managed-scripts
    name: osd-backplane
  - namespace: openshift-backplane-srep
    name: osd-delete-ownerrefs-serviceaccounts
  - namespace: openshift-backplane
    name: osd-delete-backplane-serviceaccounts
  - namespace: openshift-build-test
    name: sre-build-test
  - namespace: openshift-cloud-ingress-operator
    name: cloud-ingress-operator
  - namespace: openshift-custom-domains-operator
    name: custom-domains-operator
  - namespace: openshift-managed-upgrade-operator
    name: managed-upgrade-operator
  - namespace: openshift-marketplace
    name: osd-patch-subscription-source
  - namespace: openshift-monitoring
    name: configure-alertmanager-operator
  - namespace: openshift-monitoring
    name: osd-cluster-ready
  - namespace: openshift-monitoring
    name: osd-rebalance-infra-nodes
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter
  - namespace: openshift-monitoring
```

```
    name: sre-ebs-iops-reporter
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols
  - namespace: openshift-network-diagnostics
    name: sre-pod-network-connectivity-check-pruner
  - namespace: openshift-ocm-agent-operator
    name: ocm-agent-operator
  - namespace: openshift-rbac-permissions
    name: rbac-permissions-operator
  - namespace: openshift-splunk-forwarder-operator
    name: splunk-forwarder-operator
  - namespace: openshift-sre-pruning
    name: bz1980755
  - namespace: openshift-sre-pruning
    name: sre-pruner-sa
  - namespace: openshift-validation-webhook
    name: validation-webhook
  - namespace: openshift-velero
    name: managed-velero-operator
  - namespace: openshift-velero
    name: velero
  - namespace: openshift-backplane-srep
    name: UNIQUE_BACKPLANE_SERVICEACCOUNT_ID
Service:
  - namespace: openshift-deployment-validation-operator
    name: deployment-validation-operator-metrics
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols
  - namespace: openshift-monitoring
    name: token-refresher
  - namespace: openshift-validation-webhook
    name: validation-webhook
AddonOperator:
  - name: addon-operator
ValidatingWebhookConfiguration:
  - name: sre-hiveownership-validation
  - name: sre-namespace-validation
  - name: sre-pod-validation
  - name: sre-prometheusrule-validation
  - name: sre-regular-user-validation
  - name: sre-scc-validation
  - name: sre-techpreviewnoupgrade-validation
DaemonSet:
  - namespace: openshift-monitoring
    name: 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-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: openshift-backplane-managed-scripts-reader
- name: osd-cluster-ready
- name: osd-delete-backplane-script-resources
- name: osd-delete-ownerrefs-serviceaccounts
- name: osd-patch-subscription-source
- name: osd-rebalance-infra-nodes
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: splunk-forwarder-operator-clusterrolebinding
- name: sre-build-test
- name: sre-pod-network-connectivity-check-pruner
- name: sre-pruner-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: 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-build-test
- 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: osd-delete-backplane-script-resources
- namespace: openshift-build-test
  name: sre-build-test
- 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-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-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-security
  name: osd-rebalance-infra-nodes-openshift-security
```

```
- namespace: openshift-splunk-forwarder-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-strimzi
  name: dedicated-admins-openshift-strimzi
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-uwm-config-create
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-uwm-config-edit
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-uwm-managed-am-secret
- namespace: openshift-user-workload-monitoring
  name: osd-rebalance-infra-nodes-openshift-user-workload-monitoring
- namespace: openshift-velero
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-velero
  name: prometheus-k8s
Role:
- namespace: kube-system
  name: cluster-config-v1-reader
- namespace: kube-system
  name: cluster-config-v1-reader-cio
- namespace: openshift-aqua
  name: dedicated-admins-openshift-aqua
- namespace: openshift-backplane-managed-scripts
  name: osd-delete-backplane-script-resources
- namespace: openshift-build-test
  name: sre-build-test
- namespace: openshift-codeready-workspaces
  name: dedicated-admins-openshift-codeready-workspaces
- namespace: openshift-config
  name: dedicated-admins-project-request
- namespace: openshift-config
  name: dedicated-admins-registry-cas-project
- namespace: openshift-config
  name: muo-pullsecret-reader
- namespace: openshift-config
  name: oao-openshiftconfig-reader
- namespace: openshift-config
  name: osd-cluster-ready
- namespace: openshift-customer-monitoring
  name: dedicated-admins-openshift-customer-monitoring
- namespace: openshift-customer-monitoring
  name: prometheus-k8s-openshift-customer-monitoring
- namespace: openshift-dns
  name: dedicated-admins-openshift-dns
- namespace: openshift-dns
  name: osd-rebalance-infra-nodes-openshift-dns
- namespace: openshift-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-ingress
  name: cloud-ingress-operator
- namespace: openshift-kube-apiserver
  name: cloud-ingress-operator
- namespace: openshift-machine-api
  name: cloud-ingress-operator
- namespace: openshift-machine-api
```

```
    name: osd-cluster-ready
  - namespace: openshift-marketplace
    name: dedicated-admins-openshift-marketplace
  - namespace: openshift-monitoring
    name: backplane-cee
  - namespace: openshift-monitoring
    name: muo-monitoring-reader
  - namespace: openshift-monitoring
    name: oao-monitoring-manager
  - namespace: openshift-monitoring
    name: osd-cluster-ready
  - namespace: openshift-monitoring
    name: osd-rebalance-infra-nodes-openshift-monitoring
  - namespace: openshift-must-gather-operator
    name: backplane-cee-mustgather
  - namespace: openshift-must-gather-operator
    name: backplane-srep-mustgather
  - namespace: openshift-network-diagnostics
    name: sre-pod-network-connectivity-check-pruner
  - namespace: openshift-operators
    name: dedicated-admins-openshift-operators
  - namespace: openshift-osd-metrics
    name: prometheus-k8s
  - namespace: openshift-rbac-permissions
    name: prometheus-k8s
  - namespace: openshift-security
    name: osd-rebalance-infra-nodes-openshift-security
  - namespace: openshift-strimzi
    name: dedicated-admins-openshift-strimzi
  - namespace: openshift-user-workload-monitoring
    name: dedicated-admins-user-workload-monitoring-create-cm
  - namespace: openshift-user-workload-monitoring
    name: dedicated-admins-user-workload-monitoring-manage-am-secret
  - namespace: openshift-user-workload-monitoring
    name: 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-build-test
    name: sre-build-test
  - namespace: openshift-marketplace
    name: osd-patch-subscription-source
  - namespace: openshift-monitoring
    name: osd-rebalance-infra-nodes
  - namespace: openshift-network-diagnostics
    name: sre-pod-network-connectivity-check-pruner
  - namespace: openshift-sre-pruning
    name: builds-pruner
  - namespace: openshift-sre-pruning
    name: bz1980755
```

```
- namespace: openshift-sre-pruning
  name: deployments-pruner
Job:
- namespace: openshift-monitoring
  name: osd-cluster-ready
CredentialsRequest:
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-credentials-aws
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-credentials-gcp
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-aws-credentials
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-aws-credentials
- namespace: openshift-velero
  name: managed-velero-operator-iam-credentials-aws
- namespace: openshift-velero
  name: managed-velero-operator-iam-credentials-gcp
APIScheme:
- namespace: openshift-cloud-ingress-operator
  name: rh-api
PublishingStrategy:
- namespace: openshift-cloud-ingress-operator
  name: publishingstrategy
EndpointSlice:
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-metrics-rhtwg
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter-4cw9r
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-6tx5g
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-gmdhs
- namespace: openshift-monitoring
  name: token-refresher-v5cpg
- namespace: openshift-validation-webhook
  name: validation-webhook-bl99t
MachineHealthCheck:
- namespace: openshift-machine-api
  name: srep-infra-healthcheck
- namespace: openshift-machine-api
  name: srep-metal-worker-healthcheck
- namespace: openshift-machine-api
  name: srep-worker-healthcheck
MachineSet:
- namespace: openshift-machine-api
  name: sbasabat-mc-qhqkn-infra-us-east-1a
- namespace: openshift-machine-api
  name: sbasabat-mc-qhqkn-worker-us-east-1a
ContainerRuntimeConfig:
- name: custom-crio
KubeletConfig:
- name: custom-kubelet
SubjectPermission:
- namespace: openshift-rbac-permissions
  name: backplane-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
  - namespace: openshift-rbac-permissions
    name: sre-build-test
VeleroInstall:
  - namespace: openshift-velero
    name: cluster
PrometheusRule:
  - namespace: openshift-monitoring
    name: rhmi-sre-cluster-admins
  - namespace: openshift-monitoring
    name: rhoam-sre-cluster-admins
  - namespace: openshift-monitoring
    name: sre-alertmanager-silences-active
  - namespace: openshift-monitoring
    name: sre-alerts-stuck-builds
  - namespace: openshift-monitoring
    name: sre-alerts-stuck-volumes
  - namespace: openshift-monitoring
    name: sre-cloud-ingress-operator-offline-alerts
  - namespace: openshift-monitoring
    name: sre-configure-alertmanager-operator-offline-alerts
  - namespace: openshift-monitoring
    name: sre-control-plane-resizing-alerts
  - namespace: openshift-monitoring
    name: sre-dns-alerts
  - namespace: openshift-monitoring
    name: sre-ebs-iops-burstbalance
  - namespace: openshift-monitoring
    name: sre-elasticsearch-jobs
  - namespace: openshift-monitoring
    name: sre-elasticsearch-managed-notification-alerts
```

```
  - namespace: openshift-monitoring
    name: sre-excessive-memory
  - namespace: openshift-monitoring
    name: sre-haproxy-reload-fail
  - namespace: openshift-monitoring
    name: sre-internal-slo-recording-rules
  - namespace: openshift-monitoring
    name: sre-kubequotaexceeded
  - namespace: openshift-monitoring
    name: sre-leader-election-master-status-alerts
  - namespace: openshift-monitoring
    name: sre-managed-node-metadata-operator-alerts
  - namespace: openshift-monitoring
    name: sre-managed-notification-alerts
  - namespace: openshift-monitoring
    name: sre-managed-upgrade-operator-alerts
  - namespace: openshift-monitoring
    name: sre-managed-velero-operator-alerts
  - namespace: openshift-monitoring
    name: sre-node-unschedulable
  - namespace: openshift-monitoring
    name: sre-oauth-server
  - namespace: openshift-monitoring
    name: sre-pending-csr-alert
  - namespace: openshift-monitoring
    name: sre-proxy-managed-notification-alerts
  - namespace: openshift-monitoring
    name: sre-pruning
  - namespace: openshift-monitoring
    name: sre-pv
  - namespace: openshift-monitoring
    name: sre-router-health
  - namespace: openshift-monitoring
    name: sre-runaway-sdn-preventing-container-creation
  - namespace: openshift-monitoring
    name: sre-slo-recording-rules
  - namespace: openshift-monitoring
    name: sre-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
CatalogSource:
- namespace: openshift-addon-operator
  name: addon-operator-catalog
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-registry
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator-registry
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-catalog
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator-registry
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator-catalog
- namespace: openshift-monitoring
  name: configure-alertmanager-operator-registry
- namespace: openshift-must-gather-operator
  name: must-gather-operator-registry
- namespace: openshift-observability-operator
  name: observability-operator-catalog
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator-registry
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter-registry
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator-registry
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator-registry
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator-catalog
- namespace: openshift-velero
  name: managed-velero-operator-registry
OperatorGroup:
- namespace: openshift-addon-operator
  name: addon-operator-og
- namespace: openshift-aqua
  name: openshift-aqua
```

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

```
  name: rbac-permissions-operator
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator
- namespace: openshift-splunk-forwarder-operator
  name: openshift-splunk-forwarder-operator
- namespace: openshift-velero
  name: managed-velero-operator
PackageManifest:
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator
- namespace: openshift-addon-operator
  name: addon-operator
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator
- namespace: openshift-velero
  name: managed-velero-operator
- namespace: openshift-deployment-validation-operator
  name: managed-upgrade-operator
- namespace: openshift-custom-domains-operator
  name: managed-node-metadata-operator
- namespace: openshift-route-monitor-operator
  name: custom-domains-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator
- namespace: openshift-observability-operator
  name: observability-operator
- namespace: openshift-monitoring
  name: configure-alertmanager-operator
- namespace: openshift-must-gather-operator
  name: deployment-validation-operator
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter
Status:
- {}
Project:
- name: dedicated-admin
- name: openshift-addon-operator
- name: openshift-aqua
- name: openshift-backplane
- name: openshift-backplane-cee
- name: openshift-backplane-csa
- name: openshift-backplane-cse
- name: openshift-backplane-csm
- name: openshift-backplane-managed-scripts
- name: openshift-backplane-mobb
- name: openshift-backplane-srep
- name: openshift-backplane-tam
- name: openshift-build-test
- name: openshift-cloud-ingress-operator
- name: openshift-codeready-workspaces
```

```
- name: openshift-custom-domains-operator
- name: openshift-customer-monitoring
- name: openshift-deployment-validation-operator
- name: openshift-managed-node-metadata-operator
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-observability-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-strimzi
- name: openshift-validation-webhook
- name: openshift-velero
ClusterResourceQuota:
- name: loadbalancer-quota
- name: persistent-volume-quota
SecurityContextConstraints:
- name: pcap-dedicated-admins
- name: splunkforwarder
SplunkForwarder:
- namespace: openshift-security
  name: splunkforwarder
Group:
- name: dedicated-admins
User:
- name: backplane-cluster-admin
Backup:
- namespace: openshift-velero
  name: daily-full-backup-20221123112305
- namespace: openshift-velero
  name: daily-full-backup-20221125042537
- namespace: openshift-velero
  name: daily-full-backup-20221126010038
- namespace: openshift-velero
  name: daily-full-backup-20221127010039
- namespace: openshift-velero
  name: daily-full-backup-20221128010040
- namespace: openshift-velero
  name: daily-full-backup-20221129050847
- namespace: openshift-velero
  name: hourly-object-backup-20221128051740
- namespace: openshift-velero
  name: hourly-object-backup-20221128061740
- namespace: openshift-velero
  name: hourly-object-backup-20221128071740
- namespace: openshift-velero
  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 OPENSHIFT SERVICE ON AWS 附加组件命名空间

Red Hat OpenShift Service on AWS 附加组件是可在集群安装后安装的服务。这些额外服务包括 Red Hat OpenShift Dev Spaces、Red Hat OpenShift API Management 和 Cluster Logging Operator。对以下命名空间中资源的任何更改都会被升级过程中的附加组件覆盖，这可能会导致附加功能不支持的配置。

例 6.2. 附加组件受管命名空间列表

```
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
  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
```

6.4. RED HAT OPENSHIFT SERVICE ON AWS 验证 WEBHOOK

Red Hat OpenShift Service on AWS 验证 webhook 是由 OpenShift SRE 团队维护的一组动态准入控制。

这些 HTTP 回调（也称为 Webhook）用于各种类型的请求，以确保集群的稳定性。以下列表描述了各种 webhook，包含控制的注册操作和资源的规则。任何尝试绕过这些验证 Webhook 可能会影响集群的稳定性和支持性。

例 6.3. 验证 Webhook 列表


```
[
  {
    "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": "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."
  }
]
```