OpenShift Dedicated 4

Google Cloud 上的 OpenShift Dedicated 集群

在 Google Cloud 上安装 OpenShift Dedicated 集群

Last Updated: 2025-12-11

OpenShift Dedicated 4 Google Cloud 上的 OpenShift Dedicated 集群

在 Google Cloud 上安装 OpenShift Dedicated 集群

Legal Notice

Abstract

本文档提供有关如何在 Google Cloud 上安装 OpenShift Dedicated 集群的信息。本文档还详细介绍了如何配置集群。

Table of Contents

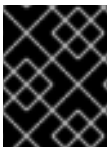
第 1 章 私有服务连接概述

您可以使用 Google Cloud 的安全增强型网络功能私有 Service Connect (PSC)在 Google Cloud 上创建私有 OpenShift Dedicated 集群。

1.1. 了解私有服务连接

私有服务连接(PSC)是 Google Cloud 网络的功能，能够跨不同项目或 Google Cloud 中的机构实现服务间的私有通信。实施 PSC 作为网络连接的一部分，可在 Google Cloud 中的私有和安全环境中部署 OpenShift Dedicated 集群，而无需任何面向公共的云资源。

有关 PSC 的更多信息，请参阅私有服务连接。



重要

PSC 仅适用于 OpenShift Dedicated 版本 4.17 及更新的版本，仅支持客户云订阅(CCS)基础架构类型。

1.2. 先决条件

除了在 Google Cloud 集群上部署任何 OpenShift Dedicated 之前需要完成的先决条件外，还必须完成以下先决条件来使用 Private Service Connect (PSC)部署私有集群：

- 在要部署集群的相同 Google Cloud 区域中使用以下子网创建的 Virtual Private Cloud (VPC)：
  - control plane 子网
  - worker 子网
  - 用于 PSC 服务附加的子网，目的设置为私有服务连接。

重要

PSC 服务附加的子网掩码必须是 /29 或更大，且必须专用于单个 OpenShift Dedicated 集群。另外，子网必须包含在置备 OpenShift Dedicated 集群时使用的 Machine CIDR 范围内。

有关如何在 Google Cloud 上创建 VPC 的详情，请参考 Google Cloud 文档中的 创建和管理 VPC 网络。

- 为 *附加资源部分* 的 *Google Cloud 防火墙先决条件中列出的* 域和端口提供从 OpenShift Dedicated 集群到互联网的路径。
- 在 Google Cloud 项目级别启用 Cloud Identity-Aware Proxy API。

除了上面列出的要求外，使用 **服务帐户** 身份验证类型配置的集群必须将 **IAP-Secured Tunnel 用户** 角色授予 **osd-ccs-admin** 服务帐户。

有关在 Google Cloud 上部署 OpenShift Dedicated 之前必须完成的先决条件的更多信息，请参阅 *客户需求*。

注意

PSC 仅支持客户云订阅(CCS)基础架构类型。要使用 PSC 在 Google Cloud 上创建 OpenShift Dedicated，*请参阅使用 Workload Identity Federation 在 Google Cloud 上创建集群*。

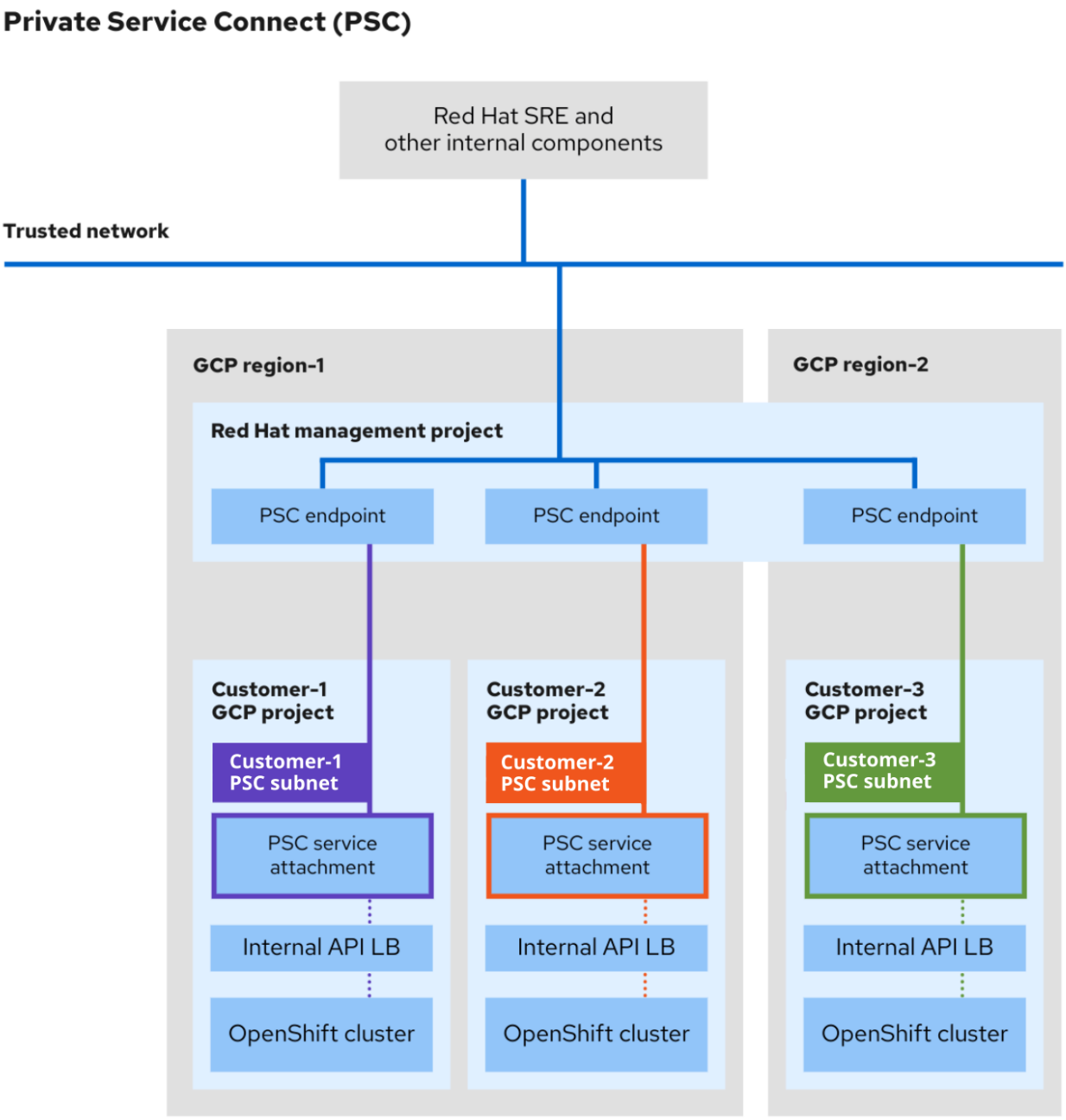
1.3. 私有服务连接架构

PSC 架构包括生成者服务和消费者服务。使用 PSC，使用者可以从其 VPC 网络内部私有访问制作者服务。同样，它允许生成者在自己的独立 VPC 网络中托管服务，并提供与其用户的专用连接。

下图显示了 Red Hat HAT SREs 和其他内部资源访问和支持使用 PSC 创建的集群的方式。

- 为客户 Google Cloud 项目中的每个 OSD 集群创建一个唯一的 PSC 服务附加。PSC 服务附加指向在客户 Google Cloud 项目中创建的集群 API 服务器负载均衡器。
- 与服务附加类似，在每个 OSD 集群的 Red Hat Management Google Cloud 项目中创建一个唯一的 PSC 端点。
- Google Cloud Private Service Connect 的专用子网在客户 Google Cloud 项目中的集群网络中创建。这是一个特殊的子网类型，其生成者服务通过 PSC 服务附加发布。此子网用于向集群 API 服务器的源 NAT (SNAT)传入请求。另外，PSC 子网必须在 Machine CIDR 范围内，且不能在多个服务附加中使用。
- 红帽内部资源和 SREs 使用 PSC 端点和服务附加之间的连接来访问私有 OSD 集群。虽然流量传输多个 VPC 网络，但它完全保留在 Google Cloud 中。
- 只有通过 Red Hat Management 项目才能访问 PSC 服务附加。

图 1.1. PSC 架构概述



1.4. 后续步骤

- 要了解更多有关 OpenShift Dedicated on Google Cloud 集群先决条件的信息，请参阅 客户需求。
- 要配置防火墙，请参阅 Google Cloud 防火墙先决条件。
- 要使用带有 Workload Identity Federation 身份验证类型的 PSC 在 Google Cloud 上创建 OpenShift Dedicated，请参阅 使用 Workload Identity Federation 身份验证在 Google Cloud 上创建集群。

第 2 章 使用 WORKLOAD IDENTITY FEDERATION 身份验证在 GOOGLE CLOUD 上创建集群

作为系统管理员或云工程师，您可以使用 Workload Identity Federation (WIF)在 Google Cloud 上置备 OpenShift Dedicated 集群。此功能建立信任关系，允许集群的 control plane 和工作负载安全假设必要的 Google Cloud 角色和访问所需的服务。这种方法消除了与管理和轮转长期 Google Cloud 服务帐户密钥相关的安全风险和操作开销。

2.1. 工作负载身份联邦概述

Workload Identity Federation (WIF)是一个 Google Cloud Identity and Access Management (IAM)功能，它为第三方提供访问客户云帐户资源的安全方法。WIF 消除了服务帐户密钥的需求，是 Google Cloud 的首选方法。

虽然服务帐户密钥可以提供对 Google Cloud 资源的强大的访问，但它们必须由用户维护，但如果它们没有正确管理，则可能会造成安全风险。WIF 不使用服务密钥作为 Google Cloud 资源的访问方法。相反，WIF 通过使用来自外部身份提供程序的凭据来为工作负载生成简短凭证来授予访问权限。然后，工作负载可以使用这些凭证来临时模拟服务帐户并访问 Google Cloud 资源。这消除了正确维护服务帐户密钥的负担，并消除未授权用户访问服务帐户密钥的风险。

以下项目提供了 Workload Identity Federation 进程的基本概述：

- Google Cloud 项目的所有者使用身份提供程序配置工作负载身份池，允许 OpenShift Dedicated 使用简短凭证访问项目的相关服务帐户。
- 此工作负载身份池配置为使用用户定义的身份提供程序(IP)验证请求。
- 要使应用程序可以访问云资源，他们首先将凭证传递给 Google 的安全令牌服务(STS)。STS 使用指定的身份提供程序来验证凭证。
- 验证凭证后，STS 会将临时访问令牌返回到调用者，使应用程序能够模拟绑定到该身份的服务帐户。

Operator 还需要访问云资源。通过使用 WIF 而不是服务帐户密钥授予这个访问权限，集群安全性会进一步增强，因为服务帐户密钥不再存储在集群中。相反，Operator 会被授予临时访问令牌来模拟服务帐户。这些令牌在短时间内有效并定期轮转。

有关 Workload Identity Federation 的更多信息，请参阅 Google Cloud 文档。

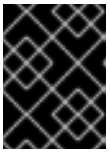
重要

工作负载 Identity Federation (WIF)仅适用于 OpenShift Dedicated 版本 4.17 及更新的版本，且仅支持客户云订阅(CCS)基础架构类型。

2.2. 先决条件

- 您已确认 Google Cloud 帐户具有必要的资源配额和限值，以便根据集群资源要求支持所需的集群大小。有关资源配额和限值的更多信息，*请参阅附加资源*。
- 您已查看了 OpenShift Dedicated 简介，以及有关 架构概念 的文档。
- 您已查看了 OpenShift Dedicated 云部署选项。
- 您已阅读并完成所需的客户流程。

- 您已从 OpenShift Cluster Manager 上的 Downloads 页面下载了 OpenShift Cluster Manager CLI (**ocm**)的最新版本。



重要

ocm 只是一个技术预览功能。有关红帽开发人员预览功能的支持范围的更多信息，请参阅 开发人员预览支持范围。

- 您已创建了 Workload Identity Federation 配置。如需更多信息，*请参阅创建工作强制身份联邦配置*。

注意

WIF 支持使用私有 Service Connect (PSC)在 Google Cloud 集群上部署私有 OpenShift Dedicated。红帽建议在部署私有集群时使用 PSC。有关 PSC 的先决条件的更多信息，请参阅 私有服务连接的先决条件。

2.3. 创建 WORKLOAD IDENTITY FEDERATION 配置

您可以在 **ocm** CLI 中使用 **auto** 模式或 **手动模式** 创建 WIF 配置。

auto 模式允许您为 OpenShift Dedicated 组件和其他 IAM 资源自动创建服务帐户。

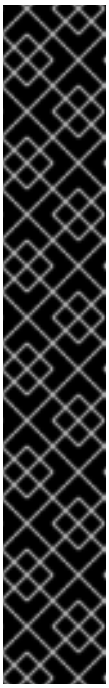
或者，您可以使用 **手动模式**。**在手动模式中**，您将获得一个 **script.sh** 文件中的命令，用于为 OpenShift Dedicated 组件和其它 IAM 资源手动创建服务帐户。

流程

- 根据您的模式首选项，运行以下命令之一来创建 WIF 配置：
  - 运行以下命令，以自动模式创建 WIF 配置：

```
$ ocm gcp create wif-config --name <wif_name> \ 1
  --project <gcp_project_id> \ 2
  --version <osd_version> 3
  --federated-project <gcp_project_id> 4
```

1. 将 **<wif_name>** 替换为 WIF 配置的名称。
2. 使用实施 WIF 配置的 Google Cloud 项目的 ID 替换。
3. 可选：**将 <osd_version> 替换为所需的 OpenShift Dedicated 版本，wif-config 需要支持。如果没有指定版本，则 wif-config 将支持最新的 OpenShift Dedicated y-stream 版本，以及最后三个支持的 OpenShift Dedicated y-stream 版本（以版本 4.17 开始）。**
4.



重要

Google Cloud 建议使用专用项目来创建和管理工作负载身份池和供应商。使用专用项目可帮助您对工作负载身份池和供应商的配置建立集中式管理，在所有项目和应用中实施统一属性映射和条件，并确保只有授权身份提供程序可以通过 WIF 进行身份验证。

仅在初始 WIF 配置创建过程中，仅在专用项目中创建和管理工作负载身份池和提供程序。--federated-project 标志无法应用到现有的 wif-configs。

如需更多信息，请参阅 使用专用项目来管理工作负载身份池和提供程序。

输出示例

```
2024/09/26 13:05:41 Creating workload identity configuration...
2024/09/26 13:05:47 Workload identity pool created with name
2e1kcps6jtgla8818vqs8tbjjls4oeub
2024/09/26 13:05:47 workload identity provider created with name oidc
2024/09/26 13:05:48 IAM service account osd-worker-oeub created
2024/09/26 13:05:49 IAM service account osd-control-plane-oeub created
2024/09/26 13:05:49 IAM service account openshift-gcp-ccm-oeub created
2024/09/26 13:05:50 IAM service account openshift-gcp-pd-csi-driv-oeub created
2024/09/26 13:05:50 IAM service account openshift-image-registry-oeub created
2024/09/26 13:05:51 IAM service account openshift-machine-api-gcp-oeub created
2024/09/26 13:05:51 IAM service account osd-deployer-oeub created
2024/09/26 13:05:52 IAM service account cloud-credential-operator-oeub created
2024/09/26 13:05:52 IAM service account openshift-cloud-network-c-oeub created
2024/09/26 13:05:53 IAM service account openshift-ingress-gcp-oeub created
2024/09/26 13:05:55 Role "osd_deployer_v4.19" updated
```

- 运行以下命令，以手动模式创建 WIF 配置：

```
$ ocm gcp create wif-config --name <wif_name> \ 1
  --project <gcp_project_id> \ 2
  --mode=manual
```

1. 将 <wif_name > 替换为 WIF 配置的名称。

2.

配置 WIF 后，将创建以下服务帐户、角色和组：

注意

Red Hat 自定义角色在每个 OpenShift y-stream 版本中进行版本，如 4.19。

表 2.1. WIF 配置服务帐户、组和角色

服务帐户/组	Google Cloud 预定义角色和红帽自定义角色
osd-deployer	osd_deployer_v<y-stream-version>
osd-control-plane	■ compute.instanceAdmin ■ compute.networkAdmin ■ compute.securityAdmin ■ compute.storageAdmin
osd-worker	■ compute.storageAdmin ■ compute.viewer
cloud-credential-operator-gcp-ro-creds	cloud_credential_operator_gcp_ro_creds_v<y-stream-version>
openshift-cloud-network-config-controller-gcp	openshift_cloud_network_config_controller_gcp_v<y-stream-version>
openshift-gcp-ccm	openshift_gcp_ccm_v<y-stream-version>
openshift-gcp-pd-csi-driver-operator	■ compute.storageAdmin ■ iam.serviceAccountUser ■ resourcemanager.tagUser ■ openshift_gcp_pd_csi_driver_operator_v<y-stream-version>

服务帐户/组	Google Cloud 预定义角色和红帽自定义角色
openshift-image-registry-gcp	openshift_image_registry_gcs_v<y-stream-version>
openshift-ingress-gcp	openshift_ingress_gcp_v<y-stream-version>
openshift-machine-api-gcp	openshift_machine_api_gcp_v<y-stream-version>
通过 SRE 组访问：sd-sre-platform-gcp-access	sre_managed_support

有关 WIF 配置角色及其分配权限的完整列表，请参阅 managed-cluster-config。

2.4. 使用 OPENSHIFT CLUSTER MANAGER 创建 WORKLOAD IDENTITY FEDERATION 集群

按照以下步骤，使用 Workload Identity Federation (WIF)在 Google Cloud 上创建 OpenShift Dedicated 集群，以通过 OpenShift Cluster Manager Web 控制台进行身份验证

先决条件

- **您已创建了 WIF 配置。如需更多信息，请参阅"创建 Workload Identity Federation 配置"。**
- **您可以访问 OpenShift Cluster Manager Web 控制台。如需更多信息，*请参阅附加资源部分中的 访问 OpenShift Cluster Manager*。**

流程

1. **登录 OpenShift Cluster Manager，再点 OpenShift Dedicated 卡上的 Create cluster。**
2. **在 Billing model 下，配置订阅类型和基础架构类型。**
   a. **选择订阅类型。如需有关 OpenShift Dedicated 订阅选项的信息，请参阅 OpenShift Cluster Manager 文档中的集群订阅和注册。**

b. 选择 **Customer cloud subscription infrastructure type**。

c. **点击 Next。**

3. 选择 **Run on Google Cloud**。

4. 选择 **Workload Identity Federation 作为 Authentication 类型。**

注意

工作负载 Identity Federation (WIF)是 Google Cloud 的建议 OpenShift Dedicated 安装身份验证方法。它通过利用简短的、最低特权凭证，消除对静态服务帐户密钥的需求，从而大大提高了集群的弹性。

a. **读取并完成所有必要的先决条件。**

b. **点击指示您读取并完成所有必要的先决条件的复选框。**

5. **从 WIF 配置下拉列表中选择一个配置的 WIF 配置。**

6. **点 Next。**

7. **在 Details 页面中，为集群提供一个名称并指定集群详情：**

a. **在 Cluster name 字段中输入集群名称。**

b. **可选：集群创建生成域前缀，作为 openshiftapps.com 上置备的集群的子域。如果集群名称小于或等于 15 个字符，则该名称用于域前缀。如果集群名称超过 15 个字符，则域前缀会随机生成为 15 个字符的字符串。**

要自定义子域前缀，请选中 Create custom domain prefix 复选框，然后在 Domain prefix 字段中输入您的域前缀名称。域前缀不能超过 15 个字符，在您的机构中必须是唯一的，且在集群创建后无法更改。

c. 从 Version 下拉菜单中选择集群版本。

注意

Workload Identity Federation (WIF)只在 OpenShift Dedicated 版本 4.17 及更新的版本中被支持。

d. 从 Channel 组 下拉菜单中选择频道组。

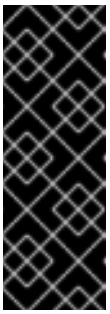
注意

频道组选项包括 Stable （默认选项）和 EUS。有关 Stable 和 EUS 频道组选项的更多信息，请参阅了解更新频道和发行版本。

e. 从 Region 下拉菜单中选择云供应商区域。

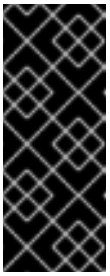
f. 选择 Single zone 或 Multi-zone 配置。

g. 可选： 选择 Enable Secure Boot support for Shielded VMs to use Shielded VMs when installation cluster。创建集群时，无法更改 对 Shielded VM 设置的启用安全引导支持。如需更多信息，请参阅 Shielded VM。



重要

要成功创建集群，如果您的机构启用了策略约束 constraints/compute.requireShieldedVm，则需要选择 Enable Secure Boot support for Shielded VM。有关 Google Cloud organizational 策略限制的更多信息，请参阅 机构策略限制。



重要

在使用裸机实例类型创建的 Google Cloud 集群上，不支持为 Shielded 虚拟机启用安全引导支持。如需更多信息，请参阅 Google Cloud 文档中的限制。

h. 选择 **Enable user workload monitoring** 以监控您自己的项目，使其与红帽站点可靠性工程师(SRE)平台指标隔离。默认启用这个选项。

8. **可选：扩展高级加密以更改加密设置。**

a. 选择 **Use custom KMS 密钥来使用自定义 KMS 密钥。如果您不希望使用自定义 KMS 密钥，请保留默认设置 Use default KMS Keys。**

b. 选择 **使用自定义 KMS 密钥 ：**

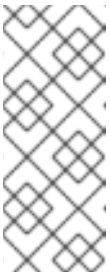
i. **从 Key ring location 下拉菜单中选择密钥环位置。**

ii. **从 Key ring 下拉菜单中选择一个密钥环。**

iii. **从 Key name 下拉菜单中选择一个键名称。**

iv. **提供 KMS 服务帐户。**

c. **可选： 如果需要集群经过 FIPS 验证，请选择启用 FIPS 加密。**



注意

如果选择了 **Enable FIPS 加密，则默认 启用额外的 etcd 加密，且无法禁用。您可以选择 Enable additional etcd encryption without select Enable FIPS encryption。**

d.

可选：如果您需要 etcd 键值加密，请选择 Enable additional etcd encryption。使用此选项时，etcd 键的值被加密，而不是键本身。这个选项除了 control plane 存储加密外，它默认加密 OpenShift Dedicated 集群中的 etcd 卷。

注意

通过在 etcd 中为密钥值启用 etcd 加密，则会出现大约 20% 的性能开销。除了加密 etcd 卷的默认 control plane 存储加密外，还会引入第二层加密的开销。只有在特别需要时才考虑启用 etcd 加密。

9.

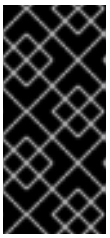
点击 Next。

10.

在 Machine pool 页面中，选择 Compute 节点实例类型 和 Compute 节点数。可用的节点数和类型取决于您的 OpenShift Dedicated 订阅。如果您使用多个可用区，则计算节点计数是每个区域。

11.

可选：展开 添加节点标签，为节点添加标签。点 Add additional label 来添加更多节点标签。



重要

此步骤指的是 Kubernetes 中的标签，而不是 Google Cloud。如需有关 Kubernetes 标签的更多信息，请参阅 标签和选择器。

12.

点击 Next。

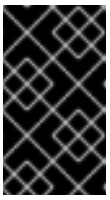
13.

在集群 隐私 对话框中，选择 Public 或 Private 来使用集群的公共或私有 API 端点和应用程序路由。如果您选择 Private，则默认选择Use Private Service Connect，且无法禁用。私有服务连接(PSC)是 Google Cloud 的安全增强网络功能。

14.

可选： 要在现有 Google Cloud Virtual Private Cloud (VPC)上安装集群：

a. 选择 **Install into an existing VPC**。



重要

只有 **Install into an existing VPC** 才支持私有 **Service Connect**。

b. 如果您要安装到现有的 **VPC** 中，并且您要为集群启用 **HTTP** 或 **HTTPS** 代理，请选择 **配置集群范围代理**。

重要

要为集群配置集群范围代理，您必须首先创建云网络地址转换(NAT)和云路由器。如需更多信息，*请参阅附加资源部分*。

15. 接受默认应用程序入口设置，或创建自己的自定义设置，选择 **Custom Settings**。

a. 可选：提供路由选择器。

b. 可选：提供排除的命名空间。

c. 选择命名空间所有权策略。

d. 选择通配符策略。

有关自定义应用程序入口设置的更多信息，请点击每个设置提供的信息图标。

16. 点击 **Next**。

17. 可选： 要将集群安装到 **Google Cloud Shared VPC** 中，请按照以下步骤操作。

注意

不支持将新的 OpenShift Dedicated 集群安装到 VPC 中，它由安装程序为不同的集群自动创建。

重要

主机项目的 VPC 所有者必须在 Google Cloud 控制台中启用项目作为主机项目，并在集群安装前将 Computer Network Administrator、Compute Security Administrator 和 DNS Administrator 角色添加到以下服务帐户：

- osd-deployer
- osd-control-plane
- openshift-machine-api-gcp

如果不这样做，会导致集群进入"安装等待"状态。如果发生这种情况，您必须联系主机项目的 VPC 所有者，才能将角色分配给上面列出的服务帐户。主机项目的 VPC 所有者在集群创建失败前有 30 天的时间授予列出的权限。如需更多信息，请参阅启用主机项目和置备 共享 VPC。

a. 选择 **Install into Google Cloud Shared VPC**。

b. 指定 **Host** 项目 **ID**。如果指定的主机项目 ID 不正确，集群创建会失败。

c. 如果您选择在现有 Google Cloud VPC 中安装集群，请提供 Virtual Private Cloud (VPC)子网设置 并选择 **Next**。您必须已创建了云网络地址转换 (NAT) 和云路由器。有关 Cloud NAT 和 Google VPC 的信息，*请参阅附加资源*。

注意

如果您要将集群安装到共享 VPC 中，VPC 名称和子网将从主机项目共享。

18. 点击 **Next**。

19. 如果您选择配置集群范围代理，在 **Cluster-wide proxy** 页面中提供代理配置详情：

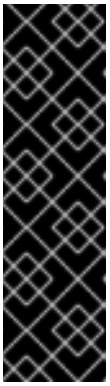
    a. 至少在以下字段之一中输入值：

    - 指定有效的 **HTTP** 代理 **URL**。
    - 指定有效的 **HTTPS** 代理 **URL**。
    - 在 **Additional trust bundle** 字段中，提供 **PEM** 编码 **X.509** 证书捆绑包。捆绑包添加到集群节点的可信证书存储中。如果使用 **TLS-inspecting** 代理，则需要额外的信任捆绑包文件，除非代理的身份证书由 **Red Hat Enterprise Linux CoreOS (RHCOS)**信任捆绑包的颁发机构签名。无论代理是透明的，还是需要使用 **http-proxy** 和 **https-proxy** 参数显式配置，这个要求都适用。

    b. 点击 **Next**。

    有关使用 **OpenShift Dedicated** 配置代理的更多信息，请参阅*配置集群范围代理*。

20. 在 **CIDR** 范围对话框中，配置自定义无类别域间路由 **(CIDR)** 范围，或使用提供的默认值。



重要

稍后无法更改 CIDR 配置。在继续操作前，请联系您的网络管理员选择。

如果集群隐私设置为 Private，则在云供应商中配置私有连接前无法访问集群。

21. 在 Cluster update 策略 页面中，配置您的更新首选项：

a. 选择集群更新方法：

- 如果要 单独调度每个更新，请选择单个更新。这是默认选项。
- 选择 Recurring updates 以在更新可用是在您的首先日期、开始时间上更新集群。

注意

您可以查看 OpenShift Dedicated 更新生命周期文档中的生命周期结束日期。如需更多信息，请参阅 OpenShift Dedicated 更新生命周期。

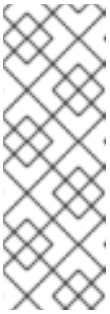
b. 根据集群更新方法提供管理员批准：

- 独立更新：如果您选择了一个需要批准的更新版本，请提供一个管理员的确认信息，并点 Approve and continue。
- 重复更新：如果您为集群选择了重复更新，请提供一个管理员的确认信息并点 Approve and continue。在没有收到管理员确认的情况下，OpenShift Cluster Manager 不会为次版本启动 y-stream 更新。

c. 如果您选择重复更新，请从下拉菜单中选择 UTC 中的星期天和升级开始时间。

d. 可选：您可以在集群安装过程中为节点排空设置宽限期。默认设置 1 小时 宽限期。

e. 点击 Next。



注意

如果出现严重影响集群的安全性或稳定性的关键安全问题，Red Hat Site Reliability Engineering (SRE) 可能会对最新 z-stream 版本进行自动更新。在通知客户后，更新会在 48 小时内应用。有关严重影响安全评级的信息，请参阅 了解红帽安全评级。

22. 查看您选择的概述并点 Create cluster 启动集群安装。安装需要大约 30-40 分钟才能完成。

23. 可选：在 Overview 选项卡中，您可以通过选择 Enable 来启用删除保护功能，它直接位于 Delete Protection: Disabled 下。这将阻止集群被删除。要禁用删除保护，请选择 Disable。默认情况下，集群会被创建，并禁用了删除保护功能。

验证

- 您可以在集群的 Overview 页面中监控安装的进度。您可以在同一页面中查看安装日志。当页面的 Details 部分中的 Status 列为 Ready 时，您的集群已就绪。

重要

如果您的集群部署在安装过程中失败，在安装过程中创建的特定资源不会自动从 Google Cloud 帐户中删除。要从 Google Cloud 帐户中删除这些资源，您必须删除失败的集群。

其他资源

- Accessing OpenShift Cluster Manager

2.5. 使用 OCM CLI 创建 WORKLOAD IDENTITY FEDERATION 集群

您可以在带有 Workload Identity Federation (WIF)的 Google Cloud 集群上，以互动或非互动模式使用 OpenShift Cluster Manager CLI (ocm)在 Google Cloud 集群上创建 OpenShift Dedicated。

注意

不支持将现有非WIF 集群迁移到 WIF 配置。此功能只能在新集群创建过程中启用。

流程

您可以使用互动模式或非互动模式创建 WIF 集群。

在交互模式中，集群属性会在创建集群时自动显示为提示。您可以根据提供的字段中指定要求输入这些提示的值。

在 非交互模式 中，您可以在命令中为特定参数指定值。

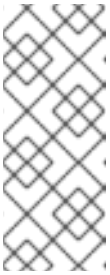
- 根据您的模式首选项，运行以下命令使用 WIF 配置在 Google Cloud 上创建 OpenShift Dedicated 集群：
  - 运行以下命令，以互动模式创建集群：

```
$ ocm create cluster --interactive (1)
```

(1)

交互模式 允许您在互动提示中指定配置选项。

  - 运行以下命令，以非互动模式创建集群：



注意

以下示例是一个可选的和必要的参数，可能与您的 非互动 模式命令不同。没有作为可选的参数是必需的。有关这些参数和其他参数的详情，请在终端窗口中运行 ocm create cluster --help flag 命令。

```
$ ocm create cluster <cluster_name> \ 1
--provider=gcp \ 2
--ccs=true \ 3
--wif-config <wif_name> \ 4
--region <gcp_region> \ 5
--subscription-type=marketplace-gcp \ 6
--marketplace-gcp-terms=true \ 7
--version <version> \ 8
--multi-az=true  \ 9
--enable-autoscaling=true \ 10
--min-replicas=3 \ 11
--max-replicas=6 \ 12
--secure-boot-for-shielded-vms=true 13
--channel-group <channel_group_name> 14
```

1

将 <cluster_name > 替换为集群的名称。

2

将值设为 gcp。

3

将值设为 true。

4

将 <wif_name > 替换为 WIF 配置的名称。

5

使用部署新集群的 Google Cloud 区域替换 。

6

可选：集群的订阅账单模型。

7

可选：如果您为 subscription-type 参数提供了 marketplace-gcp 值，则 marketplace-gcp-terms 必须等于 true。

8

9

可选：部署到多个数据中心。

10

可选：启用计算节点的自动扩展。

11

可选：最少的计算节点数量。

12

可选：计算节点的最大数量。

13

可选：安全引导启用在 Google Cloud 中使用 Shielded 虚拟机。

14

可选：将 < channel_group_name > 替换为您要为其分配集群的频道组的名称。频道组选项包括 stable 和 eus。

重要

如果指定了 OpenShift Dedicated 版本，则该版本还必须被分配的 WIF 配置支持。如果指定了不被分配的 WIF 配置支持的版本，集群创建将失败。如果发生了这种情况，将分配的 WIF 配置更新至所需的版本，或者在 --version <osd_version> 字段中使用所需版本创建新的 WIF 配置。

重要

如果您的集群部署在安装过程中失败，在安装过程中创建的特定资源不会自动从 Google Cloud 帐户中删除。要从 Google Cloud 帐户中删除这些资源，您必须删除失败的集群。

2.6. 列出工作负载身份联邦集群

您可以使用 OpenShift Cluster Manager CLI (ocm)列出已使用 Workload Identity Federation (WIF) 身份验证部署的 OpenShift Dedicated 集群。

流程

- 要列出已使用 WIF 身份验证类型部署的所有 OpenShift Dedicated 集群，请运行以下命令：
  - 使用带有 search 选项的-- parameter 标志：

```
$ ocm list clusters --parameter search="gcp.authentication.wif_config_id != ''"
```

  - 使用特定的 wif-config ID 来过滤与该配置关联的集群：

```
$ ocm list clusters --parameter search="gcp.authentication.wif_config_id =
'<wif_config_id>'" 1
```

1 将 <wif_config_id > 替换为 WIF 配置的 ID。

2.7. 更新 WORKLOAD IDENTITY FEDERATION 配置

您可以更新现有的 Workload Identity Federation (WIF)配置来支持较新的 OpenShift Dedicated y-stream 版本，并与最新的安全最佳实践一致。

注意

更新 WIF 配置仅适用于 y-stream 更新。有关更新过程的概述，包括版本语义的详细信息，请参阅 OpenShift 版本的指南和集群管理员的升级过程。

在将启用了 WIF 的 OpenShift Dedicated 集群升级到更新的版本前，还必须将 wif-config 更新至那个版本。如果您在试图升级集群版本前没有更新 wif-config 版本，集群版本升级将失败。

作为红帽对最小特权原则的持续承诺，某些之前分配给 WIF 配置中的 osd-deployer 服务帐户的权限已

被删除。这些更改通过确保服务帐户只具有执行其功能所需的权限，帮助增强集群的安全性。

有关 WIF 配置角色及其分配权限的完整列表，请参阅 managed-cluster-config。

要将现有的 WIF 配置与这些更新的权限保持一致，您可以运行 ocm gcp update wif-config 命令。此命令更新 WIF 配置，使其包含最佳操作所需的最新权限和角色。

当您更新 wif-config 或创建新时，请确保 OpenShift Cluster Manager CLI (ocm)为最新版本。不更新到最新版本的 ocm 可能会导致错误消息和服务中断。

输出示例

```
Error: failed to create wif-config: failed to create wif-config: status is 400, identifier is '400', code is 'CLUSTERS-MGMT-400', at '2025-10-06T15:18:37Z' and operation identifier is 'f9551d63-a58a-4e3c-b847-5f99ba1b0b74': Client version is out of date for WIF operations. Please update from vOCM-CLI/1.0.7 to v1.0.8 and try again.
```

您还可以通过添加专用项目来使用- federated-project 标志来管理工作负载身份池和供应商来更新已使用 WIF 的现有 OpenShift Dedicated 集群。这种最佳实践模型将工作负载身份池和提供程序分隔到专用的集中式 Google Cloud 项目中。

当您使用 -federated-project 标志更新配置时，任何关联的工作负载身份池都会移至您指定的新联邦项目，而现有的 IAM 服务帐户和自定义角色保留在原始 cluster-associated 项目中。

流程

1. 要检查 ocm 的版本，请运行以下命令：

```
$ ocm version
```

2. 可选：如果您的 ocm 版本不是最新的可用版本，请从 OpenShift Cluster Manager 上的 Downloads 页面中下载并安装最新版本。

3. 运行以下命令，将 wif-config 更新至特定的 OpenShift Dedicated 版本：

```
ocm gcp update wif-config <wif_name> \ 1
--version <version> 2
--federated-project <gcp_project_id> 3
```

1 将 <wif_name > 替换为您要更新的 WIF 配置的名称。

2 可选：将 <version > 替换为您计划更新集群的 OpenShift Dedicated y-stream 版本。如果没有指定版本，则 wif-config 将更新以支持最新的 OpenShift Dedicated y-stream 版本，以及最后三个 OpenShift Dedicated 支持的 y-stream 版本（以版本 4.17 开始）。

3 可选：使用创建和管理工作负载身份池和供应商的专用项目的 ID 替换 。如果没有指定 --federated-project 标志，工作负载身份池和提供程序将保留在与集群关联的项目中。

后续步骤

在更新 wif-config 后，之前分配给 osd-deployer 服务帐户的过时权限集将保留在帐户中。您需要手动访问角色并从中删除这些过时的权限。

按照"从 WIF 配置管理的服务帐户中删除过时的部署器权限"和"从 WIF 配置管理的服务帐户中删除过时的支持权限"中的说明，删除这些过时的权限。

另外，如果您使用 -federated-project 标志将工作负载身份池移到新的专用项目，您可以从原始集群关联的项目手动删除过时的工作负载身份池。如需更多信息，请参阅 Google Cloud 文档中的 删除池。https://docs.cloud.google.com/iam/docs/manage-workload-identity-pools-providers#delete-pool

2.7.1. 从由 WIF 配置管理的服务帐户中删除过时的部署器权限

要从由 WIF 配置管理的服务帐户中删除过时的部署器权限，请在可访问托管服务帐户的 Google Cloud 项目的终端上运行以下命令。

流程

1. 检索现有的角色定义，确保 PROJECT_ID 环境变量指向 Google Cloud 项目：

```
$ gcloud iam roles describe \
  osd_deployer_v4.18 \
  --project $PROJECT_ID \
  --format=yaml > /tmp/role.yaml
```

2. 删除不需要的权限。您可以通过从角色定义文件中过滤不需要的权限，并将更新的定义保存到新文件：

```
$ cat /tmp/role.yaml | \
grep -v "resourcemanager.projects.setIamPolicy" | \
grep -v "iam.serviceAccounts.signBlob" | \
grep -v "iam.serviceAccounts.actAs" > /tmp/updated_role.yaml
```

3. 查看原始角色定义之间的输出更改，以确保只删除不需要的权限：

```
$ diff /tmp/role.yaml /tmp/updated_role.yaml
```

4. 使用更新的角色定义文件更新 Google Cloud 中的角色，确保 PROJECT_ID 环境变量指向 Google Cloud 项目：

```
$ gcloud iam roles update \
  osd_deployer_v4.18 \
  --project=$PROJECT_ID \
  --file=/tmp/updated_role.yaml
```

2.7.2. 从由 WIF 配置管理的服务帐户中删除过时的支持权限

要删除过时的支持权限，请在可访问托管服务帐户的 Google Cloud 项目的终端上运行以下命令。

流程

1. 检索现有的角色定义，确保 PROJECT_ID 环境变量指向 Google Cloud 项目：

```
$ gcloud iam roles describe sre_managed_support --project $PROJECT_ID --
format=yaml > /tmp/role.yaml
```

2. 删除不需要的权限。您可以通过从角色定义文件中过滤不需要的权限，并将更新的定义保存

到新文件：

```
$ cat /tmp/role.yaml | grep -v "compute.firewalls.create"  > /tmp/updated_role.yaml
```

3. 查看原始角色定义之间的输出更改，以确保只删除不需要的权限：

```
$ diff /tmp/role.yaml /tmp/updated_role.yaml
```

4. 使用更新的角色定义文件更新 Google Cloud 中的角色，确保 PROJECT_ID 环境变量指向 Google Cloud 项目：

```
$ gcloud iam roles update sre_managed_support --project $PROJECT_ID --
file=/tmp/updated_role.yaml
```

2.8. 验证 WORKLOAD IDENTITY FEDERATION 配置

您可以通过运行 ocm gcp verify wif-config 命令来验证与 WIF 配置关联的资源配置是否正确。如果找到错误配置，输出将提供有关错误配置的详细信息，并建议您更新 WIF 配置。

您需要要在验证前进行验证的 WIF 配置的名称和 ID。要获取活跃 WIF 配置的名称和 ID，请运行以下命令：

```
$ ocm gcp list wif-configs
```

要确定您要验证的 WIF 配置是否正确配置，请运行以下命令：

```
$ ocm gcp verify wif-config <wif_config_name>|<wif_config_id> 1
```

1. 将 <wif_config_name & gt; 和 <wif_config_id > 分别替换为 WIF 配置的名称和 ID。

输出示例

```
Error: verification failed with error: missing role 'compute.storageAdmin'.
Running 'ocm gcp update wif-config' may fix errors related to cloud resource
```

misconfiguration.
exit status 1.

2.9. 其他资源

- 客户要求
- 项目的资源配额
- Google Cloud 帐户限值
- 所需的客户流程
- 管理工作负载身份池和供应商
- 角色和权限
- 集群最大限制
- 配置身份提供程序
- 撤销权限并可以访问 OpenShift Dedicated 集群

第 3 章 使用服务帐户身份验证在 GOOGLE CLOUD 上创建集群

3.1. 服务帐户身份验证概述

Service Account 身份验证类型使用私钥进行身份验证。服务帐户使用 RSA 密钥对，它由公钥和私钥组成，私钥是服务帐户密钥。密钥对的公钥部分存储在 Google Cloud 上，而私钥则由用户保存。私钥允许用户以服务帐户进行身份验证，并可以访问与该服务帐户关联的资产和资源。

如果未仔细管理，则服务帐户密钥存在安全风险。用户应定期轮转其服务帐户密钥，以减少泄漏或盗窃密钥的风险。

重要

由于使用服务帐户身份验证类型时潜在的安全风险，红帽建议使用 Google Cloud Workload Identity Federation (WIF)作为身份验证类型，以安装和与 Google Cloud 上部署的 OpenShift Dedicated 集群交互，因为它提供了增强的安全性。如需更多信息，*请参阅附加资源部分中的 使用 Workload Identity Federation 身份验证在 Google Cloud 上创建集群*。

3.2. 先决条件

- 您已参阅 OpenShift Dedicated 简介 以及 架构概念 的文档。
- 您已查看了 OpenShift Dedicated 云部署选项。
- 您检查并完成了所需的 客户流程。

3.3. 使用 OPENSHIFT CLUSTER MANAGER 创建带有服务帐户身份验证的集群

流程

1. 登录 OpenShift Cluster Manager，再点 Create cluster。
2. 在 Create a OpenShift cluster 页面中，在 Red Hat OpenShift Dedicated 行中选择 Create cluster。

3. 在 Billing model 下，配置订阅类型和基础架构类型：

   a. 选择订阅类型。如需有关 OpenShift Dedicated 订阅选项的信息，请参阅 OpenShift Cluster Manager 文档中的集群订阅和注册。

   注意

   取决于 OpenShift Dedicated 订阅和资源配额的订阅类型。红帽建议使用通过 Google Cloud Marketplace 购买的 On-Demand 订阅类型部署集群。这个选项提供灵活、基于消费的账单，消耗额外的容量是无法的，不需要红帽干预。

   如需更多信息，请联系您的销售代表或红帽支持。

   b. 选择 Customer Cloud Subscription 基础架构类型，在您拥有的现有云供应商帐户中部署 OpenShift Dedicated。

   c. 点 Next。

4. 选择 Run on Google Cloud。

5. 选择 Service Account 作为 Authentication type。

   注意

   红帽建议使用 Workload Identity Federation 作为 Authentication 类型。如需更多信息，*请参阅附加资源部分中的 使用 Workload Identity Federation 身份验证在 Google Cloud 上创建集群*。

6. 检查并完成列出 的先决条件。

7. 选中该复选框，确认您已经阅读并完成了所有先决条件。

8. 以 JSON 格式提供 Google Cloud 服务帐户私钥。您可以点 Browse 来查找并附加 JSON 文件，或者在 Service account JSON 字段中添加详情。

9. 点 Next 以验证您的云供应商帐户，再进入 Cluster details 页面。

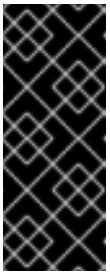
10. 在 Cluster details 页面中，为集群提供一个名称并指定集群详情：

    a. 添加集群名称。

    b. 可选：集群创建生成域前缀，作为 openshiftapps.com 上置备的集群的子域。如果集群名称小于或等于 15 个字符，则该名称用于域前缀。如果集群名称超过 15 个字符，则域前缀会随机生成到 15 个字符字符串。

       要自定义子域，请选中 Create custom domain prefix 复选框，然后在 Domain prefix 字段中输入您的域前缀名称。域前缀不能超过 15 个字符，在您的机构中必须是唯一的，且在集群创建后无法更改。

    c. 从 Version 下拉菜单中选择集群版本。



       重要

       使用私有 Service Connect (PSC)配置的集群只在 OpenShift Dedicated 版本 4.17 及更新的版本中被支持。有关 PSC 的更多信息，请参阅*附加资源*部分中的*私有服务概述*。

    d. 从 Channel 组 下拉菜单中选择频道组。

注意

频道组选项包括 Stable （默认选项）和 EUS。有关 Stable 和 EUS 频道组选项的更多信息，请参阅了解更新频道和发行版本。

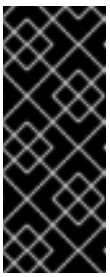
e. 从 Region 下拉菜单中选择云供应商区域。

f. 选择 Single zone 或 Multi-zone 配置。

g. 可选： 选择 Enable Secure Boot for Shielded VMs，以便在安装集群时使用 Shielded 虚拟机。创建集群时，无法更改 Shielded VM 设置的 Enable Secure Boot。如需更多信息，请参阅 Shielded VM。

重要

要成功创建集群，如果您的机构启用了策略约束 constraints/compute.requireShieldedVm，则需要选择 Enable Secure Boot support for Shielded VM。有关 Google Cloud organizational 策略限制的更多信息，请参阅 机构策略限制。



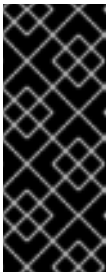
重要

在使用裸机实例类型创建的 Google Cloud 集群上，不支持为 Shielded 虚拟机启用安全引导支持。如需更多信息，请参阅 Google Cloud 文档中的限制。

h. 选择 Enable user workload monitoring 以监控您自己的项目，使其与红帽站点可靠性工程师(SRE)平台指标隔离。默认启用这个选项。

11. 可选：扩展高级加密以更改加密设置。

a. 选择 Use custom KMS 密钥来使用自定义 KMS 密钥。如果您不希望使用自定义 KMS 密钥，请保留默认设置 Use default KMS Keys。



重要

要使用自定义 KMS 密钥，IAM 服务帐户 osd-ccs-admin 必须被授予 Cloud KMS CryptoKey Encrypter/Decrypter 角色。有关授予资源角色的更多信息，请参阅授予资源的角色。

b. 选择 使用自定义 KMS 密钥 ：

i. 从 Key ring location 下拉菜单中选择密钥环位置。

ii. 从 Key ring 下拉菜单中选择一个密钥环。

iii. 从 Key name 下拉菜单中选择一个键名称。

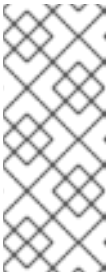
iv. 提供 KMS 服务帐户。

c. 可选： 如果需要集群经过 FIPS 验证，请选择启用 FIPS 加密。

注意

如果选择了 Enable FIPS 加密，则默认 启用额外的 etcd 加密，且无法禁用。您可以选择 Enable additional etcd encryption without select Enable FIPS encryption。

d. 可选：如果您需要 etcd 键值加密，请选择 Enable additional etcd encryption。使用此选项时，etcd 键的值被加密，而不是键本身。这个选项除了 control plane 存储加密外，它默认加密 OpenShift Dedicated 集群中的 etcd 卷。



注意

通过启用额外的 etcd 加密，您将会产生大约 20% 的性能开销。除了加密 etcd 卷的默认 control plane 存储加密外，还会引入第二层加密的开销。只有在特别需要时才考虑启用 etcd 加密。

e. 点击 **Next**。

12. 在 **Default machine pool** 页面上，从下拉菜单中选择 **Compute** 节点实例类型。

13. 可选： 选择 **Enable autoscaling** 复选框来启用自动扩展。

a. 点 **Edit cluster autoscaling settings** 来更改自动扩展设置。

b. 进行所需的更改后，点 **关闭**。

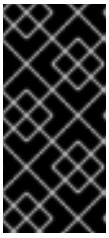
c. 选择最小和最大节点数。通过联合可用的加号和减号，或将所需的节点数输入到数字输入字段中，可以选择节点数。

14. 从下拉菜单中选择 **Compute** 节点数。

注意

如果您使用多个可用区，则计算节点计数是每个区域。创建集群后，您可以更改集群中的计算节点数量，但您无法更改机器池中的计算节点实例类型。您依赖于 OpenShift Dedicated 订阅的节点数量和类型。

15. 可选：展开 **添加节点标签**，为节点添加标签。点 **Add additional label** 添加附加节点标签，然后选择 **Next**。



重要

此步骤指的是 Kubernetes 中的标签，而不是 Google Cloud。如需有关 Kubernetes 标签的更多信息，请参阅 标签和选择器。

16. 在 Network configuration 页面中，选择 Public 或 Private 来使用集群的公共或私有 API 端点和应用程序路由。

如果您选择了 Private and selected OpenShift Dedicated 版本 4.17 或更高版本作为集群版本，则默认选择 Use Private Service Connect。私有服务连接(PSC)是 Google Cloud 的安全增强网络功能。您可以点击 Use Private Service Connect 复选框来禁用 PSC。

注意

红帽建议在 Google Cloud 上部署私有 OpenShift Dedicated 集群时使用 Private Service Connect。私有 Service Connect 确保红帽基础架构、站点可靠性工程(SRE)和私有 OpenShift Dedicated 集群之间存在安全、私有连接。

重要

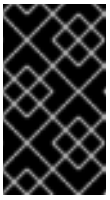
如果使用私有 API 端点，则在更新云供应商帐户中的网络设置之前，您无法访问集群。

17. 可选： 要在现有 Google Cloud Virtual Private Cloud (VPC)上安装集群：

注意

不支持将新的 OpenShift Dedicated 集群安装到 VPC 中，它由安装程序为不同的集群自动创建。

a. 选择 Install into an existing VPC。

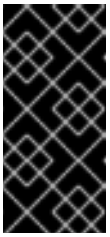


重要

只有 **Install into an existing VPC** 才支持私有 **Service Connect**。

b.

如果您要安装到现有的 **VPC** 中，并且您要为集群启用 **HTTP** 或 **HTTPS** 代理，请选择 **配置集群范围代理**。



重要

要为集群配置集群范围代理，您必须首先创建云网络地址转换(NAT)和云路由器。如需更多信息，*请参阅附加资源部分*。

18.

接受默认应用程序入口设置，或创建自己的自定义设置，选择 **Custom Settings**。

a.

可选：提供路由选择器。

b.

可选：提供排除的命名空间。

c.

选择命名空间所有权策略。

d.

选择通配符策略。

有关自定义应用程序入口设置的更多信息，请点击每个设置提供的信息图标。

19.

点 **Next**。

20.

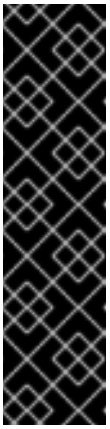
可选：将集群安装到 **Google Cloud Shared VPC** 中：

重要

要将集群安装到共享 VPC 中，您必须使用 OpenShift Dedicated 版本 4.13.15 或更高版本。另外，主机项目的 VPC 所有者必须在 Google Cloud 控制台中将项目启用为主机项目。如需更多信息，请参阅启用主机项目。

a. 选择 **Install into Google Cloud Shared VPC**。

b. 指定 **Host** 项目 **ID**。如果指定的主机项目 ID 不正确，集群创建会失败。



重要

完成集群配置向导中的步骤并点 **Create Cluster** 后，集群将进入"Installation Waiting"状态。此时，您必须联系主机项目的 VPC 所有者，其必须为动态生成的服务帐户分配以下角色： **Compute Network Administrator**、**Compute Security Administrator**、**Project IAM Admin** 和 **DNS Administrator**。主机项目的 VPC 所有者在集群创建失败前有 30 天的时间授予列出的权限。有关共享 VPC 权限的详情，请参考 **Provision Shared VPC**。

21. 如果您选择在现有 **Google Cloud VPC** 中安装集群，请提供 **Virtual Private Cloud (VPC)**子网设置 并选择 **Next**。您必须已创建了云网络地址转换 **(NAT)** 和云路由器。有关 **Cloud NAT** 和 **Google VPC** 的信息，请参阅"附加资源"部分。

注意

如果您要将集群安装到共享 VPC 中，VPC 名称和子网将从主机项目共享。

22. 如果您选择配置集群范围代理，在 **Cluster-wide proxy** 页面中提供代理配置详情：

a. 至少在以下字段之一中输入值：

- 指定有效的 **HTTP** 代理 **URL**。

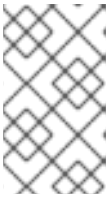
- 指定有效的 HTTPS 代理 URL。

- 在 Additional trust bundle 字段中，提供 PEM 编码 X.509 证书捆绑包。捆绑包添加到集群节点的可信证书存储中。如果使用 TLS-inspecting 代理，则需要额外的信任捆绑包文件，除非代理的身份证书由 Red Hat Enterprise Linux CoreOS (RHCOS)信任捆绑包的颁发机构签名。无论代理是透明的，还是需要使用 http-proxy 和 https-proxy 参数显式配置，这个要求都适用。

b. 点击 Next。

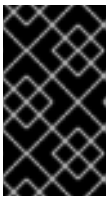
有关使用 OpenShift Dedicated 配置代理的更多信息，请参阅*配置集群范围代理*。

23. 在 CIDR 范围对话框中，配置自定义无类别域间路由 (CIDR) 范围，或使用提供的默认值。



注意

如果您要安装到 VPC 中，Machine CIDR 范围必须与 VPC 子网匹配。



重要

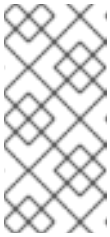
稍后无法更改 CIDR 配置。在继续操作前，请联系您的网络管理员选择。

24. 在 Cluster update 策略 页面中，配置您的更新首选项：

a. 选择集群更新方法：

- 如果要 单独调度每个更新，请选择单个更新。这是默认选项。

- 选择 Recurring updates 以在更新可用是在您的首先日期、开始时间上更新集群。



注意

您可以查看 OpenShift Dedicated 更新生命周期文档中的生命周期结束日期。如需更多信息，请参阅 OpenShift Dedicated 更新生命周期。

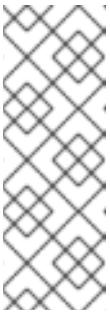
b. 根据集群更新方法提供管理员批准：

- 独立更新：如果您选择了一个需要批准的更新版本，请提供一个管理员的确认信息，并点 Approve and continue。
- 重复更新：如果您为集群选择了重复更新，请提供一个管理员的确认信息并点 Approve and continue。在没有收到管理员确认的情况下，OpenShift Cluster Manager 不会为次版本启动 y-stream 更新。

c. 如果您选择重复更新，请从下拉菜单中选择 UTC 中的星期天和升级开始时间。

d. 可选：您可以在集群安装过程中为节点排空设置宽限期。默认设置 1 小时 宽限期。

e. 点击 Next。



注意

如果出现严重影响集群的安全性或稳定性的关键安全问题，Red Hat Site Reliability Engineering (SRE) 可能会对最新 z-stream 版本进行自动更新。在通知客户后，更新会在 48 小时内应用。有关严重影响安全评级的信息，请参阅 了解红帽安全评级。

25. 查看您选择的概述并点 Create cluster 启动集群安装。安装需要大约 30-40 分钟才能完成。

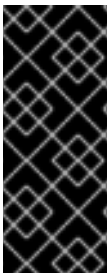
26. 可选：在 Overview 选项卡中，您可以通过选择 Enable 来启用删除保护功能，它直接位于 Delete Protection: Disabled 下。这将阻止集群被删除。要禁用删除保护，请选择 Disable。默认情况下，集群会被创建，并禁用了删除保护功能。

注意

如果您删除了安装到 Google Cloud Shared VPC 的集群，请通知 VPC 所有者主机项目，以删除在集群创建过程中引用的服务帐户的 IAM 策略角色。

验证

- 您可以在集群的 Overview 页面中监控安装的进度。您可以在同一页面中查看安装日志。当页面的 Details 部分中的 Status 列为 Ready 时，您的集群已就绪。



重要

如果您的集群部署在安装过程中失败，在安装过程中创建的特定资源不会自动从 Google Cloud 帐户中删除。要从 Google Cloud 帐户中删除这些资源，您必须删除失败的集群。

3.4. 其他资源

- 有关 Workload Identity Federation 的详情，请参考使用 Workload Identity Federation 身份验证在 Google Cloud 上创建集群。
- 有关私有服务连接(PSC)的详情，请参考 私有服务连接概述。
- 有关使用 OpenShift Dedicated 配置代理的详情，请参考配置集群范围代理。
- 有关 OpenShift Dedicated 的持久性存储的详情，请参考 OpenShift Dedicated 服务定义中的 Storage 部分。
- 有关 OpenShift Dedicated 负载均衡器的详情，请参考 OpenShift Dedicated 服务定义中的负载均衡器 部分。
- 有关 etcd 加密的更多信息，请参阅 etcd 加密服务定义。
-

有关 OpenShift Dedicated 版本的生命周期结束日期的详情，请查看 OpenShift Dedicated 更新生命周期。

- 有关集群范围代理所需的云网络地址转换(NAT)的常规信息，请参阅 Google 文档中的 Cloud NAT 概述。

- 有关集群范围代理所需的云路由器的常规信息，请参阅 Google 文档中的 Cloud Router 概述。

- 有关在 Google Cloud Provider 帐户中创建 VPC 的详情，请参考 Google 文档中的 创建和管理 VPC 网络。

- 有关配置身份提供程序的详情，请参考 配置身份提供程序。

- 有关撤销集群权限的详情，请参考 撤销权限和访问 OpenShift Dedicated 集群。

第 4 章 使用红帽云帐户在 GOOGLE CLOUD 上创建集群

通过 OpenShift Cluster Manager，您可以使用红帽拥有的标准云供应商帐户在 Google Cloud 上创建 OpenShift Dedicated 集群。

4.1. 先决条件

- 您已参阅 OpenShift Dedicated 简介 以及 架构概念 的文档。
- 您已查看了 OpenShift Dedicated 云部署选项。

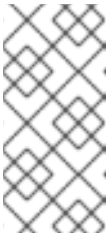
4.2. 使用 OPENSHIFT CLUSTER MANAGER 在 GOOGLE CLOUD 上创建带有红帽云帐户的集群

通过 OpenShift Cluster Manager，您可以使用红帽拥有的标准云供应商帐户在 Google Cloud 上创建 OpenShift Dedicated 集群。

流程

1. 登录 OpenShift Cluster Manager，再点 Create cluster。
2. 在 Cloud 选项卡中，点 Red Hat OpenShift Dedicated 行中的 Create cluster。
3. 在 Billing model 下，配置订阅类型和基础架构类型：
   a. 选择 Annual 订阅类型。使用红帽云帐户部署集群时，只有年度订阅类型可用。

   如需有关 OpenShift Dedicated 订阅选项的信息，请参阅 OpenShift Cluster Manager 文档中的集群订阅和注册。



注意

您必须具有 Annual 订阅类型所需的资源配额才能使用。如需更多信息，请联系您的销售代表或红帽支持。

b. 选择 Red Hat cloud account 基础架构类型，以便在由红帽拥有的云供应商帐户中部署 OpenShift Dedicated。

c. 点 Next。

4. 选择 Run on Google Cloud 并点 Next。

5. 在 Cluster details 页面中，为集群提供一个名称并指定集群详情：

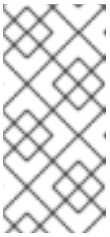
a. 添加集群名称。

b. 可选：集群创建生成域前缀，作为 openshiftapps.com 上置备的集群的子域。如果集群名称小于或等于 15 个字符，则该名称用于域前缀。如果集群名称超过 15 个字符，则域前缀会随机生成为 15 个字符的字符串。

要自定义子域，请选中 Create custom domain prefix 复选框，然后在 Domain prefix 字段中输入您的域前缀名称。域前缀不能超过 15 个字符，在您的机构中必须是唯一的，且在集群创建后无法更改。

c. 从 Version 下拉菜单中选择集群版本。

d. 从 Channel 组 下拉菜单中选择频道组。



注意

频道组选项包括 Stable （默认选项）和 EUS。有关 Stable 和 EUS 频道组选项的更多信息，请参阅了解更新频道和发行版本。

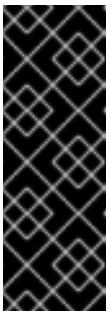
e. 从 Region 下拉菜单中选择云供应商区域。

f. 选择 Single zone 或 Multi-zone 配置。

g. 为集群选择持久性存储容量。如需更多信息，请参阅 OpenShift Dedicated 服务定义中的 *Storage* 部分。

h. 指定集群所需的负载均衡器数量。如需更多信息，请参阅 OpenShift Dedicated 服务定义中的*负载均衡器*部分。

i. 可选： 选择 Enable Secure Boot support for Shielded VMs to use Shielded VMs when installation cluster。创建集群时，无法更改 对 Shielded VM 设置的启用安全引导支持。如需更多信息，请参阅 Shielded VM。



重要

要成功创建集群，如果您的机构启用了策略约束 constraints/compute.requireShieldedVm，则需要选择 Enable Secure Boot support for Shielded VM。有关 Google Cloud organizational 策略限制的更多信息，请参阅 机构策略限制。

重要

在使用裸机实例类型创建的 Google Cloud 集群上，不支持为 Shielded 虚拟机启用安全引导支持。如需更多信息，请参阅 Google Cloud 文档中的限制。

j. 选择 Enable user workload monitoring 以监控您自己的项目，使其与红帽站点可靠性工程师(SRE)平台指标隔离。默认启用这个选项。

6. 可选：扩展高级加密以更改加密设置。

a.

可选： 如果需要集群经过 FIPS 验证，请选择启用 FIPS 加密。

注意

如果选择了 Enable FIPS 加密，则默认 启用额外的 etcd 加密，且无法禁用。您可以选择 Enable additional etcd encryption without select Enable FIPS encryption。

b.

可选：如果您需要 etcd 键值加密，请选择 Enable additional etcd encryption。使用此选项时，etcd 键的值被加密，而不是键本身。这个选项除了 control plane 存储加密外，它默认加密 OpenShift Dedicated 集群中的 etcd 卷。

注意

通过在 etcd 中为密钥值启用 etcd 加密，则会出现大约 20% 的性能开销。除了加密 etcd 卷的默认 control plane 存储加密外，还会引入第二层加密的开销。只有在特别需要时才考虑启用 etcd 加密。

c.

点 Next。

7.

在 Default machine pool 页面中，选择 Compute 节点实例类型 和 Compute 节点数。可用的节点数和类型取决于您的 OpenShift Dedicated 订阅。如果您使用多个可用区，则计算节点计数是每个区域。

注意

创建集群后，您可以更改集群中的计算节点数量，但您无法更改机器池中的计算节点实例类型。对于使用 CCS 模型的集群，您可以在安装后添加使用不同实例类型的机器池。您依赖于 OpenShift Dedicated 订阅的节点数量和类型。

8.

可选：展开 标记节点标签，为节点添加标签。点 Add label 来添加更多节点标签并选择 Next。

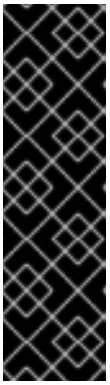
9.

在集群 隐私 对话框中，选择 Public 或 Private 来使用集群的公共或私有 API 端点和应用程

序路由。

10. 点 Next。

11. 在 CIDR 范围对话框中，配置自定义无类别域间路由 (CIDR) 范围，或使用提供的默认值。



重要

稍后无法更改 CIDR 配置。在继续操作前，请联系您的网络管理员选择。

如果集群隐私设置为 Private，则在云供应商中配置私有连接前无法访问集群。

12. 在 Cluster update 策略 页面中，配置您的更新首选项：

a. 选择集群更新方法：

- 如果要 单独调度每个更新，请选择单个更新。这是默认选项。
- 选择 Recurring updates 以在更新可用是在您的首先日期、开始时间上更新集群。

注意

您可以查看 OpenShift Dedicated 更新生命周期文档中的生命周期结束日期。如需更多信息，请参阅 OpenShift Dedicated 更新生命周期。

b. 根据集群更新方法提供管理员批准：

- 独立更新：如果您选择了一个需要批准的更新版本，请提供一个管理员的确认信息，并点 Approve and continue。

- 重复更新：如果您为集群选择了重复更新，请提供一个管理员的确认信息并点 Approve and continue。在没有收到管理员确认的情况下，OpenShift Cluster Manager 不会为次版本启动 y-stream 更新。

c. 如果您选择重复更新，请从下拉菜单中选择 UTC 中的星期天和升级开始时间。

d. 可选：您可以在集群安装过程中为节点排空设置宽限期。默认设置 1 小时 宽限期。

e. 点击 Next。

注意

如果出现严重影响集群的安全性或稳定性的关键安全问题，Red Hat Site Reliability Engineering (SRE) 可能会对最新 z-stream 版本进行自动更新。在通知客户后，更新会在 48 小时内应用。有关严重影响安全评级的信息，请参阅 了解红帽安全评级。

13. 查看您选择的概述并点 Create cluster 启动集群安装。安装需要大约 30-40 分钟才能完成。

14. 可选：在 Overview 选项卡中，您可以通过选择 Enable 来启用删除保护功能，它直接位于 Delete Protection: Disabled 下。这将阻止集群被删除。要禁用删除保护，请选择 Disable。默认情况下，集群会被创建，并禁用了删除保护功能。

验证

- 您可以在集群的 Overview 页面中监控安装的进度。您可以在同一页面中查看安装日志。当页面的 Details 部分中的 Status 列为 Ready 时，您的集群已就绪。

重要

如果您的集群部署在安装过程中失败，在安装过程中创建的特定资源不会自动从 Google Cloud 帐户中删除。要从 Google Cloud 帐户中删除这些资源，您必须删除失败的集群。

4.3. 后续步骤

- 要了解为集群配置身份提供程序，请参阅 配置身份提供程序。
- 要了解向集群授予用户管理员权限的信息，请参阅 为用户授予管理员权限。

第 5 章 删除 GOOGLE CLOUD 上的 OPENSHIFT DEDICATED 集群

作为集群所有者，您可以删除 OpenShift Dedicated 集群。

5.1. 删除集群

您可以在 Red Hat OpenShift Cluster Manager 中删除 OpenShift Dedicated 集群。

先决条件

- 已登陆到 OpenShift Cluster Manager。
- 您创建了 OpenShift Dedicated 集群。

流程

1. 在 OpenShift Cluster Manager 中，点您要删除的集群。
2. 从 Actions 下拉菜单中选择 Delete cluster。
3. 以粗体突出显示的集群名称，然后点 Delete。集群删除会自动进行。

注意

如果您删除了安装到 Google Cloud Shared VPC 的集群，请通知 VPC 所有者主机项目，以删除在集群创建过程中引用的服务帐户的 IAM 策略角色。