



OpenShift Dedicated 4

支持

OpenShift Dedicated 支持。

OpenShift Dedicated 4 支持

OpenShift Dedicated 支持。

Legal Notice

Copyright © 2025 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

提供了集群管理员工具，用于为集群、监控和故障排除收集数据。

Table of Contents

第 1 章 支持概述	3
1.1. 获得支持	3
1.2. 远程健康监控问题	3
1.3. 收集有关集群的数据	3
1.4. 故障排除问题	3
第 2 章 管理集群资源	5
2.1. 与集群资源交互	5
第 3 章 获取支持	6
3.1. 获取支持	6
3.2. 关于红帽知识库	6
3.3. 搜索红帽知识库	6
3.4. 提交支持问题单	7
3.5. 其他资源	8
第 4 章 通过连接集群进行远程健康监控	9
4.1. 关于远程健康监控	9
4.2. 显示远程健康监控收集的数据	13
4.3. 使用 INSIGHTS 发现集群中的问题	16
4.4. 使用 INSIGHTS OPERATOR	21
第 5 章 收集集群数据	24
5.1. 关于 MUST-GATHER 工具	24
5.2. 获取集群 ID	33
5.3. 查询集群节点 JOURNAL 日志	33
5.4. 网络追踪方法	34
5.5. 收集主机网络追踪	35
5.6. 从 OPENSIFT DEDICATED 节点或容器收集网络追踪	36
5.7. 为红帽支持提供诊断数据	38
5.8. 关于 TOOLBOX	39
第 6 章 集群规格总结	41
6.1. 使用集群版本对象总结集群规格	41
第 7 章 故障排除	42
7.1. 对 GCP 集群部署上的 OPENSIFT DEDICATED 进行故障排除	42
7.2. 验证节点健康状况	43
7.3. TROUBLESHOOTING OPERATOR 的问题	43
7.4. 检查 POD 问题	49
7.5. 对 SOURCE-TO-IMAGE 进行故障排除	55
7.6. 存储问题故障排除	58
7.7. 调查监控问题	58
7.8. 诊断 OPENSIFT CLI (OC) 问题	63
7.9. 红帽受管资源	65

第 1 章 支持概述

红帽提供了集群管理员工具，用于为集群、监控和故障排除收集数据。

1.1. 获得支持

[获取支持](#)：访问红帽客户门户网站查看知识库文章、提交支持问题单以及查看其他产品文档和资源。

1.2. 远程健康监控问题

[远程健康监控问题](#)：OpenShift Dedicated 会收集有关集群的遥测和配置数据，并使用 Telemeter Client 和 Insights Operator 向红帽报告。红帽使用此数据了解并解决 [连接的集群中的问题](#)。OpenShift Dedicated 使用以下方法收集数据和监控健康状况：

- **Telemetry**：遥测客户端收集并每 4 分 30 秒将标值上传至红帽。红帽将此数据用于：
 - 监控集群。
 - 推出 OpenShift Dedicated 升级。
 - 改进升级体验。
- **Insights Operator**：默认情况下，OpenShift Dedicated 安装并启用 Insights Operator，该 Operator 每两小时报告配置和组件故障状态。Insights Operator 有助于：
 - 主动识别潜在的集群问题。
 - 在 Red Hat OpenShift Cluster Manager 中提供解决方案和预防性操作。

您可以[查看遥测信息](#)。

如果您启用了远程健康报告，[使用 Insights 来识别集群的问题](#)。您可以选择禁用远程健康报告。

1.3. 收集有关集群的数据

[收集有关集群的数据](#)：红帽建议在打开支持问题单时收集您的调试信息。这有助于红帽支持执行根本原因分析。集群管理员可以使用以下方法收集有关集群的数据：

- **must-gather 工具**：使用 **must-gather** 工具来收集有关集群的信息并调试问题。
- **sosreport**：使用 **sosreport** 工具收集配置详情、系统信息和诊断数据用于调试目的。
- **集群 ID**：在向红帽支持提供信息时，获取集群的唯一标识符。
- **集群节点 journal 日志**：收集 **journald** 单元日志和独立集群节点上的 **/var/log** 中的日志，以排除与节点相关的问题。
- **网络追踪**：从特定的 OpenShift Dedicated 集群节点或容器提供给红帽支持提供网络数据包追踪，以帮助排除与网络相关的问题。

1.4. 故障排除问题

集群管理员可以监控并排除以下 OpenShift Dedicated 组件问题：

- [节点问题](#)：集群管理员可以通过查看节点的状态、资源使用量和配置来验证和排除节点相关问题。您可以查询以下内容：
 - 节点上的 kubelet 状态。
 - 集群节点日志。
- [Operator 问题](#)：集群管理员可以执行以下操作来解决 Operator 问题：
 - 验证 Operator 订阅状态。
 - 检查 Operator pod 健康状况。
 - 收集 Operator 日志。
- [Pod 问题](#)：集群管理员可以通过查看 pod 的状态并完成以下内容来排除与 pod 相关的问题：
 - 查看 pod 和容器日志。
 - 启动具有 root 访问权限的 debug pod。
- [Source-to-image 问题](#)：集群管理员可以观察 S2I 阶段，以确定 S2I 进程中的故障发生位置。收集以下内容来解决 Source-to-Image(S2I)问题：
 - Source-to-Image 诊断数据。
 - 用于调查应用程序故障的应用程序诊断数据。
- [存储问题](#)：当无法在新节点中挂载卷时，会发生多附加存储错误，因为失败的节点无法卸载附加的卷。集群管理员可执行以下操作解决多附加存储问题：
 - 使用 RWX 卷启用多个附件。
 - 使用 RWO 卷时,恢复或删除故障节点。
- [监控问题](#)：集群管理员可按照监控故障排除页面中的步骤进行操作。如果您的用户定义的项目的指标不可用，或者 Prometheus 消耗了大量磁盘空间，请检查以下内容：
 - 调查用户定义的指标不可用的原因。
 - 确定为什么 Prometheus 消耗大量磁盘空间。
- [OpenShift CLI \(oc\)问题](#)：通过增加日志级别来调查 OpenShift CLI (oc) 问题。

第 2 章 管理集群资源

您可以在 OpenShift Dedicated 中应用全局配置选项。Operator 在集群中应用这些配置设置。

2.1. 与集群资源交互

您可以使用 OpenShift Dedicated 中的 OpenShift CLI(**oc**)工具与集群资源交互。运行 **oc api-resources** 命令后看到的集群资源可以被编辑。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 您可以访问 web 控制台或已安装了 **oc** CLI 工具。

流程

1. 要查看应用了哪些配置 Operator，请运行以下命令：

```
$ oc api-resources -o name | grep config.openshift.io
```

2. 要查看您可以配置的集群资源，请运行以下命令：

```
$ oc explain <resource_name>.config.openshift.io
```

3. 要查看集群中的自定义资源定义(CRD)对象配置，请运行以下命令：

```
$ oc get <resource_name>.config -o yaml
```

4. 要编辑集群资源配置，请运行以下命令：

```
$ oc edit <resource_name>.config -o yaml
```

第 3 章 获取支持

3.1. 获取支持

如果您在执行本文档所述的某个流程或 OpenShift Dedicated 时遇到问题，请访问[红帽客户门户](#)。

通过红帽客户门户网站：

- 搜索或者浏览红帽知识库，了解与红帽产品相关的文章和解决方案。
- 提交问题单给红帽支持。
- 访问其他产品文档。

要识别集群中的问题，您可以在 [OpenShift Cluster Manager](#) 中使用 Insights。Insights 提供了问题的详细信息，并在有可用的情况下，提供了如何解决问题的信息。

如果您对本文档有任何改进建议，或发现了任何错误，请为相关文档组件提交 [JIRA 问题](#)。请提供具体详情，如章节名称和 OpenShift Dedicated 版本。

3.2. 关于红帽知识库

[红帽知识库](#)提供丰富的内容以帮助您最大程度地利用红帽的产品和技术。红帽知识库包括文章、产品文档和视频，概述了安装、配置和使用红帽产品的最佳实践。另外，您还可以搜索已知问题的解决方案，其提供简洁的根原因描述和补救措施。

3.3. 搜索红帽知识库

如果出现 OpenShift Dedicated 问题，您可以执行初始搜索来确定红帽知识库中是否已存在解决方案。

先决条件

- 您有红帽客户门户网站帐户。

流程

1. 登录到 [红帽客户门户网站](#)。
2. 点 **Search**。
3. 在搜索字段中，输入与问题相关的关键字和字符串，包括：
 - OpenShift Dedicated 组件（如 **etcd**）
 - 相关步骤（比如 **安装**）
 - 警告、错误消息和其他与输出与特定的问题相关
4. 点 **Enter** 键。
5. 可选：选择 **OpenShift Dedicated** 产品过滤器。
6. 可选：选择 **Documentation** 内容类型过滤器。

3.4. 提交支持问题单

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI(**oc**)。
- 您可以访问 Red Hat OpenShift Cluster Manager。

流程

1. 登录到[红帽客户门户网站的客户支持](#) 页面。
2. 点 **Get support**。
3. 在 **客户支持** 页面的 **Cases** 选项卡中：
 - a. 可选：根据需要更改预先填充的帐户和所有者详情。
 - b. 为您的问题选择适当的类别，如 **Bug** 或 **Defect**，然后点 **Continue**。
4. 输入以下信息：
 - a. 在 **Summary** 字段中，输入简要但描述性问题概述，以及有关所经历的症状的详细信息，以及您的预期。
 - b. 从 **Product** 下拉菜单中选择 **OpenShift Dedicated**。
5. 查看推荐的红帽知识库解决方案列表，它们可能会与您要报告的问题相关。如果建议的文章没有解决这个问题，请点 **Continue**。
6. 查看更新的推荐红帽知识库解决方案列表，它们可能会与您要报告的问题相关。这个列表的范围会缩小，因为您在创建问题单的过程中提供了更多信息。如果建议的文章没有解决这个问题，请点 **Continue**。
7. 请确保提供的帐户信息是正确的，如果需要，请相应调整。
8. 检查自动填充的 OpenShift Dedicated 集群 ID 是否正确。如果不正确，请手动提供集群 ID。
 - 使用 [OpenShift Cluster Manager](#) 手动获取集群 ID：
 - a. 导航到 **Cluster List**。
 - b. 点您需要为其创建一个支持问题单的集群名称。
 - c. 在 **Overview** 选项卡的 **Details** 部分的 **Cluster ID** 字段中找到值。
 - 使用 OpenShift Dedicated Web 控制台手动获取集群 ID：
 - a. 进入到 **Home → Overview**。
 - b. 该值包括在 **Details** 中的 **Cluster ID** 项中。
 - 另外，也可以通过 OpenShift Dedicated Web 控制台创建新的支持问题单，并自动填充集群 ID。
 - a. 从工具栏导航至 **(?) help → Open Support Case**。

b. **Cluster ID** 的值会被自动填充。

- 要使用 OpenShift CLI (**oc**) 获取集群 ID，请运行以下命令：

```
$ oc get clusterversion -o jsonpath='{.items[].spec.clusterID}'{"\n"}
```

9. 完成以下提示的问题，点 **Continue**:

- 您遇到什么情况？您期望发生什么情况？
- 对业务的影响价值。
- 您在哪里遇到此行为？什么环境？
- 此行为何时发生？发生频率？重复发生？是否只在特定时间发生？

10. 上传相关的诊断数据文件并点击 **Continue**。

11. 输入相关问题单管理详情，点 **Continue**。

12. 预览问题单详情，点 **Submit**。

3.5. 其他资源

- 有关识别集群问题的详情，请参阅[使用 Insights 识别集群中的问题](#)。

第 4 章 通过连接集群进行远程健康监控

4.1. 关于远程健康监控

OpenShift Dedicated 收集集群的遥测和配置数据，并使用 Telemeter Client 和 Insights Operator 向红帽报告。提供给红帽的数据可实现本文档概述的好处。

通过 Telemetry 和 Insights Operator 向红帽报告数据的集群被称为 *连接的集群* (connected cluster)。

Telemetry 是红帽用来描述 OpenShift Dedicated Telemeter 客户端向红帽发送的信息的术语。轻量级属性从连接的集群发送到红帽，以便启用订阅管理自动化、监控集群的健康状态、提供支持以及改进客户体验。

Insights Operator 收集 OpenShift Dedicated 配置数据并将其发送到红帽。这些数据用于生成有关集群可能潜在存在的问题的分析报告。这些 insights 通过 [OpenShift Cluster Manager](#) 与集群管理员进行交流。

本文档中提供了有关这两个工具的更多信息。

Telemetry 和 Insights Operator 的优点

Telemetry 和 Insights Operator 为最终用户提供以下优点：

- **增强了识别和解决问题的能力。** 对于一些事件，最终用户可能会认为是正常的，但从更广泛深入的角度来说，红帽会对这些事件的影响有不同的评估。因此，一些问题可以被更快地识别并解决，而不需要用户创建一个支持问题单或 [Jira issue](#)。
- **高级的版本管理。** OpenShift Dedicated 提供 **candidate**、**fast** 和 **stable** 发行频道，供您选择一个更新策略。版本从 **fast** 到 **stable** 的过程取决于更新的速度以及升级过程中的事件。通过连接的集群提供的信息，红帽可以将发行版本质量提高到 **stable** 频道，并对在 **fast** 频道中发现的问题做出更快反应。
- **有针对性地对新功能的开发进行优先级排序。** 收集的数据可让您了解哪些 OpenShift Dedicated 区域被使用最多使用。通过这些信息，红帽可以专注于开发对客户有严重影响的新功能。
- **更好的支持体验。** 在[红帽客户门户网站](#)上创建支持问题单时，可以为连接的集群提供集群 ID。这可以让红帽通过使用连接的信息，简化用户的支持体验。本文档提供有关改进的支持体验的更多信息。
- **预测分析。** 通过从连接的集群收集的信息，在 [OpenShift Cluster Manager](#) 上显示集群的 insights 会被启用。红帽正在努力应用深度学习、机器学习和智能自动化，以帮助识别 OpenShift Dedicated 集群暴露的问题。

在 OpenShift Dedicated 中，远程健康报告总是被启用。您不能选择不使用它。

4.1.1. 关于 Telemetry

Telemetry 会向红帽发送一组精选的集群监控指标子集。Telemeter 客户端每四分三十秒获取一次指标值，并将数据上传到红帽。本文档中描述了这些指标。

红帽使用这一数据流来实时监控集群，必要时将对影响客户的问题做出反应。它同时还有助于红帽向客户推出 OpenShift Dedicated 升级，以便最大程度降低服务影响，持续改进升级体验。

这类调试信息将提供给红帽支持和工程团队，其访问限制等同于访问通过问题单报告的数据。红帽利用所有连接集群信息来帮助改进 OpenShift Dedicated，提高其易用性。

其他资源

- 有关升级集群的更多信息，请参阅 [OpenShift Dedicated 升级文档](#)。

4.1.1.1. Telemetry 收集的信息

Telemetry 收集以下信息：

4.1.1.1.1. 系统信息

- 版本信息，包括 OpenShift Dedicated 集群版本并安装了用于决定更新版本可用性的更新详情
- 更新信息，包括每个集群可用的更新数、用于更新的频道和镜像存储库、更新进度信息以及更新中发生的错误数
- 安装期间生成的唯一随机标识符
- 帮助红帽支持为客户提供有用支持的配置详情，包括云基础架构级别的节点配置、主机名、IP 地址、Kubernetes pod 名称、命名空间和服务
- 在集群中安装的 OpenShift Dedicated 框架组件及其状况和状态
- 为降级 Operator 列出为 "related objects" 的所有命名空间的事件
- 有关降级软件的信息
- 有关证书的有效性的信息
- 部署 OpenShift Dedicated 的供应商平台的名称及数据中心位置

4.1.1.1.2. 大小信息

- 有关集群、机器类型和机器的大小信息，包括 CPU 内核数和每个机器所使用的 RAM 量
- etcd 成员数和存储在 etcd 集群中的对象数量

4.1.1.1.3. 使用信息

- 有关组件、功能和扩展的使用情况信息
- 有关技术预览和不受支持配置的使用详情

Telemetry 不会收集任何身份识别的信息，如用户名或密码。红帽不会收集个人信息。如果红帽发现个人信息被意外地收到，红帽会删除这些信息。有关红帽隐私实践的更多信息，请参考[红帽隐私声明](#)。

4.1.1.2. 用户 Telemetry

红帽从浏览器收集匿名用户数据。这种匿名数据包括启用了遥测功能的所有集群的用户的页面、功能和资源类型。

其他注意事项：

- 用户事件被，作为一个 SHA-1 哈希。
- 用户的 IP 地址保存为 **0.0.0.0**。

- 用户名和 IP 地址永远不会保存为单独的值。

其他资源

- 如需了解如何列出 Telemetry 收集的来自 OpenShift Dedicated 的属性的详细信息，请参阅[显示 Telemetry 收集的数据](#)。
- 如需 Telemetry 从 Prometheus 收集的属性列表，请参阅[上游 cluster-monitoring-operator 源代码](#)。

4.1.2. 关于 Insights Operator

Insights Operator 会定期收集配置和组件故障状态信息，默每两小时向红帽报告这些数据。这些信息可让红帽评估配置，它提供了比 Telemetry 报告更深入的数据。

OpenShift Dedicated 用户可以在 Red Hat Hybrid Cloud Console 上的 [Insights Advisor](#) 服务中显示每个集群的报告。如果发现了任何问题，Insights 会提供更详细的信息，并在可能的情况下提供如何解决相关问题的步骤。

Insights Operator 不会收集任何身份识别信息，如用户名、密码或证书。如需有关 Red Hat Insights 数据收集和控制的的信息，请参阅[Red Hat Insights 数据和应用程序安全性](#)。

红帽使用所有连接的集群信息以实现：

- 识别潜在的集群问题，并在 Red Hat Hybrid Cloud Console 上的 [Insights Advisor](#) 服务中提供解决方案和防止动作
- 通过为产品和支持团队提供聚合和重要信息来改进 OpenShift Dedicated
- 使 OpenShift Dedicated 更直观

4.1.2.1. Insights Operator 收集的信息

Insights Operator 收集以下信息：

- 有关集群及其组件的常规信息，以识别特定于 OpenShift Dedicated 版本和环境的问题。
- 集群的配置文件（如镜像 registry 配置）来确定设置参数不正确的设置和问题。
- 集群组件中发生的错误。
- 运行更新的进度信息，以及任何组件升级的状态。
- 部署 OpenShift Dedicated 的平台以及集群所在区域的详情
- 如果 Operator 报告了一个问题，则会收集 **openshift-*** 和 **kube-*** 项目中 OpenShift Dedicated 核心 pod 的信息。这包括状态、资源、安全上下文、卷信息等。

其他资源

- [在 OpenShift 中，Insights Operator 会收集哪些数据？](#)
- 用户可以查看 Insights Operator 的源代码，并对代码进行贡献。如需 Insights Operator 收集的项目列表，请参阅[Insights Operator 上游项目](#)。

4.1.3. 了解 Telemetry 和 Insights Operator 数据流

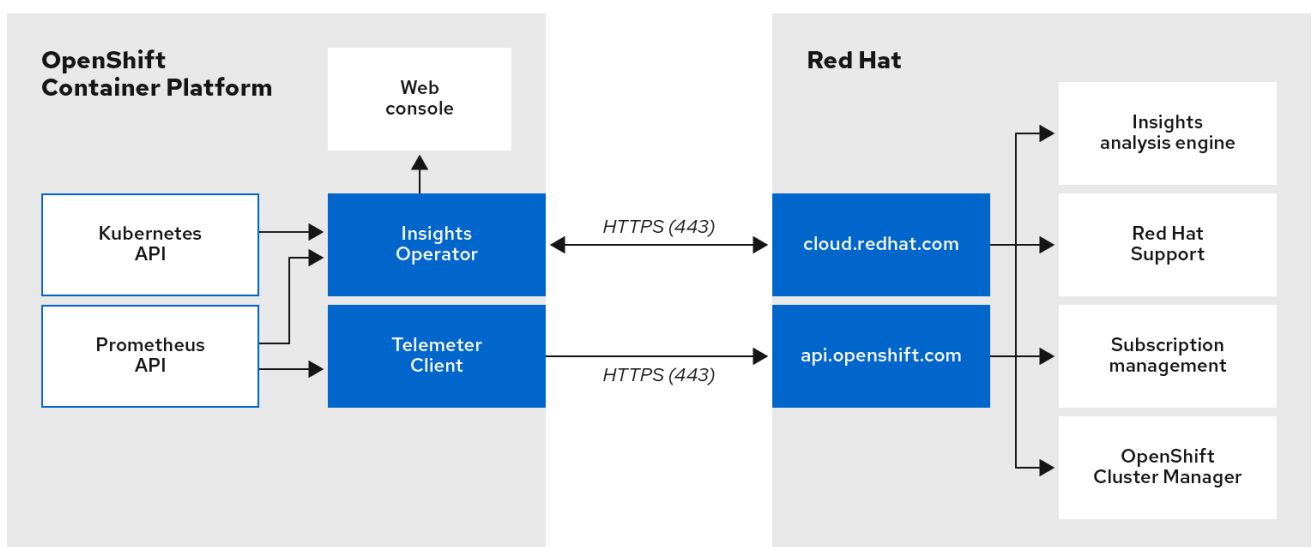
Telemeter Client 从 Prometheus API 收集所选的时间序列数据。时间序列数据每 4 分 30 秒上传到 api.openshift.com 进行处理。

Insights Operator 从 Kubernetes API 和 Prometheus API 中收集所选的数据并进行存档。该归档每两小时上传到 [OpenShift Cluster Manager](#) 进行处理。Insights Operator 还从 [OpenShift Cluster Manager](#) 下载最新的 Insights 分析。这用于填充 OpenShift Dedicated Web 控制台的 **Overview** 页面中包含的 **Insights** 状态弹出窗口。

所有与红帽的通信都使用传输层安全（TLS）和 mutual 证书验证通过加密频道进行。所有数据在传输及非活跃的情况下都会被加密。

对处理客户数据的系统是通过多因素验证和严格的授权控制来控制的。访问权限的设置是基于需要的，仅限于针对需要的操作。

telemetry 和 Insights Operator 数据流



132_OpenShift_0121

其他资源

- 如需有关 [OpenShift Dedicated 监控堆栈](#) 的更多信息，请参阅关于 OpenShift Dedicated 监控。

4.1.4. 有关如何使用远程健康监控数据的更多详情

[Telemetry 收集的信息](#)和[Insights Operator 收集的信息](#)中提供了与启用健康检查健康相关的数据收集的信息。

如本文档前面部分所述，红帽会收集您使用红帽产品的数据，如提供支持和升级、优化性能或配置、减小服务影响、识别和补救威胁、故障排除、改进提供和用户体验、响应问题、根据情况提供账单目的。

集合保护

红帽采用一些技术和机构措施来保护遥测数据和配置数据。

共享

红帽可以在红帽内部通过 Telemetry 和 Insights Operator 共享收集的数据，以提升您的用户体验。红帽可能会以汇总的方式与业务合作伙伴共享遥测和配置数据，该表格可帮助合作伙伴更好地了解其业务及其客户对红帽产品的使用，或者确保成功整合这些合作伙伴支持的产品。

第三方

红帽可能会与某些第三方合作，协助收集、分析和存储遥测和配置数据。

4.2. 显示远程健康监测收集的数据

用户控制/启用和禁用遥测和配置数据收集

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

4.2.1. 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 **dedicated-admin** 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：



注意

以下示例包含特定于 AWS 上的 OpenShift Dedicated 的一些值。

```
$ curl -G -k -H "Authorization: Bearer $(oc whoami -t)" \
https://$(oc get route prometheus-k8s-federate -n \
openshift-monitoring -o jsonpath='{.spec.host}')/federate \
--data-urlencode 'match[]={__name__=~"cluster:usage:.*"}' \
--data-urlencode 'match[]={__name__="count:up0"}' \
--data-urlencode 'match[]={__name__="count:up1"}' \
--data-urlencode 'match[]={__name__="cluster_version"}' \
--data-urlencode 'match[]={__name__="cluster_version_available_updates"}' \
--data-urlencode 'match[]={__name__="cluster_version_capability"}' \
--data-urlencode 'match[]={__name__="cluster_operator_up"}' \
--data-urlencode 'match[]={__name__="cluster_operator_conditions"}' \
--data-urlencode 'match[]={__name__="cluster_version_payload"}' \
--data-urlencode 'match[]={__name__="cluster_installer"}' \
--data-urlencode 'match[]={__name__="cluster_infrastructure_provider"}' \
--data-urlencode 'match[]={__name__="cluster_feature_set"}' \
--data-urlencode 'match[]={__name__="instance:etcd_object_counts:sum"}' \
--data-urlencode 'match[]={__name__="ALERTS",alertstate="firing"}' \
--data-urlencode 'match[]={__name__="code:apiserver_request_total:rate:sum"}' \
--data-urlencode 'match[]={__name__="cluster:capacity_cpu_cores:sum"}' \
--data-urlencode 'match[]={__name__="cluster:capacity_memory_bytes:sum"}'
```

```

--data-urlencode 'match[]={__name__="cluster:cpu_usage_cores:sum"}' \
--data-urlencode 'match[]={__name__="cluster:memory_usage_bytes:sum"}' \
--data-urlencode 'match[]={__name__="openshift:cpu_usage_cores:sum"}' \
--data-urlencode 'match[]={__name__="openshift:memory_usage_bytes:sum"}' \
--data-urlencode 'match[]={__name__="workload:cpu_usage_cores:sum"}' \
--data-urlencode 'match[]={__name__="workload:memory_usage_bytes:sum"}' \
--data-urlencode 'match[]={__name__="cluster:virt_platform_nodes:sum"}' \
--data-urlencode 'match[]={__name__="cluster:node_instance_type_count:sum"}' \
--data-urlencode 'match[]={__name__="cnv:vmi_status_running:count"}' \
--data-urlencode 'match[]={__name__="cluster:vmi_request_cpu_cores:sum"}' \
--data-urlencode 'match[]={__name__="node_role_os_version_machine:cpu_capacity_cores:sum"}' \
--data-urlencode 'match[]={__name__="node_role_os_version_machine:cpu_capacity_sockets:sum"}' \
--data-urlencode 'match[]={__name__="subscription_sync_total"}' \
--data-urlencode 'match[]={__name__="olm_resolution_duration_seconds"}' \
--data-urlencode 'match[]={__name__="csv_succeeded"}' \
--data-urlencode 'match[]={__name__="csv_abnormal"}' \
--data-urlencode 'match[]={__name__="cluster:kube_persistentvolumeclaim_resource_requests_storage_bytes:provisioner:sum"}' \
\
--data-urlencode 'match[]={__name__="cluster:kubelet_volume_stats_used_bytes:provisioner:sum"}' \
\
--data-urlencode 'match[]={__name__="ceph_cluster_total_bytes"}' \
--data-urlencode 'match[]={__name__="ceph_cluster_total_used_raw_bytes"}' \
--data-urlencode 'match[]={__name__="ceph_health_status"}' \
--data-urlencode 'match[]={__name__="odf_system_raw_capacity_total_bytes"}' \
--data-urlencode 'match[]={__name__="odf_system_raw_capacity_used_bytes"}' \
--data-urlencode 'match[]={__name__="odf_system_health_status"}' \
--data-urlencode 'match[]={__name__="job:ceph_osd_metadata:count"}' \
--data-urlencode 'match[]={__name__="job:kube_pv:count"}' \
--data-urlencode 'match[]={__name__="job:odf_system_pvs:count"}' \
--data-urlencode 'match[]={__name__="job:ceph_pools_iops:total"}' \
--data-urlencode 'match[]={__name__="job:ceph_pools_iops_bytes:total"}' \
--data-urlencode 'match[]={__name__="job:ceph_versions_running:count"}' \
--data-urlencode 'match[]={__name__="job:noobaa_total_unhealthy_buckets:sum"}' \
--data-urlencode 'match[]={__name__="job:noobaa_bucket_count:sum"}' \
--data-urlencode 'match[]={__name__="job:noobaa_total_object_count:sum"}' \
--data-urlencode 'match[]={__name__="odf_system_bucket_count", system_type="OCS", system_vendor="Red Hat"}' \
--data-urlencode 'match[]={__name__="odf_system_objects_total", system_type="OCS", system_vendor="Red Hat"}' \
--data-urlencode 'match[]={__name__="noobaa_accounts_num"}' \
--data-urlencode 'match[]={__name__="noobaa_total_usage"}' \
--data-urlencode 'match[]={__name__="console_url"}' \
--data-urlencode 'match[]={__name__="cluster:ovnkube_master_egress_routing_via_host:max"}' \
--data-urlencode 'match[]={__name__="cluster:network_attachment_definition_instances:max"}' \
--data-urlencode 'match[]={__name__="cluster:network_attachment_definition_enabled_instance_up:max"}' \
--data-urlencode 'match[]={__name__="cluster:ingress_controller_aws_nlb_active:sum"}' \
--data-urlencode 'match[]={__name__="cluster:route_metrics_controller_routes_per_shard:min"}' \
--data-urlencode 'match[]={__name__="cluster:route_metrics_controller_routes_per_shard:max"}' \
--data-urlencode 'match[]={__name__="cluster:route_metrics_controller_routes_per_shard:avg"}' \
--data-urlencode 'match[]={__name__="cluster:route_metrics_controller_routes_per_shard:median"}' \
\
--data-urlencode 'match[]={__name__="cluster:openshift_route_info:tls_termination:sum"}' \
--data-urlencode 'match[]={__name__="insightsclient_request_send_total"}' \

```

```

--data-urlencode 'match[]={__name__="cam_app_workload_migrations"}'\
--data-urlencode 'match[]={__name__="cluster:apiserver_current_inflight_requests:sum:max_over_time:2m"}'\
--data-urlencode 'match[]={__name__="cluster:alertmanager_integrations:max"}'\
--data-urlencode 'match[]={__name__="cluster:telemetry_selected_series:count"}'\
--data-urlencode 'match[]={__name__="openshift:prometheus_tsdb_head_series:sum"}'\
--data-urlencode 'match[]={__name__="openshift:prometheus_tsdb_head_samples_appended_total:sum"}'\
--data-urlencode 'match[]={__name__="monitoring:container_memory_working_set_bytes:sum"}'\
--data-urlencode 'match[]={__name__="namespace_job:scrape_series_added:topk3_sum1h"}'\
--data-urlencode 'match[]={__name__="namespace_job:scrape_samples_post_metric_relabeling:topk3"}'\
--data-urlencode 'match[]={__name__="monitoring:haproxy_server_http_responses_total:sum"}'\
--data-urlencode 'match[]={__name__="rhmi_status"}'\
--data-urlencode 'match[]={__name__="status:upgrading:version:rhoam_state:max"}'\
--data-urlencode 'match[]={__name__="state:rhoam_critical_alerts:max"}'\
--data-urlencode 'match[]={__name__="state:rhoam_warning_alerts:max"}'\
--data-urlencode 'match[]={__name__="rhoam_7d_slo_percentile:max"}'\
--data-urlencode 'match[]={__name__="rhoam_7d_slo_remaining_error_budget:max"}'\
--data-urlencode 'match[]={__name__="cluster_legacy_scheduler_policy"}'\
--data-urlencode 'match[]={__name__="cluster_master_schedulable"}'\
--data-urlencode 'match[]={__name__="che_workspace_status"}'\
--data-urlencode 'match[]={__name__="che_workspace_started_total"}'\
--data-urlencode 'match[]={__name__="che_workspace_failure_total"}'\
--data-urlencode 'match[]={__name__="che_workspace_start_time_seconds_sum"}'\
--data-urlencode 'match[]={__name__="che_workspace_start_time_seconds_count"}'\
--data-urlencode 'match[]={__name__="cco_credentials_mode"}'\
--data-urlencode 'match[]={__name__="cluster:kube_persistentvolume_plugin_type_counts:sum"}'\
--data-urlencode 'match[]={__name__="visual_web_terminal_sessions_total"}'\
--data-urlencode 'match[]={__name__="acm_managed_cluster_info"}'\
--data-urlencode 'match[]={__name__="cluster:vsphere_vcenter_info:sum"}'\
--data-urlencode 'match[]={__name__="cluster:vsphere_esxi_version_total:sum"}'\
--data-urlencode 'match[]={__name__="cluster:vsphere_node_hw_version_total:sum"}'\
--data-urlencode 'match[]={__name__="openshift:build_by_strategy:sum"}'\
--data-urlencode 'match[]={__name__="rhods_aggregate_availability"}'\
--data-urlencode 'match[]={__name__="rhods_total_users"}'\
--data-urlencode 'match[]={__name__="instance:etcd_disk_wal_fsync_duration_seconds:histogram_quantile",quantile="0.99"}'\
--data-urlencode 'match[]={__name__="instance:etcd_mvcc_db_total_size_in_bytes:sum"}'\
--data-urlencode 'match[]={__name__="instance:etcd_network_peer_round_trip_time_seconds:histogram_quantile",quantile="0.99"}'\
--data-urlencode 'match[]={__name__="instance:etcd_mvcc_db_total_size_in_use_in_bytes:sum"}'\
--data-urlencode 'match[]={__name__="instance:etcd_disk_backend_commit_duration_seconds:histogram_quantile",quantile="0.99"}'\
--data-urlencode 'match[]={__name__="jaeger_operator_instances_storage_types"}'\
--data-urlencode 'match[]={__name__="jaeger_operator_instances_strategies"}'\
--data-urlencode 'match[]={__name__="jaeger_operator_instances_agent_strategies"}'\
--data-urlencode 'match[]={__name__="appsvcs:cores_by_product:sum"}'\
--data-urlencode 'match[]={__name__="nto_custom_profiles:count"}'\
--data-urlencode 'match[]={__name__="openshift_csi_share_configmap"}'\
--data-urlencode 'match[]={__name__="openshift_csi_share_secret"}'\
--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"}' \
--data-urlencode 'match[]={__name__="openshift:openshift_network_operator_ipsec_state:info"}'
```

4.3. 使用 INSIGHTS 发现集群中的问题

Insights 会重复分析 Insights Operator 发送的数据，其中包括来自 Deployment Validation Operator (DVO) 的工作负载建议。OpenShift Dedicated 用户可以在 Red Hat Hybrid Cloud Console 上显示 [Insights Advisor](#) 服务的结果。

4.3.1. 关于 Red Hat Insights Advisor for OpenShift Dedicated

您可以使用 Insights 公告服务来评估和监控 OpenShift Dedicated 集群的健康状态。无论您是关注单个集群还是整个基础架构，都必须了解公开集群基础架构对服务可用性、容错、性能或安全性的影响。

如果集群安装了 Deployment Validation Operator (DVO)，请突出配置可能会导致集群健康问题的工作负载。

Insights 分析的结果包括在 Red Hat Hybrid Cloud Console 上的 Insights 公告服务中。在 Red Hat Hybrid Cloud 控制台中，您可以执行以下操作：

- 查看受特定建议影响的集群和工作负载。

- 使用可靠的过滤功能，将结果优化为这些建议。
- 了解更多有关单独建议、了解它们存在的风险的详细信息，并针对您的单个集群量身定制解决方案。
- 与其他利益相关者分享结果。

其他资源

- [在 Red Hat Insights for OpenShift 工作流程中使用 Deployment Validation Operator](#)

4.3.2. 了解 Insights Advisor 建议

Insights 公告服务捆绑包有关各种集群状态和组件配置的信息，它们可能会对集群和工作负载的服务可用性、容错、性能或安全性造成负面影响。这些信息集在 Insights 公告服务中称为建议。集群的建议包括以下信息：

- **Name**：有关建议的简要描述
- **Added**: 在建议发布到 Insights Advisor 服务归档时
- **Category**: 问题是否有可能对服务可用性、容错、性能或安全性造成负面影响
- **Total risk**: 通过会对您的集群或工作负载造成负面影响的 *可能性*派生的值，如果已发生，对操作的影响
- **Clusters**：检测到建议的集群列表
- **Description**：这个问题的简要概要，包括它对您的集群的影响

4.3.3. 显示集群中的潜在问题

本节论述了如何在 [OpenShift Cluster Manager](#) 上的 **Insights Advisor** 中显示 Insights 报告。

请注意，Insights 会重复分析您的集群并显示最新结果。这些结果可能会改变，如您解决了一个问题，或发现了一个新问题时。

先决条件

- 集群在 [OpenShift Cluster Manager](#) 中注册。
- 启用了远程健康报告（这是默认设置）。
- 登录到 [OpenShift Cluster Manager](#)。

流程

1. 进入 [OpenShift Cluster Manager](#) 上的 **Advisor → Recommendations**。
根据具体的结果，Insights 公告服务会显示以下之一：

- 如果 Insights 没有发现任何问题，则**不会找到匹配的建议**。
- Insights 检测到的问题列表，按风险分组（低、中、重要和严重）。
- **No clusters yet**，如果 Insights 还没有分析集群。这个分析会在集群安装、注册并连接到互联网后立即开始。

2. 如果显示任何问题，请点击条目前面的 > 图标以了解更多详情。
根据具体问题，详细信息还可以包含来自红帽有关此问题的更多信息的链接。

4.3.4. 显示所有 Insights 公告服务建议

默认情况下，Recommendations 视图仅显示集群中检测到的建议。但是，您可以查看公告服务存档中的所有建议。

先决条件

- 启用了远程健康报告（这是默认设置）。
- 集群在 Red Hat Hybrid Cloud Console [注册](#)。
- 登录到 [OpenShift Cluster Manager](#)。

流程

1. 进入 [OpenShift Cluster Manager](#) 上的 **Advisor → Recommendations**。
2. 点 **Clusters Impacted** 和 **Status** 过滤器旁边的 X 图标。
现在，您可以浏览集群的所有潜在建议。

4.3.5. Advisor 建议过滤器

Insights 公告服务可能会返回大量建议。要专注于最重要的建议，您可以将过滤器应用到 [Advisor 建议](#) 列表，以排除低优先级的建议。

默认情况下，过滤器被设置为只显示启用的建议，这些建议影响一个或多个集群。要查看 Insights 库中所有的建议或禁用的建议，您可以自定义过滤器。

要应用过滤器，请选择过滤器类型，然后根据下拉列表中可用的选项设置其值。您可以将多个过滤器应用到建议列表中。

您可以设置以下过滤器类型：

- **Name**：按名称搜索建议。
- **Total risk**: 从 **Critical**, **Important**, **Moderate**, 和 **Low** 中选择一个或多个值，代表对集群的负面影响的可能性和严重程度。
- **Impact**: 从 **Critical**, **High**, **Medium**, 和 **Low** 中选择一个或多个值，代表对集群操作的连续性影响。
- **Likelihood**: 从 **Critical**, **High**, **Medium**, 和 **Low** 中选择一个或多个值，代表当建议出现隐患时对集群有负面影响的可能性。
- **Category**: 根据您所关注的方面，从 **Service Availability**, **Performance**, **Fault Tolerance**, **Security**, 和 **Best Practice** 中选择一个或多个类别。
- **Status**：点单选按钮显示启用的建议（默认）、禁用建议或所有建议。
- **Clusters impacted**: 设置过滤器以显示当前影响一个或多个集群的建议、没有影响的建议或所有建议。

- **Risk of change:** 从 High、Moderate、low 和 Very low 中选择一个或多个值，表示解析的实现可能对集群操作带来的风险。

4.3.5.1. 过滤 Insights 公告服务建议

作为 OpenShift Dedicated 集群管理器，您可以过滤建议列表上显示的建议。通过应用过滤器，您可以减少报告的建议数量，并专注于高优先级的建议。

以下流程演示了如何设置和删除 **Category** 过滤器，但该流程也适用于其他过滤器类型。

先决条件

登录到 Hybrid Cloud 控制台中的 [OpenShift Cluster Manager](#)。

流程

1. 进入 [OpenShift > Advisor > Recommendations](#)。
2. 在 main, filter-type 下拉列表中，选择 **Category** 过滤器类型。
3. 展开 filter-value 下拉列表，再选中您要查看的每个推荐类别旁边的复选框。清除不必要的类别的复选框。
4. 可选：添加额外的过滤器来进一步重新定义列表。

列表中仅显示所选类别的建议。

验证

- 应用过滤器后，您可以查看更新的推荐列表。应用的过滤器会在默认过滤器旁边添加。

4.3.5.2. 从 Insights 公告服务建议中删除过滤

您可以将多个过滤器应用到建议列表中。准备就绪后，您可以单独删除它们或完全重置它们。

单独删除过滤器

- 点每个过滤器旁边的 **X** 图标，包括默认过滤器，以分别删除它们。

删除所有非默认过滤器

- 点 **Reset filters** 只删除您应用的过滤器，保留默认过滤器。

4.3.6. 禁用 Insights 公告服务建议

您可以禁用影响集群的具体建议，以便它们不再出现在报告中。可以禁用单个集群或所有集群的建议。



注意

禁用对所有集群的建议也适用于所有集群。

先决条件

- 启用了远程健康报告（这是默认设置）。

- 集群在 [OpenShift Cluster Manager](#) 中注册。
- 登录到 [OpenShift Cluster Manager](#)。

流程

1. 进入 [OpenShift Cluster Manager](#) 上的 **Advisor → Recommendations**。
2. 可选：根据需要使用 **Clusters Impacted** 和 **Status** 过滤器。
3. 使用以下方法之一禁用警报：
 - 禁用警报：
 - a. 单击该警报的 Options 菜单 ，然后点 **Disable recommendations**。
 - b. 输入说明并单击 **保存**。
 - 要在禁用警报前查看受此警报影响的集群：
 - a. 点要禁用的建议名称。您会被定向到单一推荐页面。
 - b. 查看 **Affected clusters** 部分中的集群列表。
 - c. 点 **Actions → Disable recommendations** 禁用所有集群的警报。
 - d. 输入说明并单击 **保存**。

4.3.7. 启用之前禁用的 Insights 公告服务建议

当所有集群都禁用了一个建议时，您不会在 Insights 公告服务中看到该建议。您可以更改此行为。

先决条件

- 启用了远程健康报告（这是默认设置）。
- 集群在 [OpenShift Cluster Manager](#) 中注册。
- 登录到 [OpenShift Cluster Manager](#)。

流程

1. 进入 [OpenShift Cluster Manager](#) 上的 **Advisor → Recommendations**。
2. 过滤在禁用的建议上显示的建议：
 - a. 在 **Status** 下拉菜单中选择 **Status**。
 - b. 在 **Filter by status** 下拉菜单中选择 **Disabled**。
 - c. 可选：清除 **Clusters impacted** 过滤器。
3. 找到启用的建议。

4. 点 Options 菜单 ，然后点 **Enable recommendations**。

4.3.8. 关于工作负载的 Insights 公告服务建议

您可以使用 Red Hat Insights for OpenShift 公告服务查看和管理影响您的集群和工作负载的建议信息。公告服务利用部署验证功能，帮助 OpenShift 集群管理员查看部署策略的所有运行时违反情况。您可以在 Red Hat Hybrid Cloud Console 的 [OpenShift > Advisor > Workloads](#) 中查看工作负载的建议。如需更多信息，请参阅[这些其他资源](#)：

- [有关 Kubernetes 工作负载的信息](#)
- [使用 Workloads 的 Deployment Validation 和 Insights Advisor 增强集群操作](#)
- [识别集群中命名空间的工作负载建议](#)
- [查看集群中命名空间的工作负载建议](#)
- [从集群中的工作负载建议中排除对象](#)

4.3.9. 在 web 控制台中显示 Insights 状态

Insights 会重复分析您的集群，可以在 OpenShift Dedicated web 控制台中显示已识别的集群潜在问题的状态。此状态显示不同类别中的问题数量，以及 [OpenShift Cluster Manager](#) 报告的链接。

先决条件

- 集群在 [OpenShift Cluster Manager](#) 中注册。
- 启用了远程健康报告（这是默认设置）。
- 已登录到 OpenShift Dedicated Web 控制台。

流程

1. 在 OpenShift Dedicated Web 控制台中进入 **Home → Overview**。
2. 点 **Status** 卡上的 **Insights**。
弹出窗口列出了按风险分组的潜在问题。点击独立类别或查看 **Insights Advisor** 中的所有建议以显示更多详情。

4.4. 使用 INSIGHTS OPERATOR

Insights Operator 会定期收集配置和组件故障状态信息，默每两小时向红帽报告这些数据。这些信息可让红帽评估配置，它提供了比 Telemetry 报告更深入的数据。OpenShift Dedicated 用户可以在 Red Hat Hybrid Cloud Console 上的 [Insights Advisor](#) 服务中显示报告。

其他资源

- 有关使用 Insights 公告服务识别集群中的问题的更多信息，请参阅[使用 Insights 识别集群中的问题](#)。

4.4.1. 了解 Insights Operator 警报

Insights Operator 通过 Prometheus 监控系统向 Alertmanager 声明警报。您可以使用以下方法之一在 OpenShift Dedicated Web 控制台中的 Alerting UI 中查看这些警报：

- 在 **Administrator** 视角中，点 **Observe** → **Alerting**。
- 在 **Developer** 视角中，点 **Observe** → <project_name> → **Alerts** 标签页。

目前，Insights Operator 在满足条件时发送以下警报：

表 4.1. Insights Operator 警报

警报	描述
InsightsDisabled	Insights Operator 被禁用。
SimpleContentAccessNotAvailable	Red Hat Subscription Management 中不启用简单的内容访问。
InsightsRecommendationActive	Insights 具有集群的活跃建议。

4.4.2. 模糊处理 Deployment Validation Operator 数据

默认情况下，当您安装 Deployment Validation Operator (DVO) 时，资源的名称和唯一标识符 (UID) 包含在 OpenShift Dedicated 的 Insights Operator 捕获和处理的数据中。集群管理员可以将 Insight Operator 配置为模糊来自 Deployment Validation Operator (DVO) 的数据。例如，您可以在发送给红帽的归档文件中模糊处理工作负载名称。

要模糊处理资源名称，您必须在 **insights-config ConfigMap** 对象中手动设置 **obfuscation** 属性，使其包含 **workload_names** 值，如以下步骤中所述。

先决条件

- 启用了远程健康报告（这是默认设置）。
- 使用 "cluster-admin" 角色登录到 OpenShift Dedicated Web 控制台。
- **insights-config ConfigMap** 对象存在于 **openshift-insights** 命名空间中。
- 集群被自我管理，并安装了 Deployment Validation Operator。

流程

1. 进入 **Workloads** → **ConfigMaps** 并选择 **Project: openshift-insights**。
2. 点 **insights-config ConfigMap** 对象打开它。
3. 点 **Actions** 并选择 **Edit ConfigMap**。
4. 点 **YAML 视图** 单选按钮。
5. 在文件中，使用 **workload_names** 值设置 **obfuscation** 属性。

```
apiVersion: v1
kind: ConfigMap
```

```
# ...  
data:  
  config.yaml: |  
    dataReporting:  
      obfuscation:  
        - workload_names  
# ...
```

6. 点击 **Save**。insights-config config-map 详情页面将打开。
7. 验证 **config.yaml obfuscation** 属性的值是否已设置为 **- workload_names**。

第 5 章 收集集群数据

在提交问题单时同时提供您的集群信息，可以帮助红帽支持为您进行排除故障。

建议您提供：

- 使用 **oc adm must-gather** 命令收集的数据
- 唯一的集群 ID

5.1. 关于 MUST-GATHER 工具

oc adm must-gather CLI 命令可收集最有助于解决问题的集群信息，包括：

- 资源定义
- 服务日志

默认情况下，**oc adm must-gather** 命令使用默认的插件镜像，并写入 **./must-gather.local**。

另外，您可以使用适当的参数运行命令来收集具体信息，如以下部分所述：

- 要收集与一个或多个特定功能相关的数据，请使用 **--image** 参数和镜像，如以下部分所述。
例如：

```
$ oc adm must-gather \
  --image=registry.redhat.io/container-native-virtualization/cnv-must-gather-rhel9:v4.19.3
```

- 要收集审计日志，请使用 **-- /usr/bin/gather_audit_logs** 参数，如以下部分所述。
例如：

```
$ oc adm must-gather -- /usr/bin/gather_audit_logs
```



注意

- 作为默认信息集合的一部分，不会收集审计日志来减小文件的大小。
- 在 Windows 操作系统上，安装 **cwRsync** 客户端，并添加到 **PATH** 变量中，以便与 **oc rsync** 命令一起使用。

当您运行 **oc adm must-gather** 时，集群的新项目中会创建一个带有随机名称的新 pod。在该 pod 上收集数据，并保存在当前工作目录中以 **must-gather.local** 开头的新目录中。

例如：

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
...					
openshift-must-gather-5drcj	must-gather-bklx4	2/2	Running	0	72s
openshift-must-gather-5drcj	must-gather-s8sdh	2/2	Running	0	72s
...					

另外，您可以使用 **--run-namespace** 选项在特定命名空间中运行 **oc adm must-gather** 命令。

例如：

```
$ oc adm must-gather --run-namespace <namespace> \
--image=registry.redhat.io/container-native-virtualization/cnv-must-gather-rhel9:v4.19.3
```

5.1.1. 为红帽支持收集您的集群数据

您可使用 **oc adm must-gather** CLI 命令收集有关您的集群的调试信息。

先决条件

- 您可以使用具有 **cluster-admin** 角色的用户访问集群。



注意

在 OpenShift Dedicated 部署中，不使用客户云订阅(CCS)模型的用户无法使用 **oc adm must-gather** 命令，因为它需要 **cluster-admin** 权限。

- 已安装 OpenShift CLI (**oc**)。

流程

1. 进入要存储 **must-gather** 数据的目录。
2. 运行 **oc adm must-gather** 命令：

```
$ oc adm must-gather
```



注意

因为这个命令会默认会选择一个随机 control plane 节点，所以 pod 可能会被调度到处于 **NotReady** 和 **SchedulingDisabled** 状态的 control plane 节点。

- a. 如果此命令失败，例如，您无法在集群中调度 pod，则使用 **oc adm inspect** 命令来收集特定资源的信息。



注意

请联络红帽支持以获取推荐收集的资源信息。

3. 从工作目录中刚刚创建的 **must-gather** 目录创建一个压缩文件。确保为唯一的 must-gather 数据提供日期和集群 ID。有关如何查找集群 ID 的更多信息，请参阅[如何在 OpenShift 集群上找到 cluster-id 或名称](#)。例如，在使用 Linux 操作系统的计算机上运行以下命令：

```
$ tar cvaf must-gather-`date +"%m-%d-%Y-%H-%M-%S"` -<cluster_id>.tar.gz
<must_gather_local_dir> ①
```

- ① 将 **<must_gather_local_dir>** 替换为实际目录名称。

4. 在[红帽客户门户网站的客户支持页面](#)中，将压缩文件附加到您的支持问题单中。

5.1.2. must-gather 标记

下表中列出的标记可用于 `oc adm must-gather` 命令。

表 5.1. `oc adm must-gather` 的 OpenShift Dedicated 标志

标记	示例命令	描述
<code>--all-images</code>	<code>oc adm must-gather --all-images=false</code>	为集群中带有 <code>operators.openshift.io/must-gather-image</code> 注解的所有 Operator 使用默认镜像收集 <code>must-gather</code> 数据。
<code>--dest-dir</code>	<code>oc adm must-gather --dest-dir='<directory_name>'</code>	在保存收集数据的本地机器上设置一个特定的目录。
<code>--host-network</code>	<code>oc adm must-gather --host-network=false</code>	运行 <code>must-gather</code> pod 作为 <code>hostNetwork: true</code> 。如果特定命令和镜像需要捕获主机级数据，则相关。
<code>--image</code>	<code>oc adm must-gather --image=[<plugin_image>]</code>	指定要运行的 <code>must-gather</code> 插件镜像。如果没有指定，则使用 OpenShift Dedicated 的默认 <code>must-gather</code> 镜像。
<code>--image-stream</code>	<code>oc adm must-gather --image-stream=[<image_stream>]</code>	指定一个 <code><image_stream></code> ，使用一个命名空间或 namespace or name:tag 值包括一个 <code>must-gather</code> 插件来运行。
<code>--node-name</code>	<code>oc adm must-gather --node-name='<node>'</code>	设置要使用的特定节点。如果没有指定，则默认使用一个随机的 master。
<code>--node-selector</code>	<code>oc adm must-gather --node-selector='<node_selector_name>'</code>	设置要使用的一个特定节点选择器。仅在指定需要同时捕获一组集群节点上的数据的命令和镜像时才相关。
<code>--run-namespace</code>	<code>oc adm must-gather --run-namespace='<namespace>'</code>	<code>must-gather</code> pod 应在其中运行的一个现有的特权命名空间。如果没有指定，会生成一个临时命名空间。
<code>--since</code>	<code>oc adm must-gather --since=<time></code>	仅返回比指定持续时间更新的日志。默认为所有日志。为了支持这个功能，推荐使用插件，但这并不是必须的。只能使用 <code>since-time</code> 或 <code>since</code> 之一。

标记	示例命令	描述
--since-time	oc adm must-gather --since-time='<date_and_time>'	仅在特定日期和时间后返回日志，以(RFC3339)格式表示。默认为所有日志。为了支持这个功能，推荐使用插件，但这并不是必须的。只能使用 since-time 或 since 之一。
--source-dir	oc adm must-gather --source-dir='<directory_name>/'	指定您要从其中复制收集的数据的 pod 中的一个特定目录。
--timeout	oc adm must-gather --timeout='<time>'	在超时前收集数据的时间长度，以秒、分钟或小时表示，如 3s、5m 或 2h。指定的时间必须大于零。如果没有指定，则默认为 10 分钟。
--volume-percentage	oc adm must-gather --volume-percentage=<percent>	指定可用于 must-gather 的 pod 分配卷的最大百分比。如果超过这个限制， must-gather 会停止收集，但仍复制收集的数据。如果没有指定，则默认为 30%。

5.1.3. 收集有关特定功能的数据

您可以通过将 **oc adm must-gather** CLI 命令与 **--image** 或 **--image-stream** 参数结合使用来收集有关特定功能的调试信息。**must-gather** 工具支持多个镜像，这样您便可通过运行单个命令收集多个功能的数据。

表 5.2. 支持的 must-gather 镜像

Image	用途
registry.redhat.io/container-native-virtualization/cnv-must-gather-rhel9:v4.19.3	OpenShift Virtualization 的数据收集。
registry.redhat.io/openshift-serverless-1/svls-must-gather-rhel8	OpenShift Serverless 的数据收集。
registry.redhat.io/openshift-service-mesh/istio-must-gather-rhel8:<installed_version_service_mesh>	Red Hat OpenShift Service Mesh 的数据收集。
registry.redhat.io/multicloud-engine/must-gather-rhel8	托管 control plane 的数据收集。
registry.redhat.io/rhmtc/openshift-migration-must-gather-rhel8:v<installed_version_migration_toolkit>	MTC 的数据收集。

Image	用途
registry.redhat.io/openshift-logging/cluster-logging-rhel9-operator:v<installed_version_logging>	用于日志记录的数据收集。
quay.io/netobserv/must-gather	Network Observability Operator 的数据收集。
registry.redhat.io/openshift-gitops-1/must-gather-rhel8:v<installed_version_GitOps>	Red Hat OpenShift GitOps 的数据收集。
registry.redhat.io/openshift4/ose-secrets-store-csi-mustgather-rhel9:v<installed_version_secret_store>	Secret Store CSI Driver Operator 的数据收集。



注意

要确定 OpenShift Dedicated 组件镜像的最新版本，请参阅红帽客户门户网站中的 [OpenShift Operator 生命周期](#) 网页。

先决条件

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

流程

1. 进入存储 **must-gather** 数据的目录。
2. 使用一个或多个 **--image** 或 **--image-stream** 参数运行 **oc adm must-gather** 命令。



注意

- 要收集除特定功能数据外的默认 **must-gather** 数据，请添加 **--image-stream=openshift/must-gather** 参数。

例如，使用以下命令可收集默认集群数据和 OpenShift Virtualization 特定信息：

```
$ oc adm must-gather \
  --image-stream=openshift/must-gather \ 1
  --image=registry.redhat.io/container-native-virtualization/cnv-must-gather-rhel9:v4.19.3 2
```

1 默认 OpenShift Dedicated **must-gather** 镜像

2 OpenShift Virtualization 的 **must-gather** 镜像

您可以将 **must-gather** 工具与额外参数搭配使用，以收集集群中与 OpenShift Logging 和 Cluster Logging Operator 特别相关的数据。对于 OpenShift Logging，运行以下命令：

```
$ oc adm must-gather --image=$(oc -n openshift-logging get deployment.apps/cluster-logging-operator \
-o jsonpath='{.spec.template.spec.containers[?(@.name == "cluster-logging-operator")].image}')

```

例 5.1. OpenShift Logging 的 must-gather 输出示例

```

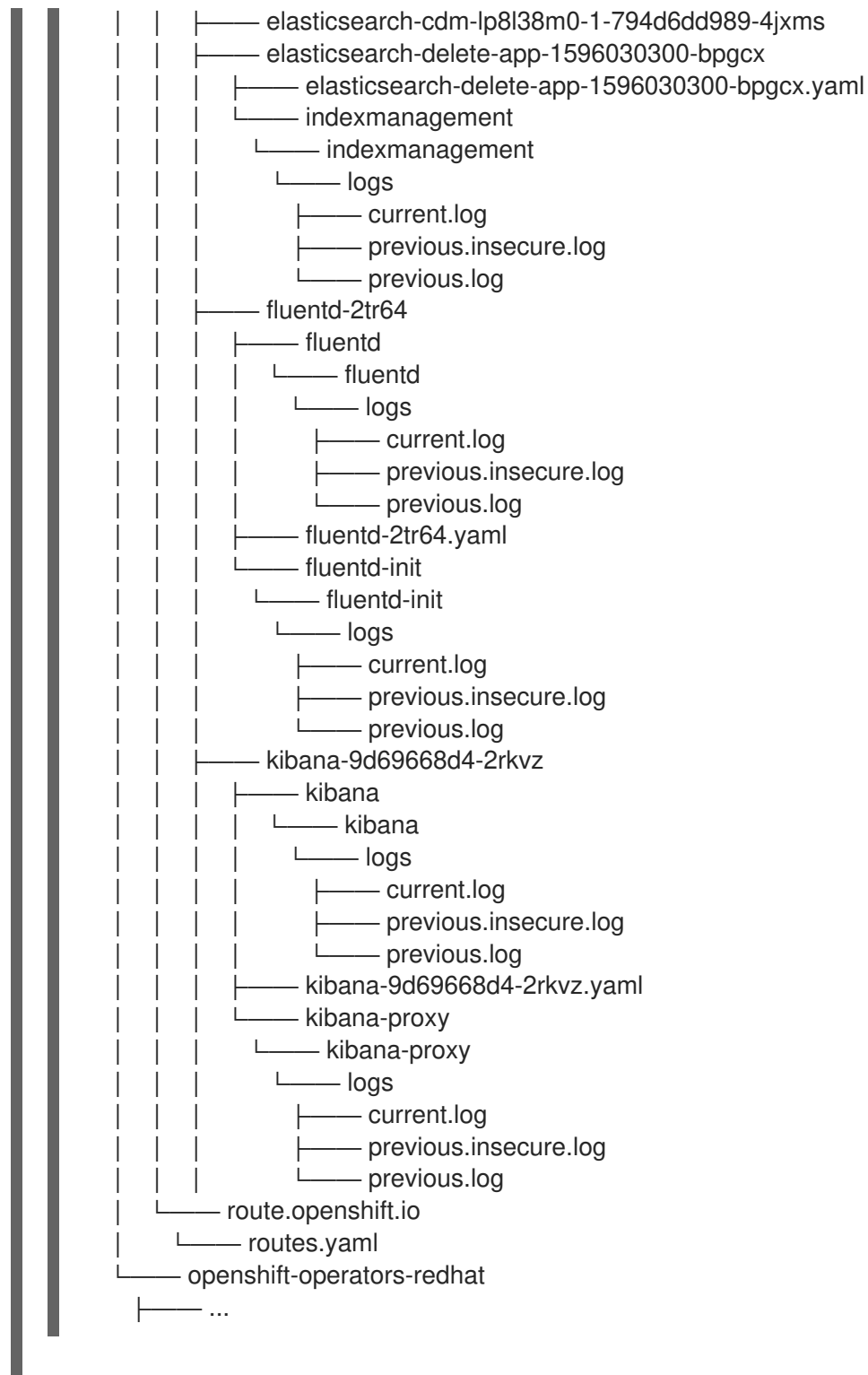
├── cluster-logging
│   ├── clo
│   │   ├── cluster-logging-operator-74dd5994f-6ttgt
│   │   ├── clusterlogforwarder_cr
│   │   ├── cr
│   │   ├── csv
│   │   ├── deployment
│   │   └── logforwarding_cr
│   ├── collector
│   │   └── fluentd-2tr64
│   ├── curator
│   │   └── curator-1596028500-zkz4s
│   ├── eo
│   │   ├── csv
│   │   ├── deployment
│   │   └── elasticsearch-operator-7dc7d97b9d-jb4r4
│   ├── es
│   │   ├── cluster-elasticsearch
│   │   │   ├── aliases
│   │   │   ├── health
│   │   │   ├── indices
│   │   │   ├── latest_documents.json
│   │   │   ├── nodes
│   │   │   ├── nodes_stats.json
│   │   │   └── thread_pool
│   │   ├── cr
│   │   ├── elasticsearch-cdm-lp8l38m0-1-794d6dd989-4jxms
│   │   └── logs
│   │       └── elasticsearch-cdm-lp8l38m0-1-794d6dd989-4jxms
│   ├── install
│   │   ├── co_logs
│   │   ├── install_plan
│   │   ├── olmo_logs
│   │   └── subscription
│   └── kibana
│       ├── cr
│       └── kibana-9d69668d4-2rk vz
├── cluster-scoped-resources
│   ├── core
│   │   ├── nodes
│   │   │   └── ip-10-0-146-180.eu-west-1.compute.internal.yaml
│   │   └── persistentvolumes
│   │       └── pvc-0a8d65d9-54aa-4c44-9ecc-33d9381e41c1.yaml
├── event-filter.html
├── gather-debug.log
├── namespaces
│   ├── openshift-logging
│   └── apps

```

```

├── daemonsets.yaml
├── deployments.yaml
├── replicaset.yaml
├── statefulsets.yaml
├── batch
│   ├── cronjobs.yaml
│   └── jobs.yaml
├── core
│   ├── configmaps.yaml
│   ├── endpoints.yaml
│   ├── events
│   │   ├── curator-1596021300-wn2ks.162634ebf0055a94.yaml
│   │   ├── curator.162638330681bee2.yaml
│   │   └── elasticsearch-delete-app-1596020400-
│   │       gm6nl.1626341a296c16a1.yaml
│   │   ├── elasticsearch-delete-audit-1596020400-
│   │   ├── 9l9n4.1626341a2af81bbd.yaml
│   │   ├── elasticsearch-delete-infra-1596020400-
│   │   ├── v98tk.1626341a2d821069.yaml
│   │   ├── elasticsearch-rollover-app-1596020400-
│   │   ├── cc5vc.1626341a3019b238.yaml
│   │   ├── elasticsearch-rollover-audit-1596020400-
│   │   ├── s8d5s.1626341a31f7b315.yaml
│   │   └── elasticsearch-rollover-infra-1596020400-
│   │       7mgv8.1626341a35ea59ed.yaml
│   ├── events.yaml
│   ├── persistentvolumeclaims.yaml
│   ├── pods.yaml
│   ├── replicationcontrollers.yaml
│   ├── secrets.yaml
│   └── services.yaml
├── openshift-logging.yaml
├── pods
│   ├── cluster-logging-operator-74dd5994f-6ttgt
│   │   ├── cluster-logging-operator
│   │   │   ├── cluster-logging-operator
│   │   │   │   └── logs
│   │   │   │       ├── current.log
│   │   │   │       ├── previous.insecure.log
│   │   │   │       └── previous.log
│   │   └── cluster-logging-operator-74dd5994f-6ttgt.yaml
│   ├── cluster-logging-operator-registry-6df49d7d4-mxxff
│   │   ├── cluster-logging-operator-registry
│   │   │   ├── cluster-logging-operator-registry
│   │   │   │   └── logs
│   │   │   │       ├── current.log
│   │   │   │       ├── previous.insecure.log
│   │   │   │       └── previous.log
│   │   └── cluster-logging-operator-registry-6df49d7d4-mxxff.yaml
│   ├── mutate-csv-and-generate-sqlite-db
│   │   ├── mutate-csv-and-generate-sqlite-db
│   │   │   └── logs
│   │   │       ├── current.log
│   │   │       ├── previous.insecure.log
│   │   │       └── previous.log
│   └── curator-1596028500-zkz4s

```



3. 使用一个或多个 **--image** 或 **--image-stream** 参数运行 **oc adm must-gather** 命令。例如，使用以下命令可收集默认集群数据和 KubeVirt 特定信息：

```

$ oc adm must-gather \
  --image-stream=openshift/must-gather \ ❶
  --image=quay.io/kubevirt/must-gather ❷

```

❶ 默认 OpenShift Dedicated **must-gather** 镜像

❷ KubeVirt 的 **must-gather** 镜像

- 从工作目录中刚刚创建的 **must-gather** 目录创建一个压缩文件。确保为唯一的 must-gather 数据提供日期和集群 ID。有关如何查找集群 ID 的更多信息，请参阅[如何在 OpenShift 集群上找到 cluster-id 或名称](#)。例如，在使用 Linux 操作系统的计算机上运行以下命令：

```
$ tar cvaf must-gather-`date +%m-%d-%Y-%H-%M-%S`-<cluster_id>.tar.gz
<must_gather_local_dir> 1
```

- 将 **<must_gather_local_dir>** 替换为实际目录名称。

- 在[红帽客户门户网站的客户支持页面](#)中，将压缩文件附加到您的支持问题单中。

其他资源

- [OpenShift Dedicated 更新生命周期](#)

5.1.4. 收集网络日志

您可以在集群中的所有节点上收集网络日志。

流程

- 使用 **-- gather_network_logs** 运行 **oc adm must-gather** 命令：

```
$ oc adm must-gather -- gather_network_logs
```



注意

默认情况下，**must-gather** 工具从集群中的所有节点收集 OVN **nbd** 和 **sbdb** 数据库。添加 **-- gather_network_logs** 选项，使其包含包含 OVN **nbd** 数据库的 OVN-Kubernetes 事务的额外日志。

- 从工作目录中刚刚创建的 **must-gather** 目录创建一个压缩文件。确保为唯一的 must-gather 数据提供日期和集群 ID。有关如何查找集群 ID 的更多信息，请参阅[如何在 OpenShift 集群上找到 cluster-id 或名称](#)。例如，在使用 Linux 操作系统的计算机上运行以下命令：

```
$ tar cvaf must-gather-`date +%m-%d-%Y-%H-%M-%S`-<cluster_id>.tar.gz
<must_gather_local_dir> 1
```

- 将 **<must_gather_local_dir>** 替换为实际目录名称。

- 在[红帽客户门户网站的客户支持页面](#)中，将压缩文件附加到您的支持问题单中。

5.1.5. 更改 must-gather 存储限制

当使用 **oc adm must-gather** 命令收集数据时，信息的默认最大存储是容器的存储容量的 30%。达到 30% 限值后，容器被终止，收集过程将停止。收集到的信息会下载到您的本地存储中。要再次运行 **must-gather** 命令，您需要一个具有更多存储容量的容器，或者调整最大卷百分比。

如果容器达到存储限制，则生成类似以下示例的错误消息。

输出示例

Disk usage exceeds the volume percentage of 30% for mounted directory. Exiting...

先决条件

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

流程

- 使用 **volume-percentage** 标志运行 **oc adm must-gather** 命令。新值不能超过 100。

```
$ oc adm must-gather --volume-percentage <storage_percentage>
```

5.2. 获取集群 ID

在向红帽支持提供信息时，提供集群的唯一标识符会很有帮助。您可以使用 OpenShift Dedicated Web 控制台自动填充集群 ID。您还可以使用 web 控制台或 OpenShift CLI (**oc**) 手工获取集群 ID。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 您可以访问 Web 控制台或安装了 OpenShift CLI (**oc**)。

流程

- 使用 [OpenShift Cluster Manager](#) 手动获取集群 ID：
 - a. 导航到 **Cluster List**。
 - b. 点您需要为其创建一个支持问题单的集群名称。
 - c. 在 **Overview** 选项卡的 **Details** 部分的 **Cluster ID** 字段中找到值。
- 使用 Web 控制台开支持问题单并自动填充集群 ID：
 - a. 从工具栏导航至 **(?) help** 并选择 **Share Feedback**。
 - b. 从 **Tell us about your experience** 窗口中点 **Open a support case**。
- 使用 web 控制台手动获取集群 ID：
 - a. 进入到 **Home → Overview**。
 - b. 该值包括在 **Details** 中的 **Cluster ID** 项中。
- 要使用 OpenShift CLI (**oc**) 获取集群 ID，请运行以下命令：

```
$ oc get clusterversion -o jsonpath='{.items[].spec.clusterID}'
```

5.3. 查询集群节点 JOURNAL 日志

您可以在独立集群节点的 `/var/log` 中收集 `journald` 单元日志和其他日志。

先决条件

- 您可以使用具有 `cluster-admin` 角色的用户访问集群。



注意

在 OpenShift Dedicated 部署中，不使用客户云订阅(CCS)模型的用户无法使用 `oc adm node-logs` 命令，因为它需要 `cluster-admin` 权限。

- 已安装 OpenShift CLI(`oc`)。

流程

1. 查询 OpenShift Dedicated 集群节点的 `kubelet journald` 单元日志。以下示例仅查询 control plane 节点：

```
$ oc adm node-logs --role=master -u kubelet 1
```

1 根据情况替换 `kubelet` 以查询其他单元日志。

2. 从集群节点上 `/var/log/` 下的特定子目录收集日志。
 - a. 获取 `/var/log/` 子目录中所含的日志列表。以下示例列出所有 control plane 节点上的 `/var/log/openshift-apiserver/` 中的文件：

```
$ oc adm node-logs --role=master --path=openshift-apiserver
```

- b. 检查 `/var/log/` 子目录中的特定日志。以下示例输出来自所有 control plane 节点的 `/var/log/openshift-apiserver/audit.log` 内容：

```
$ oc adm node-logs --role=master --path=openshift-apiserver/audit.log
```

5.4. 网络追踪方法

收集网络追踪（以数据包捕获记录的形式）可以帮助红帽支持对网络问题进行故障排除。

OpenShift Dedicated 支持以两种方式执行网络追踪。查看下表并选择符合您的需要的方法。

表 5.3. 支持的收集网络追踪方法

方法	优点和功能
收集主机网络追踪	您可以在一个或多个节点上同时指定的时间执行数据包捕获。在满足指定持续时间时，数据包捕获文件将从节点传输到客户端机器。 您可以排除特定操作触发网络通信问题的原因。运行数据包捕获，执行触发此问题的操作，并使用日志诊断问题。

方法	优点和功能
从 OpenShift Dedicated 节点或容器收集网络追踪	您可以在一个节点或一个容器中执行数据包捕获。您可以以交互方式运行 tcpdump 命令，以便您可以控制数据包捕获的持续时间。 您可以手动启动数据包捕获，触发网络通信问题，然后手动停止数据包捕获。 此方法使用 cat 命令和 shell 重定向将数据包从节点或容器捕获数据复制到客户端计算机上。

5.5. 收集主机网络追踪

有时，追踪网络通信并同时捕获多个节点上的数据包简化了与网络相关的问题的故障排除。

您可以使用 **oc adm must-gather** 命令和 **registry.redhat.io/openshift4/network-tools-rhel8** 容器镜像的组合来收集来自节点的数据包。分析数据包捕获可帮助您对网络通信问题进行故障排除。

oc adm must-gather 命令用于在特定节点上的 pod 中运行 **tcpdump** 命令。**tcpdump** 命令记录 pod 中捕获的数据包。当 **tcpdump** 命令退出时，**oc adm must-gather** 命令会用从 pod 捕获的数据包传输到您的客户端机器。

提示

以下流程中的示例命令演示了使用 **tcpdump** 命令执行数据包捕获。但是，您可以在 **--image** 参数中指定的容器镜像中运行任何命令，以便同时从多个节点收集故障排除信息。

先决条件

- 以具有 **cluster-admin** 角色的用户身份登录到 OpenShift Dedicated。



注意

在 OpenShift Dedicated 部署中，不使用客户云订阅(CCS)模型的用户无法使用 **oc adm must-gather** 命令，因为它需要 **cluster-admin** 权限。

- 已安装 OpenShift CLI (**oc**)。

流程

- 运行以下命令，在某些节点上运行来自主机网络的数据包捕获：

```
$ oc adm must-gather \
  --dest-dir /tmp/captures \>
  --source-dir 'tmp/tcpdump/' \>
  --image registry.redhat.io/openshift4/network-tools-rhel8:latest \>
  --node-selector 'node-role.kubernetes.io/worker' \>
  --host-network=true \>
  --timeout 30s \>
```

```
-- \
tcpdump -i any V/ <.>
-w /tmp/tcpdump/%Y-%m-%dT%H:%M:%S.pcap -W 1 -G 300
```

<.> **--dest-dir** 参数指定 **oc adm must-gather** 将数据包捕获到相对于客户端机器上 **/tmp/captures** 的目录中。您可以指定任何可写目录。<.> 当 **tcpdump** 在 **oc adm must-gather** 启动时的 debug pod 中运行时，**--source-dir** 参数指定数据包捕获的临时存储在 pod 上的 **/tmp/tcpdump** 目录中。<.> The **--image** 参数指定包含 **tcpdump** 命令的容器镜像。<.> **--node-selector** 参数和示例值指定在 pod 上的 **/tmp/tcpdump** 目录中执行数据包捕获。作为替代方案，您可以指定 **--node-name** 参数而不是在单个节点上运行数据包捕获。如果省略 **--node-selector** 和 **--node-name** 参数，则数据包捕获将在所有节点上执行。<.> **--host-network=true** 参数是必需的，以便在节点的网络接口上执行数据包捕获。<.> **--timeout** 参数和值指定运行 debug pod 达到 30 秒。如果没有指定 **--timeout** 参数和持续时间，则 debug pod 会运行 10 分钟。<.> **-i any** 参数用于 **tcpdump** 命令，指定捕获所有网络接口上的数据包。作为替代方案，您可以指定网络接口名称。

2. 执行访问 Web 应用等操作，在网络追踪捕获数据包时触发网络通信问题。
3. 查看 **oc adm must-gather** 从 pod 传送到客户端机器的数据包捕获文件：

```
tmp/captures
├── event-filter.html
├── ip-10-0-192-217-ec2-internal ❶
│   ├── registry-redhat-io-openshift4-network-tools-rhel8-sha256-bca...
│   └── 2022-01-13T19:31:31.pcap
├── ip-10-0-201-178-ec2-internal ❷
│   ├── registry-redhat-io-openshift4-network-tools-rhel8-sha256-bca...
│   └── 2022-01-13T19:31:30.pcap
├── ip-...
└── timestamp
```

❶ ❷ 数据包捕获保存在可识别主机名、容器和文件名的目录中。如果您没有指定 **--node-selector** 参数，则主机名的目录级别不存在。

5.6. 从 OPENSIFT DEDICATED 节点或容器收集网络追踪

在调查与网络相关的 OpenShift Dedicated 问题时，红帽可能会从特定的 OpenShift Dedicated 集群节点或特定容器请求网络数据包追踪。在 OpenShift Dedicated 中捕获网络 trace 的建议方法是通过 debug pod。

先决条件

- 您可以使用具有 **cluster-admin** 角色的用户访问集群。



注意

在 OpenShift Dedicated 部署中，没有使用客户云订阅(CCS)模型的客户无法使用 **oc debug** 命令，因为它需要 **cluster-admin** 权限。

- 已安装 OpenShift CLI (**oc**)。
- 您已有一个红帽支持问题单 ID。

流程

1. 获取集群节点列表：

```
$ oc get nodes
```

2. 在目标节点上进入一个 debug 会话。此步骤被实例化为一个名为 `<node_name>-debug` 的 debug pod:

```
$ oc debug node/my-cluster-node
```

3. 将 `/host` 设为 debug shell 中的根目录。debug pod 在 pod 中的 `/host` 中挂载主机的 root 文件系统。将根目录改为 `/host`，您可以运行主机可执行路径中包含的二进制文件：

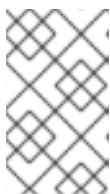
```
# chroot /host
```

4. 在 **chroot** 环境控制台中获取节点接口名称：

```
# ip ad
```

5. 启动 **toolbox** 容器，其中包括运行 **sosreport** 所需的二进制文件和插件：

```
# toolbox
```



注意

如果一个已存在的 **toolbox** pod 已在运行，则 **toolbox** 命令会输出 **'toolbox-' already exists. Trying to start...**。要避免 **tcpdump** 出现问题，请使用 **podman rm toolbox-** 删除正在运行的 toolbox 容器，并生成新 toolbox 容器。

6. 在集群节点中启动 **tcpdump** 会话，并将输出重定向到捕获文件中。这个示例使用 **ens5** 作为接口名称：

```
$ tcpdump -nn -s 0 -i ens5 -w /host/var/tmp/my-cluster-node_$(date +%d_%m_%Y-%H_%M_%S-%Z).pcap ❶
```

- ❶ **tcpdump** 捕获文件路径在 **chroot** 环境之外，因为 toolbox 容器会在 `/host` 中挂载主机的根目录。

7. 如果节点上的特定容器需要 **tcpdump** 捕获，请按照以下步骤操作。

- a. 确定目标容器 ID。**chroot host** 命令先于这一步中的 **crictl** 命令，因为 toolbox 容器在 `/host` 中挂载主机的根目录：

```
# chroot /host crictl ps
```

- b. 确定容器的进程 ID。在本例中，容器 ID 是 **a7fe32346b120**:

```
# chroot /host crictl inspect --output yaml a7fe32346b120 | grep 'pid' | awk '{print $2}'
```

- c. 在容器上启动 **tcpdump** 会话，并将输出重定向到捕获文件中。本例使用 **49628** 作为容器的进程 ID，**ens5** 是接口名称。**nsenter** 命令进入目标进程的命名空间并在命名空间中运行命令。因为本例中的目标进程是一个容器的进程 ID，**tcpdump** 命令从主机在容器的命名空间中运行：

```
# nsenter -n -t 49628 -- tcpdump -nn -i ens5 -w /host/var/tmp/my-cluster-node-my-container_$(date +%d_%m_%Y-%H_%M_%S-%Z).pcap 1
```

- 1 **tcpdump** 捕获文件路径在 **chroot** 环境之外，因为 toolbox 容器会在 **/host** 中挂载主机的根目录。

8. 使用以下方法之一向红帽支持提供 **tcpdump** 捕获文件进行分析。

- 将文件上传到现有红帽支持问题单中。
 - a. 运行 **oc debug node/<node_name>** 命令调整 **sosreport** 归档，并将输出重定向到文件中。此命令假设您已退出以前的 **oc debug** 会话：

```
$ oc debug node/my-cluster-node -- bash -c 'cat /host/var/tmp/my-tcpdump-capture-file.pcap' > /tmp/my-tcpdump-capture-file.pcap 1
```

- 1 debug 容器将主机的根目录挂载到 **/host**。在指定用于连接的目标文件时，引用 debug 容器的根目录的绝对路径，包括 **/host**。
- b. 在红帽客户门户网站网站的 [Customer Support](#) 页面中进入现有的支持问题单。
 - c. 选择 **Attach files** 并按提示上传该文件。

5.7. 为红帽支持提供诊断数据

在调查 OpenShift Dedicated 问题时，红帽支持可能会要求您将诊断数据上传到支持问题单中。可以通过红帽客户门户网站将文件上传到支持问题单中。

先决条件

- 您可以使用具有 **cluster-admin** 角色的用户访问集群。



注意

在 OpenShift Dedicated 部署中，没有使用客户云订阅(CCS)模型的客户无法使用 **oc debug** 命令，因为它需要 **cluster-admin** 权限。

- 已安装 OpenShift CLI (**oc**)。
- 您已有一个红帽支持问题单 ID。

流程

- 通过红帽客户门户网站将诊断数据上传到现有红帽支持问题单中。

- a. 使用 **oc debug node/<node_name>** 命令连接 OpenShift Dedicated 节点中包含的诊断文件，并将输出重定向到文件中。以下示例将 debug 容器中的 **/host/var/tmp/my-diagnostic-data.tar.gz** 复制到 **/var/tmp/my-diagnostic-data.tar.gz**：

```
$ oc debug node/my-cluster-node -- bash -c 'cat /host/var/tmp/my-diagnostic-data.tar.gz'
> /var/tmp/my-diagnostic-data.tar.gz ❶
```

- ❶ debug 容器将主机的根目录挂载到 **/host**。在指定用于连接的目标文件时，引用 debug 容器的根目录的绝对路径，包括 **/host**。

- b. 在红帽客户门户网站的 [Customer Support](#) 页面中进入现有的支持问题单。
- c. 选择 **Attach files** 并按提示上传该文件。

5.8. 关于 TOOLBOX

toolbox 是一个在 Red Hat Enterprise Linux CoreOS (RHCOS) 系统上启动容器的工具。该工具主要用于启动包含运行 **sosreport** 等命令所需的二进制文件和插件的容器。

toolbox 容器的主要目的是收集诊断信息并将其提供给红帽支持。但是，如果需要额外的诊断工具，您可以添加 RPM 软件包或运行标准支持工具镜像的替代镜像。

将软件包安装到 **toolbox** 容器

默认情况下，运行 **toolbox** 命令使用 **registry.redhat.io/rhel9/support-tools:latest** 镜像启动一个容器。该镜像包含最常用的支持工具。如果需要一个不是镜像的一部分的支持工具来收集特定于具体节点的数据，可以安装额外的软件包。

先决条件

- 已使用 **oc debug node/<node_name>** 命令访问节点。
- 您可以使用具有 root 权限的用户访问您的系统。

流程

1. 将 **/host** 设为 debug shell 中的根目录。debug pod 在 pod 中的 **/host** 中挂载主机的 root 文件系统。将根目录改为 **/host**，您可以运行主机可执行路径中包含的二进制文件：

```
# chroot /host
```

2. 启动 toolbox 容器：

```
# toolbox
```

3. 安装额外的软件包，如 **wget**：

```
# dnf install -y <package_name>
```

使用 **toolbox** 启动备用镜像

默认情况下，运行 **toolbox** 命令使用 **registry.redhat.io/rhel9/support-tools:latest** 镜像启动一个容器。



注意

您可以通过创建 **.toolboxrc** 文件并指定要运行的镜像来启动其他镜像。但是，OpenShift Dedicated 4 不支持运行 **support-tools** 镜像的旧版本，如 **registry.redhat.io/rhel8/support-tools:latest**。

先决条件

- 已使用 **oc debug node/<node_name>** 命令访问节点。
- 您可以使用具有 root 权限的用户访问您的系统。

流程

1. 将 **/host** 设为 debug shell 中的根目录。debug pod 在 pod 中的 **/host** 中挂载主机的 root 文件系统。将根目录改为 **/host**，您可以运行主机可执行路径中包含的二进制文件：

```
# chroot /host
```

2. 可选：如果您需要使用替代镜像而不是默认镜像，请在 root 用户 ID 的主目录中创建一个 **.toolboxrc** 文件，并指定镜像元数据：

```
REGISTRY=quay.io 1
IMAGE=fedora/fedora:latest 2
TOOLBOX_NAME=toolbox-fedora-latest 3
```

- 1 可选：指定替代容器 registry。
- 2 指定要启动的替代镜像。
- 3 可选：指定 toolbox 容器的替代名称。

3. 输入以下命令启动 toolbox 容器：

```
# toolbox
```



注意

如果一个已存在的 **toolbox** pod 已在运行，则 **toolbox** 命令会输出 **'toolbox-' already exists. Trying to start....**为了避免 **sosreport** 插件出现问题，请使用 **podman rm toolbox-** 删除正在运行的 toolbox 容器，然后生成新的 toolbox 容器。

第 6 章 集群规格总结

6.1. 使用集群版本对象总结集群规格

您可以通过查询 **clusterversion** 资源来获取 OpenShift Dedicated 集群规格概述。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI(**oc**)。

流程

1. 查询集群版本、可用性、运行时间以及常规状态：

```
$ oc get clusterversion
```

输出示例

```
NAME      VERSION AVAILABLE PROGRESSING SINCE STATUS
version  4.13.8   True      False      8h      Cluster version is 4.13.8
```

2. 获取集群规格、更新可用性和更新历史记录の詳細概述：

```
$ oc describe clusterversion
```

输出示例

```
Name:      version
Namespace:
Labels:     <none>
Annotations: <none>
API Version: config.openshift.io/v1
Kind:      ClusterVersion
# ...
Image:      quay.io/openshift-release-dev/ocp-
release@sha256:a956488d295fe5a59c8663a4d9992b9b5d0950f510a7387dbbfb8d20fc5970ce

URL:        https://access.redhat.com/errata/RHSA-2023:4456
Version:    4.13.8
History:
  Completion Time: 2023-08-17T13:20:21Z
  Image:          quay.io/openshift-release-dev/ocp-
release@sha256:a956488d295fe5a59c8663a4d9992b9b5d0950f510a7387dbbfb8d20fc5970ce

  Started Time:    2023-08-17T12:59:45Z
  State:           Completed
  Verified:        false
  Version:         4.13.8
# ...
```

第 7 章 故障排除

7.1. 对 GCP 集群部署上的 OPENSIFT DEDICATED 进行故障排除

Google Cloud Platform (GCP)集群部署错误上的 OpenShift Dedicated 可能会因为以下原因而发生，包括配额限制和设置不足、错误输入的数据、不兼容的配置等。

在以下部分介绍了如何在 GCP 集群安装错误上解析常见的 OpenShift Dedicated。

7.1.1. 对 GCP 安装错误代码上的 OpenShift Dedicated 进行故障排除

下表列出了 Google Cloud Platform (GCP)安装错误代码上的 OpenShift Dedicated，以及解决这些错误的功能。

表 7.1. GCP 安装错误代码上的 OpenShift Dedicated

错误代码	描述	解决方案
OCM3022	无效的 GCP 项目 ID。	在 Google 云控制台中验证项目 ID，并重试集群创建。
OCM3023	没有找到 GCP 实例类型。	验证实例类型并重试集群创建。 如需有关 GCP 实例类型上的 OpenShift Dedicated 的更多信息，请参阅 附加资源部分中的 Google Cloud 实例类型
OCM3024	GCP precondition 失败。	验证机构策略约束并重试集群创建。 有关机构策略约束的更多信息，请参阅 机构策略限制 。
OCM3025	超过 GCP SSD 配额限制。	在 Google Cloud 控制台或 gcloud CLI 中检查可用的持久磁盘 SSD 配额。必须至少有 896 GB SSD 可用。增加 SSD 配额限制并重试集群创建。 有关管理持久性磁盘 SSD 配额的更多信息，请参阅 分配配额 。
OCM3026	超过 GCP 计算配额限制。	增加 CPU 计算配额并重试集群安装。 有关 CPU 计算配额的更多信息，请参阅 Compute Engine 配额和限制概述 。

错误代码	描述	解决方案
OCM3027	超过 GCP 服务帐户配额限制。	确保您的配额允许额外的未使用的服务帐户。检查 GCP 帐户中配额的当前使用情况，然后重试。 有关管理您的配额的更多信息，请参阅使用控制台管理配额。

其他资源

- 如需有关 GCP 实例类型上的 OpenShift Dedicated 的更多信息，请参阅 [Google Cloud 实例类型](#)。

7.2. 验证节点健康状况

7.2.1. 查看节点状态、资源使用量和配置

查看集群节点健康状况、资源消耗统计和节点日志。另外，在单个节点上查询 **kubelet** 状态。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI(**oc**)。

流程

- 列出集群中所有节点的名称、状态和角色：

```
$ oc get nodes
```

- 总结集群中每个节点的 CPU 和内存使用情况：

```
$ oc adm top nodes
```

- 总结特定节点的 CPU 和内存使用情况：

```
$ oc adm top node my-node
```

7.3. TROUBLESHOOTING OPERATOR 的问题

Operator 是一种打包、部署和管理 OpenShift Dedicated 应用程序的方法。它可以被看作是软件厂商的工程团队的扩展，可以在 OpenShift Dedicated 监控软件的运行情况，并根据软件的当前状态实时做出决策。Operator 被设计为用来无缝地处理升级过程，并对出现的错误自动进行响应，而且不会采取“捷径”（如跳过软件备份过程来节省时间）。

OpenShift Dedicated 4 包括了一组默认的 Operator，它们是集群正常工作所需的。这些默认 Operator 由 Cluster Version Operator（CVO）管理。

作为集群管理员，您可使用 OpenShift Dedicated Web 控制台或 CLI 安装来自 OperatorHub 的应用程序 Operator。然后，您可将 Operator 订阅至一个或多个命名空间，供集群上的开发人员使用。应用程序 Operator 由 Operator Lifecycle Manager（OLM）进行管理。

如果遇到 Operator 问题，请验证 Operator 订阅状态。检查集群中的 Operator pod 健康状况，并收集 Operator 日志以进行诊断。

7.3.1. operator 订阅状况类型

订阅可报告以下状况类型：

表 7.2. 订阅状况类型

状况	描述
CatalogSourcesUnhealthy	用于解析的一个或多个目录源不健康。
InstallPlanMissing	缺少订阅的安装计划。
InstallPlanPending	订阅的安装计划正在安装中。
InstallPlanFailed	订阅的安装计划失败。
ResolutionFailed	订阅的依赖项解析失败。



注意

默认 OpenShift Dedicated 集群 Operator 由 Cluster Version Operator（CVO）管理，它们没有 **Subscription** 对象。应用程序 Operator 由 Operator Lifecycle Manager（OLM）管理，它们具有 **Subscription** 对象。

其他资源

- [目录健康要求](#)

7.3.2. 使用 CLI 查看 Operator 订阅状态

您可以使用 CLI 查看 Operator 订阅状态。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI(**oc**)。

流程

1. 列出 Operator 订阅：

```
$ oc get subs -n <operator_namespace>
```

2. 使用 **oc describe** 命令检查 **Subscription** 资源：

```
$ oc describe sub <subscription_name> -n <operator_namespace>
```

- 在命令输出中，找到 Operator 订阅状况类型的 **Conditions** 部分。在以下示例中，**CatalogSourcesUnhealthy** 条件类型具有 **false** 状态，因为所有可用目录源都健康：

输出示例

```
Name:      cluster-logging
Namespace: openshift-logging
Labels:    operators.coreos.com/cluster-logging.openshift-logging=
Annotations: <none>
API Version: operators.coreos.com/v1alpha1
Kind:      Subscription
# ...
Conditions:
  Last Transition Time: 2019-07-29T13:42:57Z
  Message:             all available catalogsources are healthy
  Reason:              AllCatalogSourcesHealthy
  Status:              False
  Type:                CatalogSourcesUnhealthy
# ...
```



注意

默认 OpenShift Dedicated 集群 Operator 由 Cluster Version Operator (CVO) 管理，它们没有 **Subscription** 对象。应用程序 Operator 由 Operator Lifecycle Manager (OLM) 管理，它们具有 **Subscription** 对象。

7.3.3. 使用 CLI 查看 Operator 目录源状态

您可以使用 CLI 查看 Operator 目录源的状态。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI(**oc**)。

流程

- 列出命名空间中的目录源。例如，您可以检查 **openshift-marketplace** 命名空间，该命名空间用于集群范围的目录源：

```
$ oc get catalogsources -n openshift-marketplace
```

输出示例

NAME	DISPLAY	TYPE	PUBLISHER	AGE
certified-operators	Certified Operators	grpc	Red Hat	55m
community-operators	Community Operators	grpc	Red Hat	55m

example-catalog	Example Catalog	grpc	Example Org	2m25s
redhat-operators	Red Hat Operators	grpc	Red Hat	55m

2. 使用 **oc describe** 命令获取有关目录源的详情和状态：

```
$ oc describe catalogsource example-catalog -n openshift-marketplace
```

输出示例

```
Name:      example-catalog
Namespace: openshift-marketplace
Labels:    <none>
Annotations: operatorframework.io/managed-by: marketplace-operator
             target.workload.openshift.io/management: {"effect": "PreferredDuringScheduling"}
API Version: operators.coreos.com/v1alpha1
Kind:      CatalogSource
# ...
Status:
  Connection State:
    Address:      example-catalog.openshift-marketplace.svc:50051
    Last Connect: 2021-09-09T17:07:35Z
    Last Observed State: TRANSIENT_FAILURE
  Registry Service:
    Created At:   2021-09-09T17:05:45Z
    Port:         50051
    Protocol:     grpc
    Service Name: example-catalog
    Service Namespace: openshift-marketplace
# ...
```

在上例的输出中，最后观察到的状态是 **TRANSIENT_FAILURE**。此状态表示目录源建立连接时出现问题。

3. 列出创建目录源的命名空间中的 pod：

```
$ oc get pods -n openshift-marketplace
```

输出示例

NAME	READY	STATUS	RESTARTS	AGE
certified-operators-cv9nn	1/1	Running	0	36m
community-operators-6v8lp	1/1	Running	0	36m
marketplace-operator-86bfc75f9b-jkgbc	1/1	Running	0	42m
example-catalog-bwt8z	0/1	ImagePullBackOff	0	3m55s
redhat-operators-smxx8	1/1	Running	0	36m

在命名空间中创建目录源时，会在该命名空间中为目录源创建一个 pod。在前面的示例中，**example-catalog-bwt8z** pod 的状态是 **ImagePullBackOff**。此状态表示拉取目录源的索引镜像存在问题。

4. 使用 **oc describe** 命令检查 pod 以获取更多详细信息：

```
$ oc describe pod example-catalog-bwt8z -n openshift-marketplace
```

输出示例

```
Name:      example-catalog-bwt8z
Namespace: openshift-marketplace
Priority:   0
Node:      ci-ln-jyryyg2-f76d1-ggdbq-worker-b-vsxjd/10.0.128.2
...
Events:
  Type    Reason            Age          From          Message
  ----    -
  Normal   Scheduled         48s          default-scheduler Successfully assigned openshift-marketplace/example-catalog-bwt8z to ci-ln-jyryyf2-f76d1-fgdbq-worker-b-vsxjd
  Normal   AddedInterface    47s          multus        Add eth0 [10.131.0.40/23] from openshift-sdn
  Normal   BackOff           20s (x2 over 46s) kubelet       Back-off pulling image "quay.io/example-org/example-catalog:v1"
  Warning   Failed            20s (x2 over 46s) kubelet       Error: ImagePullBackOff
  Normal   Pulling           8s (x3 over 47s) kubelet       Pulling image "quay.io/example-org/example-catalog:v1"
  Warning   Failed            8s (x3 over 47s) kubelet       Failed to pull image "quay.io/example-org/example-catalog:v1": rpc error: code = Unknown desc = reading manifest v1 in quay.io/example-org/example-catalog: unauthorized: access to the requested resource is not authorized
  Warning   Failed            8s (x3 over 47s) kubelet       Error: ErrImagePull
```

在前面的示例输出中，错误消息表示目录源的索引镜像因为授权问题而无法成功拉取。例如，索引镜像可能存储在需要登录凭证的 registry 中。

其他资源

- [Operator Lifecycle Manager 概念和资源 → Catalog 源](#)
- gRPC 文档：[连接状态](#)

7.3.4. 查询 Operator pod 状态

您可以列出集群中的 Operator pod 及其状态。您还可以收集详细的 Operator pod 概述。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- API 服务仍然可以正常工作。
- 已安装 OpenShift CLI(**oc**)。

流程

1. 列出集群中运行的 Operator。输出包括 Operator 版本、可用性和运行时间信息：

```
$ oc get clusteroperators
```

2. 列出在 Operator 命名空间中运行的 Operator pod，以及 pod 状态、重启和年龄：

```
$ oc get pod -n <operator_namespace>
```

3. 输出详细的 Operator pod 概述：

```
$ oc describe pod <operator_pod_name> -n <operator_namespace>
```

7.3.5. 收集 Operator 日志

如果遇到 Operator 问题，您可以从 Operator pod 日志中收集详细诊断信息。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- API 服务仍然可以正常工作。
- 已安装 OpenShift CLI(**oc**)。
- 您有 control plane 或 control plane 机器的完全限定域名。

流程

1. 列出在 Operator 命名空间中运行的 Operator pod，以及 pod 状态、重启和年龄：

```
$ oc get pods -n <operator_namespace>
```

2. 检查 Operator pod 的日志：

```
$ oc logs pod/<pod_name> -n <operator_namespace>
```

如果 Operator pod 具有多个容器，则上述命令将会产生一个错误，其中包含每个容器的名称。从独立容器查询日志：

```
$ oc logs pod/<operator_pod_name> -c <container_name> -n <operator_namespace>
```

3. 如果 API 无法正常工作，请使用 SSH 来查看每个 control plane 节点上的 Operator pod 和容器日志。将 **<master-node>.<cluster_name>.<base_domain>** 替换为适当的值。

- a. 列出每个 control plane 节点上的 pod：

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl pods
```

- b. 对于任何未显示 **Ready** 状态的 Operator pod，详细检查 Pod 的状态。将 **<operator_pod_id>** 替换为上一命令输出中列出的 Operator pod ID:

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl inspectp  
<operator_pod_id>
```

- c. 列出与 Operator pod 相关的容器：

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl ps --pod=  
<operator_pod_id>
```

- d. 对于任何未显示 **Ready** 状态的 Operator 容器，请详细检查容器的状态。将 `<container_id>` 替换为上一命令输出中列出的容器 ID:

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl inspect
<container_id>
```

- e. 检查任何未显示 **Ready** 状态的 Operator 容器的日志。将 `<container_id>` 替换为上一命令输出中列出的容器 ID:

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl logs -f
<container_id>
```



注意

运行 Red Hat Enterprise Linux CoreOS (RHCOS) 的 OpenShift Dedicated 4 集群节点不可变，它依赖于 Operator 来应用集群更改。不建议使用 SSH 访问集群节点。在尝试通过 SSH 收集诊断数据前，请运行 **oc adm must gather** 和其他 **oc** 命令看它们是否可以提供足够的信息。但是，如果 OpenShift Dedicated API 不可用，或 kubelet 在目标节点上无法正常工作，**oc** 操作将会受到影响。在这种情况下，可以使用 **ssh core@<node>.<cluster_name>.<base_domain>** 来访问节点。

7.4. 检查 POD 问题

OpenShift Dedicated 利用 Kubernetes 的 pod 概念，它是共同部署在同一主机上的一个或多个容器。pod 是可在 OpenShift Dedicated 4 上定义、部署和管理的最小计算单元。

在定义了 pod 后，它将分配到节点上运行，直到容器退出，或直到它被删除为止。根据策略和退出代码，Pod 可在退出或保留后删除，以便访问其日志。

首先要检查 pod 出现问题时 pod 的状态。如果发生 pod 故障，请观察 pod 的错误状态以识别特定镜像、容器或 pod 网络问题。根据错误状态集中诊断数据收集。查看 pod 事件消息以及 pod 和容器日志信息。通过访问命令行中运行的 pod，或根据 Pod 的部署配置启动具有 root 访问权限的调试 pod 来动态诊断问题。

7.4.1. 了解 pod 错误状态

pod 失败返回显式错误状态，可在 **oc get pods** 输出的 **status** 字段中观察到。Pod 错误状态会涵盖镜像、容器和容器网络相关的故障。

下表提供了 pod 错误状态及其描述列表。

表 7.3. Pod 错误状态

Pod 错误状态	描述
ErrImagePull	通用镜像检索错误。
ErrImagePullBackOff	镜像检索失败。

Pod 错误状态	描述
ErrInvalidImage Name	指定镜像名称无效。
ErrImageInspect	镜像检查没有成功。
ErrImageNeverPull	PullPolicy 设置为 NeverPullImage , 目标镜像没有本地存在。
ErrRegistryUnavailable	当尝试从 registry 检索镜像时, 会出现 HTTP 错误。
ErrContainerNotFound	指定容器在声明的 pod 中不存在或未由 kubelet 管理。
ErrRunInitContainer	容器初始化失败。
ErrRunContainer	pod 的容器都没有成功启动。
ErrKillContainer	没有 pod 的容器被成功终止。
ErrCrashLoopBackOff	容器已终止。kubelet 将不会试图重启它。
ErrVerifyNonRoot	容器或镜像尝试使用 root 权限运行。
ErrCreatePodSandbox	Pod 沙盒创建没有成功。
ErrConfigPodSandbox	Pod 沙盒配置没有获得。
ErrKillPodSandbox	pod 沙箱没有成功停止。
ErrSetupNetwork	网络初始化失败。
ErrTeardownNetwork	网络终止失败。

7.4.2. 检查 pod 状态

您可以查询 pod 状态和错误状态。您还可以查询 pod 的相关部署配置，并查看基础镜像的可用性。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI(**oc**)。
- 已安装了 **skopeo**。

流程

1. 切换到项目：

```
$ oc project <project_name>
```

2. 列出在命名空间中运行的 pod，以及 pod 状态、错误状态、重启和年龄：

```
$ oc get pods
```

3. 确定命名空间是否由部署配置管理：

```
$ oc status
```

如果命名空间由部署配置管理，输出包括部署配置名称和基础镜像引用。

4. 检查以上命令输出中引用的基础镜像：

```
$ skopeo inspect docker://<image_reference>
```

5. 如果基础镜像引用不正确，请更新部署配置中的引用：

```
$ oc edit deployment/my-deployment
```

6. 当部署配置退出时，配置将自动重新部署。在部署过程中的 Watch pod 的状态，以确定这个问题是否已解决：

```
$ oc get pods -w
```

7. 检查命名空间中的事件，以了解与 pod 失败相关的诊断信息：

```
$ oc get events
```

7.4.3. 检查 pod 和容器日志

您可以检查 pod 和容器日志，以查看与显式 pod 失败相关的警告和错误消息。根据策略和退出代码，pod 和容器日志在 pod 终止后仍然可用。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。

- API 服务仍然可以正常工作。
- 已安装 OpenShift CLI (**oc**)。

流程

1. 查询特定 pod 的日志：

```
$ oc logs <pod_name>
```

2. 查询 pod 中特定容器的日志：

```
$ oc logs <pod_name> -c <container_name>
```

由前面的 **oc logs** 命令所获得的日志由发送到 pod 或容器中的 stdout 的信息组成。

3. 检查 pod 中的 **/var/log/** 中包含的日志。

- a. 列出 pod 中 **/var/log** 中所含的日志文件和子目录：

```
$ oc exec <pod_name> -- ls -alh /var/log
```

输出示例

```
total 124K
drwxr-xr-x. 1 root root 33 Aug 11 11:23 .
drwxr-xr-x. 1 root root 28 Sep 6 2022 ..
-rw-rw----. 1 root utmp 0 Jul 10 10:31 bttmp
-rw-r--r--. 1 root root 33K Jul 17 10:07 dnf.librepo.log
-rw-r--r--. 1 root root 69K Jul 17 10:07 dnf.log
-rw-r--r--. 1 root root 8.8K Jul 17 10:07 dnf.rpm.log
-rw-r--r--. 1 root root 480 Jul 17 10:07 hawkey.log
-rw-rw-r--. 1 root utmp 0 Jul 10 10:31 lastlog
drwx-----. 2 root root 23 Aug 11 11:14 openshift-apiserver
drwx-----. 2 root root 6 Jul 10 10:31 private
drwxr-xr-x. 1 root root 22 Mar 9 08:05 rhsm
-rw-rw-r--. 1 root utmp 0 Jul 10 10:31 wttmp
```

- b. 查询 pod 中 **/var/log** 中所含的特定日志文件：

```
$ oc exec <pod_name> cat /var/log/<path_to_log>
```

输出示例

```
2023-07-10T10:29:38+0000 INFO --- logging initialized ---
2023-07-10T10:29:38+0000 DDEBUG timer: config: 13 ms
2023-07-10T10:29:38+0000 DEBUG Loaded plugins: builddep, changelog, config-
manager, copr, debug, debuginfo-install, download, generate_completion_cache, groups-
manager, needs-restarting, playground, product-id, repoclosure, repodiff, repograph,
repomanage, reposync, subscription-manager, uploadprofile
2023-07-10T10:29:38+0000 INFO Updating Subscription Management repositories.
```

```
2023-07-10T10:29:38+0000 INFO Unable to read consumer identity
2023-07-10T10:29:38+0000 INFO Subscription Manager is operating in container mode.
2023-07-10T10:29:38+0000 INFO
```

- c. 列出特定容器内 **/var/log** 中含有的日志文件和子目录：

```
$ oc exec <pod_name> -c <container_name> ls /var/log
```

- d. 查询特定容器中的 **/var/log** 中所含的特定日志文件：

```
$ oc exec <pod_name> -c <container_name> cat /var/log/<path_to_log>
```

7.4.4. 访问运行的 pod

您可以通过在 pod 中打开 shell，或通过端口转发获取网络访问，来动态查看正在运行的 pod。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- API 服务仍然可以正常工作。
- 已安装 OpenShift CLI (**oc**)。

流程

1. 切换到包含您要访问的 pod 的项目。这是必要的，因为 **oc rsh** 命令不支持使用 **-n** 选项指定命名空间：

```
$ oc project <namespace>
```

2. 启动到 pod 的远程 shell:

```
$ oc rsh <pod_name> ❶
```

- ❶ 如果 pod 有多个容器，除非使用 **-c <container_name>** 指定了一个容器，否则 **oc rsh** 会默认使用第一个容器。

3. 启动至 pod 中的特定容器中的一个远程 shell：

```
$ oc rsh -c <container_name> pod/<pod_name>
```

4. 创建一个端口转发会话到 pod 上的端口：

```
$ oc port-forward <pod_name> <host_port>:<pod_port> ❶
```

- ❶ 输入 **Ctrl+C** 来取消端口转发会话。

7.4.5. 启动具有 root 访问权限的 debug pod

您可以基于一个有问题的 pod 部署或部署配置，启动具有根访问权限的 debug pod。pod 用户通常使用非 root 权限运行，但运行具有临时 root 特权的 pod 进行故障排除时在调查问题时很有用：

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- API 服务仍然可以正常工作。
- 已安装 OpenShift CLI (**oc**)。

流程

1. 根据一个部署启动具有 root 访问权限的 debug pod。

- a. 获取项目部署名称：

```
$ oc get deployment -n <project_name>
```

- b. 根据部署启动带有 root 权限的 debug pod:

```
$ oc debug deployment/my-deployment --as-root -n <project_name>
```

2. 根据部署配置启动具有 root 访问权限的 debug pod。

- a. 获取项目的部署配置名称：

```
$ oc get deploymentconfigs -n <project_name>
```

- b. 根据部署配置，使用 root 权限启动 debug pod:

```
$ oc debug deploymentconfig/my-deployment-configuration --as-root -n <project_name>
```



注意

您可以将 **-- <command>** 附加到前面的 **oc debug** 命令中，以便在 debug pod 中运行单个命令，而不是运行交互式 shell。

7.4.6. 将文件复制到 pod 和容器，或从 pod 和容器中复制

您可以将文件复制到 pod 或从 pod 复制，以测试配置更改或收集诊断信息。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- API 服务仍然可以正常工作。
- 已安装 OpenShift CLI (**oc**)。

流程

1. 将文件复制到 pod:

```
$ oc cp <local_path> <pod_name>:/<path> -c <container_name> 1
```

1 如果没有指定 **-c** 选项，则会选择 pod 中的第一个容器。

2. 从 pod 复制文件：

```
$ oc cp <pod_name>:/<path> -c <container_name> <local_path> 1
```

1 如果没有指定 **-c** 选项，则会选择 pod 中的第一个容器。



注意

要使 **oc cp** 正常工作，容器内必须有 **tar**。

7.5. 对 SOURCE-TO-IMAGE 进行故障排除

7.5.1. Source-to-Image 故障排除策略

Source-to-Image (S2I) 是一种用于构建可重复生成的 Docker 格式容器镜像的工具。它通过将应用程序源代码注入容器镜像，并汇编新镜像来生成可随时运行的镜像。新镜像融合了基础镜像（构建器）和构建的源。

要确定 S2I 进程中的故障发生位置，您可以观察与以下 S2I 阶段相关的 pod 状态：

1. **在构建配置阶段**，构建 pod 用于从基础镜像和应用程序源代码创建应用程序容器镜像。
2. **在部署配置阶段**，部署 pod 用于从构建配置阶段构建的应用程序容器镜像中部署应用程序 pod。部署 pod 还会部署其他资源，如服务和路由。部署配置在构建配置成功后开始。
3. **在部署 pod 启动应用程序 pod 后**，应用程序故障可能会在运行的应用程序 pod 中发生。例如，即使应用程序 pod 处于 **Running** 状态，应用程序的行为也可能不会如预期。在这种情况下，您可以访问正在运行的应用程序 pod，以调查 pod 中的应用程序故障。

当对 S2I 问题进行故障排除时，请按照这个策略操作：

1. 监控构建、部署和应用程序 pod 状态
2. 确定发生问题 S2I 进程阶段
3. 查看与失败阶段对应的日志

7.5.2. 收集 Source-to-Image 诊断数据

S2I 工具按顺序运行构建 pod 和部署 pod。部署 pod 负责根据构建阶段创建的应用程序容器镜像部署应用程序 pod。观察构建、部署和应用程序 pod 状态，以确定 S2I 进程中的故障发生位置。然后，重点收集诊断数据。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- API 服务仍然可以正常工作。

- 已安装 OpenShift CLI(**oc**)。

流程

1. 在整个 S2I 过程中监控 pod 状态，以确定在哪个阶段发生故障：

```
$ oc get pods -w 1
```

- 1** 使用 **-w** 来监控 pod 是否有变化，直到您使用 **Ctrl+C** 退出命令。

2. 检查 pod 失败的日志以找出错误。

- 如果构建 pod 失败，请检查构建 pod 的日志：

```
$ oc logs -f pod/<application_name>-<build_number>-build
```



注意

另外，您可以使用 **oc logs -f bc/<application_name>** 来查看构建配置的日志。构建配置的日志包括来自构建 pod 的日志。

- 如果部署 pod 失败，请查看部署 pod 的日志：

```
$ oc logs -f pod/<application_name>-<build_number>-deploy
```



注意

另外，您可以使用 **oc logs -f bc/<application_name>** 来查看部署配置的日志。此操作会从部署 pod 输出日志，直到部署 pod 成功完成为止。如果在部署 pod 完成后运行，命令会输出来自应用程序 pod 的日志。部署 pod 完成后，仍可通过运行 **oc logs -f pod/<application_name>-<build_number>-deploy** 来访问其日志。

- 如果应用程序 pod 失败，或者应用程序没有如预期在正在运行的应用程序 pod 中发生，请查看应用程序 pod 的日志：

```
$ oc logs -f pod/<application_name>-<build_number>-<random_string>
```

7.5.3. 收集应用程序诊断数据以调查应用程序失败

应用程序故障可在运行的应用程序 pod 中发生。在这些情况下，您可以使用以下策略检索诊断信息：

- 检查与应用程序 pod 相关的事件。
- 查看应用程序 pod 的日志，包括不是由 OpenShift Logging 框架收集的特定应用程序日志文件。
- 以互动方式测试应用程序功能，并在应用程序容器中运行诊断工具。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。

- 已安装 OpenShift CLI(**oc**)。

流程

1. 列出与特定应用程序 pod 相关的事件。以下示例检索名为 **my-app-1-akdlg** 的应用程序 pod 的事件:

```
$ oc describe pod/my-app-1-akdlg
```

2. 检查应用程序 pod 的日志：

```
$ oc logs -f pod/my-app-1-akdlg
```

3. 在正在运行的应用程序 pod 中查询特定日志。发送到 stdout 的日志由 OpenShift Logging 框架收集，并包含在上一命令的输出中。以下查询只适用于没有发送到 stdout 的日志。
 - a. 如果应用程序日志可以在 pod 内不需要 root 权限的情况下就可以进行访问，则按如下方式处理日志文件：

```
$ oc exec my-app-1-akdlg -- cat /var/log/my-application.log
```

- b. 如果需要 root 访问权限才能查看应用程序日志，您可以启动具有 root 权限的 debug 容器，然后从容器内查看日志文件。从项目的 **DeploymentConfig** 对象启动 debug 容器。pod 用户通常使用非 root 权限运行，但运行具有临时 root 特权的 pod 进行故障排除时在调查问题时很有用：

```
$ oc debug dc/my-deployment-configuration --as-root -- cat /var/log/my-application.log
```



注意

如果您运行不使用 `-- <command>` 的 **oc debug dc/<deployment_configuration> --as-root**，则可以获得 debug pod 内带有 root 权限的一个交互式 shell。

4. 以互动方式测试应用程序功能,并在带有互动 shell 的应用程序容器中运行诊断工具。

- a. 在应用程序容器上启动一个交互式 shell:

```
$ oc exec -it my-app-1-akdlg /bin/bash
```

- b. 在 shell 中以互动方式测试应用程序功能。例如，您可以运行容器的入口点命令并观察结果。然后，在更新源代码并通过 S2I 进程重建应用程序容器前，直接从命令行测试更改。
- c. 运行容器中的诊断二进制文件。



注意

运行一些诊断二进制文件需要 root 权限。在这些情况下，您可以通过运行 **oc debug dc/<deployment_configuration> --as-root**，根据有问题的 pod 的 **DeploymentConfig** 对象启动一个带有 root 访问权限的 debug pod。然后，您可以从 debug pod 中以 root 用户身份运行诊断二进制文件。

7.6. 存储问题故障排除

7.6.1. 解决多附件错误

当节点崩溃或立即关闭时,预期会从节点卸载附加的 ReadWriteOnce(RWO)卷,以便被调度到另一节点上的 pod 使用。

但是,不可能在新节点中挂载,因为失败的节点无法卸载附加的卷。

报告了一个 multi-attach 错误：

输出示例

```
Unable to attach or mount volumes: unmounted volumes=[sso-mysql-pvol], unattached volumes=[sso-mysql-pvol default-token-x4rzc]: timed out waiting for the condition
Multi-Attach error for volume "pvc-8837384d-69d7-40b2-b2e6-5df86943eef9" Volume is already used by pod(s) sso-mysql-1-ns6b4
```

流程

要解决 multi-attach 问题,请使用以下解决方案之一：

- 使用 RWX 卷启用多个附件。
对于大多数存储解决方案,您可以使用 ReadWriteMany(RWX)卷以防止多附加错误。
- 使用 RWO 卷时,恢复或删除故障节点。
对于不支持 RWX 的存储,如 VMware vSphere,必须改为使用 RWO 卷。但是, RWO 卷无法挂载到多个节点上。

如果您遇到带有 RWO 卷的多附件错误消息,请强制在关闭或崩溃的节点上删除 pod,以避免关键工作负载中的数据丢失,例如在附加动态持久性卷时。

```
$ oc delete pod <old_pod> --force=true --grace-period=0
```

该命令会在 6 分钟后删除处于关闭或崩溃的节点上的卷。

7.7. 调查监控问题

OpenShift Dedicated 包括一个预配置、预安装和自我更新的监控堆栈,为核心平台组件提供监控。在 OpenShift Dedicated 4 中,集群管理员可以选择性地为用户定义的项目启用监控。

如果出现问题,请使用这些步骤：

- 您自己的指标不可用。
- Prometheus 消耗大量磁盘空间。
- **KubePersistentVolumeFillingUp** 警报正在触发 Prometheus。

7.7.1. 调查用户定义的项目指标不可用的原因

通过 **ServiceMonitor** 资源,您可以确定如何使用用户定义的项目中的服务公开的指标。如果您创建了 **ServiceMonitor** 资源,但无法在 Metrics UI 中看到任何对应的指标,请按该流程中所述的步骤操作。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI(**oc**)。
- 您已为用户定义的项目启用并配置了监控。
- 您已创建了 **ServiceMonitor** 资源。

流程

1. 确保您的项目和资源没有不包括在用户工作负载监控中。以下示例使用 **ns1** 项目。

- a. 验证项目没有附加 **openshift.io/user-monitoring=false** 标签：

```
$ oc get namespace ns1 --show-labels | grep 'openshift.io/user-monitoring=false'
```



注意

用户工作负载项目设置的默认标签为 **openshift.io/user-monitoring=true**。但是，除非手动应用了该标签，否则标签不可见。

- b. 验证 **ServiceMonitor** 和 **PodMonitor** 资源没有附加 **openshift.io/user-monitoring=false** 标签。以下示例检查 **prometheus-example-monitor** 服务监控器。

```
$ oc -n ns1 get servicemonitor prometheus-example-monitor --show-labels | grep 'openshift.io/user-monitoring=false'
```

- c. 如果附加了标签，请删除该标签：

从项目中删除该标签的示例

```
$ oc label namespace ns1 'openshift.io/user-monitoring-'
```

从资源中删除标签的示例

```
$ oc -n ns1 label servicemonitor prometheus-example-monitor 'openshift.io/user-monitoring-'
```

输出示例

```
namespace/ns1 unlabeled
```

2. 在服务和 **ServiceMonitor** 资源配置中，检查对应的标签是否匹配。以下示例使用 **prometheus-example-app** 服务、**prometheus-example-monitor** 服务监控和 **ns1** 项目。

- a. 获取服务中定义的标签。

```
$ oc -n ns1 get service prometheus-example-app -o yaml
```

输出示例

```
labels:
  app: prometheus-example-app
```

- b. 检查 **ServiceMonitor** 资源配置中的 **matchLabels** 定义是否与上一步中的标签输出匹配。

```
$ oc -n ns1 get servicemonitor prometheus-example-monitor -o yaml
```

输出示例

```
apiVersion: v1
kind: ServiceMonitor
metadata:
  name: prometheus-example-monitor
  namespace: ns1
spec:
  endpoints:
  - interval: 30s
    port: web
    scheme: http
  selector:
    matchLabels:
      app: prometheus-example-app
```



注意

您可以作为具有项目查看权限的开发者检查服务和 **ServiceMonitor** 资源标签。

3. 在 **openshift-user-workload-monitoring** 项目中检查 Prometheus Operator 的日志。

- a. 列出 **openshift-user-workload-monitoring** 项目中的 Pod：

```
$ oc -n openshift-user-workload-monitoring get pods
```

输出示例

NAME	READY	STATUS	RESTARTS	AGE
prometheus-operator-776fcbbd56-2nbfm	2/2	Running	0	132m
prometheus-user-workload-0	5/5	Running	1	132m
prometheus-user-workload-1	5/5	Running	1	132m
thanos-ruler-user-workload-0	3/3	Running	0	132m
thanos-ruler-user-workload-1	3/3	Running	0	132m

- b. 从 **prometheus-operator** Pod 中的 **prometheus-operator** 容器获取日志。在以下示例中，Pod 名为 **prometheus-operator-776fcbbd56-2nbfm**：

```
$ oc -n openshift-user-workload-monitoring logs prometheus-operator-776fcbbd56-2nbfm -c prometheus-operator
```

如果服务监控器出现问题，日志可能包含类似本例的错误：

```
level=warn ts=2020-08-10T11:48:20.906739623Z caller=operator.go:1829
```

```
component=prometheusoperator msg="skipping servicemonitor" error="it accesses file
system via bearer token file which Prometheus specification prohibits"
servicemonitor=eagle/eagle namespace=openshift-user-workload-monitoring
prometheus=user-workload
```

4. 在 OpenShift Dedicated Web 控制台 UI 中的 **Metrics 目标** 页面中查看您的端点的目标状态。
 - a. 登录 OpenShift Dedicated Web 控制台，再进入 **Observe → Targets**。
 - b. 在列表中找到指标端点，并在 **Status** 列中查看目标的状态。
 - c. 如果 **Status** 为 **Down**，点端点的 URL 查看该指标目标的 **Target Details** 页面的更多信息。
5. 在 **openshift-user-workload-monitoring** 项目中为 Prometheus Operator 配置 debug 级别日志记录。
 - a. 在 **openshift-user-workload-monitoring** 项目中编辑 **user-workload-monitoring-config ConfigMap** 对象：

```
$ oc -n openshift-user-workload-monitoring edit configmap user-workload-monitoring-
config
```

- b. 在 **data/config.yaml** 下为 **prometheusOperator** 添加 **logLevel: debug**，将日志级别设置为 **debug**：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    prometheusOperator:
      logLevel: debug
  # ...
```

- c. 保存文件以使改变生效。受影响的 **prometheus-operator** Pod 会自动重新部署。
 - d. 确认 **debug** 日志级别已应用到 **openshift-user-workload-monitoring** 项目中的 **prometheus-operator** 部署：

```
$ oc -n openshift-user-workload-monitoring get deploy prometheus-operator -o yaml |
grep "log-level"
```

输出示例

```
- --log-level=debug
```

Debug 级别日志记录将显示 Prometheus Operator 发出的所有调用。

- e. 检查 **prometheus-operator** Pod 是否正在运行：

```
$ oc -n openshift-user-workload-monitoring get pods
```



注意

如果配置映射中包含了一个未识别的 Prometheus Operator **loglevel** 值，则 **prometheus-operator** Pod 可能无法成功重启。

- f. 查看 debug 日志，以了解 Prometheus Operator 是否在使用 **ServiceMonitor** 资源。查看日志中的其他相关错误。

其他资源

- [指定如何监控服务](#)
- [获取有关指标目标的详细信息](#)

7.7.2. 确定为什么 Prometheus 消耗大量磁盘空间

开发人员可以使用键值对的形式为指标定义属性。潜在的键值对数量与属性的可能值数量对应。具有无限数量可能值的属性被称为未绑定属性。例如，**customer_id** 属性不绑定，因为它有无限多个可能的值。

每个分配的键值对都有唯一的时间序列。在标签中使用许多未绑定属性可导致所创建的时间序列数量出现指数增加。这可能会影响 Prometheus 性能，并消耗大量磁盘空间。

当 Prometheus 消耗大量磁盘时，您可以使用以下方法：

- 使用 Prometheus HTTP API 检查时间序列数据库(TSDB)状态，以了解有关哪些标签创建最多时间序列数据的更多信息。这样做需要集群管理员特权。
- 检查正在收集的提取示例数量。
- 要减少创建的唯一时间序列数量，您可以减少分配给用户定义的指标的未绑定属性数量



注意

使用绑定到一组有限可能值的属性可减少潜在的键-值对组合数量。

- 对可在用户定义的项目中提取的示例数量实施限制。这需要集群管理员特权。

先决条件

- 您可以使用具有 **dedicated-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI(**oc**)。

流程

1. 在 OpenShift Dedicated Web 控制台中，进入 **Observe → Metrics**。
2. 在 **Expression** 字段中输入 Prometheus Query Language (PromQL) 查询。以下示例查询有助于识别可能导致高磁盘空间消耗的高卡性指标：
 - 通过运行以下查询，您可以识别具有最高提取示例数的十个作业：

```
topk(10, max by(namespace, job) (topk by(namespace, job) (1,
scrape_samples_post_metric_relabeling)))
```

- 通过运行以下查询，您可以通过识别在上一小时内创建了最多时间序列数据的十个作业，从而找出相关的时间序列：

```
topk(10, sum by(namespace, job) (sum_over_time(scrape_series_added[1h])))
```

- 如果指标的提取示例数大于预期，请检查分配给指标的未绑定标签值数量：

- 如果指标与用户定义的项目相关，请查看分配给您的工作负载的指标键-值对。它们通过应用程序级别的 Prometheus 客户端库实施。尝试限制标签中引用的未绑定属性数量。
- 如果指标与 OpenShift Dedicated 核心项目相关，请在[红帽客户门户网站](#)上创建一个红帽支持问题单。

- 以 **dedicated-admin** 身份登录时，按照以下步骤使用 Prometheus HTTP API 查看 TSDB 状态：

- 运行以下命令来获取 Prometheus API 路由 URL：

```
$ HOST=$(oc -n openshift-monitoring get route prometheus-k8s -  
ojsonpath='{.status.ingress[].host}')
```

- 运行以下命令来提取身份验证令牌：

```
$ TOKEN=$(oc whoami -t)
```

- 运行以下命令，查询 Prometheus 的 TSDB 状态：

```
$ curl -H "Authorization: Bearer $TOKEN" -k "https://$HOST/api/v1/status/tsdb"
```

输出示例

```
"status": "success", "data": {"headStats": {"numSeries": 507473,  
"numLabelPairs": 19832, "chunkCount": 946298, "minTime": 1712253600010,  
"maxTime": 1712257935346}, "seriesCountByMetricName":  
[{"name": "etcd_request_duration_seconds_bucket", "value": 51840},  
{"name": "apiserver_request_sli_duration_seconds_bucket", "value": 47718},  
...
```

其他资源

- [为用户定义的项目设置提取间隔、评估间隔和强制实施限制](#)

7.8. 诊断 OPENSIFT CLI (oc) 问题

7.8.1. 了解 OpenShift CLI (oc) 日志级别

使用 OpenShift CLI (**oc**)，您可以从终端创建应用程序并管理 OpenShift Dedicated 项目。

如果出现特定于 **oc** 命令的问题，将 **oc** 日志级别提高为输出 API 请求、API 响应以及命令生成的 **curl** 请求详情。这提供了特定的 **oc** 命令的底层操作信息，以帮助了解故障的本质。

oc 日志级别范围从 1 到 10。下表提供了 **oc** 日志级别列表及其描述。

表 7.4. OpenShift CLI (oc) 日志级别

日志级别	描述
1 到 5	没有额外的日志记录到 stderr。
6	为 stderr 记录 API 请求。
7	将 API 请求和标头记录到 stderr。
8	记录 API 请求、标头和正文，以及 API 响应标头和正文到 stderr。
9	记录日志 API 请求、标头和正文、API 响应标头和正文，以及 curl 请求到 stderr。
10	记录日志 API 请求、标头和正文、API 响应标头和正文，以及 curl 请求到 stderr。记录的信息会更详细。

7.8.2. 指定 OpenShift CLI (oc) 日志级别

您可以通过提高命令的日志级别来调查 OpenShift CLI (oc) 问题。

OpenShift Dedicated 用户的当前会话令牌通常包含在记录的 **curl** 请求中。您还可以手动获取当前用户的会话令牌，以便在测试 **oc** 命令的底层进程的各个方面时使用。

先决条件

- 安装 OpenShift CLI (oc)。

流程

- 在运行 **oc** 命令时指定 **oc** 日志级别：

```
$ oc <command> --loglevel <log_level>
```

其中：

<command>

指定您正在运行的命令。

<log_level>

指定要应用到命令的日志级别。

- 要获取当前用户的会话令牌，请运行以下命令：

```
$ oc whoami -t
```

输出示例

```
sha256~RCV3Qcn7H-OEfqCGVI0CvnZ6...
```

7.9. 红帽受管资源

7.9.1. 概述

以下涵盖了由 Service Reliability Engineering Platform (SRE-P) 团队管理或保护的所有 OpenShift Dedicated 资源。客户不得修改这些资源，因为这样做可能会导致集群不稳定。

7.9.2. Hive 受管资源

以下列表显示了由 OpenShift Hive 管理的 OpenShift Dedicated 资源，即集中式配置管理系统。除了安装期间创建的 OpenShift Container Platform 资源外，这些资源还除外。OpenShift Hive 持续尝试保持所有 OpenShift Dedicated 集群的一致性。应该通过 OpenShift Cluster Manager 对 OpenShift Dedicated 资源进行更改，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 7.1. Hive 受管资源列表

```
Resources:
ConfigMap:
- namespace: openshift-config
  name: rosa-brand-logo
- namespace: openshift-console
  name: custom-logo
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-config
- namespace: openshift-file-integrity
  name: fr-aide-conf
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator-config
- namespace: openshift-monitoring
  name: cluster-monitoring-config
- namespace: openshift-monitoring
  name: managed-namespaces
- namespace: openshift-monitoring
  name: ocp-namespaces
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter-code
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter-trusted-ca-bundle
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-code
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-trusted-ca-bundle
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-code
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-trusted-ca-bundle
- namespace: openshift-security
  name: osd-audit-policy
- namespace: openshift-validation-webhook
  name: webhook-cert
- namespace: openshift
  name: motd
```

Endpoints:

- namespace: openshift-deployment-validation-operator
name: deployment-validation-operator-metrics
- namespace: openshift-monitoring
name: sre-dns-latency-exporter
- namespace: openshift-monitoring
name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
name: sre-stuck-ebs-vols
- namespace: openshift-scanning
name: loggerservice
- namespace: openshift-security
name: audit-exporter
- namespace: openshift-validation-webhook
name: validation-webhook

Namespace:

- name: dedicated-admin
- name: openshift-addon-operator
- name: openshift-aqua
- name: openshift-aws-vpce-operator
- name: openshift-backplane
- name: openshift-backplane-cee
- name: openshift-backplane-csa
- name: openshift-backplane-cse
- name: openshift-backplane-csm
- name: openshift-backplane-managed-scripts
- name: openshift-backplane-mobb
- name: openshift-backplane-srep
- name: openshift-backplane-tam
- name: openshift-cloud-ingress-operator
- name: openshift-codeready-workspaces
- name: openshift-compliance
- name: openshift-compliance-monkey
- name: openshift-container-security
- name: openshift-custom-domains-operator
- name: openshift-customer-monitoring
- name: openshift-deployment-validation-operator
- name: openshift-managed-node-metadata-operator
- name: openshift-file-integrity
- name: openshift-logging
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-observability-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-scanning
- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-suricata
- name: openshift-validation-webhook
- name: openshift-velero
- name: openshift-monitoring

- name: openshift
- name: openshift-cluster-version
- name: keycloak
- name: goalert
- name: configure-goalert-operator

ReplicationController:

- namespace: openshift-monitoring
name: sre-ebs-iops-reporter-1
- namespace: openshift-monitoring
name: sre-stuck-ebs-vols-1

Secret:

- namespace: openshift-authentication
name: v4-0-config-user-idp-0-file-data
- namespace: openshift-authentication
name: v4-0-config-user-template-error
- namespace: openshift-authentication
name: v4-0-config-user-template-login
- namespace: openshift-authentication
name: v4-0-config-user-template-provider-selection
- namespace: openshift-config
name: htpasswd-secret
- namespace: openshift-config
name: osd-oauth-templates-errors
- namespace: openshift-config
name: osd-oauth-templates-login
- namespace: openshift-config
name: osd-oauth-templates-providers
- namespace: openshift-config
name: rosa-oauth-templates-errors
- namespace: openshift-config
name: rosa-oauth-templates-login
- namespace: openshift-config
name: rosa-oauth-templates-providers
- namespace: openshift-config
name: support
- namespace: openshift-config
name: tony-devlab-primary-cert-bundle-secret
- namespace: openshift-ingress
name: tony-devlab-primary-cert-bundle-secret
- namespace: openshift-kube-apiserver
name: user-serving-cert-000
- namespace: openshift-kube-apiserver
name: user-serving-cert-001
- namespace: openshift-monitoring
name: dms-secret
- namespace: openshift-monitoring
name: observatorium-credentials
- namespace: openshift-monitoring
name: pd-secret
- namespace: openshift-scanning
name: clam-secrets
- namespace: openshift-scanning
name: logger-secrets
- namespace: openshift-security
name: splunk-auth

ServiceAccount:

- namespace: openshift-backplane-managed-scripts
name: osd-backplane
- namespace: openshift-backplane-srep
name: 6804d07fb268b8285b023bcf65392f0e
- namespace: openshift-backplane-srep
name: osd-delete-ownerrefs-serviceaccounts
- namespace: openshift-backplane
name: osd-delete-backplane-serviceaccounts
- namespace: openshift-cloud-ingress-operator
name: cloud-ingress-operator
- namespace: openshift-custom-domains-operator
name: custom-domains-operator
- namespace: openshift-managed-upgrade-operator
name: managed-upgrade-operator
- namespace: openshift-machine-api
name: osd-disable-cpms
- namespace: openshift-marketplace
name: osd-patch-subscription-source
- namespace: openshift-monitoring
name: configure-alertmanager-operator
- namespace: openshift-monitoring
name: osd-cluster-ready
- namespace: openshift-monitoring
name: osd-rebalance-infra-nodes
- namespace: openshift-monitoring
name: sre-dns-latency-exporter
- namespace: openshift-monitoring
name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
name: sre-stuck-ebs-vols
- namespace: openshift-network-diagnostics
name: sre-pod-network-connectivity-check-pruner
- namespace: openshift-ocm-agent-operator
name: ocm-agent-operator
- namespace: openshift-rbac-permissions
name: rbac-permissions-operator
- namespace: openshift-splunk-forwarder-operator
name: splunk-forwarder-operator
- namespace: openshift-sre-pruning
name: bz1980755
- namespace: openshift-scanning
name: logger-sa
- namespace: openshift-scanning
name: scanner-sa
- namespace: openshift-sre-pruning
name: sre-pruner-sa
- namespace: openshift-suricata
name: suricata-sa
- namespace: openshift-validation-webhook
name: validation-webhook
- namespace: openshift-velero
name: managed-velero-operator
- namespace: openshift-velero
name: velero
- namespace: openshift-backplane-srep
name: UNIQUE_BACKPLANE_SERVICEACCOUNT_ID

Service:

- namespace: openshift-deployment-validation-operator
name: deployment-validation-operator-metrics
- namespace: openshift-monitoring
name: sre-dns-latency-exporter
- namespace: openshift-monitoring
name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
name: sre-stuck-ebs-vols
- namespace: openshift-scanning
name: loggerservice
- namespace: openshift-security
name: audit-exporter
- namespace: openshift-validation-webhook
name: validation-webhook

AddonOperator:

- name: addon-operator

ValidatingWebhookConfiguration:

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

DaemonSet:

- namespace: openshift-monitoring
name: sre-dns-latency-exporter
- namespace: openshift-scanning
name: logger
- namespace: openshift-scanning
name: scanner
- namespace: openshift-security
name: audit-exporter
- namespace: openshift-suricata
name: suricata
- namespace: openshift-validation-webhook
name: validation-webhook

DeploymentConfig:

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

ClusterRoleBinding:

- name: aqua-scanner-binding
- name: backplane-cluster-admin
- name: backplane-impersonate-cluster-admin
- name: bz1980755
- name: configure-alertmanager-operator-prom
- name: dedicated-admins-cluster
- name: dedicated-admins-registry-cas-cluster
- name: logger-clusterrolebinding
- name: openshift-backplane-managed-scripts-reader
- name: osd-cluster-admin
- name: osd-cluster-ready
- name: osd-delete-backplane-script-resources

- name: osd-delete-ownerrefs-serviceaccounts
- name: osd-patch-subscription-source
- name: osd-rebalance-infra-nodes
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: splunk-forwarder-operator-clusterrolebinding
- name: sre-pod-network-connectivity-check-pruner
- name: sre-pruner-buildsdeploys-pruning
- name: velero
- name: webhook-validation

ClusterRole:

- name: backplane-cee-readers-cluster
- name: backplane-impersonate-cluster-admin
- name: backplane-readers-cluster
- name: backplane-srep-admins-cluster
- name: backplane-srep-admins-project
- name: bz1980755
- name: dedicated-admins-aggregate-cluster
- name: dedicated-admins-aggregate-project
- name: dedicated-admins-cluster
- name: dedicated-admins-manage-operators
- name: dedicated-admins-project
- name: dedicated-admins-registry-cas-cluster
- name: dedicated-readers
- name: image-scanner
- name: logger-clusterrole
- name: openshift-backplane-managed-scripts-reader
- name: openshift-splunk-forwarder-operator
- name: osd-cluster-ready
- name: osd-custom-domains-dedicated-admin-cluster
- name: osd-delete-backplane-script-resources
- name: osd-delete-backplane-serviceaccounts
- name: osd-delete-ownerrefs-serviceaccounts
- name: osd-get-namespace
- name: osd-netnamespaces-dedicated-admin-cluster
- name: osd-patch-subscription-source
- name: osd-readers-aggregate
- name: osd-rebalance-infra-nodes
- name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: sre-allow-read-machine-info
- name: sre-pruner-buildsdeploys-cr
- name: webhook-validation-cr

RoleBinding:

- namespace: kube-system
 - name: cloud-ingress-operator-cluster-config-v1-reader
- namespace: kube-system
 - name: managed-velero-operator-cluster-config-v1-reader
- namespace: openshift-aqua
 - name: dedicated-admins-openshift-aqua
- namespace: openshift-backplane-managed-scripts
 - name: backplane-cee-mustgather
- namespace: openshift-backplane-managed-scripts
 - name: backplane-srep-mustgather
- namespace: openshift-backplane-managed-scripts

```

name: osd-delete-backplane-script-resources
- namespace: openshift-cloud-ingress-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-codeready-workspaces
  name: dedicated-admins-openshift-codeready-workspaces
- namespace: openshift-config
  name: dedicated-admins-project-request
- namespace: openshift-config
  name: dedicated-admins-registry-cas-project
- namespace: openshift-config
  name: muo-pullsecret-reader
- namespace: openshift-config
  name: oao-openshiftconfig-reader
- namespace: openshift-config
  name: osd-cluster-ready
- namespace: openshift-custom-domains-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-customer-monitoring
  name: dedicated-admins-openshift-customer-monitoring
- namespace: openshift-customer-monitoring
  name: prometheus-k8s-openshift-customer-monitoring
- namespace: openshift-dns
  name: dedicated-admins-openshift-dns
- namespace: openshift-dns
  name: osd-rebalance-infra-nodes-openshift-dns
- namespace: openshift-image-registry
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-ingress
  name: cloud-ingress-operator
- namespace: openshift-kube-apiserver
  name: cloud-ingress-operator
- namespace: openshift-machine-api
  name: cloud-ingress-operator
- namespace: openshift-logging
  name: admin-dedicated-admins
- namespace: openshift-logging
  name: admin-system:serviceaccounts:dedicated-admin
- namespace: openshift-logging
  name: openshift-logging-dedicated-admins
- namespace: openshift-logging
  name: openshift-logging:serviceaccounts:dedicated-admin
- namespace: openshift-machine-api
  name: osd-cluster-ready
- namespace: openshift-machine-api
  name: sre-ebs-iops-reporter-read-machine-info
- namespace: openshift-machine-api
  name: sre-stuck-ebs-vols-read-machine-info
- namespace: openshift-managed-node-metadata-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-machine-api
  name: osd-disable-cpms
- namespace: openshift-marketplace
  name: dedicated-admins-openshift-marketplace
- namespace: openshift-monitoring

```

```
name: backplane-cee
- namespace: openshift-monitoring
  name: muo-monitoring-reader
- namespace: openshift-monitoring
  name: oao-monitoring-manager
- namespace: openshift-monitoring
  name: osd-cluster-ready
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes-openshift-monitoring
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
- namespace: openshift-must-gather-operator
  name: backplane-cee-mustgather
- namespace: openshift-must-gather-operator
  name: backplane-srep-mustgather
- namespace: openshift-must-gather-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-network-diagnostics
  name: sre-pod-network-connectivity-check-pruner
- namespace: openshift-network-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-ocm-agent-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-operators-redhat
  name: admin-dedicated-admins
- namespace: openshift-operators-redhat
  name: admin-system:serviceaccounts:dedicated-admin
- namespace: openshift-operators-redhat
  name: openshift-operators-redhat-dedicated-admins
- namespace: openshift-operators-redhat
  name: openshift-operators-redhat:serviceaccounts:dedicated-admin
- namespace: openshift-operators
  name: dedicated-admins-openshift-operators
- namespace: openshift-osd-metrics
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-osd-metrics
  name: prometheus-k8s
- namespace: openshift-rbac-permissions
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-rbac-permissions
  name: prometheus-k8s
- namespace: openshift-route-monitor-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-scanning
  name: scanner-rolebinding
- namespace: openshift-security
  name: osd-rebalance-infra-nodes-openshift-security
- namespace: openshift-security
  name: prometheus-k8s
- namespace: openshift-splunk-forwarder-operator
```

```

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

```

- namespace: openshift-logging
name: dedicated-admins-openshift-logging
 - namespace: openshift-machine-api
name: osd-cluster-ready
 - namespace: openshift-machine-api
name: osd-disable-cpms
 - namespace: openshift-marketplace
name: dedicated-admins-openshift-marketplace
 - namespace: openshift-monitoring
name: backplane-cee
 - namespace: openshift-monitoring
name: muo-monitoring-reader
 - namespace: openshift-monitoring
name: oao-monitoring-manager
 - namespace: openshift-monitoring
name: osd-cluster-ready
 - namespace: openshift-monitoring
name: osd-rebalance-infra-nodes-openshift-monitoring
 - namespace: openshift-must-gather-operator
name: backplane-cee-mustgather
 - namespace: openshift-must-gather-operator
name: backplane-srep-mustgather
 - namespace: openshift-network-diagnostics
name: sre-pod-network-connectivity-check-pruner
 - namespace: openshift-operators
name: dedicated-admins-openshift-operators
 - namespace: openshift-osd-metrics
name: prometheus-k8s
 - namespace: openshift-rbac-permissions
name: prometheus-k8s
 - namespace: openshift-scanning
name: scanner-role
 - namespace: openshift-security
name: osd-rebalance-infra-nodes-openshift-security
 - namespace: openshift-security
name: prometheus-k8s
 - namespace: openshift-suricata
name: suricata-role
 - namespace: openshift-user-workload-monitoring
name: dedicated-admins-user-workload-monitoring-create-cm
 - namespace: openshift-user-workload-monitoring
name: dedicated-admins-user-workload-monitoring-manage-am-secret
 - namespace: openshift-user-workload-monitoring
name: osd-rebalance-infra-nodes-openshift-user-workload-monitoring
 - namespace: openshift-velero
name: prometheus-k8s
- CronJob:
- namespace: openshift-backplane-managed-scripts
name: osd-delete-backplane-script-resources
 - namespace: openshift-backplane-srep
name: osd-delete-ownerrefs-serviceaccounts
 - namespace: openshift-backplane
name: osd-delete-backplane-serviceaccounts
 - namespace: openshift-machine-api
name: osd-disable-cpms
 - namespace: openshift-marketplace

```

    name: osd-patch-subscription-source
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes
- namespace: openshift-network-diagnostics
  name: sre-pod-network-connectivity-check-pruner
- namespace: openshift-sre-pruning
  name: builds-pruner
- namespace: openshift-sre-pruning
  name: bz1980755
- namespace: openshift-sre-pruning
  name: deployments-pruner
Job:
- namespace: openshift-monitoring
  name: osd-cluster-ready
CredentialsRequest:
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-credentials-aws
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-credentials-gcp
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-aws-credentials
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-aws-credentials
- namespace: openshift-velero
  name: managed-velero-operator-iam-credentials-aws
- namespace: openshift-velero
  name: managed-velero-operator-iam-credentials-gcp
APIScheme:
- namespace: openshift-cloud-ingress-operator
  name: rh-api
PublishingStrategy:
- namespace: openshift-cloud-ingress-operator
  name: publishingstrategy
ScanSettingBinding:
- namespace: openshift-compliance
  name: fedramp-high-ocp
- namespace: openshift-compliance
  name: fedramp-high-rhcos
ScanSetting:
- namespace: openshift-compliance
  name: osd
TailoredProfile:
- namespace: openshift-compliance
  name: rhcos4-high-rosa
OAuth:
- name: cluster
EndpointSlice:
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-metrics-rhtwg
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter-4cw9r
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-6tx5g
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-gmdhs
- namespace: openshift-scanning

```

```
name: loggerservice-zprbq
- namespace: openshift-security
  name: audit-exporter-nqfdk
- namespace: openshift-validation-webhook
  name: validation-webhook-97b8t
FileIntegrity:
- namespace: openshift-file-integrity
  name: osd-fileintegrity
MachineHealthCheck:
- namespace: openshift-machine-api
  name: srep-infra-healthcheck
- namespace: openshift-machine-api
  name: srep-metal-worker-healthcheck
- namespace: openshift-machine-api
  name: srep-worker-healthcheck
MachineSet:
- namespace: openshift-machine-api
  name: sbasabat-mc-qhqkn-infra-us-east-1a
- namespace: openshift-machine-api
  name: sbasabat-mc-qhqkn-worker-us-east-1a
ContainerRuntimeConfig:
- name: custom-crio
KubeletConfig:
- name: custom-kubelet
MachineConfig:
- name: 00-master-chrony
- name: 00-worker-chrony
SubjectPermission:
- namespace: openshift-rbac-permissions
  name: backplane-cee
- namespace: openshift-rbac-permissions
  name: backplane-csa
- namespace: openshift-rbac-permissions
  name: backplane-cse
- namespace: openshift-rbac-permissions
  name: backplane-csm
- namespace: openshift-rbac-permissions
  name: backplane-mobb
- namespace: openshift-rbac-permissions
  name: backplane-srep
- namespace: openshift-rbac-permissions
  name: backplane-tam
- namespace: openshift-rbac-permissions
  name: dedicated-admin-serviceaccounts
- namespace: openshift-rbac-permissions
  name: dedicated-admin-serviceaccounts-core-ns
- namespace: openshift-rbac-permissions
  name: dedicated-admins
- namespace: openshift-rbac-permissions
  name: dedicated-admins-alert-routing-edit
- namespace: openshift-rbac-permissions
  name: dedicated-admins-core-ns
- namespace: openshift-rbac-permissions
  name: dedicated-admins-customer-monitoring
- namespace: openshift-rbac-permissions
  name: osd-delete-backplane-serviceaccounts
```

VelerolInstall:

- namespace: openshift-velero
- name: cluster

PrometheusRule:

- namespace: openshift-monitoring
- name: rhmi-sre-cluster-admins
- namespace: openshift-monitoring
- name: rhoam-sre-cluster-admins
- namespace: openshift-monitoring
- name: sre-alertmanager-silences-active
- namespace: openshift-monitoring
- name: sre-alerts-stuck-builds
- namespace: openshift-monitoring
- name: sre-alerts-stuck-volumes
- namespace: openshift-monitoring
- name: sre-cloud-ingress-operator-offline-alerts
- namespace: openshift-monitoring
- name: sre-avo-pendingacceptance
- namespace: openshift-monitoring
- name: sre-configure-alertmanager-operator-offline-alerts
- namespace: openshift-monitoring
- name: sre-control-plane-resizing-alerts
- namespace: openshift-monitoring
- name: sre-dns-alerts
- namespace: openshift-monitoring
- name: sre-ebs-iops-burstbalance
- namespace: openshift-monitoring
- name: sre-elasticsearch-jobs
- namespace: openshift-monitoring
- name: sre-elasticsearch-managed-notification-alerts
- namespace: openshift-monitoring
- name: sre-excessive-memory
- namespace: openshift-monitoring
- name: sre-fr-alerts-low-disk-space
- namespace: openshift-monitoring
- name: sre-haproxy-reload-fail
- namespace: openshift-monitoring
- name: sre-internal-slo-recording-rules
- namespace: openshift-monitoring
- name: sre-kubequotaexceeded
- namespace: openshift-monitoring
- name: sre-leader-election-master-status-alerts
- namespace: openshift-monitoring
- name: sre-managed-kube-apiserver-missing-on-node
- namespace: openshift-monitoring
- name: sre-managed-kube-controller-manager-missing-on-node
- namespace: openshift-monitoring
- name: sre-managed-kube-scheduler-missing-on-node
- namespace: openshift-monitoring
- name: sre-managed-node-metadata-operator-alerts
- namespace: openshift-monitoring
- name: sre-managed-notification-alerts
- namespace: openshift-monitoring
- name: sre-managed-upgrade-operator-alerts
- namespace: openshift-monitoring
- name: sre-managed-velero-operator-alerts

- namespace: openshift-monitoring
name: sre-node-unschedulable
- namespace: openshift-monitoring
name: sre-oauth-server
- namespace: openshift-monitoring
name: sre-pending-csr-alert
- namespace: openshift-monitoring
name: sre-proxy-managed-notification-alerts
- namespace: openshift-monitoring
name: sre-pruning
- namespace: openshift-monitoring
name: sre-pv
- namespace: openshift-monitoring
name: sre-router-health
- namespace: openshift-monitoring
name: sre-runaway-sdn-preventing-container-creation
- namespace: openshift-monitoring
name: sre-slo-recording-rules
- namespace: openshift-monitoring
name: sre-telemetry-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

ManagedNotification:

- namespace: openshift-ocm-agent-operator
name: sre-elasticsearch-managed-notifications
- namespace: openshift-ocm-agent-operator
name: sre-managed-notifications
- namespace: openshift-ocm-agent-operator
name: sre-proxy-managed-notifications
- namespace: openshift-ocm-agent-operator
name: sre-upgrade-managed-notifications

OcmAgent:

- namespace: openshift-ocm-agent-operator
name: ocmagent

```

- namespace: openshift-security
  name: audit-exporter
Console:
- name: cluster
CatalogSource:
- namespace: openshift-addon-operator
  name: addon-operator-catalog
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-registry
- namespace: openshift-compliance
  name: compliance-operator-registry
- namespace: openshift-container-security
  name: container-security-operator-registry
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator-registry
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-catalog
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator-registry
- namespace: openshift-file-integrity
  name: file-integrity-operator-registry
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator-catalog
- namespace: openshift-monitoring
  name: configure-alertmanager-operator-registry
- namespace: openshift-must-gather-operator
  name: must-gather-operator-registry
- namespace: openshift-observability-operator
  name: observability-operator-catalog
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator-registry
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter-registry
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator-registry
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator-registry
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator-catalog
- namespace: openshift-velero
  name: managed-velero-operator-registry
OperatorGroup:
- namespace: openshift-addon-operator
  name: addon-operator-og
- namespace: openshift-aqua
  name: openshift-aqua
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-codeready-workspaces
  name: openshift-codeready-workspaces
- namespace: openshift-compliance
  name: compliance-operator
- namespace: openshift-container-security
  name: container-security-operator
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator

```

- namespace: openshift-customer-monitoring
name: openshift-customer-monitoring
- namespace: openshift-deployment-validation-operator
name: deployment-validation-operator-og
- namespace: openshift-managed-node-metadata-operator
name: managed-node-metadata-operator
- namespace: openshift-file-integrity
name: file-integrity-operator
- namespace: openshift-logging
name: openshift-logging
- namespace: openshift-managed-upgrade-operator
name: managed-upgrade-operator-og
- namespace: openshift-must-gather-operator
name: must-gather-operator
- namespace: openshift-observability-operator
name: observability-operator-og
- namespace: openshift-ocm-agent-operator
name: ocm-agent-operator-og
- namespace: openshift-osd-metrics
name: osd-metrics-exporter
- namespace: openshift-rbac-permissions
name: rbac-permissions-operator
- namespace: openshift-route-monitor-operator
name: route-monitor-operator
- namespace: openshift-splunk-forwarder-operator
name: splunk-forwarder-operator-og
- namespace: openshift-velero
name: managed-velero-operator

Subscription:

- namespace: openshift-addon-operator
name: addon-operator
- namespace: openshift-cloud-ingress-operator
name: cloud-ingress-operator
- namespace: openshift-compliance
name: compliance-operator-sub
- namespace: openshift-container-security
name: container-security-operator-sub
- namespace: openshift-custom-domains-operator
name: custom-domains-operator
- namespace: openshift-deployment-validation-operator
name: deployment-validation-operator
- namespace: openshift-managed-node-metadata-operator
name: managed-node-metadata-operator
- namespace: openshift-file-integrity
name: file-integrity-operator-sub
- namespace: openshift-managed-upgrade-operator
name: managed-upgrade-operator
- namespace: openshift-monitoring
name: configure-alertmanager-operator
- namespace: openshift-must-gather-operator
name: must-gather-operator
- namespace: openshift-observability-operator
name: observability-operator
- namespace: openshift-ocm-agent-operator
name: ocm-agent-operator
- namespace: openshift-osd-metrics

```

    name: osd-metrics-exporter
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator
- namespace: openshift-splunk-forwarder-operator
  name: openshift-splunk-forwarder-operator
- namespace: openshift-velero
  name: managed-velero-operator
PackageManifest:
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator
- namespace: openshift-addon-operator
  name: addon-operator
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator
- namespace: openshift-velero
  name: managed-velero-operator
- namespace: openshift-deployment-validation-operator
  name: managed-upgrade-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-container-security
  name: container-security-operator
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator
- namespace: openshift-file-integrity
  name: file-integrity-operator
- namespace: openshift-custom-domains-operator
  name: managed-node-metadata-operator
- namespace: openshift-route-monitor-operator
  name: custom-domains-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator
- namespace: openshift-observability-operator
  name: observability-operator
- namespace: openshift-monitoring
  name: configure-alertmanager-operator
- namespace: openshift-must-gather-operator
  name: deployment-validation-operator
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter
- namespace: openshift-compliance
  name: compliance-operator
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
Status:
- {}
Project:
- name: dedicated-admin

```

- name: openshift-addon-operator
- name: openshift-aqua
- name: openshift-backplane
- name: openshift-backplane-cee
- name: openshift-backplane-csa
- name: openshift-backplane-cse
- name: openshift-backplane-csm
- name: openshift-backplane-managed-scripts
- name: openshift-backplane-mobb
- name: openshift-backplane-srep
- name: openshift-backplane-tam
- name: openshift-cloud-ingress-operator
- name: openshift-codeready-workspaces
- name: openshift-compliance
- name: openshift-container-security
- name: openshift-custom-domains-operator
- name: openshift-customer-monitoring
- name: openshift-deployment-validation-operator
- name: openshift-managed-node-metadata-operator
- name: openshift-file-integrity
- name: openshift-logging
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-observability-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-scanning
- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-suricata
- name: openshift-validation-webhook
- name: openshift-velero

ClusterResourceQuota:

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

SecurityContextConstraints:

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

SplunkForwarder:

- namespace: openshift-security
- name: splunkforwarder

Group:

- name: cluster-admins
- name: dedicated-admins

User:

- name: backplane-cluster-admin

Backup:

- namespace: openshift-velero
- name: daily-full-backup-20221123112305
- namespace: openshift-velero

```

    name: daily-full-backup-20221125042537
  - namespace: openshift-velero
    name: daily-full-backup-20221126010038
  - namespace: openshift-velero
    name: daily-full-backup-20221127010039
  - namespace: openshift-velero
    name: daily-full-backup-20221128010040
  - namespace: openshift-velero
    name: daily-full-backup-20221129050847
  - namespace: openshift-velero
    name: hourly-object-backup-20221128051740
  - namespace: openshift-velero
    name: hourly-object-backup-20221128061740
  - namespace: openshift-velero
    name: hourly-object-backup-20221128071740
  - namespace: openshift-velero
    name: hourly-object-backup-20221128081740
  - namespace: openshift-velero
    name: hourly-object-backup-20221128091740
  - namespace: openshift-velero
    name: hourly-object-backup-20221129050852
  - namespace: openshift-velero
    name: hourly-object-backup-20221129051747
  - namespace: openshift-velero
    name: weekly-full-backup-20221116184315
  - namespace: openshift-velero
    name: weekly-full-backup-20221121033854
  - namespace: openshift-velero
    name: weekly-full-backup-20221128020040
Schedule:
  - namespace: openshift-velero
    name: daily-full-backup
  - namespace: openshift-velero
    name: hourly-object-backup
  - namespace: openshift-velero
    name: weekly-full-backup

```

7.9.3. OpenShift Dedicated 核心命名空间

OpenShift Dedicated 核心命名空间会在集群安装过程中安装。

例 7.2. 核心命名空间列表

```

apiVersion: v1
kind: ConfigMap
metadata:
  name: ocp-namespaces
  namespace: openshift-monitoring
data:
  managed_namespaces.yaml: |
    Resources:
      Namespace:
        - name: kube-system
        - name: openshift-apiserver

```

- name: openshift-apiserver-operator
- name: openshift-authentication
- name: openshift-authentication-operator
- name: openshift-cloud-controller-manager
- name: openshift-cloud-controller-manager-operator
- name: openshift-cloud-credential-operator
- name: openshift-cloud-network-config-controller
- name: openshift-cluster-api
- name: openshift-cluster-csi-drivers
- name: openshift-cluster-machine-approver
- name: openshift-cluster-node-tuning-operator
- name: openshift-cluster-samples-operator
- name: openshift-cluster-storage-operator
- name: openshift-config
- name: openshift-config-managed
- name: openshift-config-operator
- name: openshift-console
- name: openshift-console-operator
- name: openshift-console-user-settings
- name: openshift-controller-manager
- name: openshift-controller-manager-operator
- name: openshift-dns
- name: openshift-dns-operator
- name: openshift-etcd
- name: openshift-etcd-operator
- name: openshift-host-network
- name: openshift-image-registry
- name: openshift-ingress
- name: openshift-ingress-canary
- name: openshift-ingress-operator
- name: openshift-insights
- name: openshift-kni-infra
- name: openshift-kube-apiserver
- name: openshift-kube-apiserver-operator
- name: openshift-kube-controller-manager
- name: openshift-kube-controller-manager-operator
- name: openshift-kube-scheduler
- name: openshift-kube-scheduler-operator
- name: openshift-kube-storage-version-migrator
- name: openshift-kube-storage-version-migrator-operator
- name: openshift-machine-api
- name: openshift-machine-config-operator
- name: openshift-marketplace
- name: openshift-monitoring
- name: openshift-multus
- name: openshift-network-diagnostics
- name: openshift-network-operator
- name: openshift-nutanix-infra
- name: openshift-oauth-apiserver
- name: openshift-openstack-infra
- name: openshift-operator-lifecycle-manager
- name: openshift-operators
- name: openshift-ovirt-infra
- name: openshift-sdn
- name: openshift-ovn-kubernetes
- name: openshift-platform-operators

- name: openshift-route-controller-manager
- name: openshift-service-ca
- name: openshift-service-ca-operator
- name: openshift-user-workload-monitoring
- name: openshift-vsphere-infra

7.9.4. OpenShift Dedicated 附加组件命名空间

OpenShift Dedicated 附加组件是集群安装后可以安装的服务。这些额外服务包括 AWS CloudWatch、Red Hat OpenShift Dev Spaces、Red Hat OpenShift API Management 和 Cluster Logging Operator。以下命名空间中的资源的任何更改可能会在升级过程中被附加组件覆盖，这可能会导致附加组件功能不支持的配置。

例 7.3. 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
  rhoams: redhat-rhoam-operator
  ocs-converged: openshift-storage
  addon-operator: redhat-addon-operator
  prow-operator: prow
  cluster-logging-operator: openshift-logging
  advanced-cluster-management: redhat-open-cluster-management
  cert-manager-operator: redhat-cert-manager-operator
  dba-operator: addon-dba-operator
  reference-addon: redhat-reference-addon
  ocm-addon-test-operator: redhat-ocm-addon-test-operator
```

7.9.5. OpenShift Dedicated 验证 Webhook

OpenShift Dedicated 验证 Webhook 是由 OpenShift SRE 团队维护的一组动态准入控制。对于各种类型的请求，这些 HTTP 回调也称为 Webhook，以确保集群稳定性。Webhook 评估每个请求，并接受或拒绝它们。以下列表描述了各种带有控制注册的操作和资源的规则的 Webhook。任何尝试绕过这些验证 Webhook 都可能会影响集群的稳定性和可支持性。

例 7.4. 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": "clusterrolebindings-validation",
  "rules": [
    {
      "operations": [
        "DELETE"
      ],
      "apiGroups": [
        "rbac.authorization.k8s.io"
      ],
      "apiVersions": [
        "v1"
      ],
      "resources": [
        "clusterrolebindings"
      ],
      "scope": "Cluster"
    }
  ],
  "documentString": "Managed OpenShift Customers may not delete the cluster role bindings
under the managed namespaces: (^openshift-.*|kube-system)"
},
{
  "webhookName": "customresourcedefinitions-validation",
  "rules": [
    {
      "operations": [
        "CREATE",
        "UPDATE",
        "DELETE"
      ],
      "apiGroups": [
        "apiextensions.k8s.io"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "customresourcedefinitions"
      ],
    },
  ],

```

```

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

```

```

    "CREATE",
    "UPDATE"
  ],
  "apiGroups": [
    "operator.openshift.io"
  ],
  "apiVersions": [
    "*"
  ],
  "resources": [
    "imagecontentsourcepolicies"
  ],
  "scope": "Cluster"
}
],
"documentString": "Managed OpenShift customers may not create ImageContentSourcePolicy,
ImageDigestMirrorSet, or ImageTagMirrorSet resources that configure mirrors that would conflict
with system registries (e.g. quay.io, registry.redhat.io, registry.access.redhat.com, etc). For more
details, see https://docs.openshift.com/"
},
{
  "webhookName": "ingress-config-validation",
  "rules": [
    {
      "operations": [
        "CREATE",
        "UPDATE",
        "DELETE"
      ],
      "apiGroups": [
        "config.openshift.io"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "ingresses"
      ],
      "scope": "Cluster"
    }
  ],
  "documentString": "Managed OpenShift customers may not modify ingress config resources
because it can can degrade cluster operators and can interfere with OpenShift SRE monitoring."
},
{
  "webhookName": "ingresscontroller-validation",
  "rules": [
    {
      "operations": [
        "CREATE",
        "UPDATE"
      ],
      "apiGroups": [
        "operator.openshift.io"
      ],
      "apiVersions": [

```

```

    "resources": [
      "ingresscontroller",
      "ingresscontrollers"
    ],
    "scope": "Namespaced"
  },
  {
    "documentString": "Managed OpenShift Customer may create IngressControllers without
necessary taints. This can cause those workloads to be provisioned on infra or master nodes."
  },
  {
    "webhookName": "namespace-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          ""
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "namespaces"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift Customers may not modify namespaces specified in
the [openshift-monitoring/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": "networkpolicies-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          "networking.k8s.io"
        ],
        "apiVersions": [
          "*"
        ]
      }
    ],

```

```

    "resources": [
      "networkpolicies"
    ],
    "scope": "Namespaced"
  }
],
"documentString": "Managed OpenShift Customers may not create NetworkPolicies in namespaces managed by Red Hat."
},
{
  "webhookName": "node-validation-osd",
  "rules": [
    {
      "operations": [
        "CREATE",
        "UPDATE",
        "DELETE"
      ],
      "apiGroups": [
        ""
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "nodes",
        "nodes/*"
      ],
      "scope": "*"
    }
  ],
  "documentString": "Managed OpenShift customers may not alter Node objects."
},
{
  "webhookName": "pod-validation",
  "rules": [
    {
      "operations": [
        "*"
      ],
      "apiGroups": [
        "v1"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "pods"
      ],
      "scope": "Namespaced"
    }
  ],
  "documentString": "Managed OpenShift Customers may use tolerations on Pods that could cause those Pods to be scheduled on infra or master nodes."
},
{

```

```

"webhookName": "prometheusrule-validation",
"rules": [
  {
    "operations": [
      "CREATE",
      "UPDATE",
      "DELETE"
    ],
    "apiGroups": [
      "monitoring.coreos.com"
    ],
    "apiVersions": [
      "*"
    ],
    "resources": [
      "prometheusrules"
    ],
    "scope": "Namespaced"
  }
],
"documentString": "Managed OpenShift Customers may not create PrometheusRule in
namespaces managed by Red Hat."
},
{
  "webhookName": "regular-user-validation",
  "rules": [
    {
      "operations": [
        "*"
      ],
      "apiGroups": [
        "cloudcredential.openshift.io",
        "machine.openshift.io",
        "admissionregistration.k8s.io",
        "addons.managed.openshift.io",
        "cloudbuild.openshift.io",
        "managed.openshift.io",
        "ocmagent.managed.openshift.io",
        "splunkforwarder.managed.openshift.io",
        "upgrade.managed.openshift.io"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "*"
      ],
      "scope": "*"
    },
    {
      "operations": [
        "*"
      ],
      "apiGroups": [
        "autoscaling.openshift.io"
      ],

```

```

    "apiVersions": [
      "*"
    ],
    "resources": [
      "clusterautoscalers",
      "machineautoscalers"
    ],
    "scope": "*"
  },
  {
    "operations": [
      "*"
    ],
    "apiGroups": [
      "config.openshift.io"
    ],
    "apiVersions": [
      "*"
    ],
    "resources": [
      "clusterversions",
      "clusterversions/status",
      "schedulers",
      "apiservers",
      "proxies"
    ],
    "scope": "*"
  },
  {
    "operations": [
      "CREATE",
      "UPDATE",
      "DELETE"
    ],
    "apiGroups": [
      ""
    ],
    "apiVersions": [
      "*"
    ],
    "resources": [
      "configmaps"
    ],
    "scope": "*"
  },
  {
    "operations": [
      "*"
    ],
    "apiGroups": [
      "machineconfiguration.openshift.io"
    ],
    "apiVersions": [
      "*"
    ],
    "resources": [

```

```

        "machineconfigs",
        "machineconfigpools"
    ],
    "scope": "*"
},
{
    "operations": [
        "*"
    ],
    "apiGroups": [
        "operator.openshift.io"
    ],
    "apiVersions": [
        "*"
    ],
    "resources": [
        "kubeapiservers",
        "openshiftapiservers"
    ],
    "scope": "*"
},
{
    "operations": [
        "*"
    ],
    "apiGroups": [
        "managed.openshift.io"
    ],
    "apiVersions": [
        "*"
    ],
    "resources": [
        "subjectpermissions",
        "subjectpermissions/*"
    ],
    "scope": "*"
},
{
    "operations": [
        "*"
    ],
    "apiGroups": [
        "network.openshift.io"
    ],
    "apiVersions": [
        "*"
    ],
    "resources": [
        "netnamespaces",
        "netnamespaces/*"
    ],
    "scope": "*"
}
],
"documentString": "Managed OpenShift customers may not manage any objects in the
following APIGroups [autoscaling.openshift.io network.openshift.io machine.openshift.io

```

admissionregistration.k8s.io addons.managed.openshift.io cloudingress.managed.openshift.io splunkforwarder.managed.openshift.io upgrade.managed.openshift.io managed.openshift.io ocmagent.managed.openshift.io config.openshift.io machineconfiguration.openshift.io operator.openshift.io cloudcredential.openshift.io], nor may Managed OpenShift customers alter the APIServer, KubeAPIServer, OpenShiftAPIServer, ClusterVersion, Proxy 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 hostnetwork-v2 node-exporter nonroot nonroot-v2 privileged restricted restricted-v2]"

```
},
```

```
{
```

```
  "webhookName": "sdn-migration-validation",
```

```
  "rules": [
```

```
    {
```

```
      "operations": [
```

```
        "UPDATE"
```

```
      ],
```

```
      "apiGroups": [
```

```
        "config.openshift.io"
```

```
      ],
```

```
      "apiVersions": [
```

```
        "*"
```

```
      ],
```

```
      "resources": [
```

```
        "networks"
```

```
      ],
```

```
      "scope": "Cluster"
```

```
    }
```

```
  ],
```

"documentString": "Managed OpenShift customers may not modify the network config type because it can can degrade cluster operators and can interfere with OpenShift SRE monitoring."

```
},
```

```
{
```

```
  "webhookName": "service-mutation",
```

```
  "rules": [
```

```

{
  "operations": [
    "CREATE",
    "UPDATE"
  ],
  "apiGroups": [
    ""
  ],
  "apiVersions": [
    "v1"
  ],
  "resources": [
    "services"
  ],
  "scope": "Namespaced"
}
],
"documentString": "LoadBalancer-type services on Managed OpenShift clusters must contain
an additional annotation for managed policy compliance."
},
{
  "webhookName": "serviceaccount-validation",
  "rules": [
    {
      "operations": [
        "DELETE"
      ],
      "apiGroups": [
        ""
      ],
      "apiVersions": [
        "v1"
      ],
      "resources": [
        "serviceaccounts"
      ],
      "scope": "Namespaced"
    }
  ],
  "documentString": "Managed OpenShift Customers may not delete the service accounts under
the managed namespaces. "
},
{
  "webhookName": "techpreviewnouppgrade-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."  
}  
]
```