



# Red Hat Advanced Cluster Management for Kubernetes 2.1

管理集群

管理集群



## 管理集群

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

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Manage\_cluster.ent file |.

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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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

管理 Red Hat Advanced Cluster Management for Kubernetes 中的集群

# 目录

<b>第 1 章 管理集群</b> .....	<b>5</b>
<b>第 2 章 支持的云</b> .....	<b>6</b>
2.1. 支持的 HUB 集群供应商	6
2.2. 支持的受管集群供应商	6
2.3. 配置 KUBECTL	6
<b>第 3 章 调整集群大小</b> .....	<b>7</b>
3.1. AMAZON WEB SERVICES	7
3.2. GOOGLE CLOUD PLATFORM	7
3.3. MICROSOFT AZURE	7
3.4. VMWARE VSPHERE	8
3.5. 裸机集群	8
3.6. IBM KUBERNETES SERVICE	8
<b>第 4 章 发行镜像</b> .....	<b>9</b>
4.1. 同步可用发行镜像	9
4.1.1. 连接时维护自定义的发行镜像列表	10
4.1.2. 断开连接时维护自定义的发行镜像列表	11
<b>第 5 章 创建和修改裸机资产</b> .....	<b>12</b>
5.1. 先决条件	12
5.2. 使用控制台创建裸机资产	12
5.3. 修改裸机资产	13
5.4. 删除裸机资产	13
<b>第 6 章 创建供应商连接</b> .....	<b>14</b>
6.1. 为 AMAZON WEB SERVICES 创建供应商连接	14
6.1.1. 先决条件	14
6.1.2. 使用控制台创建供应商连接	14
6.1.3. 删除您的供应商连接	15
6.2. 为 MICROSOFT AZURE 创建供应商连接	15
6.2.1. 先决条件	15
6.2.2. 使用控制台创建供应商连接	16
6.2.3. 删除您的供应商连接	17
6.3. 为 GOOGLE CLOUD PLATFORM 创建供应商连接	17
6.3.1. 先决条件	17
6.3.2. 使用控制台创建供应商连接	17
6.3.3. 删除您的供应商连接	18
6.4. 为 VMWARE VSPHERE 创建供应商连接	18
6.4.1. 先决条件	18
6.4.2. 使用控制台创建供应商连接	19
6.4.3. 删除您的供应商连接	20
6.5. 为裸机创建供应商连接	20
6.5.1. 先决条件	20
6.5.2. 使用控制台创建供应商连接	20
6.5.3. 删除您的供应商连接	22
<b>第 7 章 创建集群</b> .....	<b>23</b>
7.1. 在 AMAZON WEB SERVICES 上创建集群	23
7.1.1. 先决条件	23
7.1.2. 使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群	23
7.1.3. 访问集群	24

7.2. 在 MICROSOFT AZURE 上创建集群	25
7.2.1. 先决条件	25
7.2.2. 使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群	25
7.2.3. 访问集群	26
7.3. 在 GOOGLE CLOUD PLATFORM 上创建集群	26
7.3.1. 先决条件	26
7.3.2. 使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群	27
7.3.3. 访问集群	28
7.4. 在 VMWARE VSPHERE 上创建集群	28
7.4.1. 先决条件	28
7.4.2. 使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群	29
7.4.3. 访问集群	30
7.5. 在裸机上创建集群	30
7.5.1. 先决条件	30
7.5.2. 使用 Red Hat Advanced Cluster Management 控制台创建集群	31
7.5.3. 访问集群	33
<b>第 8 章 MANAGEDCLUSTERSETS</b>	<b>34</b>
8.1. 创建 MANAGEDCLUSTERSET	34
8.2. 将集群添加到 MANAGEDCLUSTERSET	34
8.3. 从 MANAGEDCLUSTERSET 中删除受管集群	35
8.4. MANAGEDCLUSTERSETBINDING RESOURCE	35
<b>第 9 章 将目标受管集群导入到 HUB 集群</b>	<b>37</b>
9.1. 使用控制台导入现有集群	37
9.1.1. 先决条件	37
9.1.2. 导入集群	37
9.1.2.1. YAML 参数和描述	39
9.1.3. 删除导入的集群	39
9.2. 使用 CLI 导入受管集群	40
9.2.1. 先决条件	40
9.2.2. 支持的构架	40
9.2.3. 准备导入	40
9.2.4. 导入 klusterlet	42
9.3. 修改集群的 KLUSTERLET 附加设置	42
9.3.1. 使用 hub 集群中的控制台进行修改	43
9.3.2. 使用 hub 集群中的命令行进行修改	43
<b>第 10 章 配置特定的集群管理角色</b>	<b>44</b>
<b>第 11 章 升级集群</b>	<b>46</b>
11.1. 升级断开连接的集群	46
11.1.1. 先决条件	47
11.1.2. 准备断开连接的镜像 registry	47
11.1.3. 为 OpenShift Update Service 部署 Operator	47
11.1.4. 构建图形数据 init 容器	48
11.1.5. 为已镜像的 registry 配置证书	48
11.1.6. 部署 OpenShift Update Service 实例	49
11.1.7. 部署策略以覆盖默认 registry (可选)	50
11.1.8. 部署策略来部署断开连接的目录源	52
11.1.9. 部署策略以更改受管集群参数	54
11.1.10. 查看可用升级	56
11.1.11. 升级集群	56

---

<b>第 12 章 从管理中移除集群</b> .....	<b>58</b>
12.1. 使用控制台删除集群	58
12.2. 使用命令行删除集群	58
12.3. 在删除集群后删除剩余的资源	58





## 第 1 章 管理集群

了解如何通过使用 Red Hat Advanced Cluster Management for Kubernetes 控制台来跨云供应商环境中创建、导入和管理集群。

通过以下主题了解如何在跨云供应商环境中管理集群：

- [支持的云](#)
- [调整集群大小](#)
- [创建供应商连接](#)
- [创建集群](#)
- [ManagedClusterSets](#)
- [将目标受管集群导入到 hub 集群](#)
- [升级集群](#)

## 第 2 章 支持的云

了解 Red Hat Advanced Cluster Management for Kubernetes 支持的云供应商。此外，查找记录在案的可用受管供应商。

- [支持的 hub 集群供应商](#)
- [支持的受管集群供应商](#)
- [配置 kubectl](#)

**最佳实践：**对于受管集群供应商，请使用 Kubernetes 的最新版本。

### 2.1. 支持的 HUB 集群供应商

Red Hat OpenShift Container Platform 4.4.3 或更高版本、4.5.2 或更高版本、4.6.1 或更高版本都支持 hub 集群。

- 请参阅 [Amazon Web Services 上的 OpenShift](#)。

### 2.2. 支持的受管集群供应商

Red Hat OpenShift Container Platform 3.11.200 或更高版本、4.3.18 或更高版本、4.4.3 或更高版本、4.5.2 或更高版本、4.6.1 或更高版本都支持受管集群。

请参阅可用的受管集群选项和文档：

- 请参阅 [Amazon Web Services 上的 OpenShift](#)。
- 请参阅 [IBM Cloud \(Kubernetes 1.16 及更高版本\) 上的 Red Hat OpenShift](#)。
- 请参阅 [Red Hat OpenShift Kubernetes Engine](#)。
- 请参阅 [开始使用 IBM Cloud Kubernetes Service](#) (Kubernetes 1.16 及更高版本)。
- 请参阅 [Google Kubernetes Engine](#) (Kubernetes 1.15 及更高版本)。
- 请参阅 [Azure Kubernetes Service](#) (Kubernetes 1.17 及更高版本)。
- 请参阅 [Amazon Elastic Kubernetes Service](#) (Kubernetes 1.14.9 及更高版本)。
- 请参阅 [使用 Kubernetes 配置和管理的 vSphere](#)。

### 2.3. 配置 KUBECTL

对于以上列出的厂商文档，您可能需要了解如何配置 **kubectl**。当将受管集群导入到 hub 集群时，您必须已安装 **kubectl**。详情请参阅 [把目标受管集群导入到 hub 集群](#)。

## 第 3 章 调整集群大小

您可以自定义受管集群规格，如虚拟机大小和节点数量。请参阅以下列表中列出的每个可用供应商的推荐设置，但也请参阅文档的相关内容以了解更具体的信息：

### 3.1. AMAZON WEB SERVICES

您可以通过修改当前集群上的 **MachineSet** 参数来更改在 Amazon Web Services 环境中创建的 Red Hat OpenShift Container Platform 集群的节点数量。

**备注：**因为 Red Hat Advanced Cluster Management for Kubernetes 使用 Hive for OpenShift 来决定集群中的节点数量，所以您必须更改 **MachineSet** 参数来更改节点数量。如果您只删除或添加节点而无需更改 **MachineSet** 参数，则会添加或删除节点以匹配该参数的当前值。

请参阅适用于您的版本的 OpenShift Container Platform 文档中的[推荐的集群扩展实践](#)和[手动扩展 MachineSet](#)。

**提示：**如果使用 Red Hat Advanced Cluster Management 控制台创建集群，则它是一个 OpenShift Container Platform 集群。

如果要更改您导入的 Amazon EKS 集群的节点数量，请参阅[集群自动扩展](#)以了解有关扩展集群的信息。

### 3.2. GOOGLE CLOUD PLATFORM

您可以通过修改当前集群上的 **MachineSet** 参数来更改在 Google Cloud Platform 环境中创建的 OpenShift Container Platform 集群的节点数量。

**备注：**因为 Red Hat Advanced Cluster Management 使用 Hive for OpenShift 来决定集群中的节点数量，所以您必须更改 **MachineSet** 参数来更改节点数量。如果您只删除或添加节点而无需更改 **MachineSet** 参数，则会添加或删除节点以匹配该参数的当前值。

如需更多与扩展集群相关的信息，请参阅适用于您的版本的 OpenShift Container Platform 文档中的[推荐的集群扩展实践](#)和[手动扩展 MachineSet](#)。**提示：**如果使用 Red Hat Advanced Cluster Management 创建集群，则它是一个 OpenShift Container Platform 集群。

如果要更改您导入的 Google Kubernetes Engine 集群的节点数量，请参阅[调整集群大小](#)以了解有关扩展集群的信息。

### 3.3. MICROSOFT AZURE

您可以通过修改 hub 集群上的 **MachineSet** 参数来更改在 Microsoft Azure 环境中创建的 OpenShift Container Platform 集群的节点数量。

**备注：**因为 Red Hat Advanced Cluster Management 使用 Hive for OpenShift 来决定集群中的节点数量，所以您必须更改 **MachineSet** 参数来更改节点数量。如果您只删除或添加节点而无需更改 **MachineSet** 参数，则会添加或删除节点以匹配该参数的当前值。

请参阅适用于您的版本的 OpenShift Container Platform 文档中的[推荐的集群扩展实践](#)和[手动扩展 MachineSet](#)。**提示：**如果使用 Red Hat Advanced Cluster Management 创建集群，则它是一个 OpenShift Container Platform 集群。

如果要更改您导入的 Azure Kubernetes Services 集群的节点数量，请参阅[扩展集群](#)以了解有关扩展集群的信息。

## 3.4. VMWARE VSPHERE

您可以通过修改 hub 集群上的 **MachineSet** 参数来更改在 VMware vSphere 环境中创建的 OpenShift Container Platform 集群的节点数量。

**备注：**因为 Red Hat Advanced Cluster Management 使用 Hive for OpenShift 来决定集群中的节点数量，所以您必须更改 **MachineSet** 参数来更改节点数量。如果您只删除或添加节点而无需更改 **MachineSet** 参数，则会添加或删除节点以匹配该参数的当前值。

请参阅适用于您的版本的 OpenShift Container Platform 文档中的[推荐的集群扩展实践](#)和[手动扩展 MachineSet](#)。**提示：**如果使用 Red Hat Advanced Cluster Management 创建集群，则它是一个 OpenShift Container Platform 集群。

如果要更改您导入的 VMware vSphere 集群的节点数量，请参阅[Edit cluster 设置](#)以了解有关扩展集群的信息。

## 3.5. 裸机集群

您可以通过修改 hub 集群上的 **MachineSet** 参数来更改在裸机环境中创建的 OpenShift Container Platform 集群的节点数量。

**备注：**因为 Red Hat Advanced Cluster Management 使用 Hive for OpenShift 来决定集群中的节点数量，所以您必须更改 **MachineSet** 参数来更改节点数量。如果您只删除或添加节点而无需更改 **MachineSet** 参数，则会添加或删除节点以匹配该参数的当前值。

请参阅适用于您的版本的 OpenShift Container Platform 文档中的[推荐的集群扩展实践](#)和[手动扩展 MachineSet](#)。**提示：**如果使用 Red Hat Advanced Cluster Management 创建集群，则它是一个 OpenShift Container Platform 集群。

如果要更改您导入的裸机集群的节点数量，请参阅[使用网络自定义在裸机上安装集群](#)以了解有关扩展集群的信息。

**备注：**只有在 hub 集群是 OpenShift Container Platform 版本 4.5 或更高版本时才支持裸机集群。

## 3.6. IBM KUBERNETES SERVICE

如果要更改您导入的 IBM Kubernetes Service 集群的节点数量，请参阅[在集群中添加 worker 节点和区](#)以了解有关扩展集群的信息。

**备注：**因为 Red Hat Advanced Cluster Management 使用 Hive for OpenShift 来决定集群中的节点数量，所以您必须更改 **MachineSet** 参数来更改节点数量。如果您只删除或添加节点而无需更改 **MachineSet** 参数，则会添加或删除节点以匹配该参数的当前值。

## 第 4 章 发行镜像

当使用 Red Hat Advanced Cluster Management for Kubernetes 在供应商处创建集群时，您必须指定用于新集群的发行镜像。发行镜像指定使用哪个版本的 Red Hat OpenShift Container Platform 来构建集群。

引用发行镜像的文件是在 [acm-hive-openshift-releases](#) GitHub 仓库中维护的 **yaml** 文件。Red Hat Advanced Cluster Management for Kubernetes 使用这些文件在控制台中创建可用发行镜像的列表。仓库中包含 **clusterImageSets** 目录和 **subscription** 目录，它们是您使用发行镜像时使用的目录。

**clusterImageSets** 目录包含以下目录：

- **Fast** - 包含引用每个受支持 OpenShift Container Platform 版本的最新两个发行镜像版本的文件
- **Releases** - 包含引用每个受支持 OpenShift Container Platform 版本的所有发行镜像的文件。备注：这些版本尚未全部经过测试并确定是稳定的。
- **Stable** - 包含引用每个受支持 OpenShift Container Platform 版本的最新两个稳定发行镜像版本的文件此目录中的发行镜像经过测试和验证。

**subscription** 目录包含指定从哪里拉取发行镜像列表的文件。Red Hat Advanced Cluster Management 的默认发行镜像位于 Quay.io 目录中。它们被 [acm-hive-openshift-releases](#) GitHub 仓库中的文件引用。

### 4.1. 同步可用发行镜像

版本镜像会频繁更新，因此可能需要同步发行镜像列表，以确保可以选择最新的可用版本。发行镜像可在 [acm-hive-openshift-releases](#) GitHub 仓库中找到。

发行镜像有三个级别的稳定性：

表 4.1. 发行镜像的稳定性级别

类别	描述
stable	已确认用于正确安装和构建集群的完整测试镜像。
fast	部分进行了测试，但稳定性可能低于稳定版本。
candidate	最新镜像，但未经测试。可能会有一些程序错误。

完成以下步骤以刷新列表：

1. 克隆 [acm-hive-openshift-releases](#) GitHub 仓库。
2. 输入以下命令连接到稳定版本镜像并同步您的 Red Hat Advanced Cluster Management for Kubernetes hub 集群：

```
make subscribe-stable
```

备注：您只能在使用 Linux 或者 MacOS 操作系统时运行这个 **make** 命令。大约一分钟后，最新的 **stable** 项将可用。

- 要同步并显示快速发行镜像，请输入以下命令：

```
■
```

```
make subscribe-fast
```

备注：您只能在使用 Linux 或者 MacOS 操作系统时运行这个 **make** 命令。

运行此命令后，当前可用的镜像会在约一分钟内可在可用的 **stable** 和 **fast** 发行镜像列表中出现。

- 要同步并显示 **candidate** 发行镜像，请输入以下命令：

```
make subscribe-candidate
```

备注：您只能在使用 Linux 或者 MacOS 操作系统时运行这个 **make** 命令。

运行该命令后，当前可用的镜像会更新可用的 **stable**、**fast** 和 **candidate** 发行镜像列表。

3. 在创建集群时，查看 Red Hat Advanced Cluster Management 控制台中当前可用发行镜像的列表。
4. 使用以下格式输入命令来从这些频道中取消订阅以停止查看更新：

```
oc delete -f subscription/subscription-stable
```

#### 4.1.1. 连接时维护自定义的发行镜像列表

您可能希望确保所有集群都使用同一发行镜像。为简化操作，您可以创建自己的自定义列表，在其中包含创建集群时可用的发行镜像。完成以下步骤以管理可用发行镜像：

1. 对 [acm-hive-openshift-releases GitHub 仓库](#) 进行分叉 (fork)。
2. 将 **spec: pathname** 更改为访问已分叉的仓库的 GitHub 名称，而不是 **open-cluster-management**，由此来更新 **./subscription/channel.yaml** 文件。此步骤指定 hub 集群在哪里检索发行镜像。您更新的内容应类似以下示例：

```
spec:
  type: GitHub
  pathname: https://github.com/<forked_content>/acm-hive-openshift-releases.git
```

将 *forked\_content* 替换为已分叉仓库的路径。

3. 使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群时，为您希望可用的镜像添加 **yaml** 文件到 **./clusterImageSets/stable/** 或 **./clusterImageSets/fast/\*** 目录。\*Tip:您可以通过将更改合并到已分叉的存储库，从主存储库检索可用的 **yaml** 文件。
4. 将更改提交并合并到您的已分叉仓库。
5. 在克隆了 **acm-hive-openshift-releases** 仓库后，使用以下命令来更新 **stable** 镜像以同步 **stable** 发行镜像列表：

```
make subscribe-stable
```

备注：您只能在使用 Linux 或者 MacOS 操作系统时运行这个 **make** 命令。如果使用 Windows 操作系统，输入以下命令：

```
oc apply -k subscription/
oc delete -f subscription/subscription-fast.yaml
oc apply -f subscription/subscription-stable.yaml
```

运行此命令后，可用稳定镜像列表会在约一分钟内更新为当前可用镜像。

- 默认情况下，仅会列出稳定镜像。要同步并显示快速发行镜像，请输入以下命令：

```
make subscribe-fast
```

备注：您只能在使用 Linux 或者 MacOS 操作系统时运行这个make 命令。如果使用 Windows 操作系统，输入以下命令：

```
oc apply -k subscription/
oc apply -f subscription/subscription-fast.yaml
```

运行此命令后，可用快速镜像列表会在约 1 分钟内更新为当前可用镜像。

- 默认情况下，Red Hat Advanced Cluster Management 会预加载几个 ClusterImageSets。使用以下命令列出可用内容并删除默认值（如果需要）。

```
oc get clusterImageSets
oc delete clusterImageSet <clusterImageSet_NAME>
```

- 在创建集群时，查看 Red Hat Advanced Cluster Management 控制台中当前可用发行镜像的列表。

#### 4.1.2. 断开连接时维护自定义的发行镜像列表

在某些情况下，当节点集群没有互联网连接时，您需要维护一个自定义的发行镜像列表。您可以创建自己的自定义列表，在其中包含创建集群时可用的发行镜像。完成以下步骤以在断开连接的情况下管理可用发行镜像：

- 在连接的系统上，导航到 [acm-hive-openshift-releases GitHub 仓库](#)。
- 将 `clusterImageSets` 目录复制到可以访问断开连接的 Red Hat Advanced Cluster Management for Kubernetes hub 集群的系统中。
- 对于您希望在使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群时可用的镜像，通过手动添加 `clusterImageSet` YAML 内容来添加其 `yaml` 文件。
- 创建 `clusterImageSets` 命令：

```
oc create -f <clusterImageSet_FILE>
```

在为您要添加的每个资源运行此命令后，可用发行镜像列表将变为可用。

- 另外，您还可以将镜像 url 直接粘贴到 Red Hat Advanced Cluster Management 的创建集群控制台中。这将创建新的 `clusterImageSets`（如果此前不存在）。
- 在创建集群时，查看 Red Hat Advanced Cluster Management 控制台中当前可用发行镜像的列表。



## 第 5 章 创建和修改裸机资产

裸机资产是指被配置为运行您的云操作的虚拟服务器或物理服务器。Red Hat Advanced Cluster Management for Kubernetes 将连接到您的管理员创建的裸机资产，并可在其上创建集群。

您必须在 Red Hat Advanced Cluster Management for Kubernetes 中创建裸机资产，以便在其上创建集群。使用以下步骤创建运行由 Red Hat Advanced Cluster Management for Kubernetes 管理的集群的裸机资产。

### 5.1. 先决条件

创建裸机资产前需要满足以下先决条件：

- 在 OpenShift Container Platform 版本 4.5 或更高版本上部署了 Red Hat Advanced Cluster Management for Kubernetes hub 集群。
- 可访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群以连接到裸机资产。
- 配置了裸机资产，以及登录凭证（包含登录和管理该资产所需的权限）。备注：裸机资产的登录凭证包括您的管理员为资产提供的以下项：
  - 用户名
  - 密码
  - 基板管理控制器地址
  - 引导 NIC MAC 地址

### 5.2. 使用控制台创建裸机资产

要使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建裸机资产，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Bare metal assets。
2. 在 *Bare metal assets* 页面上，点击 Create bare metal resources。
3. 为资产输入一个名称，用于在创建集群时标识它。  
提示：要在您在控制台中输入信息时查看 yaml 内容更新，可将 YAML 开关设置为 ON。
4. 输入要用来创建裸机资源的命名空间。  
备注：裸机资产、受管裸机集群及其相关 secret 必须位于同一命名空间中。

有权访问此命名空间的用户可以在创建集群时将此资产与集群相关联。

5. 输入基板管理控制器地址。这是实现与主机通信的控制器。支持以下协议：
  - IPMI，如需更多信息，请参阅 [IPMI 2.0 规格](#)。
  - iDRAC，如需更多信息，请参阅 [Dell Remote Access Controller 9 \(iDRAC9\) 的支持](#)。
  - iRMC，请参阅 [Data Sheet:FUJITSU Software ServerView Suite 集成 Remote Management Controller - iRMC S5](#) 了解更多信息。
  - Redfish，如需更多信息，请参阅 [Redfish 规格](#)。



6. 为裸机资产输入用户名和密码。
7. 为裸机资产添加引导 NIC MAC 地址。这是主机的联网 NIC 的 MAC 地址，用于在裸机资产上置备主机。

您可以继续在[裸机上创建集群](#)。

### 5.3. 修改裸机资产

如果您需要修改裸机资产的设置，请完成以下步骤：

1. 在 Red Hat Advanced Cluster Management for Kubernetes 控制台导航中选择：Automate infrastructure > Bare metal asset
2. 选择表中您要修改的资产的选项菜单。
3. 选择 Modify。

### 5.4. 删除裸机资产

当裸机资产不再用于任何集群时，您可以将其从可用的裸机资产列表中删除。删除未使用的资产既可以简化您的可用资产列表，又可以防止意外选择该资产。

要删除裸机资产，请完成以下步骤：

1. 在 Red Hat Advanced Cluster Management for Kubernetes 控制台导航中选择：Automate infrastructure > Bare metal asset
2. 选择表中要删除的资产的选项菜单。
3. 选择 Delete。

## 第 6 章 创建供应商连接

要使用 Red Hat Advanced Cluster Management for Kubernetes 在云服务供应商处创建 Red Hat OpenShift Container Platform 集群，需要具有 [供应商连接](#)。

供应商连接存储供应商的访问凭证和配置信息。每个供应商帐户都需要其自身的供应商连接，就像单个供应商的每个域一样。

以下文件详细介绍了为每个受支持供应商创建连接文档所需的信息：

- [为 Amazon Web Services 创建供应商连接](#)
- [为 Microsoft Azure 创建供应商连接](#)
- [为 Google Cloud Platform 创建供应商连接](#)
- [为 VMware vSphere 创建供应商连接](#)
- [为裸机创建供应商连接](#)

### 6.1. 为 AMAZON WEB SERVICES 创建供应商连接

您需要具有供应商连接才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 Amazon Web Services (AWS) 上部署和管理 OpenShift 集群。

备注：这个过程必须在使用 Red Hat Advanced Cluster Management for Kubernetes 创建集群之前完成。

#### 6.1.1. 先决条件

创建供应商连接前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在 Amazon Web Services 上创建 Kubernetes 集群
- Amazon Web Services (AWS) 登录凭证，其中包括访问密钥 ID 和 secret 访问密钥。请参[阅了解和获取您的安全凭证](#)。
- 允许在 AWS 上安装集群的帐户权限。有关如何配置的说明，请参[阅配置 AWS 帐户](#)。

#### 6.1.2. 使用控制台创建供应商连接

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建供应商连接，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 在 Clusters 页面上，选择 *Provider connections* 选项卡。此时会显示现有供应商连接。
3. 选择 Add a connection。
4. 选择 Amazon Web Services 作为您的供应商。

5. 为供应商连接添加名称。
6. 从列表中为您的供应商连接选择一个命名空间。  
提示：为方便起见，同时为了提高安全性，创建一个命名空间，专门用于托管您的供应商连接。
7. 另外，您还可以为您的供应商连接添加基本 DNS 域。如果您将基本 DNS 域添加到供应商连接中，则当使用这个供应商连接创建集群时，会自动填充到正确的字段中。
8. 为您的 Amazon Web Services 帐户添加 AWS 访问密钥 ID。登录 [AWS](#) 以查找该 ID。
9. 添加 AWS Secret 访问密钥。
10. 输入 Red Hat OpenShift Pull Secret。您可以从 [Pull secret](#) 下载 pull secret。
11. 添加可让您连接到集群的 SSH 私钥和 SSH 公钥。您可以使用现有密钥对，或使用密钥生成程序创建新密钥对。请参阅 [生成 SSH 私钥并将其添加到代理中](#)，以了解有关如何生成密钥的更多信息。
12. 点击 Create。当您创建供应商连接时，会将其添加到供应商连接列表中。

要创建使用此供应商连接的集群，您可以完成在 [Amazon Web Services 上创建集群](#) 中的步骤。

### 6.1.3. 删除您的供应商连接

当您不再管理使用某个供应商连接的集群时，请删除供应商连接以保护供应商连接中的信息。

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 选择 Provider connections。
3. 选择您要删除的供应商连接旁的选项菜单。
4. 选择 Delete connection。

## 6.2. 为 MICROSOFT AZURE 创建供应商连接

您需要具有供应商连接才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 Microsoft Azure 上创建和管理 Red Hat OpenShift Container Platform 集群。

备注：这个过程是使用 Red Hat Advanced Cluster Management for Kubernetes 创建集群的先决条件。

### 6.2.1. 先决条件

创建供应商连接前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在 Azure 上创建 Kubernetes 集群
- Azure 登录凭证，其中包括您的基域资源组和 Azure Service Principal JSON。请参阅 [azure.microsoft.com](https://azure.microsoft.com)。
- 允许在 Azure 上安装集群的帐户权限。如需更多信息，请参阅 [如何配置 Cloud Services](#) 和 [配置 Azure 帐户](#)。

## 6.2.2. 使用控制台创建供应商连接

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建供应商连接，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 在 *Clusters* 页面上，选择 *Provider connections* 选项卡。  
此时会显示现有供应商连接。
3. 选择 Add a connection。
4. 选择 Microsoft Azure 作为您的供应商。
5. 为供应商连接添加名称。
6. 从列表中为您的供应商连接选择一个命名空间。  
提示：为方便起见，同时为了提高安全性，您可以创建一个命名空间，专门用于托管您的供应商连接。
7. 另外，您还可以为您的供应商连接添加基本 DNS 域。如果您将基本 DNS 域添加到供应商连接中，则当使用这个供应商连接创建集群时，会自动填充到正确的字段中。
8. 为您的 Azure 帐户添加基域资源组名称。此条目是您使用 Azure 帐户创建的资源名称。您可以在 Azure 界面中选择 Home > DNS Zones 来查找您的基域资源组名称。您的基域资源组名称位于条目的 *Resource Group* 列中，其中包含应用到您帐户的基本 DNS 域。
9. 添加您的客户端 ID。当您使用以下命令创建服务主体时，这个值作为 `appid` 属性被生成：

```
az ad sp create-for-rbac --role Contributor --name <service_principal>
```

将 `service_principal` 替换为您的服务主体名。

10. 添加您的客户端 Secret。当您使用以下命令创建服务主体时，这个值作为 `password` 属性被生成：

```
az ad sp create-for-rbac --role Contributor --name <service_principal>
```

将 `service_principal` 替换为您的服务主体名。

11. 添加您的订阅 ID。这个值是以下命令输出中的 `id` 属性：

```
az account show
```

12. 添加您的租户 ID。这个值是以下命令输出中的 `tenantId` 属性：

```
az account show
```

13. 输入 Red Hat OpenShift Pull Secret。您可以从 [Pull secret](#) 下载 pull secret。
14. 添加用于连接到集群的 SSH 私钥和 SSH 公钥。您可以使用现有密钥对，或使用密钥生成程序创建新密钥对。请参阅[生成 SSH 私钥并将其添加到代理中](#)，以了解有关如何生成密钥的更多信息。
15. 点击 Create。当您创建供应商连接时，会将其添加到供应商连接列表中。

要创建使用此供应商连接的集群，您可以完成在 [Microsoft Azure 上创建集群](#) 中的步骤。

### 6.2.3. 删除您的供应商连接

当您不再管理使用某个供应商连接的集群时，请删除供应商连接以保护供应商连接中的信息。

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 选择 Provider connections。
3. 选择您要删除的供应商连接的选项菜单。
4. 选择 Delete connection。

## 6.3. 为 GOOGLE CLOUD PLATFORM 创建供应商连接

您需要具有供应商连接才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 Google Cloud Platform (GCP) 上创建和管理 Red Hat OpenShift Container Platform 集群。

备注：这个过程是使用 Red Hat Advanced Cluster Management for Kubernetes 创建集群的先决条件。

### 6.3.1. 先决条件

创建供应商连接前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在 GCP 上创建 Kubernetes 集群
- GCP 登录凭证，其中包括用户 Google Cloud Platform 项目 ID 和 Google Cloud Platform 服务帐户 JSON 密钥。请参阅[创建和管理项目](#)。
- 允许在 GCP 上安装集群的帐户权限。有关如何配置帐户的说明，请参阅[配置 GCP 项目](#)。

### 6.3.2. 使用控制台创建供应商连接

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建供应商连接，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 在 Clusters 页面上，选择 *Provider connections* 选项卡。  
此时会显示现有供应商连接。
3. 选择 Add a connection。
4. 选择 Google Cloud Platform 作为您的供应商。
5. 为供应商连接添加名称。
6. 从列表中为您的供应商连接选择一个命名空间。  
提示：为方便和安全起见，创建一个命名空间，专门用于托管您的供应商连接。
7. 另外，您还可以为您的供应商连接添加基本 DNS 域。如果您将基本 DNS 域添加到供应商连接中，则当使用这个供应商连接创建集群时，会自动填充到正确的字段中。

8. 为您的 GCP 帐户添加 *Google Cloud Platform 项目 ID*。登录到 [GCP](#) 以检索您的设置。
9. 添加 *Google Cloud Platform 服务帐户 JSON 密钥* 完成以下步骤创建带有正确权限的服务帐户：
  - a. 在 GCP 主菜单中，选择 IAM & Admin 并启动 Service Accounts applet。
  - b. 选择 Create Service Account。
  - c. 提供服务帐户的 *Name*、*Service account ID* 和 *Description*。
  - d. 选择 Create 来创建服务帐户。
  - e. 选择 Owner 角色，然后点 Continue。
  - f. 点 Create Key
  - g. 选择 JSON 并点 Create。
  - h. 将生成的文件保存到您的计算机中。
  - i. 提供 *Google Cloud Platform 服务帐户 JSON 密钥* 的内容。
10. 输入 *Red Hat OpenShift Pull Secret*。您可以从 [Pull secret](#) 下载 pull secret。
11. 添加 *SSH 私钥* 和 *SSH 公钥* 以便您访问集群。您可以使用现有密钥对，或使用密钥生成程序创建新密钥对。请参阅 [生成 SSH 私钥并将其添加到代理中](#)，以了解有关如何生成密钥的更多信息。
12. 点击 Create。当您创建供应商连接时，会将其添加到供应商连接列表中。

要在创建集群时使用此连接，您可以完成在 [Google Cloud Platform 上创建集群](#) 中的步骤。

### 6.3.3. 删除您的供应商连接

当您不再管理使用某个供应商连接的集群时，请删除供应商连接以保护供应商连接中的信息。

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 选择 Provider connections。
3. 选择您要删除的供应商连接旁的选项菜单。
4. 选择 Delete connection。

## 6.4. 为 VMWARE VSPHERE 创建供应商连接

您需要具有供应商连接才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 VMware vSphere 上部署和管理 Red Hat OpenShift Container Platform 集群。备注：仅支持 OpenShift Container Platform 版本 4.5.x 及更新的版本。

备注：此流程必须在使用 Red Hat Advanced Cluster Management 创建集群前完成。

### 6.4.1. 先决条件

创建供应商连接前必须满足以下先决条件：



- 在 OpenShift Container Platform 版本 4.5 或更高版本上部署了 Red Hat Advanced Cluster Management hub 集群。
- 可通过互联网访问 Red Hat Advanced Cluster Management hub 集群，以便它在 VMware vSphere 上创建 Kubernetes 集群。
- 使用安装程序置备的基础架构时为 OpenShift Container Platform 配置了 VMware vSphere 登录凭证和 vCenter 要求。请参阅在 [vSphere 上安装集群](#)。这些凭证包括以下信息：
  - vCenter 帐户权限。
  - 集群资源。
  - DHCP 可用。
  - ESXi 主机的时间已同步（例如：NTP）。

### 6.4.2. 使用控制台创建供应商连接

要从 Red Hat Advanced Cluster Management 控制台创建供应商连接，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 在 Clusters 页面上，选择 *Provider connections* 选项卡。  
此时会显示现有供应商连接。
3. 选择 Add a connection。
4. 选择 VMware vSphere 作为您的供应商。
5. 为供应商连接添加名称。
6. 从列表中为您的供应商连接选择一个命名空间。  
提示：为方便起见，同时为了提高安全性，创建一个命名空间，专门用于托管您的供应商连接。
7. 另外，您还可以为您的供应商连接添加基本 DNS 域。如果您将基本 DNS 域添加到供应商连接中，则当使用这个供应商连接创建集群时，会自动填充到正确的字段中。
8. 添加 VMware vCenter 服务器完全限定主机名或 IP 地址。该值必须在 vCenter 服务器 root CA 证书中定义。如果可能，请使用完全限定主机名。
9. 添加 VMware vCenter 用户名。
10. 添加 VMware vCenter 密码。
11. 添加 VMware vCenter root CA 证书
  - a. 您可以使用 VMware vCenter 服务器的证书在 download.zip 软件包中下载证书，地址为 [https://<vCenter\\_address>/certs/download.zip](https://<vCenter_address>/certs/download.zip)。将 vCenter\_address 替换为 vCenter 服务器的地址。
  - b. 解包 download.zip。
  - c. 使用 certs/<platform> 目录中包含 .0 扩展名的证书。提示：您可以使用 ls certs/<platform> 命令列出平台的所有可用证书。  
将 <platform> 替换为您的平台的缩写：lin、mac 或 win。

例如：`certs/lin/3a343545.0`

12. 添加 *VMware vSphere 集群名称*
13. 添加 *VMware vSphere 数据中心*
14. 添加 *VMware vSphere 默认数据存储*
15. 输入 *Red Hat OpenShift Pull Secret*。您可以从 [Pull secret](#) 下载 pull secret。
16. 添加可让您连接到集群的 *SSH 私钥和 SSH 公钥*。您可以使用现有密钥对，或使用密钥生成程序创建新密钥对。如需更多信息，请参阅[生成 SSH 私钥并将其添加到代理中](#)。
17. 点击 Create。当您创建供应商连接时，会将其添加到供应商连接列表中。

要创建使用此供应商连接的集群，完成在 [VMware vSphere 上创建集群](#) 中的步骤。

### 6.4.3. 删除您的供应商连接

当您不再管理使用某个供应商连接的集群时，请删除供应商连接以保护供应商连接中的信息。

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 选择 Provider connections。
3. 选择您要删除的供应商连接旁的选项菜单。
4. 选择 Delete connection。

## 6.5. 为裸机创建供应商连接

您需要具有供应商连接才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在裸机环境中部署和管理 Red Hat OpenShift Container Platform 集群。

### 6.5.1. 先决条件

创建供应商连接前需要以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群。在管理裸机集群时，必须在 Red Hat OpenShift Container Platform 版本 4.5 或更高版本上安装了 hub 集群。
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在裸机服务器上创建 Kubernetes 集群
- 您的裸机服务器登录凭证，其中包括 libvirt URI、SSH 私钥和 SSH 已知主机列表；请参阅[生成 SSH 私钥并将其添加到代理中](#)
- 允许在裸机基础架构上安装集群的帐户权限

### 6.5.2. 使用控制台创建供应商连接

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建供应商连接，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。



2. 在 *Clusters* 页面上，选择 *Provider connections* 选项卡。  
此时会显示现有供应商连接。
3. 选择 *Add connection*。
4. 选择 *Bare metal* 作为您的供应商。
5. 为供应商连接添加名称。
6. 从列表中为您的供应商连接选择一个命名空间。  
提示：为方便起见，同时为了提高安全性，创建一个命名空间，专门用于托管您的供应商连接。
7. 另外，您还可以为您的供应商连接添加基本 DNS 域。如果您将基本 DNS 域添加到供应商连接中，则当使用这个供应商连接创建集群时，会自动填充到正确的字段中。
8. 添加 *libvirt* URL。如需更多信息，请参阅 [连接 URL](#)。
9. 输入 *Red Hat OpenShift Pull Secret*。您可以从 [Pull secret](#) 下载 pull secret。
10. 添加 *SSH 私钥* 和 *SSH 公钥* 以便您访问集群。您可以使用现有密钥，或使用密钥生成程序创建新密钥。请参阅 [生成 SSH 私钥并将其添加到代理中](#)，以了解有关如何生成密钥的更多信息。
11. 添加您的 SSH 已知主机列表。
12. 只适用于断开连接的安装：使用所需信息，为断开连接的安装完成配置 部分中的字段：
  - **镜像 Registry 镜像**：这个值包含断开连接的 registry 路径。该路径包含所有用于断开连接的安装镜像的主机名、端口和库路径。示例：`repository.com:5000/openshift/ocp-release`。该路径会在 `install-config.yaml` 中创建一个到 Red Hat OpenShift Container Platform 发行镜像的镜像内容源策略映射。例如，`repository.com:5000` 生成此 `imageContentSource` 内容：
 

```
imageContentSources:
- mirrors:
  - registry.example.com:5000/ocp4
  source: quay.io/openshift-release-dev/ocp-release-nightly
- mirrors:
  - registry.example.com:5000/ocp4
  source: quay.io/openshift-release-dev/ocp-release
- mirrors:
  - registry.example.com:5000/ocp4
  source: quay.io/openshift-release-dev/ocp-v4.0-art-dev
```
  - **Bootstrap OS 镜像**：此值包含用于 bootstrap 机器的镜像的 URL。
  - **集群操作系统镜像**：此值包含用于 Red Hat OpenShift Container Platform 集群机器的镜像的 URL。
  - **其他 Trust Bundle**：此值提供访问镜像 registry 所需的证书文件内容。  
备注：如果您要从断开连接的环境中的 hub 部署受管集群，并希望在安装后自动导入它们，请使用 `YAML` 编辑器将 `Image Content Source Policy` 添加到 `install-config.yaml` 文件中。以下示例中显示了一个示例：

```
imageContentSources:
- mirrors:
  - registry.example.com:5000/rhacm2
```

source: registry.redhat.io/rhacm2

13. 点 **Create**。当您创建供应商连接时，会将其添加到供应商连接列表中。

要创建使用此供应商连接的集群，您可以完成[在裸机上创建集群](#)中的步骤。

### 6.5.3. 删除您的供应商连接

当您不再管理使用某个供应商连接的集群时，请删除供应商连接以保护供应商连接中的信息。

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 选择 Provider connections。
3. 选择您要删除的供应商连接旁的选项菜单。
4. 选择 Delete connection。

## 第 7 章 创建集群

了解如何使用 Red Hat Advanced Cluster Management for Kubernetes 跨云供应商创建 Red Hat OpenShift Container Platform 集群。

- [在 Amazon Web Services 上创建集群](#)
- [在 Google Cloud Platform 上创建集群](#)
- [在 Microsoft Azure 上创建集群](#)
- [在 VMware vSphere 上创建集群](#)
- [在裸机上创建集群](#)

### 7.1. 在 AMAZON WEB SERVICES 上创建集群

您可以使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 Amazon Web Services (AWS) 上创建一个 Red Hat OpenShift Container Platform 集群。

#### 7.1.1. 先决条件

在 AWS 上创建集群前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在 Amazon Web Services 上创建 Kubernetes 集群
- AWS 供应商连接。如需更多信息，请参阅[为 Amazon Web Services 创建供应商连接](#)。
- 在 AWS 中配置了域。有关如何配置域的说明，请参阅[配置 AWS 帐户](#)。
- Amazon Web Services (AWS) 登录凭证，其中包括用户名、密码、访问密钥 ID 和 secret 访问密钥。请参阅[了解和获取您的安全凭证](#)。
- Red Hat OpenShift Container Platform 镜像 pull secret。请参阅[使用镜像 pull secret](#)。

备注：如果更改了云供应商访问密钥，则必须手动更新置备的集群访问密钥。如需更多信息，请参阅[已知问题](#)，[不支持置备的集群的自动 secret 更新](#)。

#### 7.1.2. 使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 在 Clusters 页面上，点击 Add Cluster。
3. 选择 Create a cluster。  
备注：此过程用于创建集群。如果您有一个要导入的现有集群，请参阅[将目标受管集群导入到 hub 集群](#)以了解这些步骤。
4. 为集群输入一个名称。此名称用于集群的主机名。  
提示：要在您在控制台中输入信息时查看 yaml 内容更新，可将 YAML 开关设置为 ON。

5. 为基础架构平台选择 Amazon Web Services。
6. 指定您要用于集群的发行镜像。这可标识用于创建集群的 Red Hat OpenShift Container Platform 镜像的版本。如果要使用的版本可用，您可以从镜像列表中选择镜像。如果您要使用的镜像不是标准镜像，您可以输入您要使用的镜像的 url。有关发行镜像的更多信息，请参阅[发行镜像](#)。
7. 从列表上的可用连接中选择您的供应商连接。如果您没有配置供应商连接，或想要配置一个新供应商连接，请参阅[添加连接](#)。如需了解更多与创建供应商相关的信息，请参阅[为 Amazon Web Services 创建供应商连接](#)。
8. 输入您为 AWS 帐户配置的基域信息。如果已有与所选供应商连接关联的基域，则该值会在那个字段中填充。您可以修改它的值来覆盖它。如需更多信息，请参阅[配置 AWS 帐户](#)。此名称用于集群的主机名。
9. 添加您要与集群关联的 *标签 (Label)*。这些标签有助于识别集群并限制搜索结果。
10. 为集群配置 *节点池*。  
节点池定义用于集群的节点的位置和大小。  
  
*区域*指定节点所处的地理位置。距离更近的区域可能会提供更快的性能，但距离更远的区域可能更为分散。
  - **Master 池**：master 池中为您的集群创建三个 Master 节点。Master 节点共享集群活动的管理。您可以选择区域中的多个区以实现更为分散的 master 节点组。您可在创建实例后更改实例的类型和大小，但也可以在此部分中指定。默认值为 *mx4.xlarge - 4 vCPU, 16 GiB RAM - 通用目的*，根存储为 500 GiB。
  - **Worker 池**：您可以在 worker 池中创建一个或多个 worker 节点，以运行集群的容器工作负载。它们可以位于单个 worker 池中，也可以分布在多个 worker 池中。
11. 可选：配置集群网络选项。
12. 可选：为集群配置标签。
13. 点 Create。在创建和导入过程完成后，您可以查看您的集群详情。  
备注：您不必运行 `kubectl` 命令，它为导入集群提供集群的详情。当创建集群时，它由 Red Hat Advanced Cluster Management for Kubernetes 管理自动配置。

### 7.1.3. 访问集群

要访问由 Red Hat Advanced Cluster Management for Kubernetes 管理的集群，请完成以下步骤：

1. 从 Red Hat Advanced Cluster Management for Kubernetes 导航菜单中导航到 Automate infrastructure > Clusters。
2. 选择您创建的或想要访问的集群的名称。此时会显示集群详情。
3. 选择 Reveal credentials 来查看集群的用户名和密码。记下这些值以便在登录到集群时使用。
4. 选择 Console URL 以链接到集群。
5. 使用在第 3 步中找到的用户 ID 和密码登录集群。
6. 为您要访问的集群选择 Actions > Launch to cluster。  
提示：如果知道登录凭证，可以通过为您要访问的集群选择 Actions > Launch to cluster 来访问集群。

## 7.2. 在 MICROSOFT AZURE 上创建集群

您可以使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 Microsoft Azure 上部署一个 Red Hat OpenShift Container Platform 集群。

### 7.2.1. 先决条件

在 Azure 上创建集群前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在 Azure 上创建 Kubernetes 集群
- Azure 供应商连接。如需更多信息，请参阅为 [Microsoft Azure 设置供应商连接](#)。
- 在 Azure 中配置了域。有关如何配置域的说明，请参阅为 [Azure 云服务配置自定义域名](#)。
- Azure 登录凭证，其中包括用户名和密码。请参阅 [azure.microsoft.com](#)。
- Azure 服务主体，其中包括 `clientId`、`clientSecret` 和 `tenantId`。请参阅 [azure.microsoft.com](#)。
- Red Hat OpenShift Container Platform 镜像 pull secret。请参阅 [使用镜像 pull secret](#)。

备注：如果更改了云供应商访问密钥，则必须手动更新置备的集群访问密钥。如需更多信息，请参阅已知问题，[不支持置备的集群的自动 secret 更新](#)。

### 7.2.2. 使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 在 *Clusters* 页面上，点击 Add Cluster。
3. 选择 Create a cluster。  
备注：此过程用于创建集群。如果您有一个要导入的现有集群，请参阅[将目标受管集群导入到 hub 集群](#)以了解这些步骤。
4. 为集群输入一个名称。此名称用于集群的主机名。  
提示：要在您在控制台中输入信息时查看 `yaml` 内容更新，可将 `YAML` 开关设置为 ON。
5. 为基础架构平台选择 Microsoft Azure。
6. 指定您要用于集群的发行镜像。这可标识用于创建集群的 Red Hat OpenShift Container Platform 镜像的版本。如果要使用的版本可用，您可以从镜像列表中选择镜像。如果您要使用的镜像不是标准镜像，您可以输入您要使用的镜像的 `url`。有关发行镜像的更多信息，请参阅[发行镜像](#)。
7. 从列表上的可用连接中选择您的供应商连接。如果您没有配置供应商连接，或想要配置一个新供应商连接，请参阅[添加连接](#)。如需了解更多与创建供应商相关的信息，请参阅为 [Microsoft Azure 创建供应商连接](#)。
8. 输入您为 Azure 帐户配置的基域信息。如果已有与所选供应商连接关联的基域，则该值会在那个字段中填充。您可以修改它的值来覆盖它。如需更多信息，请参阅为 [Azure 云服务配置自定义域名](#)。此名称用于集群的主机名。

9. 添加您要与集群关联的 **标签 (Label)**。这些标签有助于识别集群并限制搜索结果。
10. 为集群配置 **节点池**。  
节点池定义用于集群的节点的位置和大小。

**区域**指定节点所处的地理位置。距离更近的区域可能会提供更快性能，但距离更远的区域可能更为分散。

- **Master 池**：master 池中为您的集群创建三个 Master 节点。Master 节点共享集群活动的管理。您可以选择区域中的多个区以实现更为分散的 master 节点组。您可在创建实例后更改实例的类型和大小，但也可以在此部分中指定。默认值为 *Standard\_D2s\_v3 - 2 vCPU, 8 GiB RAM - 通用目的*，根存储为 512 GiB。
  - **Worker 池**：您可以在 worker 池中创建一个或多个 worker 节点，以运行集群的容器工作负载。它们可以位于单个 worker 池中，也可以分布在多个 worker 池中。
11. 可选：配置集群网络选项。
  12. 可选：为集群配置标签。
  13. 点 **Create**。在创建和导入过程完成后，您可以查看您的集群详情。  
备注：您不必运行 `kubectl` 命令，它为导入集群提供集群的详情。当创建集群时，它由 Red Hat Advanced Cluster Management for Kubernetes 管理自动配置。

### 7.2.3. 访问集群

要访问由 Red Hat Advanced Cluster Management for Kubernetes 管理的集群，请完成以下步骤：

1. 从 Red Hat Advanced Cluster Management for Kubernetes 导航菜单中导航到 **Automate infrastructure > Clusters**。
2. 选择您创建的或想要访问的集群的名称。此时会显示集群详情。
3. 选择 **Reveal credentials** 来查看集群的用户名和密码。记下这些值以便在登录到集群时使用。
4. 选择 **Console URL** 以链接到集群。
5. 使用在第 3 步中找到的用户 ID 和密码登录集群。
6. 为您要访问的集群选择 **Actions > Launch to cluster**。  
提示：如果知道登录凭证，可以通过为您要访问的集群选择 **Actions > Launch to cluster** 来访问集群。

## 7.3. 在 GOOGLE CLOUD PLATFORM 上创建集群

按照步骤在 Google Cloud Platform (GCP) 上创建 Red Hat OpenShift Container Platform 集群有关 Google Cloud Platform 的更多信息，请参阅 [Google Cloud Platform](#)。

### 7.3.1. 先决条件

在 GCP 上创建集群前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在 GCP 上创建 Kubernetes 集群



- GCP 供应商连接。如需更多信息，请参阅[Google Cloud Platform 设置供应商连接](#)。
- 在 GCP 中配置了域。有关如何配置域的说明，请参阅[设置自定义域](#)。
- GCP 登录凭证，其中包括用户名和密码。
- Red Hat OpenShift Container Platform 镜像 pull secret。请参阅[使用镜像 pull secret](#)。

备注：如果更改了云供应商访问密钥，则必须手动更新置备的集群访问密钥。如需更多信息，请参阅[已知问题](#)，[不支持置备的集群的自动 secret 更新](#)。

### 7.3.2. 使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 在 *Clusters* 页面上，点击 Add Cluster。
3. 选择 Create a cluster。  
备注：此过程用于创建集群。如果您有一个要导入的现有集群，请参阅[将目标受管集群导入到 hub 集群](#)以了解这些步骤。
4. 为集群输入一个名称。在命名 GCP 集群时有一些限制。这些限制包括，名称不要以 goog 开始；名称的任何部分都不要包含与 google 类似的内容。如需了解完整的限制列表，请参阅[Bucket 命名指南](#)。  
此名称用于集群的主机名。

提示：要在您在控制台中输入信息时查看 yaml 内容更新，可将 YAML 开关设置为 ON。

5. 为基础架构平台选择 Google Cloud。
6. 指定您要用于集群的发行镜像。这可标识用于创建集群的 Red Hat OpenShift Container Platform 镜像的版本。如果要使用的版本可用，您可以从镜像列表中选择镜像。如果您要使用的镜像不是标准镜像，您可以输入您要使用的镜像的 url。有关发行镜像的更多信息，请参阅[发行镜像](#)。
7. 从列表上的可用连接中选择您的供应商连接。如果您没有配置供应商连接，或想要配置一个新供应商连接，请参阅[添加连接](#)。如需了解更多与创建供应商相关的信息，请参阅[Google Cloud Platform 创建供应商连接](#)。
8. 输入您为 Google Cloud Platform 帐户配置的基域信息。如果已有与所选供应商连接关联的基域，则该值会在那个字段中填充。您可以修改它的值来覆盖它。如需更多信息，请参阅[设置自定义域](#)。此名称用于集群的主机名。
9. 添加您要与集群关联的 *标签 (Label)*。这些标签有助于识别集群并限制搜索结果。
10. 为集群配置 *节点池*。  
节点池定义用于集群的节点的位置和大小。

*区域*指定节点所处的地理位置。距离更近的区域可能会提供更快性能，但距离更远的区域可能更为分散。

- **Master 池**：master 池中为您的集群创建三个 Master 节点。Master 节点共享集群活动的管理。您可以选择区域中的多个区以实现更为分散的 master 节点组。您可在创建实例后更改实例的类型和大小，但也可以在此部分中指定。默认值为 *n1-standard-1 - n1-standard-11 vCPU - 通用目的*，根存储为 500 GiB。

- **Worker 池**：您可以在 worker 池中创建一个或多个 worker 节点，以运行集群的容器工作负载。它们可以位于单个 worker 池中，也可以分布在多个 worker 池中。

11. 可选：配置集群网络选项。
12. 可选：为集群配置标签。
13. 点 Create。

在创建和导入过程完成后，您可以查看您的集群详情。

+ 备注：您不必运行 `kubectl` 命令，它为导入集群提供集群的详情。当创建集群时，它由 Red Hat Advanced Cluster Management for Kubernetes 管理自动配置。

### 7.3.3. 访问集群

要访问由 Red Hat Advanced Cluster Management for Kubernetes 管理的集群，请完成以下步骤：

1. 从 Red Hat Advanced Cluster Management for Kubernetes 导航菜单中导航到 Automate infrastructure > Clusters。
2. 选择您创建的或想要访问的集群的名称。此时会显示集群详情。
3. 选择 Reveal credentials 来查看集群的用户名和密码。记下这些值以便在登录到集群时使用。
4. 选择 Console URL 以链接到集群。
5. 使用在第 3 步中找到的用户 ID 和密码登录集群。
6. 为您要访问的集群选择 Actions > Launch to cluster。  
提示：如果知道登录凭证，可以通过为您要访问的集群选择 Actions > Launch to cluster 来访问集群。

## 7.4. 在 VMWARE VSPHERE 上创建集群

您可以使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 VMware vSphere 上部署 Red Hat OpenShift Container Platform 集群。

### 7.4.1. 先决条件

在 vSphere 上创建集群前必须满足以下先决条件：

- 在 OpenShift Container Platform 版本 4.5 或更高版本上部署的 Red Hat Advanced Cluster Management hub 集群。
- 可通过互联网访问 Red Hat Advanced Cluster Management hub 集群，以便它在 vSphere 上创建 Kubernetes 集群。
- vSphere 供应商连接。如需更多信息，请参阅 [VMware vSphere 创建供应商连接](#)。
- Red Hat OpenShift 镜像 pull secret。请参阅 [使用镜像 pull secret](#)。
- 用于部署的 VMware 实例的以下信息：
  - API 和 Ingress 实例所需的静态 IP 地址。



- 以下的 DNS 记录：
  - `api.<cluster_name>.<base_domain>`，它必须指向静态 API VIP。
  - `*.apps.<cluster_name>.<base_domain>`，它必须指向 Ingress VIP 的静态 IP 地址。

## 7.4.2. 使用 Red Hat Advanced Cluster Management for Kubernetes 控制台创建集群

要从 Red Hat Advanced Cluster Management 控制台创建集群，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 在 *Clusters* 页中，点 Add Cluster。
3. 选择 Create a cluster。  
备注：此过程用于创建集群。如果您有一个要导入的现有集群，请参阅[将目标受管集群导入到 hub 集群](#)以了解这些步骤。
4. 为集群输入一个名称。此名称用于集群的主机名。  
备注：这个值必须与创建供应商连接先决条件中列出的 DNS 记录的名称匹配。  
  
提示：要在您在控制台中输入信息时查看 yaml 内容更新，可将 YAML 开关设置为 ON。
5. 为基础架构平台选择 VMware vSphere。
6. 指定您要用于集群的发行镜像。这将标识用于创建集群的 OpenShift Container Platform 镜像的版本。如果要使用的版本可用，您可以从镜像列表中选择镜像。如果要使用的镜像不是标准镜像，您可以输入要使用的镜像的 URL。如需更多信息，请参阅[发行镜像](#)。备注：仅支持 OpenShift Container Platform 版本 4.5.x 或更高版本的发行镜像。
7. 从列表上的可用连接中选择您的供应商连接。如果您没有配置供应商连接，或想要配置一个新供应商连接，请参阅[添加连接](#)。如需了解更多与创建供应商相关的信息，请参阅[创建供应商连接](#)。
8. 输入您为 vSphere 帐户配置的基域信息。如果已有与所选供应商连接关联的基域，则该值会在那个字段中填充。您可以修改它的值来覆盖它。备注：这个值必须与创建 prerequisites 部分中列出的 DNS 记录的名称匹配。此名称用于集群的主机名。
9. 添加您要与集群关联的 *标签 (Label)*。这些标签有助于识别集群并限制搜索结果。
10. 为集群配置 *节点池*。  
节点池定义用于集群的节点的位置和大小。

您可以在 worker 池中创建一个或多个 worker 节点，以运行集群的容器工作负载。它们可以位于单个 worker 池中，也可以分布在多个 worker 池中。

11. 配置集群网络选项，如下所示：
  - a. Network type - VMware vSphere 网络名称。
  - b. API VIP - 用于内部 API 通信的 IP 地址。备注：这个值必须与创建 prerequisites 部分中列出的 DNS 记录的名称匹配。如果没有提供，DNS 必须预先配置，以便 `api.` 可以正确解析。
  - c. Ingress VIP - 用于入口流量的 IP 地址。备注：这个值必须与创建 prerequisites 部分中列出的 DNS 记录的名称匹配。如果没有提供，则必须预先配置 DNS，以便 `test.apps` 可以被正确解析。
12. 可选：为集群配置标签。

- 点 **Create**。在创建和导入过程完成后，您可以查看您的集群详情。  
备注：当您创建集群时，它由 Red Hat Advanced Cluster Management 管理自动配置。您不必运行 `kubectl` 命令，它为导入集群提供集群的详情。

### 7.4.3. 访问集群

要访问由 Red Hat Advanced Cluster Management 管理的集群，请完成以下步骤：

- 如果知道登录凭证，您可以通过选择集群的 *Options* 菜单并选择 **Launch to cluster** 来访问集群。
- 如果您不知道登录凭证
  - 在 Red Hat Advanced Cluster Management 导航菜单中导航到 **Automate infrastructure > Clusters**。
  - 选择您创建的或想要访问的集群的名称。此时会显示集群详情。
  - 选择 **Reveal credentials** 来查看集群的用户名和密码。使用登录到集群时的这些值。
- 选择 **Console URL** 以链接到集群。
- 使用在第 3 步中找到的用户 ID 和密码登录集群。
- 为您要访问的集群选择 **Actions > Launch to cluster**。  
提示：如果知道登录凭证，可以通过为您要访问的集群选择 **Actions > Launch to cluster** 来访问集群。

## 7.5. 在裸机上创建集群

您可以使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在裸机环境中创建一个 Red Hat OpenShift Container Platform 集群。

### 7.5.1. 先决条件

在裸机环境中创建集群前需要满足以下先决条件：

- 在 OpenShift Container Platform 版本 4.5 或更高版本上部署了 Red Hat Advanced Cluster Management for Kubernetes hub 集群。
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群（连接），或连接到连接到互联网（断开连接）的内部或镜像 registry，以检索用于创建集群所需的镜像。
- 裸机供应商连接；如需更多信息，请参阅[为裸机环境创建供应商连接](#)
- 裸机环境的登录凭证，其中包括用户名、密码和基板管理控制器地址
- Red Hat OpenShift Container Platform 镜像 pull secret；请参阅[使用镜像 pull secret](#)  
备注：
  - 裸机资产、受管裸机集群及其相关 secret 必须位于同一命名空间中。
  - 如果更改了云供应商访问密钥，则必须手动更新置备的集群访问密钥。如需更多信息，请参阅[已知问题](#)，[不支持置备的集群的自动 secret 更新](#)。

## 7.5.2. 使用 Red Hat Advanced Cluster Management 控制台创建集群

要从 Red Hat Advanced Cluster Management 控制台创建集群，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 在 Clusters 页面上，点击 Add Cluster。
3. 选择 Create a cluster。  
备注：此过程用于创建集群。如果您有一个要导入的现有集群，请参阅[将目标受管集群导入到 hub 集群](#)以了解这些步骤。
4. 为集群输入一个名称。对于裸机集群，此名称不能是一个任意名称。它与集群 URL 相关联。确保使用的集群名称与您的 DNS 和网络设置一致。  
提示：要在您在控制台中输入信息时查看 yaml 内容更新，可将 YAML 开关设置为 ON。
5. 为基础架构平台选择 Bare Metal。
6. 指定您要用于集群的发行镜像。这可标识用于创建集群的 Red Hat OpenShift Container Platform 镜像的版本。如果要使用的版本可用，您可以从镜像列表中选择镜像。如果您要使用的镜像不是标准镜像，您可以输入您要使用的镜像的 url。有关发行镜像的更多信息，请参阅[发行镜像](#)。
7. 从列表上的可用连接中选择您的供应商连接。如果您没有配置，或想要配置一个新的，请参阅[添加供应商](#)。如需了解更多与创建供应商相关的信息，请参阅[为裸机创建供应商连接](#)。
8. 输入您在裸机环境中配置的基域信息。如果已有与所选供应商连接关联的基域，则该值会在那个字段中填充。您可以修改它的值来覆盖它。对于裸机集群，此设置与集群 URL 相关联。请确定您使用的基域与您的 DNS 和网络设置一致。
9. 从与供应商连接关联的主机列表中选择您的主机。最少选择三个与虚拟机监控程序在同一网桥网络上的资产。
10. 配置集群网络选项。

参数	描述	必需/可选
Base DNS domain	此基础域用于创建到 OpenShift Container Platform 集群组件的路由。它在集群供应商的 DNS 中被配置为授权启动 (SOA) 记录。在集群创建后无法更改此设置。	必需
Network type	要部署的 Pod 网络供应商插件。OpenShiftSDN 插件是 OpenShift Container Platform 4.3 中唯一支持的插件。OVNKubernetes 插件在 OpenShift Container Platform 4.3 中仅是一个技术预览。默认值为 <b>OVNKubernetes</b> 。	必需

参数	描述	必需/可选
Cluster network CIDR	从其中分配 Pod IP 地址的 IP 地址块。OpenShiftSDN 网络插件支持多个集群网络。多个集群网络的地址块不得互相重叠。请选择足够大的地址池，以适配预期的工作负载。默认值为 10.128.0.0/14。	必需
Network host prefix	分配给每个单独节点的子网前缀长度。例如，如果 hostPrefix 设为 23，则每个节点从给定的 CIDR 中分配一个 /23 子网，允许 $510 (2^{(32-23)} - 2)$ 个 pod IP 地址。默认值为 23。	必需
Service network CIDR	服务的 IP 地址块。OpenShiftSDN 只允许一个 serviceNetwork 块。该地址不能与任何其他网络块相重叠。默认值为 172.30.0.0/16。	必需
Machine CIDR	OpenShift Container Platform 主机使用的 IP 地址块。该地址块不得与任何其他网络块重叠。默认值为 10.0.0.0/16。	必需
置备网络 CIDR	用于置备的网络的 CIDR。示例格式为：172.30.0.0/16。	必需
置备网络接口	连接到置备网络的 control plane 节点上的网络接口名称。	必需
置备网络桥接	附加到置备网络中的桥接名称。	必需
外部网络桥接	附加到外部网络的管理程序桥接名称。	必需
API VIP	用于内部 API 通信的虚拟 IP。DNS 必须预先配置为有 A/AAAA 或 CNAME 记录，以便 <b>api.&lt;cluster_name&gt;.&lt;Base DNS domain&gt;</b> 路径可以正确解析。	必需

参数	描述	必需/可选
Ingress VIP	用于入口流量的虚拟 IP。DNS 必须预先配置为有 A/AAAA 或 CNAME 记录，以便 *.apps.<cluster_name>.<Base DNS domain> 路径可以正确解析。	选填

11. 可选：为集群配置标签。
12. 可选：如果要更改设置以包含 configmap，请更新高级设置。
13. 点 Create。在创建和导入过程完成后，您可以查看您的集群详情。  
备注：您不必运行 kubectl 命令，它为导入集群提供集群的详情。当创建集群时，它由 Red Hat Advanced Cluster Management for Kubernetes 管理自动配置。

### 7.5.3. 访问集群

要访问由 Red Hat Advanced Cluster Management for Kubernetes 管理的集群，请完成以下步骤：

1. 从 Red Hat Advanced Cluster Management for Kubernetes 导航菜单中导航到 Automate infrastructure > Clusters。
2. 选择您创建的或想要访问的集群的名称。此时会显示集群详情。
3. 选择 Reveal credentials 来查看集群的用户名和密码。记下这些值以便在登录到集群时使用。
4. 选择 Console URL 以链接到集群。
5. 使用在第 3 步中找到的用户 ID 和密码登录集群。
6. 为您要访问的集群选择 Actions > Launch to cluster。  
提示：如果知道登录凭证，可以通过为您要访问的集群选择 Actions > Launch to cluster 来访问集群。

## 第 8 章 MANAGEDCLUSTERSETS

**ManagedClusterSet** 是一个受管集群的组。通过使用 **ManagedClusterSet**，您可以一起管理对组中所有受管集群的访问。您也可以创建一个 **ManagedClusterSetBinding** 资源来将 **ManagedClusterSet** 资源绑定到一个命名空间。

### 8.1. 创建 MANAGEDCLUSTERSET

您可以在 **ManagedClusterSet** 中将受管集群分组在一起，以限制受管集群的用户访问权限。

需要的访问权限：集群管理员

**ManagedClusterSet** 是一个集群范围的资源，因此您必须在创建 **ManagedClusterSet** 的集群中具有集群管理权限。受管集群不能包含在多个 **ManagedClusterSet** 中。完成以下步骤以创建一个

**ManagedClusterSet**:

1. 在 **yaml** 文件中添加 **ManagedClusterSet** 的以下定义：

```
apiVersion: cluster.open-cluster-management.io/v1alpha1
kind: ManagedClusterSet
metadata:
  name: <clusterset1>
```

将 *clusterset1* 替换为 **ManagedClusterSet** 的名称。

### 8.2. 将集群添加到 MANAGEDCLUSTERSET

创建 **ManagedClusterSet** 后，您必须添加一个或多个受管集群。完成以下步骤以添加受管集群：

1. 确保有一个 **RBAC ClusterRole** 条目，供您在 **managedclustersets/join** 的虚拟子资源上创建。没有这个权限，就无法将受管集群分配给 **ManagedClusterSet**。如果此条目不存在，请将其添加到您的 **yaml** 文件中。示例条目类似以下内容：

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: clusterrole1
rules:
- apiGroups: ["cluster.open-cluster-management.io"]
  resources: ["managedclustersets/join"]
  resourceNames: ["clusterset1"]
  verbs: ["create"]
```

将 *clusterset1* 替换为 **ManagedClusterSet** 的名称。

备注：如果要受管集群从一个 **ManagedClusterSet** 移到另一个，则必须在两个 **ManagedClusterSet** 中都有该权限。

2. 在 **yaml** 文件中查找受管集群的定义。在受管集群定义的这个部分添加与以下内容类似的标签：

```
apiVersion: cluster.open-cluster-management.io/v1
kind: ManagedCluster
metadata:
```

```

name: cluster1
spec:
  hubAcceptsClient: true

```

在本例中，*cluster1* 是受管集群的名称。

3. 添加一个标签，指定 **ManagedClusterSet**，格式为：**cluster.open-cluster-management.io/clusterset: clusterset1**。  
您的代码类似以下示例：

```

apiVersion: cluster.open-cluster-management.io/v1
kind: ManagedCluster
metadata:
  name: cluster1
  labels:
    cluster.open-cluster-management.io/clusterset: clusterset1
spec:
  hubAcceptsClient: true

```

在本例中，*cluster1* 是添加到 *clusterset1* **ManagedClusterSet** 的集群。

备注：如果受管集群之前分配给了一个已删除的 **ManagedClusterSet**，受管集群可能会有一个 **ManagedClusterSet** 已被指定到不存在的集群集合。如果出现这种情况，请用新名称替换。

### 8.3. 从 MANAGEDCLUSTERSET 中删除受管集群

您可能想要从 **ManagedClusterSet** 中删除受管集群，将其移到不同的 **ManagedClusterSet** 中，或从集合的管理设置中移除。

要从 **ManagedClusterSet** 中删除受管 集群,请完成以下步骤：

1. 运行以下命令在 **ManagedClusterSet** 中显示受管集群 列表：

```
kubectl get managedclusters -l cluster.open-cluster-management.io/clusterset=<clusterset1>
```

将 *clusterset1* 替换为 **ManagedClusterSet** 的名称。

2. 找到您要删除的集群条目。
3. 从您要删除的集群的 **yaml** 条目中删除该标签。参阅以下标签代码示例：

```

labels:
  cluster.open-cluster-management.io/clusterset: clusterset1

```

备注：如果要受管集群从一个 **ManagedClusterSet** 移到另一个，则必须在两个 **ManagedClusterSet** 上都有 RBAC 权限。

### 8.4. MANAGEDCLUSTERSETBINDING RESOURCE

创建一个 **ManagedClusterSetBinding** 资源，将 **ManagedClusterSet** 资源绑定到一个命名空间。在同一命名空间中创建的应用程序和策略只能访问绑定的 **ManagedClusterSet** 资源中包含的受管集群。

创建 **ManagedClusterSetBinding** 时，**ManagedClusterSetBinding** 的名称必须与要绑定的 **ManagedClusterSet** 的名称匹配。

您的 ManagedClusterSetBinding 资源可能类似以下信息：

```
apiVersion: cluster.open-cluster-management.io/v1alpha1
kind: ManagedClusterSetBinding
metadata:
  namespace: project1
  name: clusterset1
spec:
  clusterSet: clusterset1
```

您必须在目标 ManagedClusterSet 上具有 bind 权限。查看以下 ClusterRole 资源示例，其中包含允许用户绑定到 **clusterset1** 的规则：

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: clusterrole1
rules:
- apiGroups: ["cluster.open-cluster-management.io"]
  resources: ["managedclustersets/bind"]
  resourceNames: ["clusterset1"]
  verbs: ["create"]
```

有关角色操作的更多信息，请参阅[基于角色的访问控制](#)。



## 第 9 章 将目标受管集群导入到 HUB 集群

您可以从不同的 Kubernetes 云供应商导入集群。导入后，目标集群就成为 Red Hat Advanced Cluster Management for Kubernetes hub 集群的受管集群。除非另有指定，否则在可以访问 hub 集群和目标受管集群的任意位置完成导入任务。

hub 集群无法管理任何其他 hub 集群,但可以管理自己。hub 集群被配置为自动导入和自助管理。您不需要手动导入 hub 集群。

但是，如果您删除 hub 集群并尝试再次导入它，则需要添加 `local-cluster:true` 标签。

从以下说明中进行选择以通过控制台或 CLI 设置受管集群：

所需的用户类型或访问级别：集群管理员

- [使用控制台导入现有集群](#)
- [使用 CLI 导入受管集群](#)
- [修改集群的 klusterlet 附加设置](#)

### 9.1. 使用控制台导入现有集群

安装 Red Hat Advanced Cluster Management for Kubernetes 后，就可以导入集群来进行管理。您可以从控制台和 CLI 导入。按照以下步骤从控制台导入。在此过程中，您需要通过终端来进行身份验证。

- [先决条件](#)
- [导入集群](#)
- [删除集群](#)

#### 9.1.1. 先决条件

- 您需要一个已部署的 Red Hat Advanced Cluster Management for Kubernetes hub 集群。如果您要导入裸机集群，必须在 Red Hat OpenShift Container Platform 版本 4.4 或更高版本上安装了 hub 集群。
- 您需要一个要管理的集群，以及互联网连接。
- 安装 `kubect`l。要安装 `kubect`l，请参阅 [Kubernetes 文档](#)中的 [安装和设置 kubectl。](#)
- 您需要 `base64` 命令行工具。

所需的用户类型或访问级别：集群管理员

#### 9.1.2. 导入集群

您可以从 Red Hat Advanced Cluster Management for Kubernetes 控制台中为每个可用的云供应商导入现有集群。

备注：hub 集群无法管理不同的 hub 集群。hub 集群被设置为自动导入和管理自身，因此您不必手动导入 hub 集群来管理自己。

1. 从导航菜单中，将鼠标悬停在 Automate infrastructure 上，然后点击 Clusters。

2. 点 Add cluster。
3. 点击 Import an existing cluster。
4. 提供集群名称。默认情况下，命名空间会设为与集群名称相同的值。最佳实践：保留命名空间值，不要编辑。
5. 可选：点击以展开 Edit cluster import YAML 文件，并修改端点配置。请参阅 [表 1.YAML 文件参数和描述](#)，了解有关每个参数的详情。
6. 可选：导入后，您可以点击 Configure advanced parameters 添加标签，并使用这些标签进行搜索。
7. 可选：配置 MANAGED CLUSTER URLS。通过配置 MANAGED CLUSTER URLS，运行 `oc get managedcluster` 命令时显示的 URL 会在表中显示。

- a. 如果还没有打开，请使用 web 控制台中的开关打开 YAML 内容，以便查看其内容。
- b. 把 `manageClusterClientConfigs` 项添加到 `import.yaml` 文件中的 `ManagedCluster spec`，如下例所示：

```
apiVersion: cluster.open-cluster-management.io/v1
kind: ManagedCluster
metadata:
  labels:
    cloud: auto-detect
    vendor: auto-detect
    name: cluster-test
    name: cluster-test
spec:
  hubAcceptsClient: true
  managedClusterClientConfigs:
  - url: https://multicloud-console.apps.new-managed.dev.redhat.com
  ---
apiVersion: agent.open-cluster-management.io/v1
...
```

替换 URL 值是受管集群的外部访问 URL 地址。

8. 点击 Generate Command 检索用于部署 `open-cluster-management-agent-addon` 的命令。
9. 在 *Import an existing cluster* 窗口中，将鼠标悬停在 Copy command 图标上并点击以复制提供给您导入命令和令牌。您必须点击 Copy 图标来接收准确的副本。重要：命令中包含复制到每个导入集群的 pull secret 信息。具有访问导入集群权限的所有用户都可以查看 pull secret 信息。考虑在 <https://cloud.redhat.com/> 或通过创建服务帐户来创建二级 pull secret，以便您的个人凭证不会遭到破坏。如需更多信息，请参阅 [使用镜像 pull secret](#) 或 [了解并创建服务帐户](#)。
10. 在终端中，向受管集群进行身份验证。为目标受管集群配置 `kubectl`。请参阅 [支持的云](#) 了解如何配置 `kubectl`。
11. 要将 `open-cluster-management-agent-addon` 部署到受管集群，请运行您在第 8 步中生成并复制的命令。
12. 点击 View cluster 查看集群的 Overview 页面和摘要。

备注：您可以继续导入更多集群。点击 Import another 以重复这个过程。

### 9.1.2.1. YAML 参数和描述

表 1：下表列出了 YAML 文件中可用的参数和描述：

参数	描述	默认值
clusterLabels	提供集群标签；您可以在文件中添加标签	none
clusterLabels.cloud	集群的供应商标签	auto-detect
clusterLabels.vendor	集群的 Kubernetes 厂商标签	auto-detect
clusterLabels.environment	集群的环境标签	none
clusterLabels.region	在其中设置集群的区域	none
applicationManager.enabled	启用多集群管理器应用程序部署，部署订阅控制器和可部署资源控制器	true
searchCollector.enabled	启用搜索集合和索引	true
policyController.enabled	启用监管和风险仪表盘策略功能	true, updateInterval:15
certPolicyController.enabled	根据分布式策略监控证书过期时间	true
iamPolicyController	根据分布式策略监控身份控制	true
serviceRegistry.enabled	作为服务 registry，用于发现由应用程序可部署资源在受管集群间部署的服务。	false
serviceRegistry.dnsSuffix	registry DNS 名称的后缀，添加到目标集群 DNS 域名的末尾。	mcm.svc
serviceRegistry.plugins	包含已启用插件的逗号分隔列表。支持的插件： <b>kube-service</b> 、 <b>kube-ingress</b> 和 <b>istio</b> 。	kube-service
version	<b>open-cluster-management-agent-addon</b> 的版本	2.1.0

### 9.1.3. 删除导入的集群

完成以下步骤以删除导入的集群以及在受管集群上创建的 **open-cluster-management-agent-addon**。

1. 在 *Clusters* 页面的表中查找您导入的集群。

## 2. 点 Actions > Detach cluster 从管理中删除集群。

备注：如果您试图分离名为 `local-cluster` 的 hub 集群，请注意 `disableHubSelfManagement` 的默认设置为 `false`。此设置会导致 hub 集群在分离时会重新导入自己并管理自己，并协调 `MultiClusterHub` 控制器。hub 集群可能需要几小时时间来完成分离过程并重新导入。如果要在等待进程完成后重新导入 hub 集群，您可以输入以下命令来重启 `multiclusterhub-operator` pod 并更快地重新导入：

```
oc delete po -n open-cluster-management `oc get pod -n open-cluster-management | grep multiclusterhub-operator | cut -d' ' -f1`
```

您可以通过将 `disableHubSelfManagement` 值改为 `true` 来更改 hub 集群的值，如[在线安装](#)所述。

## 9.2. 使用 CLI 导入受管集群

安装 Red Hat Advanced Cluster Management for Kubernetes 后，就可以导入集群来进行管理。您可以从控制台和 CLI 导入。按照以下步骤从 CLI 导入。

- [先决条件](#)
- [支持的构架](#)
- [导入 klusterlet](#)

重要：hub 集群无法管理不同的 hub 集群。hub 集群被设置为自动导入并管理自己。您不必手动导入 hub 集群来自己管理。

但是，如果您删除 hub 集群并尝试再次导入它，则需要添加 `local-cluster:true` 标签。

### 9.2.1. 先决条件

- 您需要一个已部署的 Red Hat Advanced Cluster Management for Kubernetes hub 集群。如果要导入裸机集群，则必须在 Red Hat OpenShift Container Platform 版本 4.5 或更高版本上安装了 hub 集群。
- 您需要一个要管理的单独集群，以及互联网连接。
- 您需要 Red Hat OpenShift Container Platform CLI 版本 4.3 或更高版本来运行 `oc` 命令。如需有关安装和配置 Red Hat OpenShift CLI `oc` 的信息，请参阅[CLI 入门](#)。
- 您需要安装 Kubernetes CLI `kubectl`。要安装 `kubectl`，请参阅[Kubernetes 文档](#)的[安装和设置 kubectl](#)。  
备注：从控制台下载 CLI 工具的安装文件。

### 9.2.2. 支持的构架

- Linux
- macOS

### 9.2.3. 准备导入

1. 登录到您的 `hub` 集群。运行以下命令：

```
oc login
```

2. 在 hub 集群上运行以下命令来创建命名空间。备注：`<cluster_name>` 中定义的集群名称也用作 `.yaml` 文件和命令中的集群命名空间：

```
oc new-project ${CLUSTER_NAME}
oc label namespace ${CLUSTER_NAME} cluster.open-cluster-
management.io/managedCluster=${CLUSTER_NAME}
```

3. 使用以下 YAML 示例编辑示例 `ManagedCluster` 集群：

```
apiVersion: cluster.open-cluster-management.io/v1
kind: ManagedCluster
metadata:
  name: <cluster_name>
spec:
  hubAcceptsClient: true
```

4. 将文件保存为 `managed-cluster.yaml`。

5. 使用以下命令应用 YAML 文件：

```
oc apply -f managed-cluster.yaml
```

6. 创建 `klusterlet` 插件配置文件。输入以下示例 YAML：

```
apiVersion: agent.open-cluster-management.io/v1
kind: KlusterletAddonConfig
metadata:
  name: <cluster_name>
  namespace: <cluster_name>
spec:
  clusterName: <cluster_name>
  clusterNamespace: <cluster_name>
  applicationManager:
    enabled: true
  certPolicyController:
    enabled: true
  clusterLabels:
    cloud: auto-detect
    vendor: auto-detect
  iamPolicyController:
    enabled: true
  policyController:
    enabled: true
  searchCollector:
    enabled: true
  version: 2.1.0
```

7. 将文件保存为 `klusterlet-addon-config.yaml`。

8. 应用 YAML。运行以下命令：

```
oc apply -f klusterlet-addon-config.yaml
```

ManagedCluster-Import-Controller 将生成一个名为 `${CLUSTER_NAME}-import` 的 secret。`${CLUSTER_NAME}-import` secret 包括 `import.yaml`，用户会把它应用到一个受管集群来安装 `klusterlet`。

### 9.2.4. 导入 klusterlet

**重要：** 导入命令中包含复制到每个导入集群的 pull secret 信息。具有访问导入集群权限的所有用户都可以查看 pull secret 信息。

1. 获取由受管集群导入控制器生成的 `klusterlet-crd.yaml`。  
运行以下命令：

```
oc get secret ${CLUSTER_NAME}-import -n ${CLUSTER_NAME} -o jsonpath={.data.crd.yaml} | base64 --decode > klusterlet-crd.yaml
```

2. 获取由受管集群控制器生成的 `import.yaml`。运行以下命令：

```
oc get secret ${CLUSTER_NAME}-import -n ${CLUSTER_NAME} -o jsonpath={.data.import.yaml} | base64 --decode > import.yaml
```

3. 登录到目标受管集群。
4. 应用在第 1 步中生成的 `klusterlet-crd.yaml`。运行以下命令：

```
kubectl apply -f klusterlet-crd.yaml
```

5. 应用在第 2 步中生成的 `import.yaml` 文件。运行以下命令：

```
kubectl apply -f import.yaml
```

6. 验证目标受管集群上的 Pod 状态。运行以下命令：

```
kubectl get pod -n open-cluster-management-agent
```

7. 验证您的导入集群的 **JOINED** 和 **AVAILABLE** 状态。在 `hub` 集群中运行以下命令：

```
kubectl get managedcluster ${CLUSTER_NAME}
```

8. 在受管集群的状态为 **AVAILABLE** 后，会安装附加组件。验证目标受管集群上的附加组件的 Pod 状态。运行以下命令：

```
kubectl get pod -n open-cluster-management-agent-addon
```

## 9.3. 修改集群的 KLUSTERLET 附加设置

您可以使用 `hub` 集群修改 `klusterlet` 附加组件的设置。

`klusterlet addon` 控制器根据 `klusterletaddonconfigs.agent.open-cluster-management.io` Kubernetes 资源中的设置管理启用和禁用的功能。

以下设置可以在 `klusterletaddonconfigs.agent.open-cluster-management.io` Kubernetes 资源中更新：

设置名称	值
applicationmanager	<b>true 或 false</b>
policyController	<b>true 或 false</b>
searchCollector	<b>true 或 false</b>
certPolicyController	<b>true 或 false</b>
iamPolicyController	<b>true 或 false</b>

### 9.3.1. 使用 hub 集群中的控制台进行修改

您可以使用 hub 集群修改 `klusterletaddonconfigs.agent.open-cluster-management.io` 资源设置。完成以下步骤以更改设置：

1. 向 hub 集群的 Red Hat Advanced Cluster Management for Kubernetes 控制台进行身份验证。
2. 在 hub 集群控制台的主菜单中选择 Search。
3. 在搜索参数中输入以下值：`kind:klusterletaddonconfigs`
4. 选择您要更新的端点资源。
5. 找到 `spec` 部分并选择 Edit 以编辑内容。
6. 修改设置。
7. 选择 Save 以应用您的更改。

### 9.3.2. 使用 hub 集群中的命令行进行修改

您必须有权访问 `<cluster-name>` 命名空间才能使用 hub 集群修改设置。完成以下步骤：

1. 在 hub 集群中进行身份验证。
2. 输入以下命令以编辑资源：

```
kubectl edit klusterletaddonconfigs.agent.open-cluster-management.io <cluster-name> -n <cluster-name>
```

3. 找到 `spec` 部分。
4. 根据需要修改您的设置。

## 第 10 章 配置特定的集群管理角色

安装 Red Hat Advanced Cluster Management for Kubernetes 时，默认配置在 Red Hat Advanced Cluster Management hub 集群上提供 `cluster-admin` 角色。此权限允许您在 hub 集群中创建、管理和导入受管集群。在某些情况下，您可能想要限制对由 hub 集群管理的某些受管集群的访问，而不是提供对 hub 集群上所有受管集群的访问。

您可以通过定义集群角色并将其应用到用户或组来限制对特定受管集群的访问。完成以下步骤以配置和应用角色：

1. 通过创建包含以下内容的 YAML 文件来定义集群角色：

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: <clusterrole-name>
rules:
- apiGroups:
  - cluster.open-cluster-management.io
  resources:
  - managedclusters
  resourceNames:
  - <managed-cluster-name>
  verbs:
  - get
  - list
  - watch
  - update
  - delete
  - deletecollection
  - patch
- apiGroups:
  - cluster.open-cluster-management.io
  resources:
  - managedclusters
  verbs:
  - create
- apiGroups:
  - ""
  resources:
  - namespaces
  resourceNames:
  - <managed-cluster-name>
  verbs:
  - create
  - get
  - list
  - watch
  - update
  - delete
  - deletecollection
  - patch
- apiGroups:
  - register.open-cluster-management.io
  resources:

```



```
- managedclusters/accept
verbs:
- update
```

将 *clusterrole-name* 替换为您要创建的集群角色的名称。

将 *managed-cluster-name* 替换为您希望用户有权访问的受管集群的名称。

2. 输入以下命令应用 **clusterrole** 定义：

```
oc apply <filename>
```

将 *filename* 替换为您在上一步中创建的 YAML 文件的名称。

3. 输入以下命令将 **clusterrole** 绑定到指定用户或组：

```
oc adm policy add-cluster-role-to-user <clusterrole-name> <username>
```

将 *clusterrole-name* 替换为您在上一步中应用的集群角色的名称。使用您要将集群角色绑定的用户名替换 *username*。

## 第 11 章 升级集群

创建要通过 Red Hat Advanced Cluster Management for Kubernetes 管理的 Red Hat OpenShift Container Platform 集群后，您可以使用 Red Hat Advanced Cluster Management for Kubernetes 控制台将这些集群升级到受管集群使用的版本频道中可用的最新次版本。

在连接的环境中，会在 Red Hat Advanced Cluster Management 控制台中为需要升级的每个集群自动识别更新。

在断开连接的环境中升级集群的过程需要一些额外的步骤来配置和镜像所需的发行镜像。它使用 Red Hat OpenShift Update Service 的 operator 来识别升级。如果您位于断开连接的环境中，请参阅 [升级断开连接的集群](#) 以了解所需步骤。

备注：要升级到主要版本，您必须验证您是否满足升级到该版本的所有先决条件。在可以使用控制台升级集群前，您必须更新受管集群上的版本频道。更新受管集群上的版本频道后，Red Hat Advanced Cluster Management for Kubernetes 控制台会显示可用于升级的最新版本。

重要：您无法使用 Red Hat Advanced Cluster Management for Kubernetes 控制台升级 Red Hat OpenShift Kubernetes Service 集群。

此升级方法只适用于处于 *Ready* 状态的 Red Hat OpenShift Container Platform 集群。

要在连接的环境中升级集群，请完成以下步骤：

1. 从导航菜单中导航到 Automate infrastructure > Clusters。如果有可用的升级，会在 *Distribution version* 列中显示。
2. 选择您要升级的集群。请记住：集群必须处于 *Ready* 状态，且必须是 Red Hat OpenShift Container Platform 集群才能使用控制台升级。
3. 选择 Upgrade。
4. 选择每个集群的新版本。
5. 选择 Upgrade。

### 11.1. 升级断开连接的集群

您可以将 Red Hat OpenShift Update Service 与 Red Hat Advanced Cluster Management for Kubernetes 搭配使用，以便在断开连接的环境中升级您的集群。

重要：Red Hat OpenShift Update Service 是一个 Red Hat OpenShift Container Platform Operator，在 OpenShift Container Platform 4.4 中作为技术预览提供。它并不适合在生产环境中使用。

在某些情况下，安全性考虑会阻止集群直接连接到互联网。这使得您很难知道什么时候可以使用升级，以及如何处理这些升级。配置 OpenShift Update Service 可能会有所帮助。

OpenShift Update Service 是一个独立的操作对象，它监控受管集群在断开连接的环境中的可用版本，并使其可用于在断开连接的环境中升级集群。配置 OpenShift Update Service 后，它可以执行以下操作：

1. 监测何时会有适用于断开连接的集群的升级。
2. 使用图形数据文件识别哪些更新需要被镜像到您的本地站点进行升级。

3. 使用 Red Hat Advanced Cluster Management 控制台通知您的集群可以使用升级。

### 11.1.1. 先决条件

您必须满足以下先决条件，才能使用 OpenShift Update Service 升级断开连接的集群：

- 已部署了一个在 Red Hat OpenShift Container Platform 版本 4.5 或更高版本上运行的 Red Hat Advanced Cluster Management hub 集群，并配置了受限 OLM。如需了解如何配置受限 OLM 的详细信息，请参阅[在受限网络中使用 Operator Lifecycle Manager](#)。  
提示：配置受限 OLM 时，记录目录源镜像。
- 由 Red Hat Advanced Cluster Management hub 集群管理的 OpenShift Container Platform 集群
- 访问您可以镜像集群镜像的本地存储库的凭证。如需了解有关如何创建此存储库的更多信息，请参阅[在受限网络中创建镜像 registry](#)。  
备注：您升级的集群当前版本的镜像必须始终作为镜像之一提供。如果升级失败，集群会在试图升级时恢复到集群的版本。

### 11.1.2. 准备断开连接的镜像 registry

您必须镜像要升级到的镜像，以及您要从本地镜像 registry 升级到的当前镜像。完成以下步骤以镜像镜像：

1. 创建一个包含类似以下示例内容的脚本文件：

```
UPSTREAM_REGISTRY=quay.io
PRODUCT_REPO=openshift-release-dev
RELEASE_NAME=ocp-release
OCP_RELEASE=4.5.2-x86_64
LOCAL_REGISTRY=$(hostname):5000
LOCAL_SECRET_JSON=/path/to/pull/secret

oc adm -a ${LOCAL_SECRET_JSON} release mirror \
--
from=${UPSTREAM_REGISTRY}/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE} \
--to=${LOCAL_REGISTRY}/ocp4 \
--to-release-image=${LOCAL_REGISTRY}/ocp4/release:${OCP_RELEASE}
```

将 `/path/to/pull/secret` 替换为 OpenShift Container Platform pull secret 的路径。

2. 运行该脚本来对镜像进行镜像、配置设置并将发行镜像与发行内容分开。

提示：在创建 `ImageContentSourcePolicy` 时，您可以使用此脚本最后一行的输出。

### 11.1.3. 为 OpenShift Update Service 部署 Operator

要在 OpenShift Container Platform 环境中为 OpenShift Update Service 部署 Operator，请完成以下步骤：

1. 在 hub 集群中，访问 OpenShift Container Platform operator hub。
2. 选择 Red Hat OpenShift Update Service Operator 来部署 Operator。如果需要，更新默认值。Operator 的部署会创建一个名为 `openshift-cincinnati` 的新项目。

### 3. 等待 Operator 的安装完成。

提示：您可以通过在 OpenShift Container Platform 命令行中输入 `oc get pods` 命令来检查安装的状态。验证 Operator 是否处于 **running** 状态。

#### 11.1.4. 构建图形数据 init 容器

OpenShift Update Service 使用图形数据信息来决定可用的升级。在连接的环境中，OpenShift Update Service 会直接从 [Cincinnati 图形数据 GitHub 仓库](#) 中提取可用于升级的图形数据信息。由于要配置断开连接的环境，所以必须使用 `init` 容器使图形数据在本地存储库中可用。完成以下步骤以创建图形数据 `init` 容器：

##### 1. 输入以下命令克隆 `graph data` Git 存储库：

```
git clone https://github.com/openshift/cincinnati-graph-data
```

##### 2. 创建一个包含您的图形数据 `init` 信息的文件。您可以在 `cincinnati-operator` GitHub 仓库中找到此 [Dockerfile](#) 示例。该文件的内容在以下示例中显示：

```
FROM registry.access.redhat.com/ubi8/ubi:8.1

RUN curl -L -o cincinnati-graph-data.tar.gz https://github.com/openshift/cincinnati-graph-data/archive/master.tar.gz

RUN mkdir -p /var/lib/cincinnati/graph-data/

CMD exec /bin/bash -c "tar xvfz cincinnati-graph-data.tar.gz -C /var/lib/cincinnati/graph-data/ --strip-components=1"
```

在本例中：

- **FROM** 值是 OpenShift Update Service 查找镜像的外部 registry。
- **RUN** 命令创建目录并打包升级文件。
- **CMD** 命令将软件包文件复制到本地库并提取文件进行升级。

##### 3. 运行以下命令来构建 图形数据 `init` 容器：

```
podman build -f <path_to_Dockerfile> -t
${DISCONNECTED_REGISTRY}/cincinnati/cincinnati-graph-data-container:latest
podman push ${DISCONNECTED_REGISTRY}/cincinnati/cincinnati-graph-data-
container:latest --authfile=/path/to/pull_secret.json
```

将 `path_to_Dockerfile` 替换为您在上一步中创建文件的路径。

将 `${DISCONNECTED_REGISTRY}/cincinnati/cincinnati-graph-data-container` 替换为 `graph data init` 容器的路径。

将 `/path/to/pull_secret` 替换为 `pull secret` 文件的路径。

备注：如果没有安装 `podman`，您也可以将命令中的 `podman` 替换为 `docker`。

#### 11.1.5. 为已镜像的 registry 配置证书

如果您使用安全的外部容器 registry 来存储已镜像的 OpenShift Container Platform 发行镜像，OpenShift Update Service 需要访问此 registry 来构建升级图。完成以下步骤以配置您的 CA 证书以用于 OpenShift Update Service Pod:

1. 查找位于 `image.config.openshift.io` 的 OpenShift Container Platform 外部 registry API。这是存储外部 registry CA 证书的位置。  
如需更多信息，请参阅 OpenShift Container Platform 文档中的 [在 OpenShift Container Platform 中使用 Image Registry Operator](#)。
2. 在 `openshift-config` 命名空间中创建 ConfigMap。
3. 在密钥 `cincinnati-registry` 中添加您的 CA 证书。OpenShift Update Service 使用此设置来定位您的证书：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: trusted-ca
data:
  cincinnati-registry: |
    -----BEGIN CERTIFICATE-----
    ...
    -----END CERTIFICATE-----
```

4. 编辑 `image.config.openshift.io` API 中的 `cluster` 资源，将 `additionalTrustedCA` 字段设置为您创建的 ConfigMap 的名称。

```
oc patch image.config.openshift.io cluster -p '{"spec":{"additionalTrustedCA":
{"name":"trusted-ca"}}}' --type merge
```

将 `trusted-ca` 替换为新 ConfigMap 的路径。

OpenShift Update Service Operator 会监视 `image.config.openshift.io` API 和您在 `openshift-config` 命名空间中创建的 ConfigMap 以获取更改，然后在 CA 证书已更改时重启部署。

### 11.1.6. 部署 OpenShift Update Service 实例

当在 hub 集群上完成 OpenShift Update Service 实例部署时，此实例就位于集群升级的镜像位置，并可供断开连接的受管集群使用。完成以下步骤以部署实例：

1. 如果您不想使用 Operator 的默认命名空间 (`openshift-cincinnati`)，为 OpenShift Update Service 实例创建一个命名空间：
  - a. 在 OpenShift Container Platform hub 集群控制台导航菜单中，选择 Administration > Namespaces。
  - b. 点 Create Namespace。
  - c. 添加命名空间的名称以及您的命名空间的任何其他信息。
  - d. 选择 Create 来创建命名空间。
2. 在 OpenShift Container Platform 控制台的 *Installed Operators* 部分中，选择 Red Hat OpenShift Update Service Operator。
3. 在菜单中选择 Create Instance。

4. 粘贴 OpenShift Update Service 实例中的内容。您的 YAML 实例可能类似以下清单：

```
apiVersion: cincinnati.openshift.io/v1beta1
kind: Cincinnati
metadata:
  name: openshift-update-service-instance
  namespace: openshift-cincinnati
spec:
  registry: <registry_host_name>:<port>
  replicas: 1
  repository: ${LOCAL_REGISTRY}/ocp4/release
  graphDataImage: '<host_name>:<port>/cincinnati-graph-data-container'
```

将 `spec.registry` 值替换为镜像的本地断开连接 registry 的路径。

将 `spec.graphDataImage` 值替换为图形数据 init 容器的路径。提示：这与您运行 `podman push` 命令来推送图形数据 init 容器时使用的值相同。

5. 选择 Create 来创建实例。
6. 在 hub 集群 CLI 中输入 `oc get pods` 命令来查看实例创建的状态。它可能需要一段时间，但当命令结果显示实例和运算符正在运行时，进程就会完成。

### 11.1.7. 部署策略以覆盖默认 registry（可选）

备注：本节中的步骤仅在将发行版本镜像到您的镜像 registry 时应用。

OpenShift Container Platform 具有一个默认的镜像 registry 值，用于指定它找到升级软件包的位置。在断开连接的环境中，您可以创建一个策略来替换该值，并将该值替换为您对发行版本镜像进行镜像的本地镜像 registry 的路径。

对于这些步骤，策略名为 `ImageContentSourcePolicy`。完成以下步骤以创建策略：

1. 登录到 hub 集群的 OpenShift Container Platform 环境。
2. 在 OpenShift Container Platform 导航中，选择 Administration > Custom Resource Definitions。
3. 选择 *Instances* 选项卡。
4. 选择设置断开连接的 OLM 时创建的 `ImageContentSourcePolicy` 名称，以查看其内容。
5. 选择 *YAML* 选项卡以 **YAML** 格式查看内容。
6. 复制 `ImageContentSourcePolicy` 的整个内容。
7. 在 Red Hat Advanced Cluster Management 控制台中选择 Govern risk > Create policy。
8. 将 **YAML** 切换设置为 *On* 以查看策略的 **YAML** 版本。
9. 删除 **YAML** 代码中的所有内容。
10. 将以下 **YAML** 内容粘贴到窗口以创建自定义策略：

```
apiVersion: policy.open-cluster-management.io/v1
kind: Policy
```

```

metadata:
  name: policy-pod
  namespace: default
  annotations:
    policy.open-cluster-management.io/standards:
    policy.open-cluster-management.io/categories:
    policy.open-cluster-management.io/controls:
spec:
  disabled: false
  policy-templates:
  - objectDefinition:
    apiVersion: policy.open-cluster-management.io/v1
    kind: ConfigurationPolicy
    metadata:
      name: policy-pod-sample-nginx-pod
    spec:
      object-templates:
      - complianceType: musthave
        objectDefinition:
          apiVersion: v1
          kind: Pod
          metadata:
            name: sample-nginx-pod
            namespace: default
          status:
            phase: Running
          remediationAction: inform
          severity: low
        remediationAction: enforce
    ---
    apiVersion: policy.open-cluster-management.io/v1
    kind: PlacementBinding
    metadata:
      name: binding-policy-pod
      namespace: default
    placementRef:
      name: placement-policy-pod
      kind: PlacementRule
      apiGroup: apps.open-cluster-management.io
    subjects:
    - name: policy-pod
      kind: Policy
      apiGroup: policy.open-cluster-management.io
    ---
    apiVersion: apps.open-cluster-management.io/v1
    kind: PlacementRule
    metadata:
      name: placement-policy-pod
      namespace: default
    spec:
      clusterConditions:
      - status: "True"
        type: ManagedClusterConditionAvailable
      clusterSelector:
        matchExpressions:
        [] # selects all clusters if not specified

```

11. 将模板 `objectDefinition` 部分中的内容替换为类似以下内容的内容，以添加 `ImageContentSourcePolicy` 的设置：

```
apiVersion: operator.openshift.io/v1alpha1
kind: ImageContentSourcePolicy
metadata:
  name: ImageContentSourcePolicy
spec:
  repositoryDigestMirrors:
  - mirrors:
    - <path-to-local-mirror>
    source: registry.redhat.io
```

- 使用本地镜像存储库的路径替换 `path-to-local-mirror`。
- 提示：您可以通过输入 `oc adm release mirror` 命令来查找到本地镜像的路径。

12. 选择 `Enforce if supported`。

13. 选择 `Create` 来创建策略。

### 11.1.8. 部署策略来部署断开连接的目录源

将 `Catalogsource` 策略推送到受管集群，将默认位置从连接的位置更改为您断开连接的本地 registry。

1. 在 Red Hat Advanced Cluster Management 控制台中，选择 `Automate infrastructure > Clusters`。
2. 在集群列表中找到要接收策略的受管集群。
3. 记录下受管集群 `name` 标签的值。标签格式为 `name=managed-cluster-name`。该值会在推送策略时使用。
4. 在 Red Hat Advanced Cluster Management 控制台菜单中，选择 `Govern risk > Create policy`。
5. 将 `YAML` 切换设置为 `On` 以查看策略的 `YAML` 版本。
6. 删除 `YAML` 代码中的所有内容。
7. 将以下 `YAML` 内容粘贴到窗口以创建自定义策略：
8. 将以下 `YAML` 内容粘贴到窗口以创建自定义策略：

```
apiVersion: policy.open-cluster-management.io/v1
kind: Policy
metadata:
  name: policy-pod
  namespace: default
  annotations:
    policy.open-cluster-management.io/standards:
    policy.open-cluster-management.io/categories:
    policy.open-cluster-management.io/controls:
spec:
  disabled: false
  policy-templates:
```



```

- objectDefinition:
  apiVersion: policy.open-cluster-management.io/v1
  kind: ConfigurationPolicy
  metadata:
    name: policy-pod-sample-nginx-pod
  spec:
    object-templates:
      - complianceType: musthave
        objectDefinition:
          apiVersion: v1
          kind: Pod
          metadata:
            name: sample-nginx-pod
            namespace: default
          status:
            phase: Running
          remediationAction: inform
          severity: low
        remediationAction: enforce
---
apiVersion: policy.open-cluster-management.io/v1
kind: PlacementBinding
metadata:
  name: binding-policy-pod
  namespace: default
placementRef:
  name: placement-policy-pod
  kind: PlacementRule
  apiGroup: apps.open-cluster-management.io
subjects:
- name: policy-pod
  kind: Policy
  apiGroup: policy.open-cluster-management.io
---
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: placement-policy-pod
  namespace: default
spec:
  clusterConditions:
    - status: "True"
      type: ManagedClusterConditionAvailable
  clusterSelector:
    matchExpressions:
      [] # selects all clusters if not specified

```

#### 9. 在策略中添加以下内容：

```

apiVersion: config.openshift.io/v1
kind: OperatorHub
metadata:
  name: cluster
spec:
  disableAllDefaultSources: true

```

## 10. 添加以下内容：

```

apiVersion: operators.coreos.com/v1alpha1
kind: CatalogSource
metadata:
  name: my-operator-catalog
  namespace: openshift-marketplace
spec:
  sourceType: grpc
  image: <registry_host_name>:<port>/olm/redhat-operators:v1
  displayName: My Operator Catalog
  publisher: grpc

```

将 `spec.image` 值替换为本地受限目录源镜像的路径。

11. 在 Red Hat Advanced Cluster Management 控制台导航中，选择 Automate infrastructure > Clusters 来检查受管集群的状态。应用策略时，集群状态为 **ready**。

## 11.1.9. 部署策略以更改受管集群参数

将 `ClusterVersion` 策略推送到受管集群，以更改其检索升级的默认位置。

1. 在受管集群中，输入以下命令确认 `ClusterVersion` upstream 参数目前是默认公共 OpenShift Update Service 操作对象：

```
oc get clusterversion -o yaml
```

返回的内容可能类似以下内容：

```

apiVersion: v1
items:
- apiVersion: config.openshift.io/v1
  kind: ClusterVersion
  [...]
spec:
  channel: stable-4.4
  upstream: https://api.openshift.com/api/upgrades_info/v1/graph

```

2. 在 hub 集群中，输入以下命令来识别到 OpenShift Update Service 操作对象：`oc get routes`。  
提示：请注意这个值供后续步骤使用。
3. 在 hub 集群 Red Hat Advanced Cluster Management 控制台菜单中，选择 Govern risk > Create a policy。
4. 将 YAML 切换设置为 On 以查看策略的 YAML 版本。
5. 删除 YAML 代码中的所有内容。
6. 将以下 YAML 内容粘贴到窗口以创建自定义策略：

```

apiVersion: policy.open-cluster-management.io/v1
kind: Policy
metadata:
  name: policy-pod
  namespace: default

```

```

annotations:
  policy.open-cluster-management.io/standards:
  policy.open-cluster-management.io/categories:
  policy.open-cluster-management.io/controls:
spec:
  disabled: false
  policy-templates:
  - objectDefinition:
    apiVersion: policy.open-cluster-management.io/v1
    kind: ConfigurationPolicy
    metadata:
      name: policy-pod-sample-nginx-pod
    spec:
      object-templates:
      - complianceType: musthave
        objectDefinition:
          apiVersion: v1
          kind: Pod
          metadata:
            name: sample-nginx-pod
            namespace: default
          status:
            phase: Running
          remediationAction: inform
          severity: low
        remediationAction: enforce
    ---
    apiVersion: policy.open-cluster-management.io/v1
    kind: PlacementBinding
    metadata:
      name: binding-policy-pod
      namespace: default
    placementRef:
      name: placement-policy-pod
      kind: PlacementRule
      apiGroup: apps.open-cluster-management.io
    subjects:
    - name: policy-pod
      kind: Policy
      apiGroup: policy.open-cluster-management.io
    ---
    apiVersion: apps.open-cluster-management.io/v1
    kind: PlacementRule
    metadata:
      name: placement-policy-pod
      namespace: default
    spec:
      clusterConditions:
      - status: "True"
        type: ManagedClusterConditionAvailable
      clusterSelector:
        matchExpressions:
        [] # selects all clusters if not specified

```

7. 将以下内容添加到 *policy* 项中的 *policy.spec* 部分：

```

apiVersion: config.openshift.io/v1
kind: ClusterVersion
metadata:
  name: version
spec:
  channel: stable-4.4
  upstream: https://example-cincinnati-policy-engine-uri/api/upgrades_info/v1/graph

```

将 `spec.upstream` 值替换为 hub 集群 OpenShift Update Service 操作对象的路径。

提示：您可以完成以下步骤以确定操作对象的路径：

- a. 在 hub 集群上运行 `oc get routes -A` 命令。
  - b. 找到到 `cincinnati` 的路由。+ 到操作对象的路径是 `HOST/PORT` 字段的值。
8. 在受管集群 CLI 中，使用以下命令确认 `ClusterVersion` 中的上游参数已使用本地 hub 集群 OpenShift Update Service URL 更新：

```
oc get clusterversion -o yaml
```

结果应该类似以下内容：

```

apiVersion: v1
items:
- apiVersion: config.openshift.io/v1
  kind: ClusterVersion
  [...]
  spec:
    channel: stable-4.4
    upstream: https://<hub-cincinnati-uri>/api/upgrades_info/v1/graph

```

### 11.1.10. 查看可用升级

您可以通过完成以下步骤来查看受管集群可用升级列表：

1. 登录您的 Red Hat Advanced Cluster Management 控制台。
  2. 在导航菜单中，选择 Automate Infrastructure > Clusters。
  3. 选择处于 *Ready* 状态的一个集群。
  4. 在 Actions 菜单中选择 Upgrade cluster。
  5. 验证可选的升级路径是否可用。
- 备注：如果当前版本没有镜像到本地镜像存储库，则不会显示可用的升级版本。

### 11.1.11. 升级集群

配置断开连接的 registry 后，Red Hat Advanced Cluster Management 和 OpenShift Update Service 使用断开连接的 registry 来确定升级是否可用。如果没有可用的升级，请确保您有集群当前级别的发行镜像，且至少有一个后续级别的镜像位于本地存储库中。如果集群当前版本的发行镜像不可用，则没有可用的升级。

完成以下步骤进行升级：

1. 在 Red Hat Advanced Cluster Management 控制台中，选择 Automate infrastructure > Clusters。
2. 查找您要确定是否有可用的升级的集群。
3. 如果有可用的升级，集群的 Distribution version 栏表示有可用的升级可用。
4. 选择集群的 *Options* 菜单，然后选择 Upgrade cluster。
5. 为升级选择目标版本，然后选择 Upgrade。

受管集群已更新至所选版本。

## 第 12 章 从管理中移除集群

当您从管理中删除通过 Red Hat Advanced Cluster Management for Kubernetes 创建的 OpenShift Container Platform 集群时，您可以将其分离 (*detach*) 或销毁 (*destroy*)。

分离集群会将其从管理中移除，但不会完全删除。如果要管理它，可以再次导入集群。只有集群处于 *Ready* 状态时方可使用这个选项。

销毁集群会将其从管理中移除，并删除集群的组件。这是永久性的，删除后无法再次导入和管理它。

### 12.1. 使用控制台删除集群

1. 从导航菜单中导航到 Automate infrastructure > Clusters。
2. 选择您要从管理中删除的集群旁边的选项菜单。
3. 选择 Destroy cluster 或 Detach cluster。  
提示：您可以选择要分离或销毁的集群的复选框来分离或销毁多个集群。然后选择 Detach 或 Destroy。

备注：如果您试图分离名为 **local-cluster** 的 hub 集群，请注意 **disableHubSelfManagement** 的默认设置为 **false**。此设置会导致 hub 集群在分离时会重新导入自己并管理自己，并协调 **MultiClusterHub** 控制器。hub 集群可能需要几小时时间来完成分离过程并重新导入。如果要在等待进程完成后重新导入 hub 集群，您可以输入以下命令来重启 **multiclusterhub-operator** pod 并更快地重新导入：

```
oc delete po -n open-cluster-management `oc get pod -n open-cluster-management | grep multiclusterhub-operator | cut -d ' ' -f1`
```

您可以通过将 **disableHubSelfManagement** 值改为 **true** 来更改 hub 集群的值，如[在线安装](#)所述。

### 12.2. 使用命令行删除集群

要使用 hub 集群的命令行分离受管集群，请运行以下命令：

```
oc delete managedcluster $CLUSTER_NAME
```

备注：如果您试图分离名为 **local-cluster** 的 hub 集群，请注意 **disableHubSelfManagement** 的默认设置为 **false**。此设置会导致 hub 集群在分离时会重新导入自己并管理自己，并协调 **MultiClusterHub** 控制器。hub 集群可能需要几小时时间来完成分离过程并重新导入。如果要在等待进程完成后重新导入 hub 集群，您可以输入以下命令来重启 **multiclusterhub-operator** pod 并更快地重新导入：

```
oc delete po -n open-cluster-management `oc get pod -n open-cluster-management | grep multiclusterhub-operator | cut -d ' ' -f1`
```

您可以通过将 **disableHubSelfManagement** 值改为 **true** 来更改 hub 集群的值，如[在线安装](#)所述。

### 12.3. 在删除集群后删除剩余的资源

如果受管集群上有剩余的资源，则需要额外的步骤以确保删除所有剩余的组件。需要这些额外步骤的情况，包括以下示例：

- 受管集群在完全创建前会被分离，但 **klusterlet** 等一些组件会保留在受管集群中。

- 在分离受管集群前，管理集群的 hub 丢失或销毁，因此无法从 hub 中分离受管集群。
- 当受管集群被分离后，受管集群将处于非在线状态。

如果其中一个情况适用于您试图分离的受管集群，则有些资源将无法从受管集群中删除。完成以下步骤以分离受管集群：

1. 确保配置了 `oc` 命令行界面。

2. 确保您在受管集群中配置了 `KUBECONFIG`。

如果运行 `oc get ns | grep open-cluster-management-agent`，您应该看到两个命名空间：

```
open-cluster-management-agent    Active 10m
open-cluster-management-agent-addon Active 10m
```

3. 从 `deploy` Git 仓库下载 [cleanup-managed-cluster](#) 脚本。

4. 输入以下命令运行 `cleanup-managed-cluster.sh` 脚本：

```
./cleanup-managed-cluster.sh
```

5. 运行以下命令以确保这两个命名空间被删除：

```
oc get ns | grep open-cluster-management-agent
```