OpenShift Container Platform 4.3

支持

获取 OpenShift Container Platform 支持

Last Updated: 2020-09-16

OpenShift Container Platform 4.3 支持

获取 OpenShift Container Platform 支持

法律通告

摘要

本文档提供了有关从红帽获取 OpenShift Container Platform 支持的信息。文中还包含有关通过 Telemetry 和 Insights Operator 进行远程健康监控的信息。

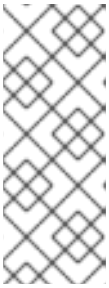
目录

第 1 章 获取支持

1.1. 获取支持

如果您在执行本文档所述的某个流程时遇到问题，请访问红帽客户门户。您可通过该客户门户：

- 搜索或浏览红帽知识库，了解有关红帽产品的技术支持文章。
- 提交问题单给红帽支持。



注意

在提交问题单的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。

  - 这类信息可使用 **oc adm must-gather** 命令来收集。
  - 唯一的集群 ID。进入 **（?） Help → Open Support Case**，在提交问题单时自动填充集群 ID。

- 访问其他产品文档。

如果您对本文档有任何改进建议，或发现了任何错误，请访问 Bugzilla，针对 **OpenShift Container Platform** 产品的 **Documentation**组件提交 Bugzilla 报告。请提供具体详情，如章节名称和 OpenShift Container Platform 版本。

第 2 章 收集集群数据

在提交问题单时，提供有关您的集群的调试信息通常有助于红帽支持为您更好地解决问题。

建议您提供：

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

2.1. 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，如：

- 资源定义
- 审计日志
- 服务日志

您在运行该命令时，可通过包含 **--image** 参数来指定一个或多个镜像。指定镜像后，该工具便会收集有关相应功能或产品的信息。

您在运行 **oc adm must-gather** 时，集群上会创建一个新 Pod。在该 Pod 上收集数据，并保存至以 **must-gather.local** 开头的一个新目录中。此目录在当前工作目录中创建。

2.2. 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。

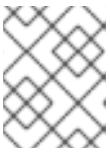
先决条件

- 使用具有 **cluster-admin** 角色的用户访问集群。
- 已安装 OpenShift Container Platform 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

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。请联络红帽支持以获取推荐收集的资源信息。

注意

如果集群使用受限网络，您必须在运行 **oc adm must-gather** 命令前导入默认的 must-gather 镜像。

```
$ oc import-image is/must-gather -n openshift
```

3. 从工作目录中刚刚创建的 **must-gather** 目录创建一个压缩文件。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.tar.gz must-gather.local.5421342344627712289/ 1
```

1 务必将 **must-gather-local.5421342344627712289/** 替换为实际目录名称。

4. 在红帽客户门户中为您的问题单附上压缩文件。

2.3. 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 Container Platform 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

- 使用具有 **cluster-admin** 角色的用户访问集群。
- 访问安装的 web 控制台或 OpenShift CLI（**oc**）。

流程

- 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 → Open Support Case**。
  b. 'Cluster ID' 的值会被自动填充 。
- 使用 web 控制台手动获取集群 ID：
  a. 导航到 **Home → Dashboards → 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}{"\n"}'
```

第 3 章 通过连接集群进行远程健康监控

3.1. 关于远程健康监控

OpenShift Container Platform 会收集有关集群健康、使用情况和集群大小的匿名聚合信息，并通过两个集成组件（Telemetry 和 Insights Operator）向红帽报告。红帽利用这些信息便可改进 OpenShift Container Platform，并更快地对影响客户的问题做出反应。这还可以简化红帽客户的订阅和授权流程，并使 Red Hat OpenShift Cluster Manager 服务能够提供有关您的集群及其健康和订阅状态的概述信息。

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)*。

3.1.1. 关于 Telemetry

Telemetry 会向红帽发送一组精选的集群监控指标子集。这些指标会持续发送并描述：

- OpenShift Container Platform 集群的大小
- OpenShift Container Platform 组件的健康和状态
- 正在进行的任何升级的健康和状态
- 有关 OpenShift Container Platform 组件和功能的有限使用情况信息
- 有关集群监控组件所报告的警报的摘要信息

红帽将使用这一持续数据流实时监控集群的健康，必要时将对影响客户的问题做出反应。同时还有助于红帽向客户推出 OpenShift Container Platform 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 Container Platform，提高其易用性。所有这些信息都不会与第三方共享。

3.1.1.1. Telemetry 收集的信息

Telemetry 收集的主要信息包括：

- 每个集群可用的更新数
- 用于更新的频道和镜像仓库
- 更新期间发生的错误数
- 正在运行的更新的进度信息
- 每个集群的机器数
- 机器的 CPU 内核数和 RAM 大小
- etcd 集群中的成员数，以及当前存储在 etcd 集群中的对象数
- 每种机器类型（infra 或 master）使用的 CPU 内核数和 RAM 大小
- 每个集群使用的 CPU 内核数和 RAM 大小
- 每个集群的 OpenShift Container Platform 框架组件的使用情况

- OpenShift Container Platform 集群的版本
- 集群上安装的任何 OpenShift Container Platform 框架组件（如 Cluster Version Operator、Cluster Monitoring、Image Registry、Elasticsearch for Logging）的健康、情况和状态。
- 安装期间生成的随机的唯一标识符
- OpenShift Container Platform 部署平台的名称，如 Amazon Web Services

Telemetry 不会收集任何身份识别的信息，如用户名、密码、用户资源的名称或地址。

3.1.2. 关于 Insights Operator

Insights Operator 会定期收集匿名配置和组件故障状态，并向红帽报告。这类信息是通过 **must-gather** 工具所收集信息的子集，方便红帽访问重要配置，以及相比 Telemetry 报告来说更深层次的故障数据。这些数据每天分多次发送，其内容包括：

- 有关集群运行环境的重要配置信息
- 有关集群及其主要组件状态的详情
- 有关报告故障的基础架构 Pod 或节点的调试信息

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 Container Platform，提高其易用性。所有这些信息都不会与第三方共享。

3.1.2.1. Insights Operator 收集的信息

Insights Operator 收集的主要信息包括：

- 集群及其组件的版本以及集群的唯一标识符
- 用于更新的频道和镜像仓库
- 有关集群组件中发生的错误的详情
- 正在运行的更新的进度和健康信息以及任何组件升级的状态
- 有关与红帽支持相关的集群配置的匿名详情
- 有关可能影响红帽支持的任何技术预览或不受支持配置的详情
- 有关 OpenShift Container Platform 部署平台（如 Amazon Web Services）以及集群所在区域的详情
- 有关已降级的 OpenShift Container Platform 集群 Operator 的 Pod 的信息
- 标记为 **NotReady** 的节点的信息
- 为 Degraded operator 列出为 "related objects" 的所有命名空间的事件

Insights Operator 不会收集任何身份识别信息，如用户名、密码、用户资源的名称或地址。

3.2. 显示远程健康监控收集的数据

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

3.2.1. 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。

先决条件

- 安装 OpenShift 命令行界面 (CLI)，通常称为 **oc**。
- 您必须作为 **cluster-admin** 角色用户登录集群。

流程

1. 找到在 OpenShift Container Platform 集群中运行的 Prometheus 服务的 URL：

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

2. 访问此 URL。
3. 在 **Expression** 中输入查询条件并点 **Execute**：

```
{__name__="up"} or {__name__="cluster_version"} or
{__name__="cluster_version_available_updates"} or {__name__="cluster_operator_up"} or
{__name__="cluster_operator_conditions"} or {__name__="cluster_version_payload"} or
{__name__="cluster_version_payload_errors"} or
{__name__="instance:etcd_object_counts:sum"} or
{__name__="ALERTS",alertstate="firing"} or
{__name__="code:apiserver_request_count:rate:sum"} or
{__name__="kube_pod_status_ready:etcd:sum"} or
{__name__="kube_pod_status_ready:image_registry:sum"} or
{__name__="cluster:capacity_cpu_cores:sum"} or
{__name__="cluster:capacity_memory_bytes:sum"} or
{__name__="cluster:cpu_usage_cores:sum"} or
{__name__="cluster:memory_usage_bytes:sum"} or
{__name__="openshift:cpu_usage_cores:sum"} or
{__name__="openshift:memory_usage_bytes:sum"} or
{__name__="cluster:node_instance_type_count:sum"}
```

此查询复制 Telemetry 对正在运行的 OpenShift Container Platform 集群的 Prometheus 服务所做的请求，并返回由 Telemetry 收集的完整时间序列集。

3.2.2. 显示 Insights Operator 收集的数据

您可以查看 Insights Operator 收集的数据。

先决条件

- 使用具有 **cluster-admin** 角色的用户访问集群。

流程

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

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

2. 复制 Insights Operator 收集的最近数据存档：

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

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

3.3. 不使用远程健康报告功能

您可能需要选择不报告集群健康和使用情况数据。例如，您可能需要遵守您所在组织报告监控数据所适用的隐私法或标准。

要选择不使用远程健康报告，您必须：

1. 修改全局集群 pull secret，以禁用远程健康报告。
2. 更新集群，以使用这个修改后的 pull secret。

3.3.1. 禁用远程健康报告的后果

客户可在 OpenShift Container Platform 中可选择不报告健康和使用情况信息。但是，红帽通过连接的集群可加快对问题的反应速度，为客户提供更好支持，同时更好地了解产品升级对集群的影响。

红帽强烈建议，即使需要在生产环境集群中禁用这个功能，在预生产环境集群和测试集群中启用健康和使用情况报告功能，。这样红帽便可在您的环境中参与对 OpenShift Container Platform 质量的审核，并对产品问题做出更快反应。

选择不使用连接的集群的一些后果包括：

- 如果没有提交问题单，红帽将无法监控产品升级是否成功，以及您的集群的健康状况。
- 红帽将无法使用匿名配置数据来更好地分类客户问题单，无法识别客户认为比较重要的配置。
- Red Hat OpenShift Cluster Manager 将无法显示您的集群数据，包括健康和使用情况信息。
- 没有自动使用情况报告功能，您必须通过 cloud.redhat.com 手动输入您的订阅授权信息。

即使在受限网络中，Telemetry 和 Insights 数据仍可通过正确配置代理来报告。

3.3.2. 修改全局集群 pull secret，以禁用远程健康报告

您可以修改现有全局集群 pull secret，以禁用远程健康报告。该操作将同时禁用 Telemetry 和 Insights Operator。

先决条件

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

流程

1. 把全局集群 pull secret 下载到本地文件系统。

```
$ oc extract secret/pull-secret -n openshift-config --to=.
```

2. 在文本编辑器中编辑所下载的 **.dockerconfigjson** 文件。
3. 删除 **cloud.openshift.com** JSON 条目，如：

```
"cloud.openshift.com":{"auth":"<hash>","email":"<email_address>"}
```

4. 保存该文件。

现在，您可以更新集群，使用修改后的 pull secret。

3.3.3. 更新全局集群 pull secret

您可为集群更新全局 pull secret。

警告

集群资源必须调整为新的 pull secret，这样可暂时限制集群的可用性。

先决条件

- 您有新的或修改的 pull secret 文件可上传。
- 您可以使用具有 **cluster-admin** 角色的用户访问集群。

流程

- 运行以下命令为您的集群更新全局 pull secret：

```
$ oc set data secret/pull-secret -n openshift-config --from-file=.dockerconfigjson=<pull-secret-location> 1
```

1 提供新 pull secret 文件的路径。

该更新将推广至所有节点，可能需要一些时间，具体取决于集群大小。在这段时间中，节点会排空 (drain)，Pod 将在剩余节点上重新调度。