



OpenShift Dedicated 4

安装、访问和删除 OpenShift Dedicated 集群

安装、访问和删除 OpenShift Dedicated 集群

OpenShift Dedicated 4 安装、访问和删除 OpenShift Dedicated 集群

安装、访问和删除 OpenShift Dedicated 集群

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

本文档提供有关如何安装 OpenShift Dedicated 集群的信息。本文档还详细介绍了如何配置身份提供程序。

目录

第 1 章 在 AWS 上创建集群	3
1.1. 先决条件	3
1.2. 使用 CCS 在 AWS 上创建集群	3
1.3. 使用红帽云帐户在 AWS 上创建集群	8
1.4. 其他资源	10
第 2 章 在 GCP 上创建集群	11
2.1. 先决条件	11
2.2. 使用 CCS 在 GCP 上创建集群	11
2.3. 使用 GOOGLE CLOUD MARKETPLACE 在 GCP 上创建集群	16
2.4. 使用红帽云帐户在 GCP 上创建集群	21
2.5. 使用 RED HAT MARKETPLACE 在 GCP 上创建集群	23
2.6. 其他资源	27
第 3 章 配置身份提供程序	29
3.1. 了解身份提供程序	29
3.2. 配置 GITHUB 身份提供程序	30
3.3. 配置 GITLAB 身份提供程序	31
3.4. 配置 GOOGLE 身份提供程序	32
3.5. 配置 LDAP 身份提供程序	33
3.6. 配置 OPENID 身份提供程序	35
3.7. 配置 HTPASSWD 身份提供程序	37
3.8. 访问集群	38
第 4 章 撤销权限并可以访问 OPENSIFT DEDICATED 集群	39
4.1. 从用户撤销管理员权限	39
4.2. 撤销对集群的用户访问权限	39
第 5 章 删除 OPENSIFT DEDICATED 集群	41
5.1. 删除集群	41

第 1 章 在 AWS 上创建集群

您可以通过客户云订阅(CCS)模型，或使用红帽拥有的 AWS 基础架构帐户，在 Amazon Web Services (AWS)上安装 OpenShift Dedicated。

1.1. 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](#)。

1.2. 使用 CCS 在 AWS 上创建集群

通过使用客户云订阅 (CCS) 账单模型，您可以在您拥有的现有 Amazon Web Services (AWS) 帐户中创建 OpenShift Dedicated 集群。

如果您使用 CCS 模型在 AWS 帐户中部署和管理 OpenShift Dedicated，则必须满足几个先决条件。

先决条件

- 您已配置了 AWS 帐户以用于 OpenShift Dedicated。
- 您没有在 AWS 帐户中部署任何服务。
- 您已配置了支持所需集群大小的 AWS 帐户配额和限制。
- 您有一个 **osdCcsAdmin** AWS Identity 和 Access Management (IAM) 用户，并附加了 **AdministratorAccess** 策略。
- 您已在 AWS 机构中设置了服务控制策略 (SCP)。如需更多信息，请参阅 [最低所需的服务控制策略\(SCP\)](#)。
- 有 AWS 的 **Business Support** 或更高支持。
- 如果要配置集群范围代理，请验证可以从安装集群的 VPC 访问代理。该代理还必须从 VPC 的专用子网访问。

流程

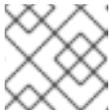
1. 登录 [OpenShift Cluster Manager](#)，再点 **Create cluster**。
2. 在 **Create a OpenShift cluster** 页面中，在 **Red Hat OpenShift Dedicated** 行中选择 **Create cluster**。
3. 在 **Billing model** 下，配置订阅类型和基础架构类型：
 - a. 选择订阅类型。如需有关 OpenShift Dedicated 订阅选项的信息，请参阅 [OpenShift Cluster Manager 文档中的集群订阅和注册](#)。



注意

取决于 OpenShift Dedicated 订阅和资源配额的订阅类型。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 Amazon Web Services**。
 5. 选择云供应商后，检查并完成列出的**先决条件**。选中该复选框，确认您已经阅读并完成了所有先决条件。
 6. 提供 AWS 帐户详情：
 - a. 输入 **AWS 帐户 ID**。
 - b. 为 AWS IAM 用户帐户输入 **AWS 访问密钥 ID** 和 **AWS secret 访问密钥**。

**注意**

在 AWS 中撤销这些凭证会导致无法访问使用这些凭证创建的任何集群。

- c. 可选：您可以选择 **Bypass AWS 服务控制策略(SCP)检查** 来禁用 SCP 检查。

**注意**

有些 AWS SCP 可能会导致安装失败，即使您有所需的权限。禁用 SCP 检查可进行安装。即使绕过了检查，SCP 仍然会被强制使用。

7. 点 **Next** 以验证您的云供应商帐户，再进入 **Cluster details** 页面。
8. 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：集群创建会生成域前缀，作为您在 **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，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给 15 个字符的字符串。
要自定义子域，请选择 **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，在您的机构内必须是唯一的，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 **Region** 下拉菜单中选择云供应商区域。
 - e. 选择 **Single zone** 或 **Multi-zone** 配置。
 - f. 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。
 - g. 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。

- h. 可选：如果要提供自己的 AWS 密钥管理服务(KMS) 密钥 Amazon 资源名称(ARN)，请选择 **Encrypt persistent volumes with customer key**。密钥用于加密集群中的所有 control plane、基础架构、worker 节点根卷和持久性卷。



重要

只有从默认存储类创建的持久性卷(PV)才会使用此特定密钥加密。

使用任何其他存储类创建的 PV 仍然会被加密，但 PV 不会使用此密钥加密，除非存储类被特别配置为使用这个密钥。

- i. 点 **Next**。

9. 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。您依赖于 OpenShift Dedicated 订阅的节点数量和类型。

10. 选择 Instance Metadata Service (IMDS) 类型，可以使用 IMDSv1 和 IMDSv2 类型，或者您的 EC2 实例只使用 IMDSv2。您可以通过两种方式从正在运行的实例访问实例元数据：

- 实例元数据服务版本 1 (IMDSv1)- 请求/响应方法
- 实例元数据服务版本 2 (IMDSv2)- 面向会话的方法



重要

在集群创建后无法更改实例元数据服务设置。



注意

IMDSv2 使用面向会话的请求。使用面向会话的请求时，您可以创建一个会话令牌，它定义会话持续时间，至少为 1 秒，最多为 6 小时。在指定持续时间中，您可以对后续请求使用相同的会话令牌。在指定持续时间过期后，您必须创建一个新的会话令牌，以用于将来的请求。

有关 IMDS 的更多信息，请参阅 [AWS 文档中的实例元数据和用户数据](#)。

11. 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**。
12. 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。

**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。

13. 可选：要在现有 AWS Virtual Private Cloud (VPC) 上安装集群：
 - a. 选择 **Install into an existing VPC**。
 - b. 如果您要安装到现有的 VPC 中，并选择使用私有 API 端点，您可以选择 **Use a PrivateLink**。这个选项允许使用 AWS PrivateLink 端点的 Red Hat Site Reliability Engineering (SRE) 连接到集群。

**注意**

在集群创建后无法更改 **Use a PrivateLink** 选项。

- c. 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**。
14. 点 **Next**。
15. 如果您选择在现有 AWS 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**

您必须确保您的 VPC 配置了一个公有和私有子网，以及您要安装到的每个可用区的专用子网。如果您选择使用 PrivateLink，则只需要专用子网。

- a. 可选：扩展 **Additional security groups** 并选择额外的自定义安全组，以应用到默认创建的机器池中的节点。您必须已创建了安全组，并将其与您为这个集群选择的 VPC 关联。您无法在创建集群时将安全组添加到默认机器池中。
默认情况下，您指定的安全组会为所有节点类型添加。清除 **Apply the same security groups to all node types** 复选框，以为每个节点类型应用不同的安全组。

如需更多信息，请参阅 *附加资源* 下的 *安全组* 的要求。

16. 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。如果您使用 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 **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*。

17. 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。



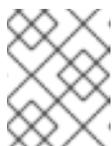
重要

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。

18. 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](#)。

19. 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。

20. 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，该功能直接位于 **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，集群禁用了删除保护功能来创建。

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。

1.3. 使用红帽云帐户在 AWS 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 Amazon Web Services (AWS) 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](#)。

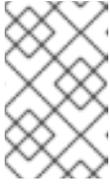


注意

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 Amazon Web Services** 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：集群创建会生成域前缀，作为您在 **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，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，请选择 **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，在您的机构内必须是唯一的，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 **Region** 下拉菜单中选择云供应商区域。
 - e. 选择 **Single zone** 或 **Multi-zone** 配置。
 - f. 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。
 - g. 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。

- 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。
- i. 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。

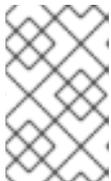


注意

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。

j. 点 **Next**。

6. 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。

7. 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**。
8. 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。
9. 点 **Next**。
10. 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。

11. 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](#)。

12. 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。
13. 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，该功能直接位于 **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，集群禁用了删除保护功能来创建。

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。

1.4. 其他资源

- 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 CCS 部署所需的 AWS 服务控制策略的详情，请参阅 [最低所需的服务控制策略\(SCP\)](#)。
- 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](#)。
- 有关自定义额外安全组要求的详情，请参考 [其他自定义安全组](#)。

第 2 章 在 GCP 上创建集群

您可以通过客户云订阅 (CCS) 模型，或使用由红帽拥有的 GCP 基础架构帐户，使用您自己的 GCP 帐户在 Google Cloud Platform (GCP) 上安装 OpenShift Dedicated。

2.1. 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](#)。

2.2. 使用 CCS 在 GCP 上创建集群

通过使用客户云订阅 (CCS) 账单模型，您可以在您拥有的现有 Google Cloud Platform (GCP) 帐户中创建一个 OpenShift Dedicated 集群。

如果您使用 CCS 模型在 GCP 帐户中部署和管理 OpenShift Dedicated，则必须满足几个先决条件。

先决条件

- 您已配置了 GCP 帐户以用于 OpenShift Dedicated。
- 您已配置了支持所需集群大小所需的 GCP 帐户配额和限制。
- 您已创建了 GCP 项目。



注意

项目名称必须是 10 个字符或更少。

- 您已在 GCP 项目中启用了 Google Cloud Resource Manager API。有关为项目启用 API 的更多信息，请参阅 [Google Cloud 文档](#)。
- 在 GCP 中有一个名为 **osd-ccs-admin** 的 IAM 服务帐户，并附加以下角色：
 - Compute Admin
 - DNS Administrator
 - Security Admin
 - Service Account Admin
 - Service Account Key Admin
 - Service Account User
 - 机构策略查看器
 - 服务管理管理员
 - Service Usage Admin
 - Storage Admin

- Compute Load Balancer Admin
- 角色查看器
- Role Administrator
- 您已为 **osd-ccs-admin** GCP 服务帐户创建了密钥，并将其导出到名为 **osServiceAccount.json** 的文件中。



注意

有关为您的 GCP 服务帐户创建密钥并将其导出到 JSON 文件的更多信息，请参阅 Google Cloud 文档中的[创建服务帐户密钥](#)。

- 考虑从 GCP 获得 **Production Support** 或更高级别的支持。
- 为防止潜在的冲突，请考虑在安装 OpenShift Dedicated 之前没有置备项目中的其他资源。
- 如果要配置集群范围代理，请验证可以从安装集群的 VPC 访问代理。

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。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 Platform**。
 5. 选择云供应商后，检查并完成列出的**先决条件**。选中该复选框，确认您已经阅读并完成了所有先决条件。
 6. 以 JSON 格式提供您的 GCP 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。
 7. 点 **Next** 以验证您的云供应商帐户，再进入 **Cluster details** 页面。
 8. 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：集群创建会生成域前缀，作为您在 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，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给 15 个字符的字符串。
要自定义子域，请选择 **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，在您的机构内必须是唯一的，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 **Region** 下拉菜单中选择云供应商区域。
- e. 选择 **Single zone** 或 **Multi-zone** 配置。
- f. 可选：选择 **Enable Secure Boot for Shielded VMs** 以便在安装集群时使用 Shielded 虚拟机。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**。如需有关 GCP 机构策略约束的更多信息，请参阅 [机构策略限制](#)。

- g. 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。
9. 可选：扩展高级加密以更改加密设置。
- a. 选择 **Use Custom KMS keys** 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](#)。

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**。
- 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. 可选：如果需要集群经过 FIPS 验证，请选择启用 **FIPS 加密**。
 - d. 点击 **Next**。
10. 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。您依赖于 OpenShift Dedicated 订阅的节点数量和类型。

11. 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**。
12. 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。



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。

13. 可选：要在现有 GCP Virtual Private Cloud (VPC) 上安装集群：
 - a. 选择 **Install into an existing VPC**。
 - 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**。
14. 点击 **Next**。
15. 可选：要将集群安装到 GCP 共享 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 GCP 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，该所有者必须分配动态生成的服务帐户，角色如下：**Computer Network Administrator**、**Compute Security Administrator** 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](#)。

16. 如果您选择在现有 GCP 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。

17. 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。如果您使用 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](#)。
18. 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。

19. 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](#)。

20. 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。

21. 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，该功能直接位于 **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，集群禁用了删除保护功能来创建。



注意

如果您删除了安装到 GCP 共享 VPC 中的集群，请通知主机项目的 VPC 所有者，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。

2.3. 使用 GOOGLE CLOUD MARKETPLACE 在 GCP 上创建集群

当通过 OpenShift Cluster Manager Hybrid Cloud Console 在 Google Cloud 上创建 OpenShift Dedicated (OSD) 集群时，客户可以选择 Google Cloud Marketplace 作为首选账单模型。此账单模式允许红帽客户利用其 [Google Committed Use Discounts \(CUD\)](#) 到通过 Google Cloud Marketplace 购买的 OpenShift Dedicated。此外，OSD 定价是基于实际的消费情况的，客户通过 Google Cloud 帐户直接计费。

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 **On-Demand** 订阅类型。
 - b. 从下拉菜单中选择 **Google Cloud Marketplace**。
 - c. 选择 **Customer Cloud Subscription** 基础架构类型。
 - d. 点击 **Next**。
4. 在 **Cloud provider** 页面中，阅读提供的前提条件和 Google 条款和条件。添加您的服务帐户密钥。
 - a. 点 **Review Google terms and Agreements** 链接。
 - b. 要继续创建集群，请点指示您同意 Google 术语和协议的复选框。
 - c. 添加您的服务帐户密钥。



注意

如需有关服务帐户密钥的更多信息，请点位于 **Service account key** 旁边的信息图标。

- d. 点 **Next** 以验证您的云供应商帐户，再进入 **Cluster details** 页面。
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：集群创建会生成域前缀，作为您在 **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，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，请选择 **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，在您的机构内必须是唯一的，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 **Region** 下拉菜单中选择云供应商区域。
 - e. 选择 **Single zone** 或 **Multi-zone** 配置。
 - f. 可选：选择 **Enable Secure Boot for Shielded VMs** 以便在安装集群时使用 Shielded 虚拟机。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**。如需有关 GCP 机构策略约束的更多信息，请参阅 [机构策略限制](#)。

- g. 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：扩展高级加密以更加密设置。
- a. 选择 **Use Custom KMS keys** 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](#)。

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

7. 点击 **Next**。
8. 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。



注意

创建集群后，您可以更改计算节点的数量，但您无法更改创建的机器池中的计算节点实例类型。您可在安装后添加使用自定义实例类型的机器池。您依赖于 OpenShift Dedicated 订阅的节点数量和类型。

9. 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。
10. 点击 **Next**。
11. 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。

12. 可选：要在现有 GCP Virtual Private Cloud (VPC) 上安装集群：
 - a. 选择 **Install into an existing VPC**。
 - 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**。
13. 点击 **Next**。
14. 可选：要将集群安装到 GCP 共享 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 GCP 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，该所有者必须分配动态生成的服务帐户，角色如下：**Computer Network Administrator**、**Compute Security Administrator** 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](#)。

15. 如果您选择在现有 GCP 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。

16. 点击 **Next**。
17. 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。如果您使用 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](#)。

18. 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。

19. 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](#)。

20. 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。

21. 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，该功能直接位于 **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，集群禁用了删除保护功能来创建。

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。

2.4. 使用红帽云帐户在 GCP 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 Platform (GCP) 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. 点击 **Next**。
4. 选择 **Run on Google Cloud Platform** 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：集群创建会生成域前缀，作为您在 [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，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，请选择 **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，在您的机构内必须是唯一的，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 **Region** 下拉菜单中选择云供应商区域。
 - e. 选择 **Single zone** 或 **Multi-zone** 配置。
 - f. 可选：选择 **Enable Secure Boot for Shielded VMs** 以便在安装集群时使用 Shielded 虚拟机。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**。如需有关 GCP 机构策略约束的更多信息，请参阅[机构策略限制](#)。

- 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. 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。
- j. 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。

- k. 点击 **Next**。

6. 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。

7. 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**。
8. 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。
9. 点 **Next**。
10. 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。

11. 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](#)。

12. 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。
13. 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，该功能直接位于 **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，集群禁用了删除保护功能来创建。

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。

2.5. 使用 RED HAT MARKETPLACE 在 GCP 上创建集群

当通过 OpenShift Cluster Manager Hybrid Cloud Console 在 Google Cloud 上创建 OpenShift Dedicated (OSD) 集群时，客户可以选择 Red Hat Marketplace 作为首选账单模型。OSD 定价基于消费，客户通过 Red Hat Marketplace 帐户直接计费。

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 **On-Demand** 订阅类型。
 - b. 从下拉菜单中选择 **Red Hat Marketplace**。

- c. 点击 **Next**。
4. 在 **Cloud provider** 页面中：
 - a. 选择 **Google Cloud** 作为您的云供应商。
 - b. 点显示您已读取和完成继续创建集群所需的所有先决条件的复选框。
 - c. 添加您的服务帐户密钥。



注意

如需有关服务帐户密钥的更多信息，请点位于 **Service account key** 旁边的信息图标。

- d. 点 **Next** 以验证您的云供应商帐户，再进入 **Cluster details** 页面。
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：集群创建会生成域前缀，作为您在 **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，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，请选择 **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，在您的机构内必须是唯一的，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 **Region** 下拉菜单中选择云供应商区域。
 - e. 选择 **Single zone** 或 **Multi-zone** 配置。
 - f. 可选：选择 **Enable Secure Boot for Shielded VMs**，以便在安装集群时使用 **Shielded** 虚拟机。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**。如需有关 GCP 机构策略约束的更多信息，请参阅[机构策略限制](#)。

- g. 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**以更更改加密设置。
 - a. 选择 **Use Custom KMS keys**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](#)。

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**。
- 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. 可选：如果需要集群经过 FIPS 验证，请选择启用 **FIPS 加密**。
7. 点击 **Next**。
 8. 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。



注意

创建集群后，您可以更改计算节点的数量，但您无法更改创建的机器池中的计算节点实例类型。您可在安装后添加使用自定义实例类型的机器池。您依赖于 OpenShift Dedicated 订阅的节点数量和类型。

9. 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。
10. 点击 **Next**。
11. 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。
12. 可选：要在现有 GCP Virtual Private Cloud (VPC) 上安装集群：
 - a. 选择 **Install into an existing VPC**。
 - 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**。
13. 点击 **Next**。

14. 可选：要将集群安装到 GCP 共享 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 GCP 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，该所有者必须分配动态生成的服务帐户，角色如下：**Computer Network Administrator**、**Compute Security Administrator** 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](#)。

15. 如果您选择在现有 GCP 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。

16. 点击 **Next**。
17. 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。如果您使用 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](#)。
18. 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。

19. 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](#)。

20. 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。

21. 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，该功能直接位于 **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，集群禁用了删除保护功能来创建。

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。

2.6. 其他资源

- 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)的一般信息，请参阅 Google 文档中的 [云 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](#)。

第 3 章 配置身份提供程序

创建 OpenShift Dedicated 集群后，您必须配置身份提供程序，以确定用户如何登录以访问集群。

3.1. 了解身份提供程序

OpenShift Dedicated 包含内置的 OAuth 服务器。开发人员和管理员获取 OAuth 访问令牌，以完成自身的 API 身份验证。作为管理员，您可以在安装集群后通过配置 OAuth 来指定身份提供程序。配置身份提供程序可让用户登录和访问集群。

3.1.1. 支持的身份提供程序

您可以配置以下类型的身份提供程序：

用户身份提供程序	描述
Github 或 GitHub Enterprise	配置 GitHub 身份提供程序，针对 GitHub 或 GitHub Enterprise 的 OAuth 身份验证服务器验证用户名和密码。
GitLab	配置 GitLab 身份提供程序，以使用 GitLab.com 或任何其他 GitLab 实例作为身份提供程序。
Google	使用 Google's OpenID Connect integration 配置 Google 身份提供程序。
LDAP	配置 LDAP 身份提供程序，使用简单绑定身份验证来针对 LDAPv3 服务器验证用户名和密码。
OpenID Connect	配置 OpenID Connect (OIDC) 身份提供程序，以使用授权代码流与 OIDC 身份提供程序集成 。
htpasswd	<p>为单个静态管理用户配置 htpasswd 身份提供程序。您可以以用户身份登录到集群来排除问题。</p> <div style="display: flex; align-items: flex-start;"> <div style="flex: 1;">  </div> <div style="flex: 2;"> <p>重要</p> <p>htpasswd 身份提供程序选项仅用于创建单一静态管理用户。htpasswd 不支持作为 OpenShift Dedicated 的通用身份提供程序。有关配置单个用户的步骤，请参阅 配置 htpasswd 身份提供程序。</p> </div> </div>

3.1.2. 身份提供程序参数

以下是所有身份提供程序通用的参数：

参数	描述
name	此提供程序名称作为前缀放在提供程序用户名前，以此组成身份名称。

参数	描述
mappingMethod	<p>定义在用户登录时如何将新身份映射到用户。输入以下值之一：</p> <p>claim 默认值。使用身份的首选用户名置备用户。如果具有该用户名的用户已映射到另一身份，则失败。</p> <p>lookup 查找现有的身份、用户身份映射和用户，但不自动置备用户或身份。这允许集群管理员手动或使用外部流程设置身份和用户。使用此方法需要手动置备用户。</p> <p>add 使用身份的首选用户名置备用户。如果已存在具有该用户名的用户，此身份将映射到现有用户，添加到该用户的现有身份映射中。如果配置了多个身份提供程序并且它们标识同一组用户并映射到相同的用户名，则需要进行此操作。</p>



注意

在添加或更改身份提供程序时，您可以通过把 **mappingMethod** 参数设置为 **add**，将新提供程序中的身份映射到现有的用户。

3.2. 配置 GITHUB 身份提供程序

配置 GitHub 身份提供程序，针对 GitHub 或 GitHub Enterprise 的 OAuth 身份验证服务器验证用户名和密码，并访问您的 OpenShift Dedicated 集群。OAuth 有助于 OpenShift Dedicated 和 GitHub 或 GitHub Enterprise 之间的令牌交换流。



警告

配置 GitHub 身份验证后，用户可以使用 GitHub 凭证登录 OpenShift Dedicated。要防止具有任何 GitHub 用户 ID 的任何人登录到 OpenShift Dedicated 集群，您必须将访问权限限制为只有特定 GitHub 机构或团队中的访问。

先决条件

- OAuth 应用程序必须直接由 GitHub 机构管理员在 GitHub [机构设置](#) 中创建。
- [GitHub 机构或团队](#) 在您的 GitHub 帐户中设置。

流程

1. 在 [OpenShift Cluster Manager](#) 中，进入到 **Clusters** 页面，再选择您需要为其配置身份提供程序的集群。
2. 点 **Access control** 选项卡。
3. 点 **Add identity provider**。



注意

您还可以点在集群创建后显示的警告信息中的 **Add OAuth 配置** 链接来配置身份提供程序。

4. 从下拉菜单中选择 **GitHub**。
5. 输入身份提供程序的唯一名称。之后无法更改此名称。
 - 在提供的字段中自动生成 **OAuth 回调 URL**。您将使用它来注册 GitHub 应用。

```
https://oauth-openshift.apps.<cluster_name>.  
<cluster_domain>/oauth2callback/<idp_provider_name>
```

例如：

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/github
```

6. 在 [GitHub 上注册应用程序](#)。
7. 返回到 OpenShift Dedicated，然后从下拉菜单中选择映射方法。在大多数情况下推荐使用 **声明**。
8. 输入 GitHub 提供的 **客户端 ID** 和 **客户端 secret**。
9. 输入一个 **主机名**。在使用托管 GitHub Enterprise 实例时，必须输入一个主机名。
10. 可选：您可以指定证书颁发机构 (CA) 文件来验证配置的 GitHub Enterprise URL 的服务器证书。点 **Browse** 找到并附加 **CA 文件** 到身份提供程序。
11. 选择 **Use organizations** 或 **Use teams** 以限制对特定 GitHub 组织或 GitHub 团队的访问。
12. 输入您要限制访问权限的机构或团队名称。点 **Add more** 指定用户可以成为用户所属的多个机构或团队。
13. 单击 **Confirm**。

验证

- 配置的身份提供程序可以在 **Cluster details** 页面的 **Access control** 选项卡中看到。

3.3. 配置 GITLAB 身份提供程序

配置 GitLab 身份提供程序，以使用 [GitLab.com](#) 或任何其他 GitLab 实例作为身份提供程序。

前提条件

- 如果使用 GitLab 版本 7.7.0 到 11.0，您可以使用 **OAuth 集成** 进行连接。如果使用 GitLab 版本 11.1 或更高版本，您可以使用 **OpenID Connect (OIDC)** 进行连接，而不使用 OAuth。

流程

1. 在 [OpenShift Cluster Manager](#) 中，进入到 **Clusters** 页面，再选择您需要为其配置身份提供程序的集群。

2. 点 **Access control** 选项卡。
3. 点 **Add identity provider**。



注意

您还可以点在集群创建后显示的警告信息中的 **Add OAuth 配置** 链接来配置身份提供程序。

4. 从下拉菜单中选择 **GitLab**。
5. 输入身份提供程序的唯一名称。之后无法更改此名称。
 - 在提供的字段中自动生成 **OAuth 回调 URL**。您将提供此 URL 到 GitLab。

```
https://oauth-openshift.apps.<cluster_name>.  
<cluster_domain>/oauth2callback/<idp_provider_name>
```

例如：

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/gitlab
```

6. 在 [GitLab 中添加新应用程序](#)。
7. 返回到 OpenShift Dedicated，然后从下拉菜单中选择映射方法。在大多数情况下推荐使用 **声明**。
8. 输入 GitLab 提供的**客户端 ID** 和**客户端 secret**。
9. 输入 GitLab 供应商的 **URL**。
10. 可选：您可以使用证书颁发机构 (CA) 文件来验证配置的 GitLab URL 的服务器证书。点 **Browse** 找到并附加 **CA 文件**到身份提供程序。
11. 单击 **Confirm**。

验证

- 配置的身份提供程序可以在 **Cluster details** 页面的 **Access control** 选项卡中看到。

3.4. 配置 GOOGLE 身份提供程序

配置 Google 身份提供程序，以便用户通过 Google 凭证进行身份验证。



警告

使用 Google 作为身份提供程序时，任何 Google 用户都能与您的服务器进行身份验证。您可以使用 **hostedDomain** 配置属性，将身份验证限制为特定托管域的成员。

流程

1. 在 [OpenShift Cluster Manager](#) 中，进入到 **Clusters** 页面，再选择您需要为其配置身份提供程序的集群。
2. 点 **Access control** 选项卡。
3. 点 **Add identity provider**。



注意

您还可以点在集群创建后显示的警告信息中的 **Add OAuth 配置** 链接来配置身份提供程序。

4. 从下拉菜单中选择 **Google**。
5. 输入身份提供程序的唯一名称。之后无法更改此名称。
 - 在提供的字段中自动生成 **OAuth 回调 URL**。您将为 Google 提供此 URL。

```
https://oauth-openshift.apps.<cluster_name>.  
<cluster_domain>/oauth2callback/<idp_provider_name>
```

例如：

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/google
```

6. 使用 [Google's OpenID Connect integration](#) 配置 Google 身份提供程序。
7. 返回到 OpenShift Dedicated，然后从下拉菜单中选择映射方法。在大多数情况下推荐使用 **声明**。
8. 输入注册 Google 项目的 **客户端 ID**，以及 Google 发布的 **客户端 secret**。
9. 输入托管域，将用户限制到 Google Apps 域。
10. 单击 **Confirm**。

验证

- 配置的身份提供程序可以在 **Cluster details** 页面的 **Access control** 选项卡中看到。

3.5. 配置 LDAP 身份提供程序

配置 LDAP 身份提供程序，以使用简单绑定身份验证针对 LDAPv3 服务器验证用户名和密码。

前提条件

- 在配置 LDAP 身份提供程序时，您需要输入配置的 **LDAP URL**。配置的 URL 是 RFC 2255 URL，指定要使用的 LDAP 主机和搜索参数。URL 的语法是：

```
ldap://host:port/basedn?attribute?scope?filter
```

URL 组件	描述
ldap	对于常规 LDAP，使用 ldap 字符串。对于安全 LDAP (LDAPS)，改为使用 ldaps 。
host:port	LDAP 服务器的名称和端口。LDAP 默认为 localhost:389 ，LDAPS 则默认为 localhost:636 。
basedn	所有搜索都应从中开始的目录分支的 DN。至少，这必须是目录树的顶端，但也可指定目录中的子树。
attribute	要搜索的属性。虽然 RFC 2255 允许使用逗号分隔属性列表，但无论提供多少个属性，都仅使用第一个属性。如果没有提供任何属性，则默认使用 uid 。建议选择一个在您使用的子树中的所有条目间是唯一的属性。
scope	搜索的范围。可以是 one 或 sub 。如果未提供范围，则默认使用 sub 范围。
filter	有效的 LDAP 搜索过滤器。如果未提供，则默认为 (objectClass=*)

在进行搜索时，属性、过滤器和提供的用户名会组合在一起，创建类似如下的搜索过滤器：

```
(<filter>(<attribute>=<username>))
```



重要

如果 LDAP 目录需要身份验证才能搜索，请指定用于执行条目搜索的 **bindDN** 和 **bindPassword**。

流程

1. 在 [OpenShift Cluster Manager](#) 中，进入到 **Clusters** 页面，再选择您需要为其配置身份提供程序的集群。
2. 点 **Access control** 选项卡。
3. 点 **Add identity provider**。



注意

您还可以点在集群创建后显示的警告信息中的 **Add Oauth 配置** 链接来配置身份提供程序。

4. 从下拉菜单中选择 **LDAP**。
5. 输入身份提供程序的唯一名称。之后无法更改此名称。
6. 从下拉菜单中选择映射方法。在大多数情况下推荐使用 **声明**。
7. 输入 **LDAP URL** 以指定要使用的 LDAP 搜索参数。
8. 可选：输入 **绑定 DN** 和 **绑定密码**。

9. 输入将 LDAP 属性映射到身份的属性。
 - 输入 **ID** 属性，其值应用作用户 ID。点 **Add more** 来添加多个 ID 属性。
 - 可选：输入一个 **Preferred username** 属性，其值应用作显示名称。点 **Add more** 来添加多个首选用户名属性。
 - 可选：输入 **Email** 属性，其值应用作电子邮件地址。点 **Add more** 来添加多个电子邮件属性。
10. 可选：点 **Show advanced Options** 将证书颁发机构 (CA) 文件添加到 LDAP 身份提供程序中，以验证所配置 URL 的服务器证书。点 **Browse** 找到并附加 **CA 文件** 到身份提供程序。
11. 可选：在高级选项下，您可以选择使 LDAP 供应商**不安全**。如果您选择这个选项，则无法使用 CA 文件。



重要

如果您使用不安全的 LDAP 连接 (ldap:// 或端口 389) ,则必须在配置向导中检查 **Insecure** 选项。

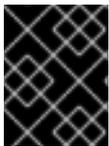
12. 单击 **Confirm**。

验证

- 配置的身份提供程序可以在 **Cluster details** 页面的 **Access control** 选项卡中看到。

3.6. 配置 OPENID 身份提供程序

配置 OpenID 身份提供程序，以使用[授权代码流](#)与 OpenID Connect 身份提供程序集成。



重要

OpenShift Dedicated 中的 Authentication Operator 要求配置 OpenID Connect 身份提供程序实现 [OpenID Connect Discovery](#) 规格。

声明可读取自从 OpenID 身份提供程序返回的 JWT **id_token** ; 若有指定，也可读取自从 Issuer URL 返回的 JSON。

必须至少配置一个声明，以用作用户的身份。

您还可以指定将哪些声明用作用户的首选用户名、显示名称和电子邮件地址。如果指定了多个声明，则使用第一个带有非空值的声明。标准的声明是：

声明	描述
preferred_username	置备用户时的首选用户名。用户希望使用的简写名称，如 janedoe 。通常，与身份验证系统中用户的登录或用户名对应的值，如用户名或电子邮件。
email	电子邮件地址。

声明	描述
name	显示名称。

如需更多信息，请参阅 [OpenID 声明文档](#)。

先决条件

- 在配置 OpenID Connect 前，请查看您要用于 OpenShift Dedicated 集群的任何红帽产品或服务的安装先决条件。

流程

- 在 [OpenShift Cluster Manager](#) 中，进入到 **Clusters** 页面，再选择您需要为其配置身份提供程序的集群。
- 点 **Access control** 选项卡。
- 点 **Add identity provider**。



注意

您还可以点在集群创建后显示的警告信息中的 **Add OAuth 配置** 链接来配置身份提供程序。

- 从下拉菜单中选择 **OpenID**。
- 输入身份提供程序的唯一名称。之后无法更改此名称。
 - 在提供的字段中自动生成 **OAuth 回调 URL**。

```
https://oauth-openshift.apps.<cluster_name>.<cluster_domain>/oauth2callback/<idp_provider_name>
```

例如：

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/openid
```
- 按照 [创建授权请求](#) 中的步骤，在 OpenID 身份提供程序中注册新的 OpenID Connect 客户端。
- 返回到 OpenShift Dedicated，然后从下拉菜单中选择映射方法。在大多数情况下推荐使用 **声明**。
- 输入 OpenID 提供的 **客户端 ID** 和 **客户端 secret**。
- 输入 **Issuer URL**。这是 OpenID 供应商断言为 Issuer 标识符的 URL。它必须使用没有 URL 查询参数或片段的 https 方案。
- 输入 **Email** 属性，其值应用作电子邮件地址。点 **Add more** 来添加多个电子邮件属性。
- 输入 **Name** 属性，其值应用作首选用户名。点 **Add more** 来添加多个首选用户名。
- 输入 **Preferred username** 属性，其值应用作显示名称。点 **Add more** 来添加多个显示名称。

13. 可选：点 **Show advanced Options** 将证书颁发机构 (CA) 文件添加到 OpenID 身份提供程序中。
14. 可选：在高级选项下，您可以添加 **其他范围**。默认情况下，请求 **OpenID** 范围。
15. 单击 **Confirm**。

验证

- 配置的身份提供程序可以在 **Cluster details** 页面的 **Access control** 选项卡中看到。

3.7. 配置 HTPASSWD 身份提供程序

配置 htpasswd 身份提供程序，以创建具有集群管理特权的单个静态用户。您可以以用户身份登录集群来排除问题。



重要

htpasswd 身份提供程序选项仅用于创建单一静态管理用户。htpasswd 不支持作为 OpenShift Dedicated 的通用身份提供程序。

流程

1. 在 [OpenShift Cluster Manager](#) 中，进入到 **Clusters** 页并选择您的集群。
2. 选择 **Access control** → **Identity provider**。
3. 点 **Add identity provider**。
4. 从 **Identity Provider** 下拉菜单中选择 **HTPasswd**。
5. 在身份提供程序的 **Name** 字段中添加唯一名称。
6. 为静态用户使用推荐的用户名和密码，或者自行创建。



注意

在以下步骤中选择 **Add** 后，此步骤中定义的凭证不可见。如果丢失了凭证，您必须重新创建身份提供程序并再次定义凭证。

7. 选择 **Add** 来创建 htpasswd 身份提供程序和单一静态用户。
8. 授予静态用户权限来管理集群：
 - a. 在 **Access control** → **Cluster Roles and Access** 下，选择 **Add user**。
 - b. 输入您在上一步中创建的静态用户的 **用户 ID**。
 - c. 选择一个组。
 - 如果您要使用 Customer Cloud Subscription (CCS) 基础架构类型安装 OpenShift Dedicated，请选择 **dedicated-admins** 或 **cluster-admins** 组。**dedicated-admins** 组中的用户具有 OpenShift Dedicated 的标准管理特权。**cluster-admins** 组中的用户对集群具有完全的管理访问权限。

- 如果您要使用 Red Hat Cloud account infrastructure 类型安装 OpenShift Dedicated, 则会自动选择 **dedicated-admins** 组。

d. 选择 **Add user** 为用户授予管理权限。

验证

- 配置的 htpasswd 身份提供程序在 **Access control** → **Identity provider** 页面中可见。



注意

创建身份提供程序后，同步通常在两分钟内完成。您可以在 htpasswd 身份提供程序可用后以用户身份登录集群。

- 单、管理用户在 **Access control** → **Cluster Roles** 和 **Access** 页面中可见。也会显示用户的管理组成员资格。

其他资源

- [客户管理员用户](#)

3.8. 访问集群

配置身份提供程序后，用户可从 Red Hat OpenShift Cluster Manager 访问集群。

先决条件

- 已登陆到 [OpenShift Cluster Manager](#)。
- 您创建了 OpenShift Dedicated 集群。
- 已为集群配置身份提供程序。
- 将您的用户帐户添加到配置的身份提供程序中。

流程

1. 在 [OpenShift Cluster Manager](#) 中点您要访问的集群。
2. 点 **Open Console**。
3. 点身份提供程序，并提供您的凭证以登录到集群。
4. 点 **Open console** 为集群打开 Web 控制台。
5. 点身份提供程序，并提供您的凭证以登录到集群。完成您的供应商提供的任何授权请求。

第 4 章 撤销权限并可以访问 OPENSIFT DEDICATED 集群

作为集群所有者，您可以撤销 admin 权限和用户对 OpenShift Dedicated 集群的访问权限。

4.1. 从用户撤销管理员权限

按照本节中的步骤从用户撤销 **dedicated-admin** 权限。

先决条件

- 已登陆到 [OpenShift Cluster Manager](#)。
- 您创建了 OpenShift Dedicated 集群。
- 您已为集群配置了 GitHub 身份提供程序，并添加了身份提供程序用户。
- 为用户授予 **dedicated-admin** 权限。

流程

1. 进入到 [OpenShift Cluster Manager](#) 并选择您的集群。
2. 点 **Access control** 选项卡。
3. 在 **Cluster Roles and Access** 选项卡中，选择用户旁的  并点 **Delete**。

验证

- 撤销权限后，用户将不再列为您的集群的 OpenShift Cluster Manager 页面中的 **Access control** → **Cluster Roles and Access** 下的 **dedicated-admins** 组的一部分。

4.2. 撤销对集群的用户访问权限

您可以将身份提供程序用户从配置的身份提供程序中删除来撤销集群访问权限。

您可以为 OpenShift Dedicated 集群配置不同类型的身份提供程序。以下示例流程为为集群配置身份的 GitHub 组织或团队的成员撤销集群访问权限。

先决条件

- 您有一个 OpenShift Dedicated 集群。
- 您有一个 GitHub 用户帐户。
- 您已为集群配置了 GitHub 身份提供程序，并添加了身份提供程序用户。

流程

1. 进入 github.com 并登录到您的 GitHub 帐户。
2. 从 GitHub 机构或团队中删除该用户：

- 如果您的身份提供程序配置使用 GitHub 组织，请按照 GitHub 文档中的[从您的机构中删除成员](#)的步骤进行操作。
- 如果您的身份提供程序配置使用 GitHub 机构中的团队，请按照 GitHub 文档中的[从团队中删除机构成员](#)的步骤进行操作。

验证

- 从身份提供程序中删除用户后，用户无法在集群中进行身份验证。

第 5 章 删除 OPENSIFT 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。

- 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 GCP 共享 VPC 中的集群，请通知主机项目的 VPC 所有者，以删除在集群创建过程中引用的服务帐户的 IAM 策略角色。