OpenShift Dedicated 4

集群管理

配置 OpenShift Dedicated 集群

Last Updated: 2023-01-29

OpenShift Dedicated 4 集群管理

配置 OpenShift Dedicated 集群

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

摘要

本文档提供有关配置 OpenShift Dedicated 集群的信息。

目录

第 1 章 管理管理角色和用户 **5**
1.1. 了解管理角色 5
1.1.1. cluster-admin 角色 5
1.1.2. dedicated-admin 角色 5
1.2. 管理 OPENSHIFT DEDICATED 管理员 5
1.2.1. 添加用户 5
1.2.2. 删除用户 6

第 2 章 配置私有连接 **7**
2.1. 为 AWS 配置私有连接 7
2.1.1. 了解 AWS 云基础架构访问 7
2.1.2. 配置 AWS 基础架构访问权限 7
2.1.3. 配置 AWS VPC 对等点 9
2.1.4. 配置 AWS VPN 9
2.1.5. 配置 AWS 直接连接 10
2.2. 配置私有集群 11
2.2.1. 在集群创建过程中启用私有集群 11
2.2.2. 启用现有集群成为私有集群 12
2.2.3. 启用现有私有集群是公共的 13

第 3 章 节点 **14**
3.1. 关于机器池 14
3.1.1. Machines 14
3.1.2. 机器集 14
3.1.3. 机器池 14
3.1.4. 多个区集群中的机器池 14
3.1.5. 其他资源 14
3.2. 管理计算节点 15
3.2.1. 创建机器池 15
3.2.2. 手动扩展计算节点 17
3.2.3. 节点标签 17
3.2.3.1. 将节点标签添加到机器池 17
3.2.4. 为机器池添加污点 18
3.2.5. 其他资源 19
3.3. 关于在集群中自动扩展节点 19
3.3.1. 在集群中启用自动扩展节点 19
使用 Red Hat OpenShift Cluster Manager 在现有集群中启用自动扩展节点 19
3.3.2. 禁用集群中的自动扩展节点 20
使用 Red Hat OpenShift Cluster Manager 禁用现有集群中的自动扩展节点 20
3.3.3. 关于集群自动扩展 20
3.3.4. 其他资源 22

第 4 章 日志记录 **23**
4.1. 访问 OPENSHIFT DEDICATED 集群的服务日志 23
4.1.1. 使用 OpenShift Cluster Manager 查看服务日志 23
4.1.2. 添加集群通知联系人 23

第 5 章 监控用户定义的项目 **24**
5.1. 了解监控堆栈 24
5.1.1. 了解监控堆栈 24
5.1.1.1. 用于监控用户定义的项目的组件 24
5.1.1.2. 用户定义的项目的监控目标 25

5.1.2. 其他资源 25
5.1.3. 后续步骤 25
5.2. 访问用户定义的项目的监控 25
5.2.1. 后续步骤 25
5.3. 配置监控堆栈 25
5.3.1. 对监控的维护和支持 26
5.3.1.1. 对用户定义的项目的支持注意事项 26
5.3.2. 配置监控堆栈 26
5.3.3. 可配置的监控组件 27
5.3.4. 将监控组件移到其他节点 28
5.3.5. 为监控用户定义的项目的组件分配容限 30
5.3.6. 配置持久性存储 31
5.3.6.1. 持久性存储的先决条件 31
5.3.6.2. 配置本地持久性卷声明 31
5.3.6.3. 修改 Prometheus 指标数据的保留时间 33
5.3.7. 控制用户定义的项目中未绑定指标属性的影响 34
5.3.7.1. 为用户定义的项目设置提取示例限制 34
5.3.8. 为监控组件设置日志级别 36
5.3.9. 后续步骤 37
5.4. 为用户定义的项目启用警报路由 37
5.4.1. 了解用户定义的项目的警报路由 37
5.4.2. 为用户定义的警报路由启用一个单独的 Alertmanager 实例 38
5.4.3. 授予用户权限来为用户定义的项目配置警报路由 39
5.5. 管理指标 39
5.5.1. 了解指标 40
5.5.2. 为用户定义的项目设置指标集合 40
5.5.2.1. 部署示例服务 40
5.5.2.2. 指定如何监控服务 42
5.5.3. 查询指标 43
5.5.3.1. 以管理员身份查询所有项目的指标 43
5.5.3.2. 以开发者身份查询用户定义的项目的指标 44
5.5.3.3. 探索视觉化指标 45
5.5.4. 后续步骤 46
5.6. 警报 46
5.6.1. 在 Administrator 和 Developer 视角中访问 Alerting UI 46
5.6.2. 搜索和过滤警报、静默和警报规则 46
了解警报过滤器 46
了解静默过滤器 47
了解警报规则过滤器 47
在 Developer 视角中搜索和过滤警报、静默和警报规则 48
5.6.3. 获取关于警报、静默和警报规则的信息 48
5.6.4. 管理静默 50
5.6.4.1. 静默警报 50
5.6.4.2. 编辑静默 51
5.6.4.3. 使静默到期 52
5.6.5. 为用户定义的项目管理警报规则 52
5.6.5.1. 为用户定义的项目优化警报 53
5.6.5.2. 为用户定义的项目创建警报规则 53
5.6.5.3. 减少不查询平台指标的警报规则的延迟 54
5.6.5.4. 访问用户定义的项目的警报规则 55
5.6.5.5. 在单个视图中列出所有项目的警报规则 56
5.6.5.6. 为用户定义的项目删除警报规则 56
5.6.6. 将自定义配置应用到 Alertmanager 以进行用户定义的警报路由 57

5.6.7. 后续步骤 58
5.7. 查看监控仪表板 58
5.7.1. 以开发者身份查看监控仪表板 59
5.7.2. 后续步骤 59
5.8. 监控问题的故障排除 60
5.8.1. 确定为什么用户定义的项目指标不可用 60

第 1 章 管理管理角色和用户

1.1. 了解管理角色

1.1.1. cluster-admin 角色

作为带有客户 Cloud Subscriptions(CCS)的 OpenShift Dedicated 集群的管理员，您可以访问 **cluster-admin** 角色。创建集群的用户可以将 **cluster-admin** 用户角色添加到帐户，以获取最大管理员特权。创建集群时，这些特权不会自动分配给您的用户帐户。在登录到具有 cluster-admin 角色的帐户时，用户最多具有控制和配置集群的不受限制的访问权限。Webhook 会阻止一些配置，以防止破坏集群，或者因为它们在 OpenShift Cluster Manager 混合云 控制台中管理，且任何集群更改都会被覆盖。cluster-admin 角色的使用受到红帽附录 4 协议中列出的限制。作为最佳实践，将 **cluster-admin** 用户的数量限制为尽量少。

1.1.2. dedicated-admin 角色

作为 OpenShift Dedicated 集群的管理员，您的帐户具有对机构中集群中所有用户创建项目的额外权限和访问权限。使用 **dedicated-admin** 角色登录到帐户时，开发人员 CLI 命令（在 **oc** 命令下）可让您提高项目中对象的可见性和管理功能，而管理员 CLI 命令（在 **oc adm** 命令下）允许您完成额外的操作。

注意

虽然您的帐户具有这些权限，但实际的集群维护和主机配置仍由 OpenShift Operations 团队执行。

1.2. 管理 OPENSHIFT DEDICATED 管理员

管理员角色使用集群上的 **cluster-admin** 或 **dedicated-admin** 组来管理。此组的现有成员可以通过 OpenShift Cluster Manager 混合云控制台 编辑成员资格。

1.2.1. 添加用户

流程

1. 导航到 **Cluster Details** 页面和 **Access Control** 选项卡。
2. 点 **Add user** 按钮（仅限前用户）。
3. 输入用户名并选择组。
4. 点击 **Add** 按钮。

注意

将用户添加到 **cluster-admin** 组的过程可能需要几分钟来完成。

注意

现有的 **dedicated-admin** 用户也不能添加到 **cluster-admin** 组。您必须先将用户从 **dedicated-admin** 组中删除，然后才能将用户添加到 **cluster-admin** 组。

1.2.2. 删除用户

流程

1. 导航到 **Cluster Details** 页面和 **Access Control** 选项卡。
2. 点击用户和组组合  右侧的 Options 菜单并选择 **Delete**。

第 2 章 配置私有连接

2.1. 为 AWS 配置私有连接

2.1.1. 了解 AWS 云基础架构访问

注意

AWS 云基础架构访问权限不适用于创建集群时所选的客户 Cloud Subscription(CCS)基础架构类型，因为 CCS 集群已部署到您的帐户中。

Amazon Web Services(AWS)基础架构访问权限允许 客户门户网站 机构管理员和集群所有者启用 AWS Identity and Access Management(IAM)用户，以联合访问其 OpenShift Dedicated 集群的 AWS 管理控制台。可以为客户 AWS 用户授予 AWS 访问权限，并实施私有集群访问权限以适应 OpenShift Dedicated 环境的需求。

1. 开始为 OpenShift Dedicated 集群配置 AWS 基础架构访问权限。通过创建 AWS 用户和组，并提供该用户对 OpenShift Dedicated AWS 帐户的访问权限。
2. 访问 OpenShift Dedicated AWS 帐户后，请使用以下一个或多个方法建立集群的私有连接：
   - 配置 AWS VPC 对等点：启用 VPC 对等在两个专用 IP 地址间路由网络流量。
   - 配置 AWS VPN：建立虚拟专用网络，以安全地将您的私有网络连接到 Amazon Virtual Private Cloud。
   - 配置 AWS 直接连接：配置 AWS Direct Connect，以在您的专用网络和 AWS Direct Connect 位置之间建立专用网络连接。

配置云基础架构访问后，了解更多有关配置私有集群的信息。

2.1.2. 配置 AWS 基础架构访问权限

Amazon Web Services(AWS)基础架构访问权限允许 客户门户网站 机构管理员和集群所有者启用 AWS Identity and Access Management(IAM)用户，以联合访问其 OpenShift Dedicated 集群的 AWS 管理控制台。管理员可以在 **Network Management** 或 **只读访问** 选项之间进行选择。

先决条件

- 具有 IAM 权限的 AWS 帐户。

流程

1. 登录到您的 AWS 帐户。如果需要，您可以按照 AWS 文档 的内容来创建新的 AWS 帐户。
2. 在 AWS 帐户中使用 **STS:AllowAssumeRole** 权限创建一个 IAM 用户。
   a. 打开 AWS 管理控制台的 IAM 仪表板。
   b. 在 **Policies** 部分，点 **Create Policy**。
   c. 选择 **JSON** 标签，将现有文本替换为以下内容：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "*"
    }
  ]
}
```

d. 单击 **Next:Tags**。

e. 可选：添加标签。点 **Next:Review**

f. 提供适当的名称和描述，然后点 **Create Policy**。

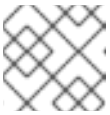
g. 在 **Users** 部分，点 **Add user**。

h. 提供一个适当的用户名。

i. 选择 **AWS Management Console 访问** 作为 AWS 访问类型。

j. 根据您的机构需要调整密码要求，然后点 **Next:Permissions**。

k. 点击 **附加现有策略直接** 选项。搜索并检查在前面的步骤中创建的策略。



注意

不建议设置权限边界。

l. 点 **Next: Tags**，然后点 **Next: Review**。确认配置正确。

m. 单击 **Create user**，会出现一个成功页面。

n. 收集 IAM 用户的 Amazon 资源名称(ARN)。ARN 将的格式如下：**arn:aws:iam::000111222333:user/username**。单击 **Close**。

3. 在浏览器中打开 OpenShift Cluster Manager Hybrid Cloud Console，然后选择您要允许 AWS 基础架构访问的集群。

4. 选择 **Access control** 选项卡，并滚动到 **AWS Infrastructure Access** 部分。

5. 粘贴 **AWS IAM ARN** 并选择 **Network Management** 或 **Read-only** 权限，然后点 **Grant 角色**。

6. 将 **AWS OSD 控制台 URL** 复制到您的剪贴板。

7. 使用您的帐户 ID 或别名、IAM 用户名和密码登录到 AWS 帐户。

8. 在新的浏览器标签页中，粘贴 AWS OSD 控制台 URL，该 URL 用于路由到 AWS Switch Role 页面。

9. 您的帐户编号和角色将被填写。如有必要，选择显示名称，然后单击 **Switch Role**。

验证

- 现在，您会看到位于 **最近访问的服务下的 VPC**。

2.1.3. 配置 AWS VPC 对等点

Virtual Private Cloud(VPC)对等连接是两个 VPC 之间的网络连接，可让您使用私有 IPv4 地址或 IPv6 地址在它们间路由流量。您可以配置 Amazon Web Services(AWS) VPC，其中包含 OpenShift Dedicated 集群与另一个 AWS VPC 网络对等。

警告

如果 VPC 安装集群被 Red Hat OpenShift Cluster Manager 对等，则无法完全删除私有集群。

AWS 支持独立于 中国的所有商业区域间的区域 VPC 同行。

先决条件

- 收集发起对等请求所需的客户 VPC 的以下信息：
  - 客户 AWS 帐号
  - 客户 VPC ID
  - 客户 VPC 区域
  - 客户 VPC CIDR
- 检查 OpenShift Dedicated Cluster VPC 使用的 CIDR 块。如果它重叠或与客户 VPC 的 CIDR 块重叠，则无法将这些两个 VPC 间的 peer 对话; 请参阅 Amazon VPC Unsupported VPC peering configuration 文档。如果 CIDR 块没有重叠，您可以继续进行操作。

流程

1. 启动 VPC 对等请求。
2. 接受 VPC 对等请求。
3. 更新 VPC 对等连接 的路由表。

其他资源

- 如需更多信息，请参阅 AWS VPC 指南。

2.1.4. 配置 AWS VPN

您可以配置 Amazon Web Services(AWS)OpenShift Dedicated 集群，使用客户的上门硬件虚拟专用网络(VPN)设备。默认情况下，您启动到 AWS Virtual Private Cloud(VPC)的实例无法与您自己的（远程）网络通信。您可以通过创建 AWS 站点到Site VPN 连接并将路由配置为通过连接传输流量，启用从 VPC 访问远程网络。

注意

AWS VPN 目前不提供将 NAT 应用到 VPN 流量的受管选项。如需了解更多详细信息，请参阅 AWS 知识库。

不支持通过私有连接路由所有流量，如 **0.0.0.0/0**。这要求删除互联网网关，这些网关禁用 SRE 管理流量。

先决条件

- 硬件 VPN 网关设备模型和软件版本，如 Cisco ASA 运行 8.3。请参阅 AWS 文档，确认 AWS 是否支持您的网关设备。
- VPN 网关设备的公共静态 IP 地址。
- BGP 或静态路由：如果 BGP，则需要 ASN。如果静态路由，必须至少配置一个静态路由。
- 可选：可访问服务的 IP 和端口/协议来测试 VPN 连接。

流程

1. 创建客户网关 来配置 VPN 连接。
2. 如果您还没有附加到预期的 VPC 的虚拟专用网关，请创建并附加 虚拟专用网关。
3. 配置路由并启用 VPN 路由传播。
4. 更新您的安全组。
5. 建立站点到Site VPN 连接。

注意

记录 VPC 子网信息，您必须作为远程网络添加到您的配置中。

其他资源

- 有关详情和故障排除帮助，请参阅 AWS VPN 指南。

2.1.5. 配置 AWS 直接连接

Amazon Web Services(AWS)Direct Connect 需要连接到 Direct Connect Gateway(DXGateway)的托管虚拟接口(VIF)，该网关与 Virtual Gateway(VGW)或 Transit Gateway 相关联，以便在同一个帐户或其他帐户中访问远程虚拟私有云(VPC)。

如果您没有现有的 DXGateway，典型的流程涉及创建托管 VIF（在 AWS 帐户中创建的 DXGateway 和 VGW）。

如果您有一个现有的 DXGateway 连接到一个或多个现有的 VGW，该过程涉及 AWS 帐户将 Association Proposal 发送到 DXGateway 所有者。DXGateway 所有者必须确保所提议的 CIDR 不会与他们关联的任何其他 VGW 冲突。

先决条件

- 确认 OpenShift Dedicated VPC 的 CIDR 范围不会与您关联的任何其他 VGW 冲突。

- 收集以下信息：
  - Direct Connect Gateway ID。
  - 与虚拟接口关联的 AWS 帐户 ID。
  - 为 DXGateway 分配 BGP ASN。可选：也可以使用 Amazon 默认 ASN。

流程

1. 创建一个 VIF 或 查看您现有的 VIFs，以确定您需要创建的直接连接类型。
2. 创建网关。
   a. 如果 Direct Connect VIF 类型为 **Private**，请创建一个虚拟专用网关。
   b. 如果 Direct Connect VIF 是 **Public**，请创建一个直接连接网关。
3. 如果您有一个要使用的现有网关，请创建一个关联提议， 并将建议发送到 DXGateway 所有者进行批准。

警告

当连接到现有的 DXGateway 时，您负责 成本。

其他资源

- 如需更多信息，请参阅 AWS 直接连接指南。

2.2. 配置私有集群

OpenShift Dedicated 集群可以被私有，以便可以在企业网络中托管内部应用程序。另外，私有集群只能配置为仅具有内部 API 端点来提高安全性。

OpenShift Dedicated 可从 **OpenShift Cluster Manager** 内选择公共和私有集群配置。可在集群创建或建立集群后配置隐私设置。

2.2.1. 在集群创建过程中启用私有集群

您可以在创建新集群时启用私有集群设置。

先决条件

- 必须将以下私有连接配置为允许私有访问：
  - VPC Peering
  - Cloud VPN
  - DirectConnect（仅限 AWS）

- TransitGateway（仅限 AWS）
- Cloud Interconnect（仅限GCP）

流程

1. 登录 OpenShift Cluster Manager 混合云控制台。
2. 点 **Create cluster** → **OpenShift Dedicated** → **Create cluster**。
3. 配置集群详情。
4. 选择您首选的网络配置时，请选择 **高级**。
5. 选择 **Private**。

警告

当设置为 **Private** 时，除非已按照先决条件中所述配置了云供应商中的私有连接，否则无法访问您的集群。

6. 点 **Create cluster**。集群创建过程开始，需要大约 30-40 分钟完成。

验证

- 在 **Overview** 标签页中的 **Installing cluster** 标题表示集群已被安装，您可以从这个标题中查看安装日志。**Details** 标题下的 **Status** 指示符表示 **集群** 何时使用。

2.2.2. 启用现有集群成为私有集群

在创建集群后，您稍后可以启用集群为私有集群。

先决条件

- 必须将以下私有连接配置为允许私有访问：
  - VPC Peering
  - Cloud VPN
  - DirectConnect（仅限 AWS）
  - TransitGateway（仅限 AWS）
  - Cloud Interconnect（仅限GCP）

流程

1. 登录 OpenShift Cluster Manager 混合云控制台。
2. 选择您要进行私有的公共集群。

3. 在 **Networking** 选项卡中，选择 **Control Plane API endpoint** 下的 **Make API private**。

> 警告
>
> 当设置为 **Private** 时，除非已按照先决条件中所述配置了云供应商中的私有连接，否则无法访问您的集群。

4. 点 **更改设置**。

> 注意
>
> 在私有和公共之间迁移集群可能需要几分钟的时间才能完成。

2.2.3. 启用现有私有集群是公共的

创建私有集群后，您可以稍后启用集群变为公共集群。

流程

1. 登录 OpenShift Cluster Manager 混合云控制台。
2. 选择您要公开的私有集群。
3. 在 **Networking** 选项卡中，取消选择 **在 Control Plane API 端点下制作 API私有**。
4. 点 **更改设置**。

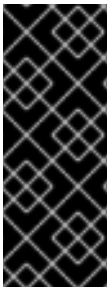
> 注意
>
> 在私有和公共之间迁移集群可能需要几分钟的时间才能完成。

第 3 章 节点

3.1. 关于机器池

OpenShift Dedicated 将机器池用作云基础架构之上的弹性动态置备方法。

主要资源有机器、机器集和机器池。



重要

自 OpenShift Dedicated 版本 4.8.35, 4.9.26, 4.10.6 开始，OpenShift Dedicated 默认每个 pod pid pid 限制为 **4096**。如果要启用这个 PID 限制，必须将 OpenShift Dedicated 集群升级到这些版本或更新版本。带有之前版本的 OpenShift Dedicated 集群使用默认 PID 限制为 **1024**。

您不能在任何 OpenShift Dedicated 集群上配置每个 pod 的 PID 限制。

3.1.1. Machines

机器是描述 worker 节点主机的基本单元。

3.1.2. 机器集

MachineSet 资源是计算机器组。如果需要更多机器或必须缩减机器，请更改计算机器设置所属的机器池中的副本数量。

3.1.3. 机器池

机器池是到计算机器集的更高级别构造。

机器池创建计算机器集，它们是跨可用区相同的配置克隆。机器池在 worker 节点上执行所有主机节点置备管理操作。如果需要更多机器或必须缩减规模，请更改机器池中的副本数量，以满足您的计算需求。您可以手动配置扩展或设置自动扩展。

默认情况下，会创建一个集群和一个机器池。您可以向现有集群添加额外的机器池，修改默认机器池，以及删除机器池。

单个集群中可以存在多个机器池，它们各自有不同的类型或不同的节点。

3.1.4. 多个区集群中的机器池

当您在多个可用区(Multi-AZ)集群中创建机器池时，一个机器池有 3 个区域。机器池依次创建一个 3 个计算机器集 - 一个用于集群中的每个区。这些计算机器集各自管理其对应可用区中的一个或多个机器。

如果您创建新的 Multi-AZ 集群，则机器池会自动复制到这些区。如果将机器池添加到现有的 Multi-AZ，则会在这些区域中自动创建新池。同样，删除机器池将从所有区域中删除它。由于这种多元效果，在多 AZ 集群中使用机器池在创建机器池时可以消耗更多项目的配额。

3.1.5. 其他资源

- 关于自动扩展

3.2. 管理计算节点

本文档论述了如何使用 OpenShift Dedicated 管理计算（也称为 worker）节点。

在机器池中配置了计算节点的大部分更改。机器池是集群中一组具有相同配置的计算节点，从而简化管理。

您可以编辑机器池配置选项，如扩展、添加节点标签和添加污点。

3.2.1. 创建机器池

安装 OpenShift Dedicated 集群时会创建一个默认机器池。安装后，您可以使用 OpenShift Cluster Manager 为集群创建额外的机器池。

重要

可用的计算（也称为 worker）节点实例类型、自动扩展选项和节点数取决于 OpenShift Dedicated 订阅、资源配额和部署场景。如需更多信息，请联系您的销售代表或红帽支持。

先决条件

- 已创建一个 OpenShift Dedicated 集群。

流程

1. 导航到 OpenShift Cluster Manager Hybrid Cloud Console 并选择您的集群。
2. 在 **Machine pool** 选项卡下，单击 **Add machine pool**。
3. 添加 **机器池名称**。
4. 从下拉菜单中选择 **Worker 节点实例类型**。实例类型定义机器池中每个计算节点的 vCPU 和内存分配。

注意

您无法在创建池后更改机器池的实例类型。

5. 可选：为机器池配置自动扩展：
   a. 选择 **Enable autoscaling** 来自动扩展机器池中的机器数量，以满足部署需求。

注意

如果您有 capabilities. **cluster.autoscale_clusters** 订阅，则 **Enable autoscaling** 选项仅适用于 OpenShift Dedicated。如需更多信息，请联系您的销售代表或红帽支持。

   b. 设置自动扩展的最小和最大节点数限值。集群自动扩展不会减少或增加机器池节点超过您指定的限制。
      - 如果您使用单一可用区部署集群，请 **设置最小和最大节点数**。这会在可用性区域中定义最小和最大计算节点限值。

- 如果您使用多个可用区部署集群，请为每个区设置 **最小节点，并为每个** 区设置 **最大节点**。这将定义每个区的最小和最大计算节点限值。

注意

另外，也可以在创建机器池后为机器池设置自动扩展首选项。

6. 如果没有启用自动扩展，请选择一个计算节点计数：

   - 如果您使用单一可用区部署集群，请从下拉菜单中选择 **Worker 节点数**。这将定义要调配到区域的机器池的计算节点数量。
   - 如果您使用多个可用区部署集群，请 **从下拉菜单中选择一个 Worker 节点数（每个区域）**。这将定义每个区域要调配到机器池的计算节点数量。

7. 可选：为机器池添加节点标签和污点：

   a. 展开 **Edit node labels 和 taints** 菜单。

   b. 在 **Node labels** 下，为节点标签添加 **Key** 和 **Value** 条目。

   c. 在 **Taints** 下，为污点添加 **Key** 和 **Value** 条目。

   d. 对于每个污点，从下拉菜单中选择一个 **Effect**。可用选项包括 **NoSchedule**、**PreferNoSchedule** 和 **NoExecute**。

注意

或者，您可以在创建机器池后添加节点标签和污点。

8. 可选： 如果您使用客户 Cloud Subscription(CCS)模型在 AWS 上部署 OpenShift Dedicated，如果使用 Amazon EC2 Spot 实例，如果您想将机器池配置为将机器部署为非保障的 AWS Spot 实例，请使用 Amazon EC2 Spot 实例：

   a. 选择 **Use Amazon EC2 Spot Instances**。

   b. 保留 **Use On-Demand 实例价格**，以使用 on-demand 实例价格。另外，选择 **Set maximum price** 来为 Spot 实例定义最大每小时价格。
   有关 Amazon EC2 Spot 实例的更多信息，请参阅 AWS 文档。

重要

您的 Amazon EC2 Spot 实例可以随时中断。将 Amazon EC2 Spot 实例用于可容许中断的工作负载。

注意

如果为机器池选择 **Use Amazon EC2 Spot 实例**，则无法在创建机器池后禁用该选项。

9. 单击 **Add machine pool** 以创建机器池。

验证

- 验证机器池在 Machine pool 页面中可见，且配置如预期。

3.2.2. 手动扩展计算节点

如果您还没有为机器池启用自动扩展，您可以手动扩展池中的计算（也称为 worker）节点数量，以满足您的部署需求。

您必须单独扩展每个机器池。

先决条件

- 已创建一个 OpenShift Dedicated 集群。
- 您有一个现有的机器池。

流程

1. 导航到 OpenShift Cluster Manager Hybrid Cloud Console 并选择您的集群。
2. 在 **Machine pool** 选项卡下，点您要扩展的机器池的选项菜单  。
3. 选择 **Scale**。
4. 指定节点数：
   - 如果使用单一可用区部署集群，请在下拉菜单中指定 **节点数**。
   - 如果您使用多个可用区部署集群，请在下拉菜单中指定 **每个区的节点数**。

   注意

   您的订阅决定了您可以选择的节点数量。
5. 单击 **Apply** 以扩展机器池。

验证

- 在 **Machine pool** 选项卡下，验证机器池的 **节点数** 是否如预期。

3.2.3. 节点标签

标签是应用于 **Node** 对象的键值对。您可以使用标签来组织对象集合，并控制 pod 调度。

您可以在集群创建或之后添加标签。可以随时修改或更新标签。

其他资源

- 如需有关标签的更多信息，请参阅 Kubernetes 标签和选择器概述。

3.2.3.1. 将节点标签添加到机器池

随时为计算（也称为 worker）节点添加或编辑标签，以与您相关的方式管理节点。例如，您可以将类型工作负载分配给特定的节点。

标签作为键值对分配。每个密钥都必须在其分配到的对象上唯一。

先决条件

- 已创建一个 OpenShift Dedicated 集群。
- 您有一个现有的机器池。

流程

1. 导航到 OpenShift Cluster Manager Hybrid Cloud Console 并选择您的集群。
2. 在 **Machine pool** 选项卡下，点您要在其中添加标签的机器池的选项菜单  。
3. 选择 **Edit labels**。
4. 如果您在要删除的机器池中已有标签，请在标签旁边选择 **x** 以删除它。
5. 使用 **<key>=<value>** 格式添加标签并按 enter 键。例如，添加 **app=db** 并按 enter 键。如果格式正确，则会突出显示键值对。
6. 如果要添加额外的标签，请重复前面的步骤。
7. 点 **Save** 将标签应用到机器池。

验证

1. 在 **Machine pool** 选项卡下，选择机器池旁边的 > 来展开视图。
2. **在展开的视图中，验证您的标签是否列在 Labels 下。**

3.2.4. 为机器池添加污点

您可以在机器池中为 compute（也称为 worker）节点添加污点，以控制哪些 pod 调度到它们。将污点应用到机器池时，调度程序无法将 pod 放置到池中，除非 pod 规格包含污点的容限。

先决条件

- **已创建一个 OpenShift Dedicated 集群。**
- **您有一个现有的机器池。**

流程

1. **导航到 OpenShift Cluster Manager Hybrid Cloud Console 并选择您的集群。**
2. **在 Machine pool 选项卡下，点您要将污点添加到的机器池的选项菜单**  **。**
3. 选择 **Edit taints**。

4. 为您的污点添加 Key 和 Value 条目。
5. 从下拉菜单中选择您的污点的 Effect。可用选项包括 NoSchedule、PreferNoSchedule 和 NoExecute。
6. 如果要向机器池添加更多污点，请选择 Add taint。
7. 点 Save 将污点应用到机器池。

验证

1. 在 Machine pool 选项卡下，选择机器池旁边的 > 来展开视图。
2. 在展开的视图中，验证您的污点是否列在 Taints 下。

3.2.5. 其他资源

- 关于机器池
- 启用自动扩展
- 禁用自动扩展
- OpenShift Dedicated 服务定义

3.3. 关于在集群中自动扩展节点

重要

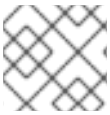
只有在通过 Red Hat Marketplace 购买的集群才可用自动扩展。

自动缩放器选项可以配置为自动扩展集群中的机器数量。

当由于资源不足而无法在任何当前节点上调度 Pod 时，或者在需要另一个节点来满足部署需求时，集群自动扩展会增加集群的大小。集群自动扩展不会将集群资源增加到超过您指定的限制。

另外，当一个相当长的时间（如资源使用率较低且所有重要 pod 都可以安置在其他节点上时），集群自动扩展会减小集群的大小。

启用自动扩展时，还必须设置 worker 节点的最小和最大数量。



注意

只有集群所有者和机构管理员才能扩展或删除集群。

3.3.1. 在集群中启用自动扩展节点

您可以通过编辑现有集群的机器池定义来在 worker 节点上启用自动扩展来增加或减少可用的节点数量。

使用 Red Hat OpenShift Cluster Manager 在现有集群中启用自动扩展节点
从 OpenShift Cluster Manager 控制台在机器池定义中启用自动扩展。

流程

1. 在 OpenShift Cluster Manager Hybrid Cloud Console 中，导航到 Clusters 页面，再选择您要启用自动扩展的集群。
2. 在所选集群中，选择 Machine pool 选项卡。
3. 点击您要为  启用自动扩展的机器池末尾的 Options 菜单，然后选择 Scale。
4. 在 Edit node count 对话框中，选择 Enable autoscaling 复选框。
5. 选择 Apply 以保存更改，并为集群启用自动扩展。

3.3.2. 禁用集群中的自动扩展节点

您可以通过编辑现有集群的机器池定义，在 worker 节点上禁用自动扩展来增加或减少可用的节点数量。

您可以使用 OpenShift Cluster Manager 控制台在集群中禁用自动扩展。

使用 Red Hat OpenShift Cluster Manager 禁用现有集群中的自动扩展节点
从 OpenShift Cluster Manager 控制台在机器池定义中禁用自动扩展。

流程

1. 在 OpenShift Cluster Manager Hybrid Cloud Console 中，导航到 Clusters 页面，再选择必须禁用自动扩展的集群。
2. 在所选集群中，选择 Machine pool 选项卡。
3. 点击带有自动扩展的机器池  末尾的 Options 菜单，然后选择 Scale。
4. 在"编辑节点数"对话框中，取消选择 启用自动扩展 复选框。
5. 选择 Apply 以保存这些更改并从集群中禁用自动扩展。

将自动扩展应用到 OpenShift Dedicated 集群涉及部署集群自动扩展，然后为集群中的每种机器类型部署机器自动扩展。

重要

您只能在 Machine API 正常工作的集群中配置集群自动扩展。

3.3.3. 关于集群自动扩展

集群自动扩展会调整 OpenShift Dedicated 集群的大小，以满足其当前的部署需求。它使用 Kubernetes 样式的声明性参数来提供基础架构管理，而且这种管理不依赖于特定云提供商的对象。集群自动控制会在集群范围内有效，不与特定的命名空间相关联。

当由于资源不足而无法在任何当前 worker 节点上调度 pod 时，或者在需要另一个节点来满足部署需求时，集群自动扩展会增加集群的大小。集群自动扩展不会将集群资源增加到超过您指定的限制。

集群自动扩展会计算所有节点上的总内存和 CPU，尽管它不管理 control plane 节点。这些值不是单计算机导向型。它们是整个集群中所有资源的聚合。例如，如果您设置最大内存资源限制，集群自动扩展在计算当前内存用量时包括集群中的所有节点。然后，该计算用于确定集群自动扩展是否具有添加更多

worker 资源的容量。

重要

确保您所创建的 ClusterAutoscaler 资源定义中的 maxNodesTotal 值足够大，足以满足计算集群中可能的机器总数。此值必须包含 control plane 机器的数量以及可扩展至的机器数量。

每隔 10 秒，集群自动扩展会检查集群中不需要哪些节点，并移除它们。如果满足以下条件，集群自动扩展会考虑要删除的节点：

- 节点使用率低于集群的节点 *利用率级别* 阈值。节点使用率级别是请求的资源的总和，由分配给节点的资源划分。如果您没有在 ClusterAutoscaler 自定义资源中指定值，集群自动扩展会使用默认值 0.5，它对应于 50% 的利用率。
- 集群自动扩展可以将节点上运行的所有 pod 移到其他节点。
- 集群自动扩展没有缩减禁用注解。

如果节点上存在以下类型的 pod，集群自动扩展不会删除该节点：

- 具有限制性 pod 中断预算（PDB）的 Pod。
- 默认不在节点上运行的 Kube 系统 Pod。
- 没有 PDB 或 PDB 限制性太强的 Kube 系统 pod。
- 不受控制器对象支持的 Pod,如部署、副本集或有状态集。
- 具有本地存储的 Pod。
- 因为缺乏资源、节点选择器或关联性不兼容或有匹配的反关联性等原因而无法移至其他位置的 Pod。
- 具有 "cluster-autoscaler.kubernetes.io/safe-to-evict": "false" 注解的 Pod，除非同时也具有 "cluster-autoscaler.kubernetes.io/safe-to-evict": "true" 注解。

例如，您可以将最大 CPU 限值设置为 64 个内核，并将集群自动扩展配置为每个创建具有 8 个内核的机器。如果您的集群从 30 个内核开始，集群自动扩展可最多添加具有 32 个内核的 4 个节点，共 62 个。

如果配置集群自动扩展，则需要额外的使用限制：

- 不要直接修改位于自动扩展节点组中的节点。同一节点组中的所有节点具有相同的容量和标签，并且运行相同的系统 Pod。
- 指定适合您的 Pod 的请求。
- 如果需要防止 Pod 被过快删除，请配置适当的 PDB。
- 确认您的云提供商配额足够大，能够支持您配置的最大节点池。
- 不要运行其他节点组自动扩展器，特别是云提供商提供的自动扩展器。

pod 横向自动扩展（HPA）和集群自动扩展以不同的方式修改集群资源。HPA 根据当前的 CPU 负载更改部署或副本集的副本数。如果负载增加，HPA 会创建新的副本，不论集群可用的资源量如何。如果没有足够的资源，集群自动扩展会添加资源，以便 HPA 创建的 pod 可以运行。如果负载减少，HPA 会停止一些副本。如果此操作导致某些节点利用率低下或完全为空，集群自动扩展会删除不必要的节点。

集群自动扩展会考虑 pod 优先级。如果集群没有足够的资源，则“Pod 优先级和抢占”功能可根据优先级调度 Pod，但集群自动扩展会确保集群具有运行所有 Pod 需要的资源。为满足这两个功能，集群自动扩展包含一个优先级截止函数。您可以使用此截止函数来调度“尽力而为”的 Pod，它们不会使集群自动扩展增加资源，而是仅在有可用备用资源时运行。

优先级低于截止值的 Pod 不会导致集群扩展或阻止集群缩减。系统不会添加新节点来运行 Pod，并且可能会删除运行这些 Pod 的节点来释放资源。

3.3.4. 其他资源

- 关于 machinepools

第 4 章 日志记录

4.1. 访问 OPENSHIFT DEDICATED 集群的服务日志

您可以使用 Red Hat OpenShift Cluster Manager 查看 OpenShift Dedicated 集群的服务日志。该服务会详细记录集群事件，如负载均衡器配额更新和调度的维护升级。日志还显示集群资源更改，如添加或删除用户、组和身份提供程序。

另外，您还可以为 OpenShift Dedicated 集群添加通知联系人。订阅的用户会收到需要客户操作、已知集群事件、升级维护和其他主题的集群事件的电子邮件。

4.1.1. 使用 OpenShift Cluster Manager 查看服务日志

您可以使用 Red Hat OpenShift Cluster Manager 查看 OpenShift Dedicated 集群的服务日志。

先决条件

- 已安装 OpenShift Dedicated 集群。

流程

1. 导航到 OpenShift Cluster Manager Hybrid Cloud Console 并选择您的集群。
2. 在集群的 Overview 页面中，在 Cluster history 部分查看服务日志。
3. 可选：从下拉菜单中选择 Description 或 Severity 来过滤集群服务日志。您可以通过在搜索栏中输入特定项来进一步过滤。
4. 可选：点击 Download history 以 JSON 或 CSV 格式下载集群的服务日志。

4.1.2. 添加集群通知联系人

您可以为 OpenShift Dedicated 集群添加通知联系人。当发生事件触发集群通知电子邮件时，订阅的用户会收到通知。

流程

1. 导航到 OpenShift Cluster Manager Hybrid Cloud Console 并选择您的集群。
2. 在 Support 选项卡中，在 通知联系人 标题下点击 Add notification contact。
3. 输入您要添加的联系人的红帽用户名或电子邮件。

注意

用户名或电子邮件地址必须与部署了集群的红帽机构的用户帐户相关。

4. 点 Add contact。

验证

- 成功添加联系后，您会看到确认消息。用户显示在 Support 选项卡上的 Notification contacts 标题下。

第 5 章 监控用户定义的项目

5.1. 了解监控堆栈

在 OpenShift Dedicated 中，您可以从红帽站点可靠性工程师(SRE)平台指标隔离来监控您自己的项目。您可以监控自己的项目，而无需额外的监控解决方案。

注意

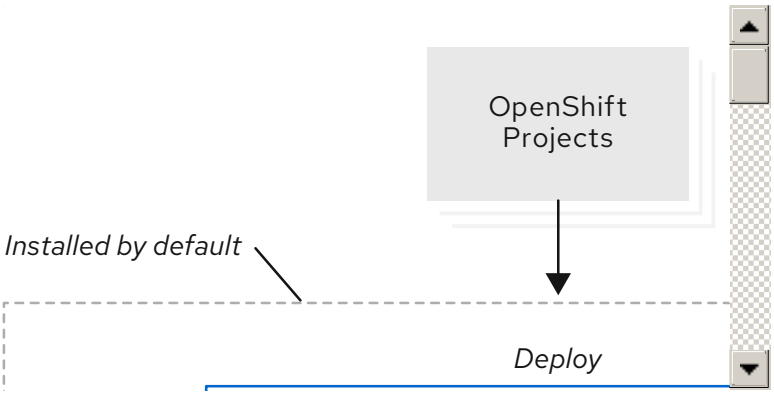
仔细阅读本文档中的说明，为监控用户定义的项目配置受支持的 Prometheus 实例。OpenShift Dedicated 不支持自定义 Prometheus 实例。

5.1.1. 了解监控堆栈

OpenShift Dedicated 监控堆栈基于 Prometheus 开源项目及其更广的生态系统。监控堆栈包括以下组件：

- **默认平台监控组件。在 OpenShift Dedicated 安装过程中，一组平台监控组件会在 openshift-monitoring 项目中安装并默认启用。这为核心集群组件提供了监控功能。默认监控堆栈还为集群启用远程健康状态监控。CPU 和内存等关键指标从每个命名空间中的所有工作负载收集，并可用于您使用。**
  下图中的默认安装部分说明了这些组件。

- **用于监控用户定义项目的组件。此功能默认为启用，并为用户定义的项目提供监控。下图中的用户部分说明了这些组件。**



5.1.1.1. 用于监控用户定义的项目的组件

OpenShift Dedicated 包括对监控堆栈的可选增强，供您用于监控用户定义的项目中的服务和 pod。此功能包括以下组件：

表 5.1. 用于监控用户定义的项目的组件

组件	描述
Prometheus Operator	**openshift-user-workload-monitoring** 项目中的 Prometheus Operator 在同一项目中创建、配置和管理 Prometheus 和 Thanos Ruler 实例。
Prometheus	Prometheus 是为用户定义的项目提供监控的监控系统。Prometheus 将警报发送到 Alertmanager 进行处理。但是，目前还不支持警报路由。

组件	描述
Thanos Ruler	Thanos Ruler 是 Prometheus 的一个规则评估引擎，作为一个独立的进程来部署。在 OpenShift Dedicated 4 中，Thanos Ruler 为监控用户定义的项目提供规则和警报评估。

所有这些组件都由堆栈监控，并在 OpenShift Dedicated 更新时自动更新。

5.1.1.2. 用户定义的项目的监控目标

OpenShift Dedicated 用户定义的项目默认启用监控。您可以监控：

- **通过用户定义的项目中的服务端点提供的指标。**
- **在用户定义的项目中运行的 Pod。**

5.1.2. 其他资源

- **访问用户定义的项目的监控**
- **默认监控组件**
- **默认监控目标**

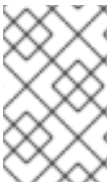
5.1.3. 后续步骤

- **访问用户定义的项目的监控**

5.2. 访问用户定义的项目的监控

安装 OpenShift Dedicated 集群时，默认启用对用户定义的项目的监控。启用对用户定义的项目的监控，您可以监控自己的 OpenShift Dedicated 项目，而无需额外的监控解决方案。

dedicated-admin 用户具有为用户定义的项目配置和访问监控的默认权限。



注意

自定义 Prometheus 实例和通过 Operator Lifecycle Manager(OLM)安装的 Prometheus Operator 可能会导致用户定义的项目监控（如果启用）出现问题。不支持自定义 Prometheus 实例。

另外，您还可以在集群安装过程中或安装后为用户定义的项目禁用监控。

5.2.1. 后续步骤

- **配置监控堆栈**

5.3. 配置监控堆栈

配置监控堆栈后，您可以查看常见配置场景并配置用户定义的项目的监控。

5.3.1. 对监控的维护和支持

配置 OpenShift Dedicated Monitoring 的支持方法是使用本文档中介绍的选项。请勿使用其他配置，因为不受支持。

重要

红帽站点可靠性工程师(SREs)不支持安装另一个 Prometheus 实例。

各个 Prometheus 发行版本的配置范例可能会发生变化，只有控制所有可能的配置时才能正常处理这样的情形。如果使用并非本节所描述的配置，您的更改可能会丢失，因为 cluster-monitoring-operator 会调节差异。根据设计，Operator 默认将一切重置到定义的状态。

5.3.1.1. 对用户定义的项目的支持注意事项

明确不支持以下修改：

- **在 OpenShift Dedicated 上安装自定义 Prometheus 实例**

5.3.2. 配置监控堆栈

在 OpenShift Dedicated 中，您可以使用 user-workload-monitoring-config ConfigMap 配置用于监控用户定义的项目工作负载的堆栈。配置配置映射配置 Cluster Monitoring Operator（CMO），CMO 会配置堆栈的组件。

先决条件

- **您可以使用具有 dedicated-admin 角色的用户访问集群。**
- **您已创建了 user-workload-monitoring-config ConfigMap 对象。**
- **已安装 OpenShift CLI（oc）。**

流程

1. **编辑 ConfigMap 对象。**
   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. **将您的配置以键值对 < component_name>: <component_configuration> 的形式添加到 data.config.yaml 下：**

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
```

```
    config.yaml: |
      <component>:
        <configuration_for_the_component>
```

相应地替换 <component> 和 <configuration_for_the_component>。

以下示例 ConfigMap 对象为 Prometheus 配置数据保留周期和最低容器资源请求。这与仅监控用户定义的项目的 Prometheus 实例相关：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    prometheus: 1
      retention: 24h 2
      resources:
        requests:
          cpu: 200m 3
          memory: 2Gi 4
```

1. 定义 Prometheus 组件，后面几行则定义其配置。
2. 为监控用户定义的项目的 Prometheus 实例配置 24 小时数据保留周期。
3. 为 Prometheus 容器定义最低 200 毫秒的资源请求。
4. 为 Prometheus 容器定义最低 2 GiB 内存的 Pod 资源请求。

2. 保存文件以将更改应用到 ConfigMap 对象。受新配置影响的 Pod 会自动重启。

警告

一旦将更改保存到监控配置映射，可能会重新部署相关项目中的 Pod 和其他资源。该项目中正在运行的监控进程也可能被重启。

5.3.3. 可配置的监控组件

下表显示了您可以配置的监控组件，以及 user-workload-monitoring-config ConfigMap 中用来指定这些组件的键：

表 5.2. 可配置的监控组件

组件	user-workload-monitoring-config 配置映射键
Prometheus Operator	prometheusOperator

组件	user-workload-monitoring-config 配置映射键
Prometheus	**prometheus**
Thanos Ruler	**thanosRuler**

5.3.4. 将监控组件移到其他节点

您可以将监控用户定义的项目工作负载的任何组件移到特定的 worker 节点。不允许将组件移到 control plane 或基础架构节点。

先决条件

- **您可以使用具有 dedicated-admin 角色的用户访问集群。**
- **您已创建了 user-workload-monitoring-config ConfigMap 对象。**
- **已安装 OpenShift CLI（oc）。**

流程

1. **要移动用于监控用户定义的项目的组件，请编辑 ConfigMap 对象：**
   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 下为组件指定 nodeSelector 约束：**

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    <component>:
      nodeSelector:
        <node_key>: <node_value>
        <node_key>: <node_value>
        <...>
```

   相应地替换 <component>，并将 <node_key>: <node_value> 替换为用于指定目标节点的键值对映射。通常只使用一个键值对。

   组件只能在以各个指定键值对作为标签的节点上运行。节点也可以有附加标签。

重要

许多监控组件都通过在集群中的不同节点间使用多个 Pod 来部署，以维持高可用性。将监控组件移到带标签的节点时，确保有足够的匹配节点来保持组件的弹性。如果只指定了一个标签，请确保有足够的节点包含该标签，以便将该组件的所有 Pod 分布到不同的节点。另外，您还可以指定多个标签，每个都与单个节点相关。

注意

如果在配置 nodeSelector 约束后监控组件仍然处于 Pending 状态，请检查 Pod 日志中与污点和容限相关的错误。

例如，要将监控用户定义的项目的组件移到带有 nodename: worker1、nodename: worker2 和 nodename: worker2 标签的特定 worker 节点，请使用：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    prometheusOperator:
      nodeSelector:
        nodename: worker1
    prometheus:
      nodeSelector:
        nodename: worker1
        nodename: worker2
    thanosRuler:
      nodeSelector:
        nodename: worker1
        nodename: worker2
```

2. 保存文件以使改变生效。受新配置影响的组件会自动移到新节点上。

警告

一旦将更改保存到监控配置映射，可能会重新部署相关项目中的 Pod 和其他资源。该项目中正在运行的监控进程也可能被重启。

其他资源

- 了解如何更新节点上的标签
- 使用节点选择器将 pod 放置到特定节点
- 参阅 Kubernetes 文档来详细了解 nodeSelector 约束

5.3.5. 为监控用户定义的项目的组件分配容限

您可以为监控用户定义的项目的组件分配容限，以便将它们移到污点 worker 节点。在 control plane 或基础架构节点上不允许调度。

先决条件

- **您可以使用具有 dedicated-admin 角色的用户访问集群。**
- **您已在 openshift-user-workload-monitoring 命名空间中创建了 user-workload-monitoring-config ConfigMap 对象。**
- **已安装 OpenShift CLI(oc)。**

流程

1. **编辑 ConfigMap 对象：**
   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. **为组件指定 tolerations：**

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    <component>:
      tolerations:
        <toleration_specification>
```

相应地替换 <component> 和 <toleration_specification>。

例如，oc adm taint nodes node1 key1=value1:NoSchedule 会将一个键为 key1 且值为 value1 的污点添加到 node1。这会防止监控组件在 node1 上部署 Pod，除非为该污点配置了容限。以下示例将 thanosRuler 组件配置为容许示例污点：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    thanosRuler:
      tolerations:
      - key: "key1"
```

```
      operator: "Equal"
      value: "value1"
      effect: "NoSchedule"
```

2. 保存文件以使改变生效。这样就会自动应用新组件放置配置。

警告

一旦将更改保存到监控配置映射，可能会重新部署相关项目中的 Pod 和其他资源。该项目中正在运行的监控进程也可能被重启。

其他资源

- 参阅 OpenShift Container Platform 文档中有关污点和容限的内容
- 参阅 Kubernetes 文档中有关污点和容限的内容

5.3.6. 配置持久性存储

如果使用持久性存储运行集群监控，您的指标将保存在持久性卷（PV）中，并可在 Pod 重新启动或重新创建后保留。如果您需要防止数据丢失的指标数据，这是理想选择。在生产环境中，强烈建议配置持久性存储。由于 IO 需求很高，使用本地存储颇有优势。

重要

请参阅 推荐的可配置存储技术。

5.3.6.1. 持久性存储的先决条件

- 使用块存储类型。

5.3.6.2. 配置本地持久性卷声明

要让监控组件使用持久性卷 (PV)，您必须配置持久性卷声明 (PVC)。

先决条件

- 您可以使用具有 dedicated-admin 角色的用户访问集群。
- 您已创建了 user-workload-monitoring-config ConfigMap 对象。
- 已安装 OpenShift CLI（oc）。

流程

1. 要为监控用户定义的项目的组件配置 PVC，编辑 ConfigMap 对象：
   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. 将组件的 PVC 配置添加到 data.config.yaml 下：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    <component>:
      volumeClaimTemplate:
        spec:
          storageClassName: <storage_class>
          resources:
            requests:
              storage: <amount_of_storage>
```

如需有关如何指定 volumeClaimTemplate 的信息，请参阅 Kubernetes 文档中与 PersistentVolumeClaim 相关的内容。

以下示例配置了一个 PVC 来为监控用户定义的项目的 Prometheus 实例声明本地持久性存储：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    prometheus:
      volumeClaimTemplate:
        spec:
          storageClassName: local-storage
          resources:
            requests:
              storage: 40Gi
```

在上例中，由 Local Storage Operator 创建的存储类称为 local-storage。

以下示例配置了一个 PVC 来声明用于 Thanos Ruler 的本地持久性存储：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    thanosRuler:
      volumeClaimTemplate:
        spec:
```

```
      storageClassName: local-storage
      resources:
        requests:
          storage: 40Gi
```

2. 保存文件以使改变生效。受新配置影响的 Pod 会自动重启，并且应用新的存储配置。

警告

一旦将更改保存到监控配置映射，可能会重新部署相关项目中的 Pod 和其他资源。该项目中正在运行的监控进程也可能被重启。

5.3.6.3. 修改 Prometheus 指标数据的保留时间

默认情况下，OpenShift Dedicated 监控堆栈将 Prometheus 数据的保留时间配置为 15 天。您可以修改监控用户定义的项目的 Prometheus 实例的保留时间，以更改数据在多久后删除的时间。

先决条件

- 您可以使用具有 dedicated-admin 角色的用户访问集群。
- 您已创建了 user-workload-monitoring-config ConfigMap 对象。
- 已安装 OpenShift CLI（oc）。

流程

1. 要修改监控用户定义的项目的 Prometheus 实例的保留时间，请编辑 ConfigMap 对象：
   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. 将保留时间配置添加到 data.config.yaml 下：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    prometheus:
      retention: <time_specification>
```

将 <time_specification> 替换为一个数字，后面紧跟 ms（毫秒）、s（秒）、m（分钟）、h（小时）、d（天）、w（周）或 y（年）。

以下示例针对监控用户定义的项目的 Prometheus 实例，将保留时间设置为 24 小时：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    prometheus:
      retention: 24h
```

2. 保存文件以使改变生效。受新配置影响的 Pod 会自动重启。

警告

一旦将更改保存到监控配置映射，可能会重新部署相关项目中的 Pod 和其他资源。该项目中正在运行的监控进程也可能被重启。

其他资源

- 了解持久性存储
- 优化存储

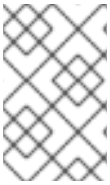
5.3.7. 控制用户定义的项目中未绑定指标属性的影响

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。

dedicated-admin 可使用以下方法控制用户定义的项目中未绑定指标属性的影响：

- 限制用户定义的项目中每个目标提取可接受的示例数量



注意

限制提取示例可帮助防止在标签中添加多个未绑定属性导致的问题。开发人员还可以通过限制其为指标定义的未绑定属性数量来防止底层原因。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。

5.3.7.1. 为用户定义的项目设置提取示例限制

您可以限制用户定义的项目中每个目标提取可接受的示例数量。

警告

如果您设置了示例限制，则在达到限制后，不会为该目标摄取更多样本数据。

先决条件

- 您可以使用具有 dedicated-admin 角色的用户访问集群。
- 您已创建了 user-workload-monitoring-config ConfigMap 对象。
- 已安装 OpenShift CLI（oc）。

流程

1. 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
```

2. 将 enforcedSampleLimit 配置添加到 data.config.yaml 中，以限制用户定义的项目中每个目标提取可接受的示例数量：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    prometheus:
      enforcedSampleLimit: 50000 1
```

1 如果指定此参数，则需要一个值。这个 enforceSampleLimit 示例将用户定义的项目中每个目标提取的示例数量限制为 50,000。

3. 保存文件以使改变生效。该限制会自动应用。

警告

将更改保存到 user-workload-monitoring-config ConfigMap 对象时，可能会重新部署 openshift-user-workload-monitoring 项目中的 Pod 和其他资源。该项目中正在运行的监控进程也可能被重启。

其他资源

- 确定为什么 Prometheus 消耗大量磁盘空间 来查询哪些指标具有最高提取示例数的步骤

5.3.8. 为监控组件设置日志级别

您可以为 Prometheus Operator、Prometheus 和 Thanos Ruler 配置日志级别。

以下日志级别可应用于 user-workload-monitoring-config ConfigMap 中的每个组件：

- debug。记录调试、信息、警告和错误消息。
- info。记录信息、警告和错误消息。
- warn。仅记录警告和错误消息。
- error。仅记录错误消息。

默认日志级别为 info。

先决条件

- 您可以使用具有 dedicated-admin 角色的用户访问集群。
- 您已创建了 user-workload-monitoring-config ConfigMap 对象。
- 已安装 OpenShift CLI（oc）。

流程

1. 编辑 ConfigMap 对象：
   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 下为组件添加 logLevel: <log_level >：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    <component>: 1
      logLevel: <log_level> 2
```

1 要将日志级别应用到的监控组件。

2 应用到组件的日志级别。

2. 保存文件以使改变生效。应用日志级别更改时，组件的 Pod 会自动重启。

警告

一旦将更改保存到监控配置映射，可能会重新部署相关项目中的 Pod 和其他资源。该项目中正在运行的监控进程也可能被重启。

3. 通过查看相关项目中的部署或 Pod 配置来确认已应用了日志级别。以下示例检查 openshift-user-workload-monitoring 项目中的 prometheus-operator 部署中的日志级别：

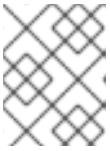
```
$ oc -n openshift-user-workload-monitoring get deploy prometheus-operator -o yaml |
grep "log-level"
```

输出示例

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

4. 检查组件的 Pod 是否正在运行。以下示例列出了 openshift-user-workload-monitoring 项目中 Pod 的状态：

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



注意

如果 ConfigMap 中包含了一个未识别的 loglevel 值，则组件的 Pod 可能无法成功重启。

5.3.9. 后续步骤

- 管理指标

5.4. 为用户定义的项目启用警报路由

在 OpenShift Dedicated 中，集群管理员可以为用户定义的项目启用警报路由。

重要

管理用户定义的项目的警报规则仅在 OpenShift Dedicated 版本 4.11 中可用。

这个过程由两个常规步骤组成：

- 为用户定义的项目启用警报路由，以使用单独的 Alertmanager 实例。
- 授予其他用户权限来为用户定义的项目配置警报路由。

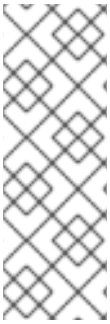
完成这些步骤后，开发人员和其他用户可以为用户定义的项目配置自定义警报和警报路由。

5.4.1. 了解用户定义的项目的警报路由

作为集群管理员，您可以为用户定义的项目启用警报路由。使用此功能，您可以允许用户使用 alert-routing-edit 角色的用户为用户定义的项目配置警报通知路由和接收器。这些通知由专用于用户定义的监控的 Alertmanager 实例路由。

然后，用户可以通过为用户定义的项目创建或编辑 AlertmanagerConfig 对象来创建和配置用户定义的警报路由，而无需管理员的帮助。

用户为用户定义的项目定义了警报路由后，用户定义的警报通知将路由到 openshift-user-workload-monitoring 命名空间中的 alertmanager-user-workload pod。



注意

以下是用户定义的项目的警报路由的限制：

- 对于用户定义的警报规则，用户定义的路由范围到定义资源的命名空间。例如，命名空间 ns1 中的路由配置仅适用于同一命名空间中的 PrometheusRules 资源。
- 当命名空间不包括在用户定义的监控中时，命名空间中的 AlertmanagerConfig 资源将成为 Alertmanager 配置的一部分。

5.4.2. 为用户定义的警报路由启用一个单独的 Alertmanager 实例

在 OpenShift Dedicated 中，您可能想要为用户定义的项目部署专用的 Alertmanager 实例，它提供与默认平台警报分开的用户定义的警报。在这些情况下，您可以选择启用一个单独的 Alertmanager 实例，以仅为用户定义的项目发送警报。

先决条件

- 您可以使用具有 cluster-admin 或 dedicated-admin 角色的用户访问集群。
- 您已为 openshift-monitoring 命名空间的 cluster-monitoring-config 配置映射中为用户定义的项目启用了监控。
- 已安装 OpenShift CLI（oc）。

流程

1. 编辑 user-workload-monitoring-config ConfigMap 对象：

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

2. 在 data/config.yaml 下，添加 alertmanager 部分的 enabled: true 和 enableAlertmanagerConfig: true ：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-workload-monitoring-config
  namespace: openshift-user-workload-monitoring
data:
  config.yaml: |
    alertmanager:
      enabled: true 1
      enableAlertmanagerConfig: true 2
```

-

1. 将 enabled 值设为 true，为集群中的用户定义的项目启用 Alertmanager 专用实例。将值设为 false 或省略键可完全为用户定义的项目禁用 Alertmanager。如果将此值设置为 false，或者如果省略了密钥，则用户定义的警报会路由到默认平台 Alertmanager 实例。

2. 将 enableAlertmanagerConfig 值设置为 true，以便用户使用 AlertmanagerConfig 对象定义自己的警报路由配置。

3. 保存文件以使改变生效。用于用户定义的项目的 Alertmanager 专用实例会自动启动。

验证

- 验证 user-workload Alertmanager 实例是否已启动：

```
# oc -n openshift-user-workload-monitoring get alertmanager
```

输出示例

```
NAME          VERSION   REPLICAS   AGE
user-workload   0.24.0    2          100s
```

5.4.3. 授予用户权限来为用户定义的项目配置警报路由

您可以授予用户权限来为用户定义的项目配置警报路由。

先决条件

- 您可以使用具有 cluster-admin 或 dedicated-admin 角色的用户访问集群。
- 要将角色分配到的用户帐户已存在。
- 已安装 OpenShift CLI（oc）。
- 您已为用户定义的项目启用了监控。

流程

- 将 alert-routing-edit 角色分配给用户定义的项目中的用户：

```
$ oc -n <namespace> adm policy add-role-to-user alert-routing-edit <user> 1
```

1. 对于 <namespace>，替换用户定义的项目的命名空间，如 ns1。对于 <user>，替换您要为其分配该角色的帐户的用户名。

其他资源

- 访问用户定义的项目的监控
- 为用户定义的项目创建警报路由

5.5. 管理指标

您可以收集指标，以监控集群组件和您自己的工作负载的表现情况。

5.5.1. 了解指标

在 OpenShift Dedicated 中，集群组件的监控方式是提取通过服务端点公开的指标。您还可以为用户定义的项目配置指标集合。借助指标，您可以监控集群组件和您自己的工作负载的表现情况。

您可以通过在应用程序级别使用 Prometheus 客户端库来定义您要为您自己的工作负载提供的指标。

在 OpenShift Dedicated 中，指标通过 /metrics 规范名称下的 HTTP 服务端点公开。您可以通过针对 http://<endpoint>/metrics 运行 curl 查询来列出服务的所有可用指标。例如，您可以向 prometheus-example-app 示例应用程序公开路由，然后运行以下命令来查看其所有可用指标：

```
$ curl http://<example_app_endpoint>/metrics
```

输出示例

```
# HELP http_requests_total Count of all HTTP requests
# TYPE http_requests_total counter
http_requests_total{code="200",method="get"} 4
http_requests_total{code="404",method="get"} 2
# HELP version Version information about this binary
# TYPE version gauge
version{version="v0.1.0"} 1
```

其他资源

- 有关 Prometheus 客户端库的详情，请参阅 Prometheus 文档。

5.5.2. 为用户定义的项目设置指标集合

您可以创建一个 ServiceMonitor 资源，从用户定义的项目中的服务端点提取指标。这假设您的应用程序使用 Prometheus 客户端库向 /metrics 规范名称公开指标。

本节介绍了如何在用户定义的项目中部署示例服务，然后创建一个 ServiceMonitor 资源来定义应该如何监控该服务。

5.5.2.1. 部署示例服务

要为用户定义的项目中服务测试监控，您可以部署示例服务。

流程

1. 为服务配置创建 YAML 文件。在本例中，该文件名为 prometheus-example-app.yaml。
2. 在该文件中添加以下部署和服务配置详情：

```
apiVersion: v1
kind: Namespace
metadata:
  name: ns1
---
apiVersion: apps/v1
kind: Deployment
```

```
  metadata:
    labels:
      app: prometheus-example-app
    name: prometheus-example-app
    namespace: ns1
  spec:
    replicas: 1
    selector:
      matchLabels:
        app: prometheus-example-app
    template:
      metadata:
        labels:
          app: prometheus-example-app
      spec:
        containers:
        - image: quay.io/brancz/prometheus-example-app:v0.2.0
          imagePullPolicy: IfNotPresent
          name: prometheus-example-app
  ---
  apiVersion: v1
  kind: Service
  metadata:
    labels:
      app: prometheus-example-app
    name: prometheus-example-app
    namespace: ns1
  spec:
    ports:
    - port: 8080
      protocol: TCP
      targetPort: 8080
      name: web
    selector:
      app: prometheus-example-app
    type: ClusterIP
```

此配置会在用户定义的 ns1 项目中部署名为 prometheus-example-app 的服务。此服务会公开自定义 version 指标。

3. 将配置应用到集群：

```
$ oc apply -f prometheus-example-app.yaml
```

部署该服务需要一些时间。

4. 您可以检查该 Pod 是否正在运行：

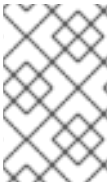
```
$ oc -n ns1 get pod
```

输出示例

```
NAME                                  READY   STATUS    RESTARTS   AGE
prometheus-example-app-7857545cb7-sbgwq   1/1     Running   0          81m
```

5.5.2.2. 指定如何监控服务

要使用服务公开的指标，必须将 OpenShift Dedicated 监控配置为从 /metrics 端点中提取指标。您可以使用一个 ServiceMonitor 自定义资源定义（CRD）应该如何监控服务，或使用一个 PodMonitor CRD 指定应该如何监控 pod。前者需要 Service 对象，而后者则不需要，允许 Prometheus 直接从 Pod 公开的指标端点中提取指标。



注意

在 OpenShift Dedicated 中，您可以使用 ServiceMonitor 资源的 tlsConfig 属性来指定在从端点提取指标时要使用的 TLS 配置。tlsConfig 属性还不可用于 PodMonitor 资源。如果需要在提取指标时使用 TLS 配置，则必须使用 ServiceMonitor。

此流程演示了如何为用户定义的项目中的服务创建 ServiceMonitor 资源。

先决条件

- **您可以使用具有 dedicated-admin 角色或 monitoring-edit 角色的用户访问集群。**
- **在本例中，您已在 ns1 项目中部署了 prometheus-example-app 示例服务。**

流程

1. **为 ServiceMonitor 资源配置创建一个 YAML 文件。在本例中，该文件名为 example-app-service-monitor.yaml。**
2. **添加以下 ServiceMonitor 资源配置详情：**

```
apiVersion: monitoring.coreos.com/v1
kind: ServiceMonitor
metadata:
  labels:
    k8s-app: prometheus-example-monitor
  name: prometheus-example-monitor
  namespace: ns1
spec:
  endpoints:
  - interval: 30s
    port: web
    scheme: http
  selector:
    matchLabels:
      app: prometheus-example-app
```

   这会定义一个 ServiceMonitor 资源，用于提取由 prometheus-example-app 示例服务公开的指标，其中包含 version 指标。

3. **将配置应用到集群：**

```
$ oc apply -f example-app-service-monitor.yaml
```

   部署 ServiceMonitor 资源需要一些时间。

4. **您可以检查 ServiceMonitor 资源是否正在运行：**

```
$ oc -n ns1 get servicemonitor
```

输出示例

```
NAME                         AGE
prometheus-example-monitor   81m
```

其他资源

- 有关 ServiceMonitor 和 PodMonitor 资源的更多信息，请参阅 Prometheus Operator API 文档。
- 访问用户定义的项目的监控。

5.5.3. 查询指标

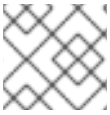
OpenShift 监控仪表板允许您运行 Prometheus Query Language(PromQL)查询来查看图表中呈现的指标。此功能提供有关集群以及您要监控的任何用户定义项目的信息。

作为 dedicated-admin，您可以在一个关于用户定义的项目的指标时查询一个或多个命名空间。

作为开发者，您必须在查询指标时指定项目名称。您必须具有所需权限才能查看所选项目的指标。

5.5.3.1. 以管理员身份查询所有项目的指标

作为具有所有项目的 view 权限的 dedicated-admin 或一个用户，您可以在 Metrics UI 中访问所有默认 OpenShift Dedicated 和用户定义的项目的指标。



注意

只有专用管理员可以访问 OpenShift Dedicated Monitoring 提供的第三方 UI。

先决条件

- 您可以使用具有 dedicated-admin 角色的用户或所有项目的查看权限访问集群。

流程

1. 从 OpenShift Web 控制台中的 Administrator 视角中，选择 Observe → Metrics。
2. 选择 Insert Metric at Cursor 来查看预定义的查询列表。
3. 要创建自定义查询，请将 Prometheus Query Language (PromQL) 查询添加到 Expression 字段。
4. 要添加多个查询，选择 Add Query。
5. 要删除查询，选择查询旁边的  ，然后选择 Delete query。
6. 要禁止运行查询，请选择查询旁边的  并选择 Disable query。

7. 选择 Run Queries 来运行您已创建的查询。图表中会直观呈现查询的指标。如果查询无效，则 UI 会显示错误消息。

注意

如果查询对大量数据进行运算，这可能会在绘制时序图时造成浏览器超时或过载。要避免这种情况，请选择 Hide graph 并且仅使用指标表来校准查询。然后，在找到可行的查询后，启用图表来绘制图形。

8. 可选：页面 URL 现在包含您运行的查询。要在以后再次使用这一组查询，请保存这个 URL。

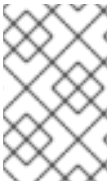
其他资源

- 有关创建 PromQL 查询的更多详情，请参阅 Prometheus query 文档。

5.5.3.2. 以开发者身份查询用户定义的项目的指标

您可以以开发者或具有项目查看权限的用户身份访问用户定义项目的指标。

在 Developer 视角中， Metrics UI 包括所选项目的一些预定义 CPU、内存、带宽和网络数据包查询。您还可以对项目的 CPU、内存、带宽、网络数据包和应用程序指标运行自定义 Prometheus Query Language (PromQL) 查询。



注意

开发者只能使用 Developer 视角，而不能使用 Administrator 视角。作为开发者，您一次只能查询一个项目的指标。开发人员无法访问 OpenShift Dedicated 监控提供的第三方 UI。

先决条件

- 对于您要查看指标的项目，您可以作为开发者或具有查看权限的用户访问集群。
- 您已为用户定义的项目启用了监控。
- 您已在用户定义的项目中部署了服务。
- 您已为该服务创建了 ServiceMonitor 自定义资源定义（CRD），以定义如何监控该服务。

流程

1. 从 OpenShift Dedicated web 控制台中的 Developer 视角，选择 Observe → Metrics。
2. 在 Project: 列表中选择您要查看指标的项目。
3. 从 Select Query 列表中选择查询，或者通过选择 Show PromQL 运行自定义 PromQL 查询。

注意

在 Developer 视角中，您一次只能运行一个查询。

其他资源

- 有关创建 PromQL 查询的更多详情，请参阅 Prometheus query 文档。

- 如需了解 以开发者或特权用户身份访问非集群指标的详情，请参阅以开发者身份查询用户定义的项目的指标

5.5.3.3. 探索视觉化指标

运行查询后，指标会显示在交互式图表中。图表中的 X 轴代表时间，Y 轴代表指标值。图形上的每个指标都以带颜色的线条显示。您可以交互式地操作图表并探索指标。

流程

在 Administrator 视角中：

1. 最初，图表中显示所有启用的查询中的所有指标。您可以要选择显示哪些指标。

注意

默认情况下，查询表会显示一个展开的视图，列出每个指标及其当前值。您可以选择 ˅ 来最小化查询的展开视图。

   - 要隐藏查询的所有指标，请点击  查询并点击 Hide all series。
   - 要隐藏特定的指标，请转至查询表，然后点击指标名称旁边带颜色的方块。
2. 要放大图表并更改时间范围，请执行以下操作之一：
   - 点击图表并在水平方向上拖动，以可视化方式选择时间范围。
   - 使用左上角的菜单来选择时间范围。
3. 要重置时间范围，请选择 Reset Zoom。
4. 要显示所有查询在特定时间点的输出，将鼠标悬停在该时间点的图表上。查询输出会出现在弹出窗口中。
5. 要隐藏图表，请选择 Hide Graph。

在 Developer 视角中：

1. 要放大图表并更改时间范围，请执行以下操作之一：
   - 点击图表并在水平方向上拖动，以可视化方式选择时间范围。
   - 使用左上角的菜单来选择时间范围。
2. 要重置时间范围，请选择 Reset Zoom。
3. 要显示所有查询在特定时间点的输出，将鼠标悬停在该时间点的图表上。查询输出会出现在弹出窗口中。

其他资源

- 请参阅有关使用 PromQL 接口的 查询指标 部分
- 监控问题的故障排除

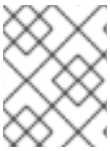
5.5.4. 后续步骤

- 警报

5.6. 警报

在 OpenShift Dedicated 中，您可以通过 Alerting UI 管理警报、静默和警报规则。

- 警报规则。警报规则包含一组概述集群中特定状态的条件。当这些条件满足时会触发警报。可为警报规则分配一个严重性来定义警报的路由方式。
- 警报。当警报规则中定义的条件为满足时会触发警报。警报提供一条通知，说明一组情况在 OpenShift Dedicated 集群中显而易见。
- 静默。可对警报应用静默，以防止在警报条件满足时发送通知。在您着手处理根本问题的同时，您可在初始通知后将警报静音。



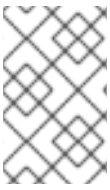
注意

Alerting UI 中可用的警报、静默和警报规则与您可访问的项目相关。例如，如果您使用 cluster-admin 或 dedicated-admin 权限登录，则可以访问所有警报、静默和警报规则。

5.6.1. 在 Administrator 和 Developer 视角中访问 Alerting UI

可通过 OpenShift Dedicated Web 控制台中的 Administrator 视角和 Developer 视角访问 Alerting UI。

- 在 Administrator 视角中，选择 Observe → Alerting。在此视角中，Alerting UI 有三个主要页面，即 Alerts、Silences 和 Alerting Rules 页面。
- 在 Developer 视角中，选择 Observe → <project_name> → Alerts。在这个视角中，警报、静默和警报规则都通过 Alerts 页面管理。Alerts 页面中显示的结果特定于所选项目。



注意

在 Developer 视角中，您可以从有权在 Project: 列表中访问的 OpenShift Dedicated 的核心项目和用户定义项目中选择。但是，如果您没有 cluster-admin 权限，则不会显示与 OpenShift Dedicated 核心项目相关的警报、静默和警报规则。

5.6.2. 搜索和过滤警报、静默和警报规则

您可以过滤 Alerting UI 中显示的警报、静默和警报规则。本节介绍每个可用的过滤选项。

了解警报过滤器

在 Administrator 视角中，Alerting UI 中的Alerts 页面针对与 OpenShift Dedicated 和用户定义的项目相关的警报提供了详细信息。该页面包括每个警报的严重性、状态和来源摘要。另外还会显示警报进入其当前状态的时间。

您可以按警报状态、严重性和来源进行过滤。默认情况下，只会显示处于 Firing 状态的 Platform 警报。下面描述了每个警报过滤选项：

- Alert State 过滤器：
  - Firing。警报正在触发，因为满足警报条件，且可选的 for 持续时间已过。只要条件一直满足，警报将继续触发。

- Pending。该警报处于活跃状态，但正在等待警报规则中指定的持续时间，然后再触发警报。
- Silenced。现在，警报在定义的时间段内处于静默状态。静默会根据您定义的一组标签选择器临时将警报静音。对于符合所有列出的值或正则表达式的警报，不会发送通知。

- Severity 过滤器：
  - Critical。触发了警报的条件可能会产生重大影响。该警报在触发时需要立即关注，并且通常会传给个人或关键响应团队。
  - Warning。该警报针对可能需要注意的事件提供警告通知，以防止问题的发生。警告通常会路由到一个问题单系统进行非即时的审阅。
  - Info。该警报仅用于提供信息。
  - None。该警报没有定义的严重性。
  - 您还可以针对与用户定义的项目相关的警报创建自定义严重性定义。

- Source 过滤器：
  - Platform。平台级别的警报仅与默认的 OpenShift Dedicated 项目相关。这些项目提供 OpenShift Dedicated 核心功能。
  - User。用户警报与用户定义的项目相关。这些警报是用户创建的，并可自定义。用户定义的工作负载监控可在安装后启用，以便您观察自己的工作负载。

了解静默过滤器
在 Administrator 视角中，Alerting UI 中的Silences 页面针对应用到 OpenShift Dedicated 和用户定义的项目中的警报的静默提供了详细信息。该页面包括每个静默的状态以及静默结束时间的摘要。

您可以按静默状态进行过滤。默认情况下，仅显示 Active 和 Pending 静默。下面描述了每个静默状态过滤器选项：

- Silence State过滤器：
  - Active。静默处于活跃状态，在静默到期前，警报将静音。
  - Pending。静默已被调度，但还没有激活。
  - Expired。静默已过期，如果满足警报条件，将发送通知。

了解警报规则过滤器
在 Administrator 视角中，Alerting UI 中的Alerting Rules 页面提供有关与 OpenShift Dedicated 和用户定义的项目相关的警报规则的详细信息。该页面包括每个警报规则的状态、严重性和来源摘要。

您可以按警报状态、严重性和来源过滤警报规则。默认情况下，只会显示 Platform 警报规则。下面描述了每个警报规则过滤选项：

- Alert State 过滤器：
  - Firing。警报正在触发，因为满足警报条件，且可选的 for 持续时间已过。只要条件一直满足，警报将继续触发。
  - Pending。该警报处于活跃状态，但正在等待警报规则中指定的持续时间，然后再触发警报。

- Silenced。现在，警报在定义的时间段内处于静默状态。静默会根据您定义的一组标签选择器临时将警报静音。对于符合所有列出的值或正则表达式的警报，不会发送通知。
- Not Firing。警报未触发。

- Severity 过滤器：
  - Critical。警报规则中定义的条件可能会产生重大影响。如果满足这些条件，需要立即关注。与该规则相关的警报通常会传给个人或关键响应团队。
  - Warning。警报规则中定义的条件可能需要注意，以防止问题的发生。与该规则相关的警报通常会路由到一个问题单系统进行非即时的审阅。
  - Info。警报规则仅提供信息警报。
  - None。该警报规则没有定义的严重性。
  - 您还可以针对与用户定义的项目相关的警报规则创建自定义严重性定义。

- Source 过滤器：
  - Platform。平台级别的警报规则仅与默认的 OpenShift Dedicated 项目相关。这些项目提供 OpenShift Dedicated 核心功能。
  - User。用户定义的工作负载警报规则与用户定义的项目相关。这些警报规则是用户创建的，并可自定义。用户定义的工作负载监控可在安装后启用，以便您观察自己的工作负载。

在 Developer 视角中搜索和过滤警报、静默和警报规则
在 Developer 视角中，Alerting UI 中的 Alerts 页面提供了与所选项目相关的警报和静默的组合视图。对于每个显示的警报，都提供了相关警报规则的链接。

在该视图中，您可以按警报状态和严重性进行过滤。默认情况下，如果您有访问所选项目的权限，则会显示项目中的所有警报。这些过滤器与针对 Administrator 视角描述的过滤器相同。

5.6.3. 获取关于警报、静默和警报规则的信息

Alerting UI 提供有关警报及其相关警报规则和静默的详细信息。

先决条件

- 对于您要查看指标的项目，您可以作为开发者或具有查看权限的用户访问集群。

流程

要在 Administrator 视角中获取有关警报的信息：

1. 打开 OpenShift Dedicated web 控制台，并浏览至 Observe → Alerting → Alerts 页面。
2. 可选：使用搜索列表中的 Name 字段按名称搜索警报。
3. 可选：通过选择 Filter 列表中的过滤器来按状态、严重性和来源过滤警报。
4. 可选：点击 Name、Severity、State 和 Source 列标题中的一个或多个标题对警报进行排序。
5. 选择警报的名称以导航到其 Alert Details 页面。该页面包含一个说明警报时间序列数据的图形。它还提供与此警报相关的信息，包括：
   - 警报的描述

- 与警报关联的消息
- 附加到警报的标签
- 其相关警报规则的链接
- 警报的静默（如果存在）

要在 Administrator 视角中获取有关静默的信息：

1. 导航到 Observe → Alerting → Silences 页面。
2. 可选：使用 Search by name 字段按名称过滤静默。
3. 可选：通过选择 Filter 列表中的过滤器来按状态过滤静默。默认情况下会应用 Active 和 Pending 过滤器。
4. 可选：点击 Name、Firing alerts 和 State 列标题中的一个或多个标题对静默进行排序。
5. 选择静默的名称以导航到其 Silence Details 页面。该页面包括以下详情：
   - 警报指定条件
   - 开始时间
   - 结束时间
   - 静默状态
   - 触发警报的数目和列表

要在 Administrator 视角中获取有关警报规则的信息：

1. 导航到 Observe → Alerting → Alerting Rules 页面。
2. 可选：通过选择 Filter 列表中的过滤器来按状态、严重性和来源过滤警报规则。
3. 可选：点击 Name、Severity、Alert State 和 Source 列标题中的一个或多个标题对警报规则进行排序。
4. 选择警报规则的名称以导航到其 Alerting Rule Details 页面。该页面提供有关警报规则的以下详情：
   - 警报规则名称、严重性和描述
   - 定义触发此警报的条件的表达式
   - 触发警报的条件得到满足的时间
   - 受警报规则约束的各个警报的图形，其中显示了触发该警报的值
   - 受警报规则约束的所有警报的列表

要在 Developer 视角中获取有关警报、静默和警报规则的信息：

1. 导航到 Observe → <project_name> → Alerts 页面。
2. 查看警报、静默或警报规则的详情：

- 要查看 Alert Details，可选择警报名称左侧的 >，然后在列表中选择警报。
- 要查看 Silence Details，可在 Alert Details 页面的 Silenced By 部分中选择静默。Silence Details 页面包括以下信息：
  - 警报指定条件
  - 开始时间
  - 结束时间
  - 静默状态
  - 触发警报的数目和列表
- 要查看 Alerting Rule Details，可在 Alerts 页面中警告右侧的 菜单中选择 View Alerting Rule。

注意

Developer 视角中仅显示与所选项目相关的警报、静默和警报规则。

5.6.4. 管理静默

您可以创建一个静默，在警报触发时停止接收有关警报的通知。在您解决根本问题的同时，在收到第一次通知后将警报置于静默状态可能很有用。

在创建静默时，您必须指定它是立即激活，还是稍后激活。您还必须设置静默在多长一段时间后到期。

您可以查看、编辑现有的静默并使其到期。

5.6.4.1. 静默警报

您可以静默特定的警报，或者静默符合您定义的指定条件的警报。

先决条件

- 您是一个集群管理员，可以使用具有 cluster-admin 集群角色的用户身份访问集群。
- 您是一个非管理员用户，可以使用具有以下用户角色的用户访问集群：
  - cluster-monitoring-view 集群角色，允许您访问 Alertmanager。
  - monitoring-alertmanager-edit 角色，允许您在 web 控制台的 Administrator 视角中创建和静默警报。
  - monitoring-rules-edit 角色，允许您在 web 控制台的 Developer 视角中创建和静默警报。

流程

静默特定的警报：

- 在 Administrator 视角中：
  1. 导航到 OpenShift Dedicated Web 控制台的 Observe → Alerting → Alerts 页面。

2. 对于您要置于静默状态的警报，请选择右列中的  并选择 Silence Alert。这时会显示 Silence Alert 表单，其中预先填充了所选警报的规格。
3. 可选：修改静默。
4. 在创建静默前您必须添加注释。
5. 若要创建静默，请选择 Silence。

- 在 Developer 视角中：
  1. 进入 OpenShift Dedicated web 控制台中的 Observe → <project_name > →Alerts 页面。
  2. 选择警报名称左侧的 > 来展开警报的详情。选择展开视图中的警报名称以打开警报的 Alert Details 页面。
  3. 选择 Silence Alert。这时会显示 Silence Alert 表单，其中预先填充了所选警报的规格。
  4. 可选：修改静默。
  5. 在创建静默前您必须添加注释。
  6. 若要创建静默，请选择 Silence。

要在 Administrator 视角中通过创建警报规格来将一组警报置于静默状态：

1. 导航到 OpenShift Dedicated web 控制台中的 Observe → Alerting → Silences 页面。
2. 选择 Create Silence。
3. 在 Create Silence 表单中设置警报的时间表、持续时间和标签详情。您还必须为静默添加注释。
4. 要为与您在上一步中输入的标签选择器匹配的警报创建静默，请选择 Silence。

5.6.4.2. 编辑静默

您可以编辑静默，这样会导致现有静默到期，并以更改后的配置创建新静默。

流程

要在 Administrator 视角中编辑静默：

1. 导航到 Observe → Alerting → Silences 页面。
2. 针对您想要修改的静默，选择最后一列中的  ，然后选择 Edit silence。
   另外，您还可以在静默的 Silence Details 页面中选择 Actions → Edit Silence。
3. 在 Edit Silence 页面中，输入您的更改并选择 Silence。这会使现有的静默到期，并以所选配置创建新静默。

要在 Developer 视角中编辑静默：

1. 导航到 Observe → <project_name> → Alerts 页面。

2. 选择警报名称左侧的 > 来展开警报的详情。选择展开视图中的警报名称以打开警报的 Alert Details 页面。
3. 在该页面的 Silenced By 部分中选择静默名称，以导航到该静默的 Silence Details 页面。
4. 选择静默的名称以导航到其 Silence Details 页面。
5. 在静默的 Silence Details 页面中选择 Actions → Edit Silence。
6. 在 Edit Silence 页面中，输入您的更改并选择 Silence。这会使现有的静默到期，并以所选配置创建新静默。

5.6.4.3. 使静默到期

您可以让静默到期。让静默到期会永久停用这一静默。

流程

在 Administrator 视角中使静默到期：

1. 导航到 Observe → Alerting → Silences 页面。
2. 针对您想要修改的静默，选择最后一列中的 ，然后选择 Expire silence。
   另外，您还可以在静默的 Silence Details 页面中选择 Actions → Expire Silence。

要在 Developer 视角中使静默到期：

1. 导航到 Observe → <project_name> → Alerts 页面。
2. 选择警报名称左侧的 > 来展开警报的详情。选择展开视图中的警报名称以打开警报的 Alert Details 页面。
3. 在该页面的 Silenced By 部分中选择静默名称，以导航到该静默的 Silence Details 页面。
4. 选择静默的名称以导航到其 Silence Details 页面。
5. 在静默的 Silence Details 页面中选择 Actions → Expire Silence。

5.6.5. 为用户定义的项目管理警报规则

OpenShift Dedicated 监控附带一组默认警报规则。作为集群管理员，您可以查看默认警报规则。

在 OpenShift Dedicated 4 中，您可以在用户定义的项目中创建、查看、编辑和删除警报规则。

重要

管理用户定义的项目的警报规则仅在 OpenShift Dedicated 版本 4.11 中可用。

警报规则注意事项

- 默认的警报规则专门用于 OpenShift Dedicated 集群。
- 有些警报规则特意使用相同的名称。它们发送关于同一事件但具有不同阈值和/或不同严重性的警报。

- 如果较低严重性警报在较高严重性警报触发的同时触发，禁止规则可防止在这种情况下发送通知。

5.6.5.1. 为用户定义的项目优化警报

要优化您自己的项目的警报，您可以在创建警报规则时考虑以下建议：

- 尽可能减少您为项目创建的警报规则数量。创建警报规则来针对会影响您的条件通知您。如果您为不会影响您的条件生成多个警报，则更难以注意到相关警报。
- 为症状而不是原因创建警报规则。创建警报规则来针对条件通知您，而无论根本原因是什么。然后可以调查原因。如果每个警报规则都只与特定原因相关，则需要更多警报规则。然后，可能会错过一些原因。
- 在编写警报规则前进行规划。确定对您很重要的症状以及一旦发生您想要采取什么操作。然后为每个症状构建警报规则。
- 提供明确的警报信息。在警报消息中说明症状和推荐操作。
- 在警报规则中包含严重性级别。警报的严重性取决于当报告的症状发生时您需要如何做出反应。例如，如果症状需要个人或关键响应团队立即关注，就应该触发关键警报。
- 优化警报路由。如果规则没有查询默认的 OpenShift Dedicated 指标，则直接在 openshift-user-workload-monitoring 项目中的 Prometheus 实例上部署警报规则。这可减少警报规则的延迟，并尽可能降低监控组件的负载。

> **警告**
>
> 用户定义的项目的默认 OpenShift Dedicated 指标提供有关 CPU 和内存用量、带宽统计和数据包速率的信息。如果您将规则直接路由到 openshift-user-workload-monitoring 项目中的 Prometheus 实例，则无法将这些指标包含在警报规则中。只有在您阅读了文档并对监控架构有了全面的了解后，才应使用警报规则优化。

其他资源

- 如需更多有关优化警报的指南，请参阅 Prometheus 警报文档
- 如需了解有关 OpenShift Dedicated 4 监控架构的详细信息，请参阅监控概述

5.6.5.2. 为用户定义的项目创建警报规则

您可以为用户定义的项目创建警报规则。这些警报规则将根据所选指标的值触发警报。

先决条件

- 您已为用户定义的项目启用了监控。
- 对于您要创建警报规则的项目，您已作为具有 monitoring-rules-edit 角色的用户登录。
- 已安装 OpenShift CLI（oc）。

流程

1. 为警报规则创建 YAML 文件。在本例中，该文件名为 **example-app-alerting-rule.yaml**。
2. 向 YAML 文件添加警报规则配置。例如：

注意

当创建警报规则时，如果在其他项目中存在具有相同名称的规则，则对其强制使用项目标签。

```
apiVersion: monitoring.coreos.com/v1
kind: PrometheusRule
metadata:
  name: example-alert
  namespace: ns1
spec:
  groups:
  - name: example
    rules:
    - alert: VersionAlert
      expr: version{job="prometheus-example-app"} == 0
```

此配置会创建一个名为 **example-alert** 的警报规则。当示例服务公开的 **version** 指标变为 **0** 时，警报规则会触发警报。

重要

用户定义的警报规则可以包含其自身项目的指标和集群指标。您不能包含其他用户定义的项目的指标。

例如，用户定义的项目 **ns1** 的警报规则可以包含来自 **ns1** 的指标和集群指标，如 CPU 和内存指标。但是，该规则无法包含来自 **ns2** 的指标。

另外，您无法为 **openshift-*** 核心 OpenShift Dedicated 项目创建警报规则。OpenShift Dedicated 监控默认为这些项目提供一组警报规则。

3. 将配置文件应用到集群：

```
$ oc apply -f example-app-alerting-rule.yaml
```

创建警报规则需要一些时间。

5.6.5.3. 减少不查询平台指标的警报规则的延迟

如果用户定义的项目的警报规则不查询默认集群指标，您可以在 **openshift-user-workload-monitoring** 项目中的 Prometheus 实例上直接部署该规则。这可绕过不需要的 Thanos Ruler，从而减少警报规则的延迟。这也有助于尽可能降低监控组件的总负载。

警告

用户定义的项目的默认 OpenShift Dedicated 指标提供有关 CPU 和内存用量、带宽统计和数据包速率的信息。如果您将规则直接部署到 openshift-user-workload-monitoring 项目中的 Prometheus 实例，则无法将这些指标包含在警报规则中。只有在您阅读了文档并对监控架构有了全面的了解后，才应使用本节中所述的流程。

先决条件

- 您已为用户定义的项目启用了监控。
- 对于您要创建警报规则的项目，您已作为具有 monitoring-rules-edit 角色的用户登录。
- 已安装 OpenShift CLI（oc）。

流程

1. 为警报规则创建 YAML 文件。在本例中，该文件名为 example-app-alerting-rule.yaml。
2. 向 YAML 文件添加警报规则配置，该文件中包含键为 openshift.io/prometheus-rule-evaluation-scope 且值为 leaf- prometheus 的标签。例如：

```
apiVersion: monitoring.coreos.com/v1
kind: PrometheusRule
metadata:
  name: example-alert
  namespace: ns1
  labels:
    openshift.io/prometheus-rule-evaluation-scope: leaf-prometheus
spec:
  groups:
  - name: example
    rules:
    - alert: VersionAlert
      expr: version{job="prometheus-example-app"} == 0
```

如果存在该标签，则会在 openshift-user-workload-monitoring 项目中的 Prometheus 实例上部署警报规则。如果不存在该标签，则会将警报规则部署到 Thanos Ruler。

1. 将配置文件应用到集群：

```
$ oc apply -f example-app-alerting-rule.yaml
```

创建警报规则需要一些时间。

- 如需了解有关 OpenShift Dedicated 4 监控架构的详细信息，请参阅监控概述。

5.6.5.4. 访问用户定义的项目的警报规则

要列出用户定义的项目的警报规则，您必须已被分配该项目的 monitoring-rules-view 角色。

先决条件

- **您已为用户定义的项目启用了监控。**
- **您已作为已被分配了项目的 monitoring-rules-view 角色的用户登录。**
- **已安装 OpenShift CLI（oc）。**

流程

1. **您可以列出 <project> 中的警报规则：**

```
$ oc -n <project> get prometheusrule
```

2. **要列出警报规则的配置，请运行以下命令：**

```
$ oc -n <project> get prometheusrule <rule> -o yaml
```

5.6.5.5. 在单个视图中列出所有项目的警报规则

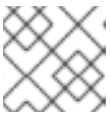
作为集群管理员，您可以在一个视图中一起列出 OpenShift Dedicated 核心项目和用户定义的项目的警报规则。

先决条件

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

流程

1. **在 Administrator 视角中，导航到 Observe → Alerting → Alerting Rules。**
2. **在 Filter 下拉菜单中选择 Platform 和 User 来源。**



注意

默认会选择 Platform 来源。

5.6.5.6. 为用户定义的项目删除警报规则

您可以为用户定义的项目删除警报规则。

先决条件

- **您已为用户定义的项目启用了监控。**
- **对于您要创建警报规则的项目，您已作为具有 monitoring-rules-edit 角色的用户登录。**
- **已安装 OpenShift CLI（oc）。**

流程

- **要删除 <namespace> 中的规则 <foo>，请运行以下命令：**

```
$ oc -n <namespace> delete prometheusrule <foo>
```

其他资源

- 请参阅 Alertmanager 文档

其他资源

- 如需了解有关 OpenShift Dedicated 监控架构的详细信息，请参阅监控概述。
- 有关警报规则的信息，请参阅 Alertmanager 文档。
- 如需有关 重新标记工作的信息，请参阅 Prometheus 重新标记文档。
- 如需更多有关优化 警报的指南，请参阅 Prometheus 警报文档。

5.6.6. 将自定义配置应用到 Alertmanager 以进行用户定义的警报路由

如果您已经启用了单独的 Alertmanager 实例，专用于用户定义的警报路由，您可以通过编辑 openshift-user-workload-monitoring 命名空间中的 alertmanager-user-workload secret 来覆盖此 Alertmanager 实例的配置。

先决条件

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

流程

1. 将当前活跃的 Alertmanager 配置输出到 alertmanager.yaml 文件：

```
$ oc -n openshift-user-workload-monitoring get secret alertmanager-user-workload --
template='{{ index .data "alertmanager.yaml" }}' | base64 --decode > alertmanager.yaml
```

2. 编辑 alertmanager.yaml 中的配置：

```
route:
  receiver: Default
  group_by:
  - name: Default
  routes:
  - matchers:
    - "service = prometheus-example-monitor" 1
    receiver: <receiver> 2
receivers:
- name: Default
- name: <receiver>
#  <receiver_configuration>
```

1 指定与路由匹配的警报。本例显示具有 service="prometheus-example-monitor" 标签的所有警报。

2 指定用于警报组的接收器。

3. 应用文件中的新配置：

```
$ oc -n openshift-user-workload-monitoring create secret generic alertmanager-user-workload --from-file=alertmanager.yaml --dry-run=client -o=yaml | oc -n openshift-user-workload-monitoring replace secret --filename=-
```

其他资源

- 参阅 PagerDuty 官方网站来进一步了解 PagerDuty。
- 参阅 PagerDuty Prometheus 集成指南来学习如何检索 service_key。
- 参阅 Alertmanager 配置来配置通过不同警报接收器发送警报。

5.6.7. 后续步骤

- 查看监控仪表板

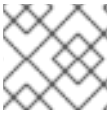
5.7. 查看监控仪表板

OpenShift Dedicated 提供了监控仪表板，可帮助您了解用户定义的项目的状态。

在 Developer 视角中，您可以访问为所选项目提供以下统计的仪表板：

- CPU 用量
- 内存用量
- 带宽信息
- 数据包速率信息

图 5.1. Developer 视角中的仪表板示例



注意

在 Developer 视角中，您一次只能查看一个项目的仪表板。

5.7.1. 以开发者身份查看监控仪表板

在 Developer 视角中，您可以查看与所选项目相关的仪表板。您必须具有监控项目的访问权限，才能查看其仪表板信息。

先决条件

- **以 dedicated-admin 身份或具有您要查看仪表板的项目查看权限的用户身份登录集群。**

流程

1. **在 OpenShift Dedicated web 控制台的 Developer 视角中，进入 Observe → Dashboard。**
2. **在 Project: 列表中选择一个项目。**
3. **在 All Workloads 列表中选择一个工作负载。**
4. **可选：在 Time Range 列表中为图形选择一个时间范围。**
5. **可选：选择一个 Refresh Interval。**
6. **将鼠标悬停在仪表板中的每个图形上，以显示具体项目的详细信息。**

5.7.2. 后续步骤

- **监控问题的故障排除**

5.8. 监控问题的故障排除

查找用户定义的项目中常见监控问题的故障排除步骤。

5.8.1. 确定为什么用户定义的项目指标不可用

如果监控用户定义的项目时没有显示指标，请按照以下步骤排除此问题。

流程

1. 查询指标名称，并验证项目是否正确：
   a. 在 OpenShift Container Platform web 控制台中的 Developer 视角中，选择 Observe → Metrics。
   b. 在 Project: 列表中选择您要查看指标的项目。
   c. 从 Select Query 列表中选择查询，或者通过选择 Show PromQL 运行自定义 PromQL 查询。
   Select Query 窗格显示指标名称。

   查询必须基于每个项目进行。显示的指标与您选择的项目相关。

2. 验证您希望指标数据的 pod 是否正在主动提供指标。对 pod 运行以下 oc exec 命令，将 podIP、端口、和 /metrics 为目标。

```
$ oc exec <sample_pod> -n <sample_namespace> -- curl <target_pod_IP>:
<port>/metrics
```

注意

您必须在安装了 curl 的 pod 上运行该命令。

以下示例显示了具有有效 version 指标的结果。

输出示例

```
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                Dload  Upload   Total   Spent    Left  Speed
# HELP version Version information about this binary-- --:--:-- --:--:--     0
# TYPE version gauge
version{version="v0.1.0"} 1
100   102  100   102    0     0  51000      0 --:--:-- --:--:-- --:--:-- 51000
```

无效的输出表示相应应用存在问题。

3. 如果使用 PodMonitor CRD，请验证 PodMonitor CRD 是否已配置为使用与标签匹配的标签指向正确的 pod。如需更多信息，请参阅 Prometheus Operator 文档。

4. 如果您使用 ServiceMonitor CRD，如果 pod 的 /metrics 端点显示指标数据，请按照以下步骤验证配置：
   a. 验证该服务是否指向正确的 /metrics 端点。此输出中的服务标签必须与服务监控标签以及后续步骤中服务定义的 /metrics 端点匹配。
   –

```
$ oc get service
```

输出示例

```
apiVersion: v1
kind: Service (1)
metadata:
  labels: (2)
    app: prometheus-example-app
  name: prometheus-example-app
  namespace: ns1
spec:
  ports:
  - port: 8080
    protocol: TCP
    targetPort: 8080
    name: web
  selector:
    app: prometheus-example-app
  type: ClusterIP
```

(1) 指定这是服务 API。

(2) 指定用于此服务的标签。

b. 查询 serviceIP、端口 和 /metrics 端点，查看您之前在 pod 上运行的curl 命令中的相同指标：

i. 运行以下命令以查找服务 IP：

```
$ oc get service -n <target_namespace>
```

ii. 查询 /metrics 端点：

```
$ oc exec <sample_pod> -n <sample_namespace> -- curl <service_IP>:
<port>/metrics
```

以下示例中返回有效的指标。

输出示例

```
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   102  100   102    0     0  51000      0 --:--:-- --:--:-- --:--:--   99k
# HELP version Version information about this binary
# TYPE version gauge
version{version="v0.1.0"} 1
```

c. 使用与匹配的标签匹配，验证 ServiceMonitor 对象是否已配置为指向所需服务。为此，请将 oc get service 输出中的 Service 对象与 oc get servicemonitor 输出中的 ServiceMonitor 对象进行比较。标签必须与才能显示的指标匹配。
例如，在前面的步骤中，注意 Service 对象如何具有 app: prometheus-example-app 标签，并且 ServiceMonitor 对象具有相同的 app: prometheus-example-app match 标签。

5. **如果一切看起来有效并且指标仍不可用，请联系支持团队以获得进一步的帮助。**