Red Hat Advanced Cluster Management for Kubernetes 2.4

安装

有关在连接和断开连接的网络环境中，对安装、多集群高级配置的要求和推荐信息，以及升级和卸载的信息。

Last Updated: 2023-03-08

Red Hat Advanced Cluster Management for Kubernetes 2.4 安装

有关在连接和断开连接的网络环境中，对安装、多集群高级配置的要求和推荐信息，以及升级和卸载的信息。

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

法律通告

摘要

有关在连接和断开连接的网络环境中，对安装、多集群高级配置的要求和推荐信息，以及升级和卸载的信息。

目录

第 1 章 安装 **4**
1.1. 要求和建议 4
1.1.1. 支持的操作系统和平台 4
1.1.2. 支持的浏览器 4
1.2. 性能和可扩展性 5
1.2.1. 受管集群的总数 5
1.2.2. 搜索可扩展性 5
1.2.2.1. 物理内存 6
1.2.2.2. 写入吞吐量（缓存恢复时间） 6
1.2.2.3. 查询执行注意事项 6
1.2.3. 可观察性功能扩展 7
1.2.3.1. 可观察性环境示例 7
1.2.3.2. 写入吞吐量 7
1.2.3.3. CPU 用量（millicores） 7
1.2.3.4. RSS 和工作集合内存 8
1.2.3.5. 用于 thanos-receive 组件的持久性卷 8
1.2.3.6. 网络传输 8
1.2.3.7. Amazon Simple Storage Service（S3） 9
1.2.4. 计划集群大小 9
1.2.4.1. 产品环境 9
1.2.4.1.1. 示例：创建和管理 2000 个单节点 OpenShift Container Platform 集群 9
1.2.4.1.2. Amazon Web Services 上的 OpenShift Container Platform 10
1.2.4.1.3. Google Cloud Platform 上的 OpenShift Container Platform 集群 10
1.2.4.1.4. Microsoft Azure 上的 OpenShift Container Platform 集群 11
1.2.4.1.5. VMware vSphere 上的 OpenShift Container Platform 集群 11
1.2.4.1.6. IBM Z 系统的 OpenShift Container Platform 11
1.2.4.1.7. IBM Power 系统上的 OpenShift Container Platform 12
1.2.4.1.8. 裸机资产上的 OpenShift Container Platform 集群 12
1.3. 在线安装 13
1.3.1. 先决条件 13
1.3.2. 确认 OpenShift Container Platform 安装 14
1.3.3. 从 OperatorHub Web 控制台界面安装 14
1.3.4. 通过 OpenShift Container Platform CLI 安装 15
1.3.5. 在基础架构节点上安装 Red Hat Advanced Cluster Management hub 集群 17
1.3.5.1. 将基础架构节点添加到 OpenShift Container Platform 集群 17
1.3.5.2. Operator Lifecycle Manager Subscription 额外配置 18
1.3.5.3. MultiClusterHub 自定义资源附加配置 18
1.4. 在断开连接的网络中安装 18
1.4.1. 先决条件 18
1.4.2. 确认 OpenShift Container Platform 安装 19
1.4.3. 在断开连接的环境中安装 19
1.5. MULTICLUSTERHUB 高级配置 21
1.5.1. 自定义镜像 Pull Secret 21
1.5.2. availabilityConfig 22
1.5.3. disableHubSelfManagement 22
1.5.4. disableUpdateClusterImageSets 22
1.5.5. customCAConfigmap 23
1.5.6. enableClusterProxyAddon（技术预览） 23
1.5.7. sslCiphers 23
1.6. 网络配置 23
1.6.1. hub 集群网络配置表 24

1.6.2. 受管集群网络配置表 25
1.6.3. 基础架构 operator 表的额外网络要求 27
1.6.4. Submariner 网络要求表 27
1.6.5. Hive 表的额外网络要求 28
1.6.6. 应用程序部署网络要求表 28
1.6.7. 命名空间连接网络要求表 28
1.7. 使用 OPERATOR 进行升级 29
1.7.1. 使用升级管理集群池 30
1.8. 升级 OPENSHIFT CONTAINER PLATFORM 30
1.9. 卸装 31
1.9.1. 先决条件：分离启用的服务 31
1.9.2. 使用命令删除资源 32
1.9.3. 使用控制台删除组件 34

第 1 章 安装

了解如何为 Kubernetes 安装和卸载 Red Hat Advanced Cluster Management for Kubernetes。在安装 Red Hat Advanced Cluster Management for Kubernetes 前，请查看每个产品所需的硬件和系统配置。您可以在带有支持版本的 Red Hat OpenShift Container Platform 的 Linux 系统上安装 Red Hat Advanced Cluster Management for Kubernetes。

1. 您必须有受支持的 OpenShift Container Platform 版本。例如，您可以在 AWS 或 Red Hat OpenShift Dedicated 上使用 Red Hat OpenShift Service。

2. 您必须从目录中为 Red Hat Advanced Cluster Management for Kubernetes 安装 Operator。

FIPS 注意：如果您没有在 **spec.ingress.sslCiphers** 中指定自己的密码，则 **multiclusterhub-operator** 会提供默认密码列表。对于 2.3，这个列表包含两个 *未被* FIPS 批准的密码。如果您从 2.3.x 或更早版本升级并希望符合 FIPS 合规性，请从 **multiclusterhub** 资源中删除以下两个密码： **ECDHE-ECDSA-CHACHA20-POLY1305** 和 **ECDHE-RSA-CHACHA20-POLY1305**。

安装 Red Hat Advanced Cluster Management for Kubernetes 来设置一个多节点集群生产环境。您可以使用标准配置或高可用性配置安装 Red Hat Advanced Cluster Management for Kubernetes。有关安装过程的更多信息，请参阅以下文档：

- 要求和建议
- 计划集群大小
- 性能和可扩展性
- 在线安装
- 在断开连接的网络中安装
- MultiClusterHub 高级配置
- 网络配置
- 使用 operator 进行升级
- 升级 OpenShift Container Platform
- 卸装

1.1. 要求和建议

在安装 Red Hat Advanced Cluster Management for Kubernetes 前，请查看以下系统配置要求和设置：

- 支持的操作系统和平台
- 支持的浏览器

1.1.1. 支持的操作系统和平台

要查看有关 hub 集群和受管集群的平台的最新信息，请参阅 Red Hat Advanced Cluster Management 2.4 支持列表。

1.1.2. 支持的浏览器

您可从 Mozilla Firefox、Google Chrome、Microsoft Edge 和 Safari 访问 Red Hat Advanced Cluster Management 控制台。请查看以下经过测试和支持的版本：

平台	支持的浏览器
Microsoft Windows	Microsoft Edge - 44 或更新版本，Mozilla Firefox - 82.0 或更新版本，Google Chrome - 版本 86.0 及更新版本
Linux	Mozilla Firefox - 82.0 及更新版本，Google Chrome - 版本 86.0 及更新版本
macOS	Mozilla Firefox - 82.0 及更新版本，Google Chrome - 版本 86.0 及更新版本，Safari - 14.0 及更新版本

1.2. 性能和可扩展性

Red Hat Advanced Cluster Management for Kubernetes 已经过测试来决定特定的可扩展性和性能数据。测试的主要领域包括集群可扩展性和搜索性能。

您可以使用这些信息来帮助规划您的环境。

备注：数据基于测试时实验室环境的结果。您的具体结果可能会根据您的环境、网络速度和产品更改而有所不同。

- 受管集群的总数
- 搜索可扩展性
- 可观察性功能扩展

1.2.1. 受管集群的总数

Red Hat Advanced Cluster Management 可管理的最大集群数量因以下几个因素而有所不同：

- 集群中的资源数量，它取决于部署的策略和应用程序数量等因素。
- hub 集群配置，如使用了多少个 pod 进行扩展。

下表显示了在测试过程中使用的 Amazon Web Services 云平台上集群的配置信息：

节点	Flavor	vCPU	RAM（GiB）	磁盘类型	磁盘大小(GiB)	数量	区域
Master	m5.2xlarge	8	32	gp2	100	3	us-east-1
Worker	m5.2xlarge	8	32	gp2	100	3 个或 5 个节点	us-east-1

1.2.2. 搜索可扩展性

Search 组件的可扩展性取决于数据存储的性能。在分析搜索性能时，以下变量非常重要：

- 物理内存
- 写入吞吐量（缓存恢复时间）
- 查询执行时间

1.2.2.1. 物理内存

搜索会将数据保留在内存中从而达到快速响应时间。所需内存与 Kubernetes 资源的数量及其在集群中的关系有比例关系。

Clusters	Kubernetes 资源	关系	观察的大小（使用模拟数据）
1 个中型	5000	9500	50 Mi
5 个中型	25,000	75,000	120 Mi
15 个中型	75,000	20,0000	492 Mi
30 个中型	150,000	450,000	1 Gi
50 个中型	250,000	750,000	2 Gi

有关如何更改搜索组件的内存数量的更多信息，请参阅 Options 来提高 redisgraph 内存。

1.2.2.2. 写入吞吐量（缓存恢复时间）

大多数处于 steady 状态的集群会生成少量资源更新。当 RedisGraph 中的数据被清除时，更新率最高，这会导致远程收集器同时同步其完整状态。当数据存储被清除后，会为不同数量的受管集群测量恢复时间。

Clusters	Kubernetes 资源	关系	模拟的平均恢复时间
1 个中型	5000	9500	少于 2 秒
5 个中型	25,000	75,000	少于 15 秒
15 个中型	75,000	200,000	2 分钟和 40 秒
30 个中型	150,000	450,000	5-8 分钟

请记住： 如果集群到 hub 的网络连接速度较慢，时间可能会增加。之前声明的写入吞吐量信息仅适用于 **persistence** 被禁用的情况。

1.2.2.3. 查询执行注意事项

有些事情可能会影响查询运行时间以及返回的结果。在计划和配置环境时请考虑以下方面：

- 搜索关键字效率不高。
  如果您搜索 **RedHat** 且管理大量集群，可能需要更长的时间来接收搜索结果。
- 第一次搜索需要更长的时间，因为收集基于用户的访问控制规则需要额外的时间。
- 完成请求的时间长度与用户有权访问的命名空间和资源数量成比例。
  注：如果您与另一个用户保存并共享搜索查询，返回的结果会根据用户的访问级别而不同。如需有关角色访问权限的更多信息，请参阅 OpenShift Container Platform 文档中的使用 RBAC 定义和应用权限。
- 经过观察，当一个有访问所有命名空间或所有受管集群权限的、非管理员用户发出的请求性能最差。

1.2.3. 可观察性功能扩展

如果要启用和使用可观察性（observability）服务，则需要规划您的环境。之后的资源消耗是用于安装可观察性组件的 OpenShift Container Platform 项目。您计划使用的值为所有可观察性组件的总和。

备注：数据基于测试时实验室环境的结果。您的具体结果可能会根据您的环境、网络速度和产品更改而有所不同。

1.2.3.1. 可观察性环境示例

在示例环境中，hub 集群和受管集群位于 Amazon Web Services 云平台中，并具有以下拓扑和配置：

节点	Flavor	vCPU	RAM（GiB）	磁盘类型	磁盘大小(GiB)	数量	区域
Master 节点	m5.4xlarge	16	64	gp2	100	3	sa-east-1
Worker节点	m5.4xlarge	16	64	gp2	100	3	sa-east-1

可观察性部署是为高可用性环境配置的。使用高可用性环境，每个 Kubernetes 部署都有两个实例，每个有状态集（StatefulSet）都有三个实例。

在示例测试过程中，会模拟不同的受管集群来推送指标，每次测试会持续 24 小时。请参见以下吞吐量：

1.2.3.2. 写入吞吐量

pods	间隔（分钟）	每分钟的时间系列
400	1	83000

1.2.3.3. CPU 用量（millicores）

在测试过程中，CPU 用量是稳定的：

Size	CPU 用量
10 个集群	400
20 个集群	800

1.2.3.4. RSS 和工作集合内存

查看以下 RSS 和工作集合内存描述：

- **内存用量 RSS:** 来自 metrics **container_memory_rss**，在测试过程中保持稳定状态。
- **内存用量工作集：**来自 metrics **container_memory_working_set_bytes**，随着测试会增加。

以下来自于一个 24 小时测试的结果：

Size	内存用量 RSS	内存用量工作集
10 个集群	9.84	4.93
20 个集群	13.10	8.76

1.2.3.5. 用于 thanos-receive 组件的持久性卷

重要：指标数据存储在 **thanos-receive** 中，直到达到了保留时间（四天）为止。其他组件不需要与 **thanos-receive** 组件一样多的卷。

磁盘用量随着测试会增加。数据代表一天后的磁盘用量，因此最终的磁盘用量要乘以 4。

请查看以下磁盘用法：

Size	磁盘用量（GiB）
10 个集群	2
20 个集群	3

1.2.3.6. 网络传输

在测试过程中，网络传输提供了稳定性。查看大小和网络传输值：

Size	入站网络传输	出站网络传输
10 个集群	每秒 6.55 MBs	每秒 5.80 MBs
20 个集群	每秒 13.08 MBs	每秒 10.9 MBs

1.2.3.7. Amazon Simple Storage Service（S3）

Amazon Simple Storage Service（S3）中的总使用量会增加。指标数据会存储在 S3 中，直到达到默认的保留时间（5 天）。请查看以下磁盘用法：

Size	磁盘用量（GiB）
10 个集群	16.2
20 个集群	23.8

1.2.4. 计划集群大小

每个 Red Hat Advanced Cluster Management for Kubernetes 集群都是唯一的，以下指南为您提供了部署大小示例。根据大小和目的对推荐进行分类。Red Hat Had Advanced Cluster Management 应用以下 3 个部分来调整支持服务的大小和位置：

- 可用域（Availability Zone）用来在集群中分离潜在的故障域。典型的集群应该在三个或多个可用域中具有几乎等同的 worker 节点容量。
- vCPU 保留（reservation）和限制（limit）在 worker 节点上建立 vCPU 容量以分配给一个容器。一个 vCPU 等同于一个 Kubernetes 计算单元。如需更多信息，请参阅 Kubernetes 中 CPU 的意义。
- 内存保留和限制会在 worker 节点上建立内存容量，以便分配给容器。保留（Reservation）是 CPU 或内存的*低限*，限值（limit）是*高限*。
- 持久性数据，这些数据由产品管理，并存储在 Kubernetes 使用的 etcd 集群中。**最佳实践：**对于 OpenShift Container Platform，在 3 个可用区间分配集群的主节点。

1.2.4.1. 产品环境

注：以下要求*不是*最低要求。

OpenShift Container Platform 节点角色	可用区	数据存储	总保留内存（*下限*）	总保留 CPU（*下限*）
Master	3	etcd x 3	OpenShift Container Platform 大小指南	每个 OpenShift 的大小指南
Worker	3	redisgraph/redis x 1	12 GB	6 个 CPU

除了 Red Hat Advanced Cluster Management，OpenShift Container Platform 集群还运行其他服务来支持集群功能。建议使用以下节点大小（在后续信息中记录的 3 个节点，在 3 个可用区间平均分布）。

1.2.4.1.1. 示例：创建和管理 2000 个单节点 OpenShift Container Platform 集群

下表显示了使用 Red Hat Advanced Cluster Management 创建 1000 个单一节点 OpenShift(SNO)集群（同时 230 及更多置备）的最低要求，并管理具有 hub 集群的 1000 个 SNO 集群：

OpenShift Container Platform 节点角色	节点数	所需的持久性卷 (PV)	使用的内存（每个实例）	使用的 CPU（每个实例）
Master	3	支持的安装程序 - 三个节点的每个节点 110 Gb，PostgreSQL - 三个节点的每个节点 25 Gb，三个节点的 etcd。**注：etcd** 守护进程必须位于 NVMe 存储中。如需更多信息，请参阅 OpenShift Container Platform 文档中的推荐的主机实践。	30 GB	10 个CPU
Worker	3	Observability - 每个节点 25 Gb，存储的对象 - 用户提供，搜索被禁用。不需要 redisgraph 。	44 GB	17 个CPU

注： 使用值是在同时创建多个集群时收集的峰值。

1.2.4.1.2. Amazon Web Services 上的 OpenShift Container Platform

如需更多信息，请参阅 OpenShift Container Platform 产品文档中的 Amazon Web Services 信息 。同时还可以参阅与机器类型相关的详细信息。

- 节点数： 3 个
- 可用区： 3 个
- 实例大小： m5.xlarge
  - vCPU：4 个
  - 内存：16 GB
  - 存储大小： 120 GB

1.2.4.1.3. Google Cloud Platform 上的 OpenShift Container Platform 集群

有关配额的更多信息，请参阅 Google Cloud Platform 产品文档。同时还可以参阅与机器类型相关的详细信息。

- 节点数： 3 个
- 可用区： 3 个
- 实例大小：N1-standard-4（0.95-6.5 GB）
  - vCPU：4 个
  - 内存：15 GB
  - 存储大小： 120 GB

1.2.4.1.4. Microsoft Azure 上的 OpenShift Container Platform 集群

详情请查看以下产品文档。

- 节点数： 3 个
- 可用区： 3 个
- 实例大小： Standard_D4_v3
  - vCPU：4 个
  - 内存：16 GB
  - 存储大小： 120 GB

1.2.4.1.5. VMware vSphere 上的 OpenShift Container Platform 集群

详情请查看以下产品文档。

- 节点数： 3 个
- 可用区： 3 个
- 实例大小：
  - 内存：16 GB
  - 存储大小： 120 GB
  - VCPU：4
  - 每个插槽的内核数： 2

1.2.4.1.6. IBM Z 系统的 OpenShift Container Platform

如需更多信息，请参阅 OpenShift Container Platform 文档中的在 IBM Z 系统上安装集群 。

- 节点数： 3 个
- 可用区： 3 个
- 实例大小：
  - 内存：16 GB

- 存储大小：100 GB
- vCPU：10
  IBM Z 系统提供配置并发多线程(SMT)的功能，可扩展每个内核上运行的 vCPU 数量。如果您配置了 SMT，则一个物理内核 (IFL) 提供两个逻辑内核（线程）。管理程序可以提供两个或多个 vCPU。

  当未启用并发多线程(SMT)或超线程时，一个 vCPU 相当于一个物理内核。启用后，使用以下公式来计算对应的比例：（每个内核数的线程）× sockets = vCPU。

  有关 SMT 的更多信息，请参阅 Simultaneous 多线程。

1.2.4.1.7. IBM Power 系统上的 OpenShift Container Platform

如需更多信息，请参阅 OpenShift Container Platform 文档中的在 Power 系统上安装集群。

- 节点数： 3 个
- 可用区： 3 个
- 实例大小：
  - 内存：16 GB
  - 存储大小： 120 GB
  - vCPU: 16
    IBM Power 系统提供配置并发多线程 (SMT) 的功能，可扩展每个内核上运行的 vCPU 数量。如果您配置了 SMT，则您的 SMT 级别决定如何满足 16 个 vCPU 的要求。最常见的配置有：
    - 在 SMT-8 上运行的两个内核（运行 IBM PowerVM 的系统默认配置）提供所需的 16 个 vCPU。
    - 在 SMT-4 上运行的四个内核提供所需的 16 个 vCPU。
      有关 SMT 的更多信息，请参阅 Simultaneous 多线程。

1.2.4.1.8. 裸机资产上的 OpenShift Container Platform 集群

详情请查看以下产品文档。

OpenShift Container Platform 裸机上可安装并支持 Red Hat Advanced Cluster Management for Kubernetes hub 集群。hub 集群可以在紧凑的裸机拓扑上运行，其中有 3 个可调度的 control plane 节点，以及 0 个额外的 worker。

- 节点数： 3 个
- 可用区： 3 个
- 实例大小：
  - 内存：16 GB
  - 存储大小： 120 GB
  - VCPU：4

1.3. 在线安装

Red Hat Advanced Cluster Management for Kubernetes 通过 Operator Lifecycle Manager 安装，它管理安装、升级和删除包含 Red Hat Advanced Cluster Management hub 集群的组件。

在开始前，请查看 要求和建议 部分，然后参阅以下文档：

需要的访问权限：集群管理员

- **OpenShift Container Platform Dedicated 环境需要访问权限：**您必须具有 **cluster-admin** 权限。默认情况下，**dedicated-admin** 角色没有在 OpenShift Container Platform Dedicated 环境中创建命名空间所需的权限。
- 默认情况下，hub 集群组件安装在 OpenShift Container Platform 集群的 worker 节点上，无需额外配置。您可以使用 OpenShift Container Platform OperatorHub Web 控制台界面或使用 OpenShift Container Platform CLI 将 hub 集群安装到 worker 节点上。
- 如果您使用基础架构节点配置了 OpenShift Container Platform 集群，您可以使用带有其他资源参数的 OpenShift Container Platform CLI 将 hub 集群安装到这些基础架构节点上。如需了解更多详细信息，*请参阅在基础架构节点上安装 Red Hat Advanced Cluster Management hub 集群*。
- 如果您计划导入不是由 OpenShift Container Platform 或 Red Hat Advanced Cluster Management 创建的 Kubernetes 集群，则需要配置镜像 pull secret。

有关如何配置高级配置的详情，请查看文档中的 MultiClusterHub 高级配置部分中的选项。

- 先决条件
- 确认 OpenShift Container Platform 安装
- 从 OperatorHub Web 控制台界面安装
- 通过 OpenShift Container Platform CLI 安装
- 在基础架构节点上安装 Red Hat Advanced Cluster Management hub 集群

1.3.1. 先决条件

在安装 Red Hat Advanced Cluster Management 前，请查看以下要求：

- 您的 Red Hat OpenShift Container Platform 集群必须通过 OpenShift Container Platform 控制台访问 OperatorHub 目录中的 Red Hat Advanced Cluster Management operator。
- 您需要访问 catalog.redhat.com。
- OpenShift Container Platform 版本 4.6 或更高版本必须部署到您的环境中，且必须通过 OpenShift Container Platform CLI 登录。OpenShift Container Platform 版本 4.6 或更高版本必须部署到您的环境中，且必须通过 OpenShift Container Platform CLI 登录。如需 OpenShift Container Platform，请参阅以下安装文档：
  - OpenShift Container Platform 版本 4.9
  - OpenShift Container Platform 版本 4.8
  - OpenShift Container Platform 版本 4.6

- 您的 OpenShift Container Platform 命令行界面（CLI）被配置为运行 **oc** 命令。如需有关安装和配置 OpenShift Container Platform CLI 的信息，请参阅 CLI 入门。
- OpenShift Container Platform 权限必须允许创建命名空间。如果没有命名空间，安装将失败。
- 需要有一个互联网连接来访问 Operator 的依赖项。
- 要在 OpenShift Container Platform Dedicated 环境中安装，请参阅以下要求：
  - 您必须已配置并运行了 OpenShift Container Platform Dedicated 环境。
  - 您必须在要安装 hub 集群的 OpenShift Container Platform Dedicated 环境中具有 **cluster-admin** 授权。

1.3.2. 确认 OpenShift Container Platform 安装

您必须有一个受支持的 OpenShift Container Platform 版本，包括 registry 和存储服务，并可以正常工作。有关安装 OpenShift Container Platform 的更多信息，请参阅 OpenShift Container Platform 文档。

1. 验证 OpenShift Container Platform 集群中是否尚未安装 Red Hat Advanced Cluster Management hub 集群。Red Hat Advanced Cluster Management 只允许在每个 OpenShift Container Platform 集群上安装一个 Red Hat Advanced Cluster Management hub 集群。如果没有安装 Red Hat Advanced Cluster Management hub 集群，请继续执行以下步骤。
2. 要确保正确设置 OpenShift Container Platform 集群，请使用以下命令访问 OpenShift Container Platform Web 控制台：

   ```
   kubectl -n openshift-console get route
   ```

   请参见以下示例输出：

   ```
   openshift-console console console-openshift-console.apps.new-coral.purple-chesterfield.com
   console   https   reencrypt/Redirect     None
   ```

3. 在浏览器中打开 URL 并检查结果。如果控制台 URL 显示 **console-openshift-console.router.default.svc.cluster.local**，当安装 OpenShift Container Platform 时把 **openshift_master_default_subdomain** 设置为这个值。请参阅以下 URL 示例 ：**https://console-openshift-console.apps.new-coral.purple-chesterfield.com**。

您可以使用控制台或 CLI 继续运行 Red Hat Advanced Cluster Management。这两个流程都已被记录在文档中。

1.3.3. 从 OperatorHub Web 控制台界面安装

最佳实践： 从 OpenShift Container Platform 导航中的 *Administrator* 视图，安装 OpenShift Container Platform 提供的 OperatorHub Web 控制台界面。

1. 选择 **Operators** > **OperatorHub** 以访问可用操作器列表，然后选择 *Advanced Cluster Management for Kubernetes* operator。
2. 在 *Operator subscription* 页中，选择安装选项：
   - 命名空间信息：
     - Red Hat Advanced Cluster Management hub 集群必须安装在自己的命名空间或项目中。

    - 默认情况下，OperatorHub 控制台安装过程会创建一个名为 **open-cluster-management** 的命名空间。**最佳实践：**继续使用 **open-cluster-management** 命名空间（如果可用）。
    - 如果已有一个名为 **open-cluster-management** 的命名空间，请选择不同的命名空间。
  - Channel：选择与要安装的发行版本相对应的频道。当您选择频道时，它会安装指定的发行版本，并确定以后获得该发行版本中的勘误更新。
  - 更新的批准策略：批准策略指定了用户需要如何处理应用到您的频道或发行版本的更新。
    - 选择 **Automatic** 以确保该版本内的任何更新被自动应用。
    - 选择 **Manual** 在有更新可用时接收通知。如果您对更新的应用有疑问，这可能是您的最佳实践。

  重要信息： 要升级到下一个次版本，您必须返回到 *OperatorHub* 页面，并为更当前的发行版本选择一个新频道。

3. 选择 **Install** 以应用您的更改并创建 Operator。
4. 创建 *MultiClusterHub* 自定义资源。
   a. 在 OpenShift Container Platform 控制台导航中，选择 **Installed Operators** > **Advanced Cluster Management for Kubernetes**。
   b. 选择 **MultiClusterHub** 标签页。
   c. 选择 **Create MultiClusterHub**。
   d. 更新 YAML 文件中的默认值。请参阅文档中的 *MultiClusterHub 高级配置* 部分中的选项。
      - 下例显示了默认模板。确认 **namespace** 是项目的命名空间。请参阅以下示例：

```
apiVersion: operator.open-cluster-management.io/v1
kind: MultiClusterHub
metadata:
  name: multiclusterhub
  namespace: <namespace>
```

5. 选择 **Create** 来初始化自定义资源。Red Hat Advanced Cluster Management hub 集群最多可能需要 10 分钟才能构建和启动。
   创建 Red Hat Advanced Cluster Management hub 集群后，**MultiClusterHub** 资源状态会在 Red Hat Advanced Cluster Management operator 的 *MultiClusterHub* 标签页中显示 *Running*。现在，您可以访问 Red Hat Advanced Cluster Management hub 集群的控制台。请参见以下步骤：
6. 在 OpenShift Container Platform 控制台导航中，选择 **Networking** > **Routes**。
7. 在列表中查看 Red Hat Advanced Cluster Management hub 集群的 URL，并导航到它以访问控制台。

1.3.4. 通过 OpenShift Container Platform CLI 安装

1. 创建一个包含 Operator 要求的 Red Hat Advanced Cluster Management hub 集群命名空间。运行以下命令，其中 **namespace** 是 Red Hat Advanced Cluster Management hub 集群命名空间的名称。在 OpenShift Container Platform 环境中，**namespace** 的值可能被称为 *Project（项目）*。

```
oc create namespace <namespace>
```

2. 将项目命名空间切换到您创建的命名空间。使用在第 1 步中创建的 Red Hat Advanced Cluster Management hub 集群命名空间的名称替换 **namespace**。

```
oc project <namespace>
```

3. 创建 YAML 文件来配置 **OperatorGroup** 资源。每个命名空间只能有一个 operator 组。将 **default** 替换为 operator 组的名称。将 **namespace** 替换为项目命名空间的名称。请参见以下示例：

```
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: <default>
spec:
  targetNamespaces:
  - <namespace>
```

4. 运行以下命令来创建 **OperatorGroup** 资源。将 **operator-group** 替换为您创建的 operator 组 YAML 文件的名称：

```
oc apply -f <path-to-file>/<operator-group>.yaml
```

5. 创建 YAML 文件来配置 OpenShift Container Platform 订阅。文件内容类似以下示例：

```
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: acm-operator-subscription
spec:
  sourceNamespace: openshift-marketplace
  source: redhat-operators
  channel: release-2.4
  installPlanApproval: Automatic
  name: advanced-cluster-management
```

注： 要在基础架构节点上安装 Red Hat Advanced Cluster Management hub 集群，请参阅 Operator Lifecycle Manager 订阅附加配置 部分。

6. 运行以下命令来创建 OpenShift Container Platform 订阅。使用您创建的订阅文件的名称替换 **subscription**：

```
oc apply -f <path-to-file>/<subscription>.yaml
```

7. 创建一个 YAML 文件来配置 **MultiClusterHub** 自定义资源。您的默认模板应当类似于以下示例。将 **namespace** 替换为项目命名空间的名称：

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

```
  name: multiclusterhub
  namespace: <namespace>
spec: {}
```

注： 要在基础架构节点上安装 Red Hat Advanced Cluster Management hub 集群，请参阅 MultiClusterHub 自定义资源附加配置 部分：

8. 运行以下命令来创建 **MultiClusterHub** 自定义资源。将 **custom-resource** 替换为自定义资源文件的名称：

```
oc apply -f <path-to-file>/<custom-resource>.yaml
```

如果此步骤失败并显示以下错误，则仍然会创建并应用这些资源。创建资源后几分钟内再次运行命令：

```
error: unable to recognize "./mch.yaml": no matches for kind "MultiClusterHub" in version
"operator.open-cluster-management.io/v1"
```

9. 运行以下命令来获取自定义资源。在运行命令后，**MultiClusterHub** 自定义资源状态可能需要最多 10 分钟才能在 **status.phase** 字段中显示为 **Running** ：

```
oc get mch -o=jsonpath='{.items[0].status.phase}'
```

10. 状态变为 **Running** 后，查看查找路由的路由列表：

```
oc get routes
```

如果您重新安装 Red Hat Advanced Cluster Management 且 pod 没有启动，请参阅故障排除重新安装失败 以了解解决这个问题的步骤。

备注：

- 具有 **ClusterRoleBinding** 的 **ServiceAccount** 会自动向 Red Hat Advanced Cluster Management 以及有权访问安装 Red Hat Advanced Cluster Management 的命名空间的用户凭证授予集群管理员特权。
- 安装还会创建一个名为 **local-cluster** 的命名空间，该命名空间在由自身管理时为 Red Hat Advanced Cluster Management hub 集群保留。因此，不能已存在名为 **local-cluster** 的命名空间。为安全起见，请不要将 **local-cluster** 命名空间的访问权限授予任何尚未具有 **cluster-administrator** 访问权限的用户。

1.3.5. 在基础架构节点上安装 Red Hat Advanced Cluster Management hub 集群

OpenShift Container Platform 集群可以配置为包含用于运行批准的管理组件的基础架构节点。在基础架构节点上运行组件可避免为运行这些管理组件的节点分配 OpenShift Container Platform 订阅配额。

将基础架构节点添加到 OpenShift Container Platform 集群后，请遵循 OpenShift Container Platform CLI 指令的安装，并将配置添加到 Operator Lifecycle Manager 订阅和 **MultiClusterHub** 自定义资源中。

1.3.5.1. 将基础架构节点添加到 OpenShift Container Platform 集群

按照 OpenShift Container Platform 文档中的 创建基础架构机器集 中所述的步骤进行操作。基础架构节点配置有 Kubernetes **污点（taint）**和标签（**label**），以便防止非管理工作负载在它们上运行。

要与 Red Hat Advanced Cluster Management 提供的基础架构节点启用兼容，请确保您的基础架构节点应用了以下 **污点** 和 **标签** ：

```
metadata:
  labels:
    node-role.kubernetes.io/infra: ""
spec:
  taints:
  - effect: NoSchedule
    key: node-role.kubernetes.io/infra
```

1.3.5.2. Operator Lifecycle Manager Subscription 额外配置

在应用 Operator Lifecycle Manager 订阅前，添加以下配置：

```
spec:
  config:
    nodeSelector:
      node-role.kubernetes.io/infra: ""
    tolerations:
    - key: node-role.kubernetes.io/infra
      effect: NoSchedule
      operator: Exists
```

1.3.5.3. MultiClusterHub 自定义资源附加配置

在应用 **MultiClusterHub** 自定义资源前添加以下附加配置：

```
spec:
  nodeSelector:
    node-role.kubernetes.io/infra: ""
```

1.4. 在断开连接的网络中安装

您可能需要在未连接到互联网的 Red Hat OpenShift Container Platform 集群中安装 Red Hat Advanced Cluster Management for Kubernetes。在断开连接的 hub 中安装的步骤包括一些在连接环境中进行安装的步骤。

您必须下载软件包副本以在安装过程中访问它们，而不是在安装过程中直接从网络访问它们。

在开始前，请查看 要求和建议 部分，然后参阅以下文档：

- 先决条件
- 确认 OpenShift Container Platform 安装
- 在断开连接的环境中安装

1.4.1. 先决条件

在安装 Red Hat Advanced Cluster Management for Kubernetes 前，需要满足以下要求：

- Red Hat OpenShift Container Platform 版本 4.6 或更高版本必须部署到您的环境中，且必须使用 CLI 登录。
- 您需要访问 catalog.redhat.com。
  注： 要管理裸机集群，您必须使用 OpenShift Container Platform 版本 4.6 或更高版本。

  请参阅 OpenShift Container Platform 版本 4.9、OpenShift Container Platform 版本 4.6。
- 您的 Red Hat OpenShift Container Platform CLI 需要版本 4.6 或更高版本，并配置为运行 **oc** 命令。如需有关安装和配置 Red Hat OpenShift CLI 的信息，请参阅 CLI 入门。
- 您的 Red Hat OpenShift Container Platform 权限必须允许创建命名空间。
- 必须有一 个有互联网连接的工作站来下载 operator 的依赖软件包。

1.4.2. 确认 OpenShift Container Platform 安装

- 您必须有一个受支持的 OpenShift Container Platform 版本，包括 registry 和存储服务，在集群中安装并正常工作。如需有关 OpenShift Container Platform 版本 4.9 的更多信息，请参阅 OpenShift Container Platform 文档。
- 连接后，运行 **kubectl -n openshift-console get route** 命令来访问 OpenShift Container Platform Web 控制台。请参见以下示例输出：

  ```
  openshift-console  console  console-openshift-console.apps.new-coral.purple-chesterfield.com  console  https  reencrypt/Redirect  None
  ```

  本例中的控制台 URL 是：**https://console-openshift-console.apps.new-coral.purple-chesterfield.com**。在浏览器中打开 URL 并检查结果。

  如果控制台 URL 显示 **console-openshift-console.router.default.svc.cluster.local**，当安装 OpenShift Container Platform 时把 **openshift_master_default_subdomain** 设置为这个值。

请参阅调整集群大小以了解如何为您的 hub 集群设置容量。

1.4.3. 在断开连接的环境中安装

重要： 您需要将所需的镜像下载到镜像 registry 中，以便在断开连接的环境中安装 Operator。如果没有下载，您可能会在部署过程中收到 **ImagePullBackOff** 错误。

按照以下步骤在断开连接的环境中安装 Red Hat Advanced Cluster Management:

1. 创建镜像 registry。如果您还没有镜像 registry，请按照 Red Hat OpenShift Container Platform 文档中的为断开连接的环境创建镜像的容器镜像的步骤来创建。
   如果已有镜像 registry，可以配置和使用现有 registry。

   注： 确保按照 OpenShift Container Platform 文档中的 从镜像 Operator 目录中提取 OperatorHub 的步骤。

2. 镜像 operator 目录。按照 Mirroring Operator catalogs for use with disconnected clusters 中的步骤对 operator 进行了镜像。
   注： 如果您要从现有的 Red Hat Operator 索引镜像中修剪软件包，请确保修剪 **advanced-cluster-management** 软件包。请参阅过滤基于 SQLite 的索引镜像。

注： 对于裸机，您需要在 **install-config.yaml** 文件中为断开连接的 registry 提供证书信息。要访问受保护的断开连接的 registry 中的镜像，必须提供证书信息，以便 Red Hat Advanced Cluster Management 可以访问 registry。

a. 复制 registry 中的证书信息。

b. 在编辑器中打开 **install-config.yaml** 文件。

c. 找到 **additionalTrustBundle: |** 条目。

d. 在 **additionalTrustBundle** 行后添加证书信息。内容结果类似以下示例：

```
additionalTrustBundle: |
  -----BEGIN CERTIFICATE-----
  certificate_content
  -----END CERTIFICATE-----
sshKey: >-
```

3. **重要：** 如果需要以下监管策略，则需要额外的镜像 registry：

- 容器安全 operator 策略：镜像位于源 **registry.redhat.io/quay**。
- Compliance operator 策略：镜像位于源 **registry.redhat.io/compliance** 中。
- Gatekeeper operator 策略：镜像位于源 **registry.redhat.io/rhacm2** 中。
  参阅以下所有三个 operator 的镜像列表示例：

```
  - mirrors:
    - <your_registry>/rhacm2
    source: registry.redhat.io/rhacm2
  - mirrors:
    - <your_registry>/quay
    source: registry.redhat.io/quay
  - mirrors:
    - <your_registry>/compliance
    source: registry.redhat.io/compliance
```

4. 保存 **install-config.yaml** 文件。

5. 创建一个包含 **ImageContentSourcePolicy** 的 YAML 文件，其名称为 **rhacm-policy.yaml**。**注：** 如果您在正在运行的集群中修改此操作，则会导致所有节点的滚动重启。

```
apiVersion: operator.openshift.io/v1alpha1
kind: ImageContentSourcePolicy
metadata:
  name: rhacm-repo
spec:
  repositoryDigestMirrors:
  - mirrors:
    - mirror.registry.com:5000/rhacm2
    source: registry.redhat.io/rhacm2
```

6. 输入以下命令应用 **ImageContentSourcePolicy** 文件：

```
oc apply -f rhacm-policy.yaml
```

7. 启用断开连接的 Operator Lifecycle Manager Red Hat Operator 和 Community Operator。Red Hat Advanced Cluster Management 包括在 Operator Lifecycle Manager Red Hat Operator 目录中。

8. 为 Red Hat Operator 目录配置离线 Operator Lifecycle Manager。按照 Red Hat OpenShift Container Platform 文档中 受限网络部分中使用 Operator Lifecycle Manager 中的步骤操作。

9. 现在，您在断开连接的 Operator Lifecycle Manager 中已有镜像，请从 Operator Lifecycle Manager 目录继续安装 Red Hat Advanced Cluster Management for Kubernetes。

如需了解所需步骤，请参阅在线安装，或返回到安装概述。

1.5. MULTICLUSTERHUB 高级配置

Red Hat Advanced Cluster Management for Kubernetes 会使用一个会部署所有需要的组件的 operator 进行安装。通过在 MultiClusterHub 自定义资源中添加一个或多个以下属性，可以在安装过程中或安装后进一步配置 Red Hat Advanced Cluster Management：

1.5.1. 自定义镜像 Pull Secret

如果您计划导入不是由 OpenShift Container Platform 或 Red Hat Advanced Cluster Management 创建的 Kubernetes 集群，生成一个包含 OpenShift Container Platform pull secret 信息的 secret，以从发行 registry 中访问授权内容。

OpenShift Container Platform 集群的 secret 要求由 OpenShift Container Platform 和 Red Hat Advanced Cluster Management 自动解决，因此如果您没有导入其他类型的 Kubernetes 集群，则不必创建 secret。您的 OpenShift Container Platform pull secret 与您的 Red Hat Customer Portal ID 相关联，在所有 Kubernetes 供应商中都是相同的。

重要： 这些 secret 是特定于命名空间的，因此请确保处于用于 hub 集群的命名空间中。

1. 进入 cloud.redhat.com/openshift/install/pull-secret 以下载 OpenShift Container Platform pull secret 文件。

2. 点 **Download pull secret**。

3. 运行以下命令来创建 secret:

```
oc create secret generic <secret> -n <namespace> --from-file=.dockerconfigjson=<path-to-pull-secret> --type=kubernetes.io/dockerconfigjson
```

   - 将 **secret** 替换为您要创建的 secret 的名称。
   - 将 **namespace** 替换为项目命名空间，因为 secret 是特定于命名空间的。
   - 将 **path-to-pull-secret** 替换为您下载的 OpenShift Container Platform pull secret 的路径。

以下示例显示了使用自定义 pull secret 的模板。将 **namespace** 替换为项目命名空间的名称。将 **secret** 替换为 pull secret 的名称：

```
apiVersion: operator.open-cluster-management.io/v1
kind: MultiClusterHub
metadata:
  name: multiclusterhub
```

```
  namespace: <namespace>
spec:
  imagePullSecret: <secret>
```

1.5.2. availabilityConfig

Red Hat Advanced Cluster Management hub 集群有两个可用功能： **High** 和 **Basic**。默认情况下，hub 集群的可用性为 **High**，hub 集群组件**副本数** 为 **2**。它提供了对故障转移功能的支持，但消耗的资源数量比可用性为 **Basic**（**副本数**为**1**） 的集群多。

以下示例显示了具有 **Basic** 可用性的模板。将 **namespace** 替换为项目的名称：

```
apiVersion: operator.open-cluster-management.io/v1
kind: MultiClusterHub
metadata:
  name: multiclusterhub
  namespace: <namespace>
spec:
  availabilityConfig: "Basic"
```

1.5.3. disableHubSelfManagement

默认情况下，Red Hat Advanced Cluster Management hub 集群会自动导入和管理。此 *受管*hub 集群名为 **local-cluster**。

如果您不希望 Red Hat Advanced Cluster Management hub 集群管理自己，请将 **disableHubSelfManagement** 的设置从 **false** 改为 **true**。如果该设置没有包括在定义自定义资源的 YAML 文件中，请添加它。hub 集群只能通过这个选项进行管理。

将这个选项设置为 **true** 并尝试手动管理 hub，会导致意外行为。

以下示例显示，如果要禁用 hub 集群自助管理功能，要使用的默认模板。将 **namespace** 替换为项目的名称：

```
apiVersion: operator.open-cluster-management.io/v1
kind: MultiClusterHub
metadata:
  name: multiclusterhub
  namespace: <namespace>
spec:
  disableHubSelfManagement: true
```

1.5.4. disableUpdateClusterImageSets

如果要确保所有集群都使用相同的发行镜像，您可以创建自己的自定义列表，以便在创建集群时可用的发行镜像。当连接到 可用发行镜像并设置 **disableUpdateClusterImageSets** 属性时，请参阅维护自定义镜像 列表中的以下说明，它将停止自定义镜像列表被覆盖。

以下示例显示了禁用对集群镜像集的更新的默认模板。将 **namespace** 替换为项目的名称：

```
apiVersion: operator.open-cluster-management.io/v1
kind: MultiClusterHub
metadata:
  name: multiclusterhub
```

```
  namespace: <namespace>
spec:
  disableUpdateClusterImageSets: true
```

1.5.5. customCAConfigmap

默认情况下，Red Hat OpenShift Container Platform 使用 Ingress Operator 创建内部 CA。

以下示例显示了用于为 Red Hat Advanced Cluster Management 提供自定义 OpenShift Container Platform 默认入口 CA 证书的默认模板。使用项目的名称替换 **namespace**。将 **configmap** 替换为 **ConfigMap** 的名称：

```
apiVersion: operator.open-cluster-management.io/v1
kind: MultiClusterHub
metadata:
  name: multiclusterhub
  namespace: <namespace>
spec:
  customCAConfigmap: <configmap>
```

1.5.6. enableClusterProxyAddon（技术预览）

ClusterProxyAddon 是一个组件。

以下示例显示了用于启用 **ClusterProxyAddon** 的默认模板。将 **namespace** 替换为项目的名称：

```
apiVersion: operator.open-cluster-management.io/v1
kind: MultiClusterHub
metadata:
  name: multiclusterhub
  namespace: <namespace>
spec:
  enableClusterProxyAddon: true
```

1.5.7. sslCiphers

默认情况下，Red Hat Advanced Cluster Management hub 集群包含所支持的 SSL 密码的完整列表。

以下示例显示了用于列出管理入口的 **sslCiphers** 的默认模板。将 **namespace** 替换为项目的名称：

```
apiVersion: operator.open-cluster-management.io/v1
kind: MultiClusterHub
metadata:
  name: multiclusterhub
  namespace: <namespace>
spec:
  ingress:
    sslCiphers:
    - "ECDHE-ECDSA-AES128-GCM-SHA256"
    - "ECDHE-RSA-AES128-GCM-SHA256"
```

1.6. 网络配置

您可以参考 hub 集群和受管集群的配置，以及额外的网络信息：

- hub 集群网络配置表
- 受管集群网络配置表
- 基础架构 operator 表的额外网络要求
- Submariner 网络要求表
- Hive 表的额外网络要求
- 应用程序部署网络要求表
- 命名空间连接网络要求表

1.6.1. hub 集群网络配置表

请参阅下表中的 hub 集群网络要求：

方向	协议	连接	端口（如果指定）	源地址	目标地址
出站到受管集群	HTTPS	从搜索控制台为受管集群的 pod 动态检索日志，使用受管集群中运行的 **klusterlet-addon-workmgr** 服务	443	None	用于访问受管集群路由的 IP 地址
出站到受管集群	HTTPS	安装过程中置备的受管集群的 Kubernetes API 服务器来安装 klusterlet	6443	None	Kubernetes 受管集群 API 服务器的 IP
到频道源的外向流量	HTTPS	频道源，包括 GitHub、Object Store 和 Helm 仓库，只有在您使用应用程序生命周期、OpenShift GitOps 或 ArgoCD 时才需要它	443	None	频道源的 IP

方向	协议	连接	端口（如果指定）	源地址	目标地址
来自受管集群的内向流量	HTTPS	用于推送只为运行 OpenShift Container Platform 版本 4.8 或更高版本的受管集群收集的指标和警报的受管集群	443	None	hub 集群访问路由的 IP 地址
来自受管集群的内向流量	HTTPS	监视受管集群的 Kubernetes API 服务器，用于监视受管集群的更改	6443	None	hub 集群 Kubernetes API 服务器的 IP 地址
出站到 ObjectStore	HTTPS	当 Cluster Backup Operator 运行时，为长期存储发送 Observability 指标数据	443	None	ObjectStore 的 IP 地址
出站到镜像存储库	HTTPS	访问 OpenShift Container Platform 和 Red Hat Advanced Cluster Management 的镜像	443	None	镜像存储库的 IP 地址

1.6.2. 受管集群网络配置表

注：在受管集群中的**注册代理**和**工作代理**不支持代理设置，因为它们通过建立 mTLS 连接与 hub 集群上的 **apiserver** 通信，该连接无法通过代理进行。

下表中查看受管集群网络要求：

方向	协议	连接	端口（如果指定）	源地址	目标地址

方向	协议	连接	端口（如果指定）	源地址	目标地址
来自 hub 集群的内向流量	HTTPS	从搜索控制台为受管集群的 pod 动态发送日志，使用受管集群中运行的 **klusterlet-addon-workmgr** 服务	443	None	用于访问受管集群路由的 IP 地址
来自 hub 集群的内向流量	HTTPS	安装过程中置备的受管集群的 Kubernetes API 服务器来安装 klusterlet	6443	None	Kubernetes 受管集群 API 服务器的 IP
出站到镜像存储库	HTTPS	访问 OpenShift Container Platform 和 Red Hat Advanced Cluster Management 的镜像	443	None	镜像存储库的 IP 地址
到 hub 集群的外向流量	HTTPS	用于推送只为运行 OpenShift Container Platform 版本 4.8 或更高版本的受管集群收集的指标和警报的受管集群	443	None	hub 集群访问路由的 IP 地址
到 hub 集群的外向流量	HTTPS	监视 hub 集群的 Kubernetes API 服务器的变化	6443	None	hub 集群 Kubernetes API 服务器的 IP 地址

方向	协议	连接	端口（如果指定）	源地址	目标地址
到频道源的外向流量	HTTPS	频道源，包括 GitHub、Object Store 和 Helm 仓库，只有在您使用应用程序生命周期、OpenShift GitOps 或 ArgoCD 时才需要它	443	None	频道源的 IP

1.6.3. 基础架构 operator 表的额外网络要求

当使用 Infrastructure Operator 安装裸机受管集群时，请参阅以下表以了解额外网络要求：

方向	协议	连接	端口（如果指定）
hub 集群到 ISO/rootfs 镜像仓库的外向流量	HTTPS（在断开连接的环境中的 HTTP）	用于在 Red Hat Advanced Cluster Management hub 上创建 ISO 镜像	443（断开连接的环境中为 80）
hub 集群在一个单一的节点 OpenShift Container Platform 受管集群中到 BMC 接口的外向流量	HTTPS（在断开连接的环境中的 HTTP）	引导 OpenShift Container Platform 集群	443
从 OpenShift Container Platform 受管集群到 hub 集群的外向流量	HTTPS	使用 **assistedService** 路由报告硬件信息	443
从 OpenShift Container Platform 受管集群到 ISO/rootfs 镜像仓库的外向流量	HTTP	下载 rootfs 镜像	80

1.6.4. Submariner 网络要求表

使用 Submariner 的集群需要三个打开的端口。下表显示了您可以使用的端口：

方向	协议	连接	端口（如果指定）
出站和入站	UDP	每个受管集群	4800

方向	协议	连接	端口（如果指定）
出站和入站	UDP	每个受管集群	4500、500 以及网关节点上 IPSec 流量的任何其他端口
入站	TCP	每个受管集群	8080

1.6.5. Hive 表的额外网络要求

当使用 Central Infrastructure Management（包括使用 Central Infrastructure Management）安装裸机受管集群时，您必须在 hub 集群和 **libvirt** 置备主机间配置第 2 层或第 3 层端口连接。在使用 Hive 创建基本集群的过程中，需要它们来与置备主机进行连接。如需更多信息，请参阅下表：

方向	协议	连接	端口（如果指定）
到 **libvirt** 置备主机的 hub 集群的内向和外向流量	IP	将 hub 集群（Hive operator 安装的位置）连接到 **libvirt** 置备主机（在创建裸机集群时作为一个 bootstrap）	

注： 这些要求只适用于安装时，在升级使用 Infrastructure Operator 安装的集群时不需要。

1.6.6. 应用程序部署网络要求表

通常，应用程序部署通信是从受管集群到 hub 集群的一种方法。连接使用 **kubeconfig**，后者由受管集群上的代理配置。受管集群中的应用程序部署需要访问 hub 集群中的以下命名空间：

- 频道资源的命名空间
- 受管集群的命名空间

1.6.7. 命名空间连接网络要求表

- 应用程序生命周期连接：
  - 命名空间 **open-cluster-management** 需要访问端口 4000 上的控制台 API。
  - 命名空间 **open-cluster-management** 需要在端口 3001 上公开 Application UI。
- 应用程序生命周期后端组件(pod)：
  在 hub 集群中，所有应用程序生命周期 pod 都安装在 **open-cluster-management** 命名空间中，包括以下 pod：
  - multicluster-operators-hub-subscription
  - multicluster-operators-standalone-subscription

- multicluster-operators-channel
- multicluster-operators-application
- multicluster-integrations
  由于这些 pod 位于 **open-cluster-management** 命名空间中：
- 命名空间 **open-cluster-management** 需要通过端口 6443 访问 Kube API。

在受管集群中，只有 **klusterlet-addon-appmgr** 应用程序生命周期 pod 安装在 **open-cluster-management-agent-addon** 命名空间中：

- 命名空间 **open-cluster-management-agent-addon** 需要通过端口 6443 访问 Kube API。

- 监管和风险：
  在 hub 集群中，需要以下访问权限：
  - 命名空间 **open-cluster-management** 需要通过端口 6443 访问 Kube API。
  - 命名空间 **open-cluster-management** 需要访问端口 5353 上的 OpenShift DNS。

  在受管集群中，需要以下访问权限：
  - 命名空间 **open-cluster-management-addon** 需要通过端口 6443 访问 Kube API。

如需了解更多信息，请参阅 Red Hat Advanced Cluster Management for Kubernetes 2.4 支持列表 。

1.7. 使用 OPERATOR 进行升级

您可以使用 Red Hat OpenShift Container Platform 控制台中的 operator 订阅设置来控制 Red Hat Advanced Cluster Management for Kubernetes 的升级。当使用 Operator 部署 Red Hat Advanced Cluster Management 的最初阶段，您可以进行以下选择：

- **Channel：**与您要安装的产品版本相对应。初始频道设置通常是安装时可用的最当前的频道。
- **Approval：** 指定是否需要在频道中批准更新，或者是否自动进行更新。
  - 如果设置为 **Automatic**，那么所选频道中的次要版本更新会在没有管理员干预的情况下部署。
  - 如果设置为 **Manual**，则每个更新到频道中的次发行本都需要管理员批准更新。

您还可以使用 Operator 升级 Red Hat Advanced Cluster Management 时使用这些设置。

需要的访问权限： OpenShift Container Platform 管理员

完成以下步骤以升级 Operator:

重要： 您在频道选择中升级到更新的版本后无法恢复到更早的版本。您必须卸载 Operator，并使用更早的版本重新安装它才能使用以前的版本。

1. 登录您的 OpenShift Container Platform operator hub。
2. 在 OpenShift Container Platform 导航中，选择 **Operators** > **Installed operator**。
3. 选择 **Red Hat Advanced Cluster Management for Kubernetes**operator。

4. 选择 *Subscription* 选项卡来编辑订阅设置。

5. 确保 *Upgrade Status* 被标记为 *Up to date*。此状态表示 Operator 处于所选频道中可用的最新版本。如果 *Upgrade Status* 表示升级处于待处理的状态，请完成以下步骤，将其更新至频道中可用的最新次版本：

   a. 点 *Approval* 字段中的 **Manual** 设置来编辑值。

   b. 选择 **Automatic** 来启用自动更新。

   c. 选择 **Save** 提交您的更改。

   d. 等待自动更新应用到 Operator。更新会自动将所需更新添加到所选频道的最新版本。当完成所有更新后，*Upgrade Status* 字段将显示 **Up to date**。
   提示： **MultiClusterHub** 自定义资源最多需要 10 分钟才能完成升级。您可以输入以下命令来检查升级是否仍然在进行中：

   ```
   oc get mch
   ```

   在进行升级时，**Status** 字段会显示 **Updating**。升级完成后，**Status** 字段会显示 **Running**。

6. 现在，*Upgrade Status* 是 **Up to date**，点 *Channel* 字段中的值来编辑它。

7. 选择下一个可用功能发行版本的频道。要导入，您必须为 {product-version:} 使用 klusterlet operator 的 **stable-2.0** 频道。升级时不能跳过频道。例如，您无法跳过 2.2.z 版本到 2.4 。

8. 选择 **Save** 保存您的更改。

9. 等待自动升级完成。当升级到下一个功能版本后，会部署对频道中最新补丁版本的更新。

10. 如果需要升级到之后的版本，请重复步骤 7-9，直到 Operator 处于所需频道的最新级别。请确定为您的最终频道部署了所有补丁版本。

11. 可选：如果您希望以后在频道中的更新需要手动批准，将 *Approval* 设置为 **Manual**。

Red Hat Advanced Cluster Management 在所选频道的最新版本中运行。

如需有关升级 Operator 的更多信息，请参阅 OpenShift Container Platform 文档中的 Operator。

1.7.1. 使用升级管理集群池

如果要管理 集群池（技术预览），则需要进一步配置来在升级前停止自动管理这些集群池。

在 **ClusterClaim** metadata.annotations 中设置 **cluster.open-cluster-management.io/createmanagedcluster: "false"**。

除非更改此设置，否则所有现有集群声明会在升级时自动导入。

1.8. 升级 OPENSHIFT CONTAINER PLATFORM

您可以对托管您的 Red Hat Advanced Cluster Management for Kubernetes hub 集群的 Red Hat OpenShift Container Platform 进行版本升级。在启动任何集群范围的升级前，备份您的数据。

在升级 OpenShift Container Platform 版本的过程中，Red Hat Advanced Cluster Management web 控制台可能会在一个简短的时间段内没有页面或数据。它会出现 HTTP 500 (Internal Server Error)、HTTP 504 (Gateway Timeout Error) 错误，或出现以前可用的数据不再可用的错误。这是升级的一个正常部

分，发生这种情况时不会丢失任何数据。这些数据和功能最终将会被恢复。

在升级期间还会重新构建搜索索引，因此在升级过程进行的查询可能不完整。

下表包含从 OpenShift Container Platform 版本 4.4.3 升级到 4.4.10 时可以观察到的情况：

表 1.1. 从 OpenShift Container Platform 版本 4.3.3 升级到 4.4.10 时可以观察到的情况列表。

升级过程已经过的时间（分钟：秒）	观察到的更改	持续时间
03:40	监管控制台会出现 HTTP 500 错误	服务在 20 秒内恢复
05:30	AppUI 会出现 HTTP 504 Gateway Timeout 错误	服务在 60 秒内恢复
06:05	集群和搜索控制台会出现 HTTP 504 Gateway Timeout	服务在 20 秒内恢复
07:00	集群和搜索控制台会出现 HTTP 504 Gateway Timeout	服务在 20 秒内恢复
07:10	拓扑和集群控制台显示页面中的错误信息	服务在 20 秒内恢复
07:35	多数控制台页面都会出现 HTTP 500	服务在 60 秒内恢复
08:30	所有页面的服务都会恢复	

1.9. 卸装

在卸载 Red Hat Advanced Cluster Management for Kubernetes 时，您会看到两个不同的卸载过程级别：*删除自定义资源* 和 *完整的 Operator 卸载*。卸载过程最多可能需要 20 分钟。

- 第一个级别是自定义资源移除，这是最基本的卸载类型，用于删除 **MultiClusterHub** 实例的自定义资源，但会保留其他所需的 Operator 资源。如果您计划使用相同的设置和组件重新安装，这个卸载级别很有用。
- 第二个级别是更完整的卸载，可删除大多数 Operator 组件，不包括自定义资源定义等组件。当您继续执行此步骤时，它会删除所有没有通过删除自定义资源而被删除的组件和订阅。在卸载后，您必须在重新安装自定义资源前重新安装 Operator。

1.9.1. 先决条件：分离启用的服务

在卸载 Red Hat Advanced Cluster Management hub 集群前，您必须分离所有由该 hub 集群管理的集群。要解决错误，分离仍由 hub 集群管理的所有集群，然后尝试再次卸载。

- 如果使用发现功能，在尝试卸载时可能会看到以下错误：

```
Cannot delete MultiClusterHub resource because DiscoveryConfig resource(s) exist
```

要禁用发现功能，请完成以下步骤：

- 从控制台导航到 **Discovered Clusters** 表，再单击 **Disable cluster discovery**。确认您要删除该服务。
- 您还可以使用终端。运行以下命令以禁用发现：

```
$ oc delete discoveryconfigs --all --all-namespaces
```

- 如果附加了受管集群，您可能会看到以下信息。**注：** 这不包括 **local-cluster**，它是您自助管理的 hub 集群：

```
Cannot delete MultiClusterHub resource because ManagedCluster resource(s) exist
```

有关分离集群的更多信息，*请参阅从管理部分删除集群*，方法是在 创建集群 中选择供应商的信息。

- 如果您有裸机资产，可能会看到以下内容：

```
Cannot delete MultiClusterHub resource because BareMetalAssets resource(s) exist
```

有关删除裸机资产的更多信息，请参阅 删除裸机资产。

- 如果您使用可观察性功能，可能会看到以下内容：

```
Cannot delete MultiClusterHub resource because MultiClusterObservability resource(s) exist
```

  - 要使用终端禁用并删除 **MultiClusterObservability**，请参阅以下步骤：
    a. 登录到您的 hub 集群。
    b. 输入以下命令删除 **MultiClusterObservability** 自定义资源：

```
oc delete mco observability
```

  - 要使用控制台删除 **MultiClusterObservability** 自定义资源，请参阅以下流程：
    a. 如果安装了 **MultiClusterObservability** 自定义资源，请选择 *MultiClusterObservability* 选项卡。
    b. 选择 **MultiClusterObservability** 自定义资源的 *Options* 菜单。
    c. 选择 **Delete MultiClusterObservability**。
    当您删除资源时，Red Hat Advanced Cluster Management hub 集群上的 **open-cluster-management-observability** 命名空间中的 pod 以及所有受管集群上的 **open-cluster-management-addon-observability** 命名空间中的 pod 都会被删除。

注 ：删除 observability 服务后，您的对象存储不会受到影响。

1.9.2. 使用命令删除资源

1. 如果还没有运行 oc 命令，请确保 OpenShift Container Platform CLI 配置为运行 **oc** 命令。如需有关如何配置 **oc** 命令的更多信息，请参阅 OpenShift Container Platform 文档中的 OpenShift CLI 入门。

2. 输入以下命令来更改到您的项目命名空间。将 *namespace* 替换为项目命名空间的名称：

```
oc project <namespace>
```

3. 输入以下命令删除 **MultiClusterHub** 自定义资源：

```
oc delete multiclusterhub --all
```

您可以输入以下命令来查看进度：

```
oc get mch -o yaml
```

4. 运行清理脚本删除所有潜在的剩余工件。

   a. 按照安装 Helm 中的内容，安装 Helm CLI 二进制版本 3.2.0 或更新版本。

   b. 将以下脚本复制到一个文件中：

```
#!/bin/bash
ACM_NAMESPACE=<namespace>
oc delete mch --all -n $ACM_NAMESPACE
helm ls --namespace $ACM_NAMESPACE | cut -f 1 | tail -n +2 | xargs -n 1 helm delete --namespace $ACM_NAMESPACE
oc delete apiservice v1beta2.webhook.certmanager.k8s.io v1.admission.cluster.open-cluster-management.io v1.admission.work.open-cluster-management.io
oc delete clusterimageset --all
oc delete configmap -n $ACM_NAMESPACE cert-manager-controller cert-manager-cainjector-leader-election cert-manager-cainjector-leader-election-core
oc delete consolelink acm-console-link
oc delete crd klusterletaddonconfigs.agent.open-cluster-management.io placementbindings.policy.open-cluster-management.io policies.policy.open-cluster-management.io userpreferences.console.open-cluster-management.io searchservices.search.acm.com
oc delete mutatingwebhookconfiguration cert-manager-webhook cert-manager-webhook-v1alpha1 ocm-mutating-webhook managedclustermutators.admission.cluster.open-cluster-management.io
oc delete oauthclient multicloudingress
oc delete rolebinding -n kube-system cert-manager-webhook-webhook-authentication-reader
oc delete scc kui-proxy-scc
oc delete validatingwebhookconfiguration cert-manager-webhook cert-manager-webhook-v1alpha1 channels.apps.open.cluster.management.webhook.validator application-webhook-validator multiclusterhub-operator-validating-webhook ocm-validating-webhook
```

   将脚本中的 **<namespace>** 替换为安装 Red Hat Advanced Cluster Management 的命名空间的名称。确保指定正确的命名空间，因为命名空间会被清理和删除。

   c. 运行该脚本删除所有从之前安装中保留的工件。如果没有剩余的工件，则会返回一个没有找到资源的信息。
   注： 如果您计划重新安装相同的 Red Hat Advanced Cluster Management 版本，您可以跳过这个过程中的下一步并重新安装自定义资源。继续以完整 Operator 的卸载过程。

5. 输入以下命令在安装它的命名空间中删除 Red Hat Advanced Cluster Management **ClusterServiceVersion** 和 **Subscription** ：

```
❯ oc get csv
NAME                                  DISPLAY                                     VERSION   REPLACES   PHASE
advanced-cluster-management.v2.4.0    Advanced Cluster Management for Kubernetes   2.4.0
Succeeded

❯ oc delete clusterserviceversion advanced-cluster-management.v2.4.0

❯ oc get sub
NAME                          PACKAGE                       SOURCE              CHANNEL
acm-operator-subscription     advanced-cluster-management   acm-custom-registry   release-2.4

❯ oc delete sub acm-operator-subscription
```

注： CSV 的订阅名称和版本可能有所不同。

1.9.3. 使用控制台删除组件

当使用 Red Hat OpenShift Container Platform 控制台卸载时，需要删除 operator。使用控制台完成以下步骤进行卸载：

1. 在 OpenShift Container Platform 控制台导航中，选择 **Operators** > **Installed Operators** > **Advanced Cluster Manager for Kubernetes**。
2. 删除 **MultiClusterHub** 自定义资源。
   a. 选择 *Multiclusterhub* 标签页。
   b. 选择 MultiClusterHub 自定义资源的 *Options* 菜单。
   c. 选择 **Delete MultiClusterHub**。
3. 参照 Removing a MultiClusterHub instance by using commands 的内容运行 clean-up 脚本。
   提示： 如果您计划重新安装相同的 Red Hat Advanced Cluster Management 版本，您可以跳过这个过程中的其余步骤并重新安装自定义资源。
4. 进入 **Installed Operators**。
5. 选择 *Options* 菜单并选择 **Uninstall operator** 来删除 *Red Hat Advanced Cluster Management* 。