



OpenShift Container Platform 4.3

在 IBM Power 上安装

安装 OpenShift Container Platform 4.3 IBM Power 集群

OpenShift Container Platform 4.3 在 IBM Power 上安装

安装 OpenShift Container Platform 4.3 IBM Power 集群

法律通告

Copyright © 2020 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

摘要

本文档提供在 IBM Power 上安装和卸载 OpenShift Container Platform 4.3 集群的说明。

目录

第1章 在 IBM POWER 上安装	3
1.1. 在 IBM POWER 上安装集群	3
1.2. 在受限网络中的 IBM POWER 上安装集群	26

第 1 章 在 IBM POWER 上安装

1.1. 在 IBM POWER 上安装集群

在 OpenShift Container Platform 版本 4.3 中，您可以在您置备的 IBM Power 系统上安装集群。



重要

非裸机平台还有其他注意事项。在尝试在此类环境中安装 OpenShift Container Platform 集群前，请参阅[有关在未经测试的平台上部署 OpenShift Container Platform 的指南](#)中的信息。

1.1.1. 先决条件

- 为集群置备[使用 NFS 的持久性存储](#)。若要部署私有镜像 registry，您的存储必须提供 ReadWriteMany 访问模式。
- 查看有关 [OpenShift Container Platform 安装和更新](#) 流程的详细信息。
- 如果使用防火墙，则必须[将其配置为允许集群需要访问的站点](#)。



注意

如果您要配置代理，请务必也要查看此站点列表。

1.1.2. OpenShift Container Platform 对互联网和 Telemetry 的访问

在 OpenShift Container Platform 4.3 中，您需要访问互联网来安装集群。默认运行的 Telemetry 服务提供有关集群健康状况和成功更新的指标，这也需要访问互联网。如果您的集群连接到互联网，Telemetry 会自动运行，而且集群会注册到 [Red Hat OpenShift Cluster Manager \(OCM\)](#)。

确认 Red Hat OpenShift Cluster Manager 清单正确后，可以由 Telemetry 自动维护，也可以使用 OCM 手动维护，[使用订阅监控](#)来跟踪帐户或多集群级别的 OpenShift Container Platform 订阅。

您必须具有以下互联网访问权限：

- 访问 [Red Hat OpenShift Cluster Manager](#) 页面，以下载安装程序并执行订阅管理。如果集群可以访问互联网，并且没有禁用 Telemetry，该服务会自动授权您的集群。
- 访问 [Quay.io](#)，以获取安装集群所需的软件包。
- 获取执行集群更新所需的软件包。



重要

如果您的集群无法直接访问互联网，则可以在置备的某些类基础架构上执行受限网络安装。在此过程中，您要下载所需的内容，并使用它在镜像 registry (mirror registry) 中填充安装集群并生成安装程序所需的软件包。对于某些安装类型，集群要安装到的环境不需要访问互联网。在更新集群之前，要更新 registry 镜像系统中的内容。

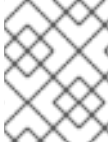
1.1.3. 具有用户置备基础架构的集群的机器要求

对于含有用户置备的基础架构的集群，您必须部署所有所需的机器。

1.1.3.1. 所需的机器

最小的 OpenShift Container Platform 集群需要下列主机：

- 一个临时 bootstrap 机器
- 三台 control plane 或 master 机器
- 至少两台计算机，也称为 worker 机器



注意

集群要求 bootstrap 机器在三台 control plane 机器上部署 OpenShift Container Platform 集群。您可在安装集群后删除 bootstrap 机器。



重要

要保持集群的高可用性，请将独立的物理主机用于这些集群机器。

bootstrap、control plane 以及计算（compute）机器必须使用 Red Hat Enterprise Linux CoreOS (RHCOS) 作为操作系统。

请注意，RHCOS 基于 Red Hat Enterprise Linux 8，并继承其所有硬件认证和要求。请查看[Red Hat Enterprise Linux 技术功能及限制](#)。

1.1.3.2. 网络连接要求

所有 Red Hat Enterprise Linux CoreOS (RHCOS) 机器在启动过程中需要 **inittarmfs** 中的网络从 Machine Config Server 获取 Ignition 配置文件。在初次启动过程中，需要一个 DHCP 服务器或设置了静态 IP 地址来建立网络连接，以下载它们的 Ignition 配置文件。

1.1.3.3. 最低资源要求

每台集群机器都必须满足以下最低要求：

机器	操作系统	vCPU	虚拟内存	存储
bootstrap	RHCOS	4	16 GB	120 GB
Control plane	RHCOS	2	16 GB	120 GB
Compute	RHCOS	RHCOS 或 RHEL 7.6	2	8 GB

1.1.3.4. 证书签名请求管理

在使用您置备的基础架构时，集群只能有限地访问自动机器管理，因此您必须提供一种在安装后批准集群证书签名请求 (CSR) 的机制。**kube-controller-manager** 只能批准 kubelet 客户端 CSR。**machine-approver** 无法保证使用 kubelet 凭证请求的提供证书的有效性，因为它不能确认是正确的机器发出了该请求。您必须决定并实施一种方法，以验证 kubelet 提供证书请求的有效性并进行批准。

1.1.4. 创建用户置备的基础架构

在部署采用用户自备的基础架构的 OpenShift Container Platform 集群前，您必须创建底层基础架构。

先决条件

- 在为集群创建支持基础架构之前，请参阅[OpenShift Container Platform 4.x Tested Integrations](#)页。

流程

1. 在每个节点上配置 DHCP 或设置静态 IP 地址。
2. 提供所需的负载均衡器。
3. 配置机器的端口。
4. 配置 DNS。
5. 确保网络可以正常工作。

1.1.4.1. 用户自备的基础架构对网络的要求

所有 Red Hat Enterprise Linux CoreOS (RHCOS) 机器在启动过程中需要 **initramfs** 中的网络从 Machine Config Server 获取 Ignition 配置。

在初次启动过程中，需要一个 DHCP 服务器或集群中的每个机器都设置了静态 IP 地址来建立网络连接，以下载它们的 Ignition 配置文件。

建议您使用 DHCP 服务器为集群进行长期机器管理。确保 DHCP 服务器已配置为向集群机器提供持久 IP 地址和主机名。

成功安装集群后，在每个 master 节点上运行的 Kubernetes API 服务器必须能够解析集群机器的节点名称。如果 API 服务器和 worker 节点位于不同的区域中，您可以配置默认 DNS 搜索区域，以便 API 服务器能够解析节点名称。另一种支持的方法是始终在节点对象和所有 DNS 请求中使用完全限定域名来指代主机。

您必须配置机器间的网络连接，以便集群组件进行通信。每台机器都必须能够解析集群中所有其他机器的主机名。

表 1.1. 所有机器到所有机器

协议	端口	描述
ICMP	N/A	网络可访问性测试
TCP	9000-9999	主机级别的服务，包括端口 9100-9101 上的节点导出器和端口 9099 上的 Cluster Version Operator。
	10250-10259	Kubernetes 保留的默认端口
	10256	openshift-sdn
UDP	4789	VXLAN 和 Geneve

协议	端口	描述
	6081	VXLAN 和 Geneve
	9000-9999	主机级别的服务，包括端口 9100-9101 上的节点导出器。
TCP/UDP	30000-32767	Kubernetes NodePort

表 1.2. 要通过控制平面的所有机器

协议	端口	描述
TCP	2379-2380	etcd 服务器、对等和指标端口
	6443	Kubernetes API

网络拓扑要求

您为集群置备的基础架构必须满足下列网络拓扑要求。



重要

OpenShift Container Platform 要求所有节点都能访问互联网，以便为平台容器提取镜像并向红帽提供遥测数据。

负载均衡器

在安装 OpenShift Container Platform 前，您必须置备两个满足以下要求的负载均衡器：

1. **API 负载均衡器**：提供一个通用端点，供用户（包括人和机器）与平台交互和配置。配置以下条件：
 - 只适用于第 4 层负载均衡。这可被称为 Raw TCP、SSL Passthrough 或者 SSL 桥接模式。如果使用 SSL Bridge 模式，必须为 API 路由启用 Server Name Indication (SNI)。
 - 无状态负载平衡算法。这些选项根据负载均衡器的实现而有所不同。



注意

API 负载均衡器正常工作不需要会话持久性。

在负载均衡器的前端和后台配置以下端口：

表 1.3. API 负载均衡器

端口	后端机器（池成员）	内部	外部	描述
----	-----------	----	----	----

端口	后端机器 (池成员)	内部	外部	描述
6443	Bootstrap 和 control plane.bootstrap 机器初始化集群 control plane 后, 您要从负载均衡器中删除 bootstrap 机器。您必须为 API 服务器健康检查探测配置 /readyz 端点。	X	X	Kubernetes API 服务器
22623	Bootstrap 和 control plane.bootstrap 机器初始化集群 control plane 后, 您要从负载均衡器中删除 bootstrap 机器。	X		机器配置服务器



注意

负载均衡器必须配置为, 从 API 服务器关闭 /readyz 端点到从池中删除 API 服务器实例时最多需要 30 秒。在 /readyz 返回错误或处于健康状态后的时间范围内, 端点必须被删除或添加。每 5 秒或 10 秒探测一次, 有两个成功请求处于健康状态, 三个成为不健康的请求经过测试。

2. **应用程序入口负载均衡器**: 提供来自集群外部的应用程序流量流量的 Ingress 点。配置以下条件:

- 只适用于第 4 层负载均衡。这可被称为 Raw TCP、SSL Passthrough 或者 SSL 桥接模式。如果使用 SSL Bridge 模式, 您必须为 Ingress 路由启用 Server Name Indication (SNI)。
- 建议根据可用选项以及平台上托管的应用程序类型, 使用基于连接的或者基于会话的持久性。

在负载均衡器的前端和后台配置以下端口:

表 1.4. 应用程序入口负载均衡器

端口	后端机器 (池成员)	内部	外部	描述
443	默认运行入口路由器 Pod、计算或 worker 的机器。	X	X	HTTPS 流量
80	默认运行入口路由器 Pod、计算或 worker 的机器。	X	X	HTTP 流量

提示

如果负载均衡器可以看到客户端的真实 IP 地址, 启用基于 IP 的会话持久性可提高使用端到端 TLS 加密的应用程序的性能。



注意

OpenShift Container Platform 集群需要正确配置入口路由器。control plane 初始化后, 您必须配置入口路由器。

1.1.4.2. 用户置备 DNS 要求

采用用户置备的基础架构的 OpenShift Container Platform 集群需要以下 DNS 记录。在每一记录中，`<cluster_name>` 是集群名称，`<base_domain>` 则是您在 `install-config.yaml` 文件中指定的集群基域。完整的 DNS 记录采用如下格式：`<component>.<cluster_name>.<base_domain>.`

表 1.5. 所需的 DNS 记录

组件	记录	描述
Kubernetes API	<code>api.<cluster_name>.<base_domain>.</code>	此 DNS A/AAAA 或 CNAME 记录必须指向 control plane 机器的负载均衡器。此记录必须能由集群外的客户端和集群内的所有节点解析。
	<code>api-int.<cluster_name>.<base_domain>.</code>	<p>此 DNS A/AAAA 或 CNAME 记录必须指向 control plane 机器的负载均衡器。此记录必须可从集群内的所有节点解析。</p> <div style="display: flex; align-items: flex-start;">  <div style="flex: 1;"> <p>重要</p> <p>API 服务器必须能够根据在 Kubernetes 中记录的主机名解析 worker 节点。如果无法解析节点名称，代理的 API 调用会失败，而且您无法从 Pod 检索日志。</p> </div> </div>
Routes	<code>*.apps.<cluster_name>.<base_domain>.</code>	通配符 DNS A/AAAA 或 CNAME 记录，指向以运行入口路由器 Pod 的机器（默认为 worker 节点）为目标的负载均衡器。此记录必须能由集群外的客户端和集群内的所有节点解析。
etcd	<code>etcd-<index>.<cluster_name>.<base_domain>.</code>	OpenShift Container Platform 要求每个 etcd 实例的 DNS A/AAAA 记录指向托管实例的 control plane 机器。etcd 实例通过 <code><index></code> 值来区分，值的范围为 0 到 n-1 ，其中 n 是集群中 control plane 机器的数量。DNS 记录必须解析到 control plane 机器的单播 IPv4 地址，并且这些记录必须可以从集群中的所有节点解析。

组件	记录	描述
	_etcd-server-ssl._tcp.<cluster_name>. <base_domain>.	对于每台 control plane 机器，OpenShift Container Platform 还需要该机器上具有 etcd 服务器的 SRV DNS 记录，其优先级为 0 ，权重为 10 ，端口则为 2380 。使用三台 control plane 机器的集群需要以下记录： <pre data-bbox="1043 495 1439 1267"> # _service._proto.name. TTL class SRV priority weight port target. _etcd-server-ssl._tcp. <cluster_name>. <base_domain>. 86400 IN SRV 0 10 2380 etcd- 0.<cluster_name>. <base_domain> _etcd-server-ssl._tcp. <cluster_name>. <base_domain>. 86400 IN SRV 0 10 2380 etcd- 1.<cluster_name>. <base_domain> _etcd-server-ssl._tcp. <cluster_name>. <base_domain>. 86400 IN SRV 0 10 2380 etcd- 2.<cluster_name>. <base_domain> </pre>

1.1.5. 生成 SSH 私钥并将其添加到代理中

如果要在集群上执行安装调试或灾难恢复，则必须为 **ssh-agent** 和安装程序提供 SSH 密钥。



注意

在生产环境中，您需要进行灾难恢复和调试。

您可以使用此密钥以 **core** 用户身份通过 SSH 连接到 master 节点。在部署集群时，此密钥会添加到 **core** 用户的 `~/.ssh/authorized_keys` 列表中。



注意

您必须使用一个本地密钥，而不要使用在特定平台上配置的密钥，如 [AWS 密钥对](#)。

流程

1. 如果还没有为计算机上免密码身份验证而配置的 SSH 密钥，请创建一个。例如，在使用 Linux 操作系统的计算机上运行以下命令：

```
$ ssh-keygen -t rsa -b 4096 -N "" \
-f <path>/<file_name> 1
```

- 1 指定 SSH 密钥的路径和文件名，如 `~/.ssh/id_rsa`。不要指定已存在的 SSH 密钥，因为它会被覆盖。

运行此命令会在指定的位置生成不需要密码的 SSH 密钥。

2. 作为后台任务启动 **ssh-agent** 进程：

```
$ eval "$(ssh-agent -s)"
Agent pid 31874
```

3. 将 SSH 私钥添加到 **ssh-agent**：

```
$ ssh-add <path>/<file_name> 1
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

- 1 指定 SSH 私钥的路径和文件名，如 `~/.ssh/id_rsa`

后续步骤

- 在安装 OpenShift Container Platform 时，为安装程序提供 SSH 公钥。

1.1.6. 获取安装程序

在安装 OpenShift Container Platform 之前，将安装文件下载到本地计算机上。

先决条件

- 必须从使用 Linux 或 macOS 的计算机安装集群。
- 需要 500 MB 本地磁盘空间来下载安装程序。

流程

1. 访问 Red Hat OpenShift Cluster Manager 网站的 [Infrastructure Provider](#) 页面。如果您有红帽帐号，请使用自己的凭证登录。如果没有，请创建一个帐户。
2. 进入适用于您的安装类型的页面，下载您的操作系统的安装程序，并将文件放在要保存安装配置文件的目录中。。



重要

安装程序会在用来安装集群的计算机上创建若干文件。在完成集群安装后，您必须保留安装程序和安装程序所创建的文件。



重要

删除安装程序创建的文件不会删除您的集群，即使集群在安装过程中失败也是如此。您必须完成针对特定云供应商的 OpenShift Container Platform 卸载流程，才能完全删除您的集群。

3. 提取安装程序。例如，在使用 Linux 操作系统的计算机上运行以下命令：

```
$ tar xvf <installation_program>.tar.gz
```

4. 在 Red Hat OpenShift Cluster Manager 站点的 [Pull Secret](#) 页面中，下载您的安装 pull secret 的 .txt 文件。通过此 pull secret，您可以进行所含授权机构提供的服务的身份验证，这些服务包括为 OpenShift Container Platform 组件提供容器镜像的 Quay.io。

1.1.7. 通过下载二进制文件安装 CLI

您需要安装 CLI (**oc**) 来使用命令行界面与 OpenShift Container Platform 进行交互。您可在 Linux、Windows 或 macOS 上安装 **oc**。



重要

如果安装了旧版本的 **oc**，则无法使用 OpenShift Container Platform 4.3 中的所有命令。下载并安装新版本的 **oc**。

1.1.7.1. 在 Linux 上安装 CLI

您可以按照以下流程在 Linux 上安装 OpenShift CLI (**oc**) 二进制文件。

流程

1. 访问 Red Hat OpenShift Cluster Manager 网站的 [Infrastructure Provider](#) 页面。
2. 选择您的基础架构供应商及安装类型。
3. 在 **Command-line interface** 部分，从下拉菜单中选择 **Linux**，并点 **Download command-line tools**。
4. 解包存档：

```
$ tar xvzf <file>
```

5. 把 **oc** 二进制代码放到 **PATH** 中的目录中。
执行以下命令可以查看当前的 **PATH** 设置：

```
$ echo $PATH
```

安装 CLI 后，就可以使用 **oc** 命令：

```
$ oc <command>
```

1.1.7.2. 在 Windows 上安装 CLI

您可以按照以下流程在 Windows 上安装 OpenShift CLI (**oc**) 二进制代码。

流程

1. 访问 Red Hat OpenShift Cluster Manager 网站的 [Infrastructure Provider](#) 页面。
2. 选择您的基础架构供应商及安装类型。
3. 在 **Command-line interface** 部分，从下拉菜单中选择 **Windows**，点 **Download command-line tools**。
4. 使用 ZIP 程序解压存档。
5. 把 **oc** 二进制代码放到 **PATH** 中的目录中。
要查看您的 **PATH**，请打开命令提示窗口并执行以下命令：

```
C:\> path
```

安装 CLI 后，就可以使用 **oc** 命令：

```
C:\> oc <command>
```

1.1.7.3. 在 macOS 上安装 CLI

您可以按照以下流程在 macOS 上安装 OpenShift CLI (**oc**) 二进制代码。

流程

1. 访问 Red Hat OpenShift Cluster Manager 网站的 [Infrastructure Provider](#) 页面。
2. 选择您的基础架构供应商及安装类型。
3. 在 **Command-line interface** 部分，从下拉菜单中选择 **MacOS**，并点 **Download command-line tools**。
4. 解包和解压存档。
5. 将 **oc** 二进制文件移到 **PATH** 的目录中。
要查看您的 **PATH**，打开一个终端窗口并执行以下命令：

```
$ echo $PATH
```

安装 CLI 后，就可以使用 **oc** 命令：

```
$ oc <command>
```

1.1.8. 手动创建安装配置文件

对于使用用户自备的基础架构的 OpenShift Container Platform 安装，您必须手动生成安装配置文件。

先决条件

- 获取 OpenShift Container Platform 安装程序和集群的访问令牌。

流程

1. 创建用来存储您所需的安装资产的安装目录：

```
$ mkdir <installation_directory>
```



重要

您必须创建目录。一些安装信息，如 bootstrap X.509 证书，有较短的过期间隔，因此不要重复使用安装目录。如果要重复使用另一个集群安装中的个别文件，可以将其复制到您的目录中。但是，一些安装数据的文件名可能会在发行版本之间有所改变。从 OpenShift Container Platform 老版本中复制安装文件时要格外小心。

2. 自定义以下 `install-config.yaml` 文件模板，并将它保存到 `<installation_directory>` 中。



注意

此配置文件必须命名为 `install-config.yaml`。

3. 备份 `install-config.yaml` 文件，以便用于安装多个集群。



重要

`install-config.yaml` 文件会在安装过程的下一步骤中消耗掉。现在必须备份它。

1.1.8.1. 裸机 `install-config.yaml` 文件示例

1.1.8.2. IBM Power 的 `install-config.yaml` 文件示例

您可以自定义 `install-config.yaml` 文件，以指定有关 OpenShift Container Platform 集群平台的更多信息，或修改所需参数的值。

```
apiVersion: v1
baseDomain: example.com 1
compute:
- hyperthreading: Enabled 2 3
  name: worker
  replicas: 0 4
controlPlane:
  hyperthreading: Enabled 5 6
  name: master 7
  replicas: 3 8
metadata:
  name: test 9
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14 10
    hostPrefix: 23 11
  networkType: OpenShiftSDN
  serviceNetwork: 12
  - 172.30.0.0/16
```

```
platform:
  none: {} 13
  fips: false 14
  pullSecret: '{"auths": ...}' 15
  sshKey: 'ssh-ed25519 AAAA...' 16
```

- 1 集群的基域。所有 DNS 记录都必须是这个基域的子域，并包含集群名称。
- 2 5 **controlPlane** 部分是一个单映射，但 **compute** 部分是一系列映射。为满足不同数据结构的要求，**compute** 部分的第一行必须以连字符 - 开头，**controlPlane** 部分的第一行则不可以连字符开头。虽然这两个部分目前都定义单个机器池，但未来的 OpenShift Container Platform 版本可能会支持在安装过程中定义多个计算池。只使用一个 control plane 池。
- 3 6 7 是否要启用或禁用并发多线程或超线程。默认情况下，启用并发多线程以提高机器内核的性能。您可以通过将参数值设为 **Disabled** 来禁用。如果您在某些集群机器上禁用并发多线程，则必须在所有集群机器上禁用。



重要

如果禁用并发多线程，请确保在容量规划时考虑到机器性能可能会显著降低的问题。

- 4 **replicas** 参数的值必须设置为 **0**。此参数控制集群为您创建和管理的 worker 数量，使用户置备的基础架构时集群不会执行这些功能。在完成 OpenShift Container Platform 安装前，您必须手动为集群部署 worker 机器。
- 8 您添加到集群的 control plane 机器数量。由于集群将这个值用作集群中 etcd 端点的数量，因此该值必须与您部署的 control plane 机器数量匹配。
- 9 您在 DNS 记录中指定的集群名称。
- 10 从中分配 Pod IP 地址的 IP 地址块。此块不得与现有的物理网络重叠。这些 IP 地址用于 Pod 网络。如果您需要从外部网络访问 Pod，请配置负载均衡器和路由器来管理流量。
- 11 分配给每个单独节点的子网前缀长度。例如，如果 **hostPrefix** 设为 **23**，则每个节点从所给的 **cidr** 中分配一个 **/23** 子网，这样就能有 $510 (2^{(32 - 23)} - 2)$ 个 Pod IP 地址。如果您需要从外部网络访问节点，请配置负载均衡器和路由器来管理流量。
- 12 用于服务 IP 地址的 IP 地址池。您只能输入一个 IP 地址池。如果您需要从外部网络访问服务，请配置负载均衡器和路由器来管理流量。
- 13 您必须将平台设置为 **none**。您无法为 IBM Power 基础架构提供额外的平台配置变量。
- 14 是否启用或禁用 FIPS 模式。默认情况下不启用 FIPS 模式。如果启用了 FIPS 模式，运行 OpenShift Container Platform 的 Red Hat Enterprise Linux CoreOS (RHCOS) 机器会绕过默认的 Kubernetes 加密套件，并使用由 RHCOS 提供的加密模块。
- 15 从 Red Hat OpenShift Cluster Manager 站点的 [Pull Secret](#) 页面中获取的 pull secret。通过此 pull secret，您可以进行所含授权机构提供的服务的身份验证，这些服务包括为 OpenShift Container Platform 组件提供容器镜像的 Quay.io。
- 16 Red Hat Enterprise Linux CoreOS (RHCOS) 中 **core** 用户的默认 SSH 密钥的公钥部分。



注意

对于您要在其上执行安装调试或灾难恢复的生产环境 OpenShift Container Platform 集群，请指定 **ssh-agent** 进程使用的 SSH 密钥。

1.1.9. 创建 Kubernetes 清单和 Ignition 配置文件

由于您必须修改一些集群定义文件并要手动启动集群机器，因此您必须生成 Kubernetes 清单和 Ignition 配置文件，集群需要这两项来创建其机器。



重要

安装程序生成的 Ignition 配置文件中所含的证书会在 24 小时后过期。您必须完成集群安装，并使集群以非降级状态运行 24 小时，以确保完成第一次证书轮转。

先决条件

- 获取 OpenShift Container Platform 安装程序。
- 创建 **install-config.yaml** 安装配置文件。

流程

1. 为集群生成 Kubernetes 清单：

```
$ ./openshift-install create manifests --dir=<installation_directory> 1
```

```
INFO Consuming Install Config from target directory
WARNING Making control-plane schedulable by setting MastersSchedulable to true for
Scheduler cluster settings
```

- 1** 对于 **<installation_directory>**，请指定含有您创建的 **install-config.yaml** 文件的安装目录。

由于您稍后会在安装过程中自行创建计算机器，因此可以忽略这个警告。

2. 修改 **<installation_directory>/manifests/cluster-scheduler-02-config.yml** Kubernetes 清单文件，以防止在 control plane 机器上调度 Pod：
 - a. 打开 **<installation_directory>/manifests/cluster-scheduler-02-config.yml** 文件。
 - b. 找到 **mastersSchedulable** 参数，并将其值设为 **False**。
 - c. 保存并退出文件。



注意

目前，由于 [Kubernetes 限制](#)，入口负载均衡器将无法访问在 control plane 机器上运行的路由器 Pod。以后的 OpenShift Container Platform 次要版本中可能不需要这一步骤。

3. 获取 Ignition 配置文件：

```
$ ./openshift-install create ignition-configs --dir=<installation_directory> 1
```

1 对于 <installation_directory>, 请指定相同的安装目录。

该目录中将生成以下文件：

```
.
├── auth
│   ├── kubeadmin-password
│   └── kubeconfig
├── bootstrap.ign
├── master.ign
├── metadata.json
└── worker.ign
```

1.1.10. 创建 Red Hat Enterprise Linux CoreOS (RHCOS) 机器

在您置备的 IBM Power 基础架构上安装集群前，必须先创建 RHCOS 机器供其使用。按照相应的步骤，使用 ISO 镜像或网络 PXE 启动来创建机器。

1.1.10.1. 使用 ISO 镜像创建 Red Hat Enterprise Linux CoreOS (RHCOS) 机器

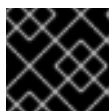
在您置备的 IBM Power 基础架构上安装集群前，必须先创建 RHCOS 机器供其使用。您可以使用 ISO 镜像来创建这些机器。

先决条件

- 获取集群的 Ignition 配置文件。
- 具有 HTTP 服务器的访问权限，以便您可从计算机进行访问，并且您创建的机器也可访问此服务器。

流程

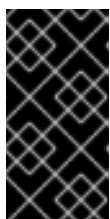
1. 将安装程序创建的 control plane、计算和 bootstrap Ignition 配置文件上传到 HTTP 服务器。记下这些文件的 URL。



重要

如果您计划在安装完成后在集群中添加更多计算机，请不要删除这些文件。

2. 从红帽客户门户上的[产品下载](#)页面或[RHCOS 镜像](#)页面，获取您选择的操作系统实例安装方法所需的 RHCOS 镜像。

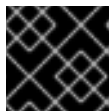


重要

RHCOS 镜像可能不会随着 OpenShift Container Platform 的每一发行版本都有改变。您必须下载最高版本的镜像，其版本号应小于或等于您安装的 OpenShift Container Platform 版本。如果可用，请使用与 OpenShift Container Platform 版本匹配的镜像版本。

您必须下载 ISO 文件和 RAW 磁盘文件。这些文件的名称类似以下示例：

- ISO: **rhcos-<version>-installer.<architecture>.iso**
 - 压缩的裸机 RAW: **rhcos-<version>-metal.<architecture>.raw.gz**
3. 将 RAW RHCOS 镜像文件上传到 HTTP 服务器并记录它的 URL。



重要

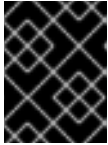
如果您计划在安装完成后在集群中添加更多计算机器，请不要删除这些文件。

4. 使用 ISO 启动 RHCOS 安装。使用如下安装选项之一：
- 将 ISO 镜像刻录到磁盘并直接启动。
 - 通过 LOM 接口使用 ISO 重定向。
5. 实例启动后，按 **TAB** 或 **E** 键编辑内核命令行。
6. 将参数添加到内核命令行：

```
coreos.inst=yes
coreos.inst.install_dev=sda ①
coreos.inst.image_url=<image_URL> ②
coreos.inst.ignition_url=http://example.com/config.ign ③
ip=<dhcp or static IP address> ④ ⑤
```

- ① 指定要安装到的系统块设备。
- ② 指定您上传到服务器的 RAW 镜像的 URL。
- ③ 指定此机器类型的 Ignition 配置文件的 URL。
- ④ 在每个节点中设置 **ip=dhcp** 或者设置单独的静态 IP 地址 (**ip=**) 和 DNS 服务器 (**nameserver=**)。For example, setting **ip=10.10.10.2::10.10.10.254:255.255.255.0:core0.example.com:enp1s0:none nameserver=4.4.4.41** sets:
 - 节点的 IP 地址为 **10.10.10.2**
 - 网关地址为 **10.10.10.254**
 - 子网掩码为 **255.255.255.0**
 - 主机名为 **core0.example.com**
 - DNS 服务器地址为 **4.4.4.41**
- ⑤ 如果使用多个网络接口或 DNS 服务器，您可以使用以下方法进一步自定义 IP 地址配置：
 - 如果您的系统有多个网络接口，您可以通过指定多个 **ip=** 条目来添加多个 IP 地址配置。
 - 如果您的系统有多个网络接口，您可以使用 DHCP 和静态 IP 配置的组合。您需要指定要使用的接口，例如 **ip=enp1s0:dhcp ip=10.10.10.2::10.10.10.254:255.255.255.0:core0.example.com:enp2s0:none**。

- 您可以为每个服务器添加一个 `nameserver=` 条目来提供多个 DNS 服务器，如 `nameserver=1.1.1.1 nameserver=8.8.8.8`。
7. 按 Enter 键完成安装。安装 RHCOS 后，系统会重启。系统重启后，它会应用您指定的 Ignition 配置文件。
 8. 继续为集群创建机器。



重要

此刻您必须创建 bootstrap 和 control plane 机器。由于计算机器中已默认部署了一些 Pod，因此在安装集群前，还要创建至少两台计算机器。

1.1.10.2. 通过 PXE 引导来创建 Red Hat Enterprise Linux CoreOS (RHCOS) 机器

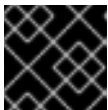
在您置备的裸机 IBM Power 基础架构上安装集群前，必须先创建 RHCOS 机器供其使用。您可以使用 PXE 引导来创建机器。

先决条件

- 获取集群的 Ignition 配置文件。
- 配置适用的 PXE 基础架构。
- 具有 HTTP 服务器的访问权限，以便您可从计算机进行访问。

流程

1. 将安装程序创建的 master、worker 和 bootstrap Ignition 配置文件上传到 HTTP 服务器。记下这些文件的 URL。



重要

如果您计划在安装完成后在集群中添加更多计算机器，请不要删除这些文件。

2. 从红帽客户门户上的 [产品下载](#) 页面或 [RHCOS 镜像](#) 页面，获取压缩的裸机 RAW 镜像、`kernel` 和 `initramfs` 文件。



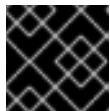
重要

RHCOS 镜像可能不会随着 OpenShift Container Platform 的每一发行版本都有改变。您必须下载最高版本的镜像，其版本号应小于或等于您安装的 OpenShift Container Platform 版本。如果可用，请使用与 OpenShift Container Platform 版本匹配的镜像版本。此流程只使用 RAW 镜像。对于裸机安装，RHCOS qcow2 镜像不被支持。

文件名包含 OpenShift Container Platform 版本号。它们类似以下示例：

- 压缩的裸机 RAW 镜像: `rhcos-<version>metal.<architecture>.raw.gz`
- `kernel`: `rhcos-<version>-installer-kernel-<architecture>`
- `initramfs`: `rhcos-<version>-installer-initramfs.<architecture>.img`

- 将裸机 RAW 镜像以及 **kernel** 和 **initramfs** 文件上传到 HTTP 服务器。



重要

如果您计划在安装完成后在集群中添加更多计算机器，请不要删除这些文件。

- 配置网络启动基础架构，以便在安装 RHCOS 后机器可从本地磁盘启动。
- 为 RHCOS 镜像配置 PXE 安装。
针对您的环境修改以下示例菜单条目之一，并验证能否正确访问镜像和 Ignition 文件：

- 对于 PXE：

```

DEFAULT pxeboot
TIMEOUT 20
PROMPT 0
LABEL pxeboot
  KERNEL http://<HTTP_server>/rhcos-<version>-installer-kernel-<architecture> 1
  APPEND ip=dhcp rd.neednet=1 initrd=http://<HTTP_server>/rhcos-<version>-installer-
initramfs.<architecture>.img console=tty0 console=ttyS0 coreos.inst=yes
coreos.inst.install_dev=sda coreos.inst.image_url=http://<HTTP_server>/rhcos-
<version>-metal.<architecture>.raw.gz
coreos.inst.ignition_url=http://<HTTP_server>/bootstrap.ign 2 3

```

- 1** 指定上传到 HTTP 服务器的 **kernel** 文件位置。
- 2** 如果您使用多个 NIC，请在 **ip** 选项中指定一个接口。例如，要在名为 **eno1** 的 NIC 上使用 DHCP，请设置 **ip=eno1:dhcp**。
- 3** 指定上传到 HTTP 服务器的 RHCOS 文件的位置。**initrd** 参数值是 **initramfs** 文件的位置，**coreos.inst.image_url** 参数值是压缩的裸机 RAW 镜像的位置，**coreos.inst.ignition_url** 参数值则是 bootstrap Ignition 配置文件的位置。

- 继续为集群创建机器。



重要

此刻您必须创建 bootstrap 和 control plane 机器。由于计算机器上已默认部署了一些 Pod，因此在安装集群前，还要创建至少两台计算机器。

1.1.11. 创建集群

要创建 OpenShift Container Platform 集群，请等待您通过安装程序生成的 Ignition 配置文件所置备的机器上完成 bootstrap 过程。

先决条件

- 为集群创建所需的基础架构。
- 已获得安装程序并为集群生成了 Ignition 配置文件。
- 已使用 Ignition 配置文件为集群创建 RHCOS 机器。

- 您的机器能够直接访问互联网。

流程

1. 监控 bootstrap 过程：

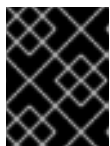
```
$ ./openshift-install --dir=<installation_directory> wait-for bootstrap-complete \ 1
--log-level=info 2
INFO Waiting up to 30m0s for the Kubernetes API at https://api.test.example.com...
INFO API v1.16.2 up
INFO Waiting up to 30m0s for bootstrapping to complete...
INFO It is now safe to remove the bootstrap resources
```

1 对于 **<installation_directory>**，请指定安装文件保存到的目录的路径。

2 要查看不同的安装详情，请指定 **warn**、**debug** 或 **error**，而不要指定 **info**。

Kubernetes API 服务器提示已在 control plane 机器上完成 bootstrap 时，命令运行成功。

2. bootstrap 过程完成后，请从负载均衡器中删除 bootstrap 机器。



重要

此时您必须从负载均衡器中删除 bootstrap 机器。您还可以删除或重新格式化机器本身。

1.1.12. 登录集群

您可以通过导出集群 **kubeconfig** 文件，以默认系统用户身份登录集群。**kubeconfig** 文件包含关于集群的信息，供 CLI 用于将客户端连接到正确集群和 API 服务器。该文件特只适用于一个特定的集群，在 OpenShift Container Platform 安装过程中创建。

先决条件

- 部署 OpenShift Container Platform 集群。
- 安装 **oc** CLI。

流程

1. 导出 **kubeadmin** 凭证：

```
$ export KUBECONFIG=<installation_directory>/auth/kubeconfig 1
```

1 对于 **<installation_directory>**，请指定安装文件保存到的目录的路径。

2. 使用导出的配置，验证能否成功运行 **oc** 命令：

```
$ oc whoami
system:admin
```


1.1.13. 批准机器的 CSR

将机器添加到集群时，会为您添加的每台机器生成两个待处理证书签名请求（CSR）。您必须确认这些 CSR 已获得批准，或根据需要自行批准。

先决条件

- 您已将机器添加到集群中。

流程

1. 确认集群可以识别这些机器：

```
$ oc get nodes

NAME      STATUS    ROLES    AGE   VERSION
master-0  Ready     master   63m   v1.16.2
master-1  Ready     master   63m   v1.16.2
master-2  Ready     master   64m   v1.16.2
worker-0  NotReady  worker   76s   v1.16.2
worker-1  NotReady  worker   70s   v1.16.2
```

输出将列出您创建的所有机器。

2. 检查待处理的 CSR，并确保添加到集群中的每台机器都有 **Pending** 或 **Approved** 状态的客户端和服务器请求：

```
$ oc get csr

NAME      AGE   REQUESTOR                                     CONDITION
csr-8b2br  15m   system:serviceaccount:openshift-machine-config-operator:node-
bootstrapper Pending 1
csr-8vnps  15m   system:serviceaccount:openshift-machine-config-operator:node-
bootstrapper Pending
csr-bfd72  5m26s system:node:ip-10-0-50-126.us-east-2.compute.internal
Pending 2
csr-c57lv  5m26s system:node:ip-10-0-95-157.us-east-2.compute.internal
Pending
...
```

1 客户端请求 CSR。

2 服务器请求 CSR。

在本例中，两台机器加入了集群。您可能在列表中看到更多已批准的 CSR。

3. 如果 CSR 没有获得批准，请在所添加机器的所有待处理 CSR 都处于 **Pending** 状态后，为您的集群机器批准这些 CSR：



注意

由于 CSR 会自动轮转，因此请在将机器添加到集群后一小时内批准您的 CSR。如果没有在一小时内批准，证书将会轮转，每个节点将会存在多个证书。您必须批准所有这些证书。批准初始 CSR 后，集群的 **kube-controller-manager** 会自动批准后续的节点客户端 CSR。您必须实施一个方法来自动批准 kubelet 提供的证书请求。

- 若要单独批准，请对每个有效的 CSR 运行以下命令：

```
$ oc adm certificate approve <csr_name> ❶
```

- ❶ **<csr_name>** 是当前 CSR 列表中 CSR 的名称。

- 要批准所有待处理的 CSR，请运行以下命令：

```
$ oc get csr -o go-template='{{range .items}}{{if not .status}}{{.metadata.name}}{\n"}\n{{end}}' | xargs oc adm certificate approve
```

其他信息

- 如需有关 CSR 的更多信息，请参阅[证书签名请求](#)。

1.1.14. 初始 Operator 配置

在 control plane 初始化后，您必须立即配置一些 Operator 以便它们都可用。

先决条件

- 您的 control plane 已初始化。

流程

- 观察集群组件上线：

```
$ watch -n5 oc get clusteroperators
```

NAME	VERSION	AVAILABLE	PROGRESSING	DEGRADED	SINCE
authentication	4.3.0	True	False	False	69s
cloud-credential	4.3.0	True	False	False	12m
cluster-autoscaler	4.3.0	True	False	False	11m
console	4.3.0	True	False	False	46s
dns	4.3.0	True	False	False	11m
image-registry	4.3.0	True	False	False	5m26s
ingress	4.3.0	True	False	False	5m36s
kube-apiserver	4.3.0	True	False	False	8m53s
kube-controller-manager	4.3.0	True	False	False	7m24s
kube-scheduler	4.3.0	True	False	False	12m
machine-api	4.3.0	True	False	False	12m
machine-config	4.3.0	True	False	False	7m36s
marketplace	4.3.0	True	False	False	7m54m
monitoring	4.3.0	True	False	False	7h54s

network	4.3.0	True	False	False	5m9s
node-tuning	4.3.0	True	False	False	11m
openshift-apiserver	4.3.0	True	False	False	11m
openshift-controller-manager	4.3.0	True	False	False	5m943s
openshift-samples	4.3.0	True	False	False	3m55s
operator-lifecycle-manager	4.3.0	True	False	False	11m
operator-lifecycle-manager-catalog	4.3.0	True	False	False	11m
service-ca	4.3.0	True	False	False	11m
service-catalog-apiserver	4.3.0	True	False	False	5m26s
service-catalog-controller-manager	4.3.0	True	False	False	5m25s
storage	4.3.0	True	False	False	5m30s

2. 配置不可用的 Operator。

1.1.14.1. 镜像 registry 存储配置

对于不提供默认存储的平台，**Image-registry** Operator 最初将不可用。安装后，您必须配置 registry 使用的存储，这样 Registry Operator 才可用。

提供了配置 PersistentVolume 的说明，这是生产集群所需要的；也提供了将空目录配置为存储位置的说明，这仅适用于非生产集群。

1.1.14.1.1. 为裸机配置 registry 存储

1.1.14.1.2. 为 IBM Power 配置 registry 存储

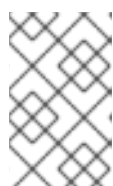
作为集群管理员，在安装后需要配置 registry 来使用存储。

先决条件

- 具有 Cluster Administrator 权限
- 在裸机上有一个集群。IBM Power。
- 为集群置备持久性存储，如 Red Hat OpenShift Container Storage。若要部署私有镜像 registry，您的存储必须提供 ReadWriteMany 访问模式。
- 必须有“100Gi”容量。

流程

1. 为了配置 registry 使用存储，需要修改 **configs.imageregistry/cluster** 资源中的 **spec.storage.pvc**。



注意

当使用类似 NFS 的共享存储时，强烈建议使用 **supplementalGroups** 策略，即指明安全性上下文的允许补充组，而不是 **fsGroup** ID。详情请参考 NFS 组 ID 文档。

2. 验证您没有 registry Pod：

```
$ oc get pod -n openshift-image-registry
```



注意

- 如果存储类型为 **emptyDIR**，则副本数不能超过 **1**。
- 如果存储类型是 **NFS**，您必须启用 **no_wdelay** 和 **root_squash** 挂载选项。
例如：

```
# cat /etc/exports
/mnt/data *(rw,sync,no_wdelay,root_squash,insecure,fsid=0)
sh-4.3# exportfs -rv
exporting */mnt/data
```

3. 检查 registry 配置：

```
$ oc edit configs.imageregistry.operator.openshift.io

storage:
  pvc:
    claim:
```

将 **claim** 字段留空以允许自动创建一个 **image-registry-storage** PVC。

4. 检查 **clusteroperator** 的状态：

```
$ oc get clusteroperator image-registry
```

1.1.14.1.3. 在非生产集群中配置镜像 registry 存储

您必须为 Image Registry Operator 配置存储。对于非生产集群，您可以将镜像 registry 设置为空目录。如果您这样做，重启 registry 后会丢失所有镜像。

流程

- 将镜像 registry 存储设置为空目录：

```
$ oc patch configs.imageregistry.operator.openshift.io cluster --type merge --patch '{"spec": {"storage":{"emptyDir":{}}}'
```



警告

仅可为非生产集群配置这个选项。

如果在 Image Registry Operator 初始化其组件前运行此命令，**oc patch** 命令会失败并显示以下错误：

```
Error from server (NotFound): configs.imageregistry.operator.openshift.io "cluster" not found
```

等待几分钟，然后再次运行该命令。

1.1.15. 在用户置备的基础架构上完成安装

完成 Operator 配置后，可以在您提供的基础架构上完成集群安装。

先决条件

- 您的 control plane 已初始化。
- 已完成初始 Operator 配置。

流程

1. 确认所有集群组件都已上线：

```
$ watch -n5 oc get clusteroperators
```

NAME	VERSION	AVAILABLE	PROGRESSING	DEGRADED	SINCE
authentication	4.3.0	True	False	False	10m
cloud-credential	4.3.0	True	False	False	22m
cluster-autoscaler	4.3.0	True	False	False	21m
console	4.3.0	True	False	False	10m
dns	4.3.0	True	False	False	21m
image-registry	4.3.0	True	False	False	16m
ingress	4.3.0	True	False	False	16m
kube-apiserver	4.3.0	True	False	False	19m
kube-controller-manager	4.3.0	True	False	False	18m
kube-scheduler	4.3.0	True	False	False	22m
machine-api	4.3.0	True	False	False	22m
machine-config	4.3.0	True	False	False	18m
marketplace	4.3.0	True	False	False	18m
monitoring	4.3.0	True	False	False	18m
network	4.3.0	True	False	False	16m
node-tuning	4.3.0	True	False	False	21m
openshift-apiserver	4.3.0	True	False	False	21m
openshift-controller-manager	4.3.0	True	False	False	17m
openshift-samples	4.3.0	True	False	False	14m
operator-lifecycle-manager	4.3.0	True	False	False	21m
operator-lifecycle-manager-catalog	4.3.0	True	False	False	21m
service-ca	4.3.0	True	False	False	21m
service-catalog-apiserver	4.3.0	True	False	False	16m
service-catalog-controller-manager	4.3.0	True	False	False	16m
storage	4.3.0	True	False	False	16m

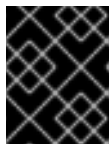
当所有集群 Operator 状态都是 **AVAILABLE** 时，您可以完成安装。

2. 监控集群完成：

```
$ ./openshift-install --dir=<installation_directory> wait-for install-complete 1  
INFO Waiting up to 30m0s for the cluster to initialize...
```

- 1** 对于 **<installation_directory>**，请指定安装文件保存到的目录的路径。

Cluster Version Operator 完成从 Kubernetes API 服务器部署 OpenShift Container Platform 集群时，命令运行成功。



重要

安装程序生成的 Ignition 配置文件中所含的证书会在 24 小时后过期。您必须以非降级状态持续运行集群 24 小时，以确保完成第一次证书轮转。

3. 确认 Kubernetes API 服务器正在与 Pod 通信。

a. 要查看所有 Pod 的列表，请使用以下命令：

```
$ oc get pods --all-namespaces
```

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
openshift-apiserver-operator	openshift-apiserver-operator-85cb746d55-zqhs8	1/1	Running	0	9m
openshift-apiserver	apiserver-67b9g	1/1	Running	0	3m
openshift-apiserver	apiserver-ljcmx	1/1	Running	0	1m
openshift-apiserver	apiserver-z25h4	1/1	Running	0	2m
openshift-authentication-operator	authentication-operator-69d5d8bf84-vh2n8	1/1	Running	0	5m
...					

b. 使用以下命令，查看上一命令的输出中所列 Pod 的日志：

```
$ oc logs <pod_name> -n <namespace> ①
```

① 指定 Pod 名称和命名空间，如上一命令的输出中所示。

如果 Pod 日志显示，Kubernetes API 服务器可以与集群机器通信。

1.1.16. 后续步骤

- [自定义集群](#)。
- 若有需要，您可以[选择不使用远程健康报告](#)。

1.2. 在受限网络中的 IBM POWER 上安装集群

在 OpenShift Container Platform 版本 4.3 中，您可以在受限网络中置备的 IBM Power 基础架构上安装集群。



重要

非裸机平台还有其他注意事项。在尝试在此类环境中安装 OpenShift Container Platform 集群前，请参阅[有关在未经测试的平台上部署 OpenShift Container Platform 的指南](#)中的信息。

1.2.1. 先决条件

- 在堡垒主机上创建镜像 registry，并获取您的 OpenShift Container Platform 版本的 `imageContentSources` 数据。



重要

由于安装介质位于堡垒主机上，因此请使用该计算机完成所有安装步骤。

- 为集群置备持久性存储。若要部署私有镜像 registry，您的存储必须提供 ReadWriteMany 访问模式。
- 查看有关 [OpenShift Container Platform 安装和更新](#) 流程的详细信息。
- 如果使用防火墙并计划使用遥测（telemetry），您必须将防火墙配置为允许集群需要访问的站点。



注意

如果您要配置代理，请务必也要查看此站点列表。

1.2.2. 关于在受限网络中安装

在 OpenShift Container Platform 4.3 中，可以执行不需要有效的互联网连接来获取软件组件的安装。受限网络安装只能在您置备的基础架构上完成，不能在安装程序置备的基础架构上完成，因此您的平台选择会受到限制。

要完成受限网络安装，您必须创建一个 registry，镜像 OpenShift Container Platform registry 的内容并包含其安装介质。您可以在堡垒主机上创建此镜像，该主机可同时访问互联网和您的封闭网络，也可以使用满足您的限制条件的其他方法。



重要

受限网络安装始终使用用户置备的基础架构。由于用户置备安装配置的复杂性，在尝试受限网络安装前，请考虑完成标准用户置备基础架构安装。通过完成此测试安装，您可以更轻松地隔离和排查您在受限网络中安装时可能出现的问题。

1.2.2.1. 其他限制

受限网络中的集群还有以下额外限制：

- ClusterVersion 状态包含 **Unable to retrieve available updates** 错误。
- 默认情况下，您无法使用 Developer Catalog 的内容，因为您无法访问所需的 ImageStreamTag。

1.2.3. 具有用户置备基础架构的集群的机器要求

对于含有用户置备的基础架构的集群，您必须部署所有所需的机器。

1.2.3.1. 所需的机器

最小的 OpenShift Container Platform 集群需要下列主机：

- 一个临时 bootstrap 机器
- 三台 control plane 或 master 机器
- 至少两台计算机器，也称为 worker 机器



注意

集群要求 bootstrap 机器在三台 control plane 机器上部署 OpenShift Container Platform 集群。您可在安装集群后删除 bootstrap 机器。



重要

要保持集群的高可用性，请将独立的物理主机用于这些集群机器。

bootstrap、control plane 以及计算（compute）机器必须使用 Red Hat Enterprise Linux CoreOS (RHCOS) 作为操作系统。

请注意，RHCOS 基于 Red Hat Enterprise Linux 8，并继承其所有硬件认证和要求。请查看[Red Hat Enterprise Linux 技术功能及限制](#)。

1.2.3.2. 网络连接要求

所有 Red Hat Enterprise Linux CoreOS (RHCOS) 机器在启动过程中需要 **initramfs** 中的网络从 Machine Config Server 获取 Ignition 配置文件。在初次启动过程中，需要一个 DHCP 服务器或设置了静态 IP 地址来建立网络连接，以下载它们的 Ignition 配置文件。

1.2.3.3. 最低资源要求

每台集群机器都必须满足以下最低要求：

机器	操作系统	vCPU	虚拟内存	存储
bootstrap	RHCOS	4	16 GB	120 GB
Control plane	RHCOS	2	16 GB	120 GB
Compute	RHCOS	RHCOS 或 RHEL 7.6	2	8 GB

1.2.3.4. 证书签名请求管理

在使用您置备的基础架构时，集群只能有限地访问自动机器管理，因此您必须提供一种在安装后批准集群证书签名请求 (CSR) 的机制。**kube-controller-manager** 只能批准 kubelet 客户端 CSR。**machine-approver** 无法保证使用 kubelet 凭证请求的提供证书的有效性，因为它不能确认是正确的机器发出了该请求。您必须决定并实施一种方法，以验证 kubelet 提供证书请求的有效性并进行批准。

1.2.4. 创建用户置备的基础架构

在部署采用用户置备的基础架构的 OpenShift Container Platform 集群前，您必须创建底层基础架构。

先决条件

- 在为集群创建支持基础架构之前，请参阅[OpenShift Container Platform 4.x Tested Integrations](#)页。

流程

1. 在每个节点上配置 DHCP 或设置静态 IP 地址。
2. 提供所需的负载均衡器。
3. 配置机器的端口。
4. 配置 DNS。
5. 确保网络可以正常工作。

1.2.4.1. 用户置备的基础架构对网络的要求

所有 Red Hat Enterprise Linux CoreOS (RHCOS) 机器在启动过程中需要 **initramfs** 中的网络从 Machine Config Server 获取 Ignition 配置。

在初次启动过程中，需要一个 DHCP 服务器或集群中的每个机器都设置了静态 IP 地址来建立网络连接，以下载它们的 Ignition 配置文件。

建议您使用 DHCP 服务器为集群进行长期机器管理。确保 DHCP 服务器已配置为向集群机器提供持久 IP 地址和主机名。

成功安装集群后，在每个 master 节点上运行的 Kubernetes API 服务器必须能够解析集群机器的节点名称。如果 API 服务器和 worker 节点位于不同的区域中，您可以配置默认 DNS 搜索区域，以便 API 服务器能够解析节点名称。另一种支持的方法是始终在节点对象和所有 DNS 请求中使用完全限定域名来指代主机。

您必须配置机器间的网络连接，以便集群组件进行通信。每台机器都必须能够解析集群中所有其他机器的主机名。

表 1.6. 所有机器到所有机器

协议	端口	描述
ICMP	N/A	网络可访问性测试
TCP	9000-9999	主机级别的服务，包括端口 9100-9101 上的节点导出器和端口 9099 上的 Cluster Version Operator。
	10250-10259	Kubernetes 保留的默认端口
	10256	openshift-sdn
UDP	4789	VXLAN 和 Geneve
	6081	VXLAN 和 Geneve

协议	端口	描述
	9000-9999	主机级别的服务，包括端口 9100-9101 上的节点导出器。
TCP/UDP	30000-32767	Kubernetes NodePort

表 1.7. 要通过控制平面的所有机器

协议	端口	描述
TCP	2379-2380	etcd 服务器、对等和指标端口
	6443	Kubernetes API

网络拓扑要求

您为集群置备的基础架构必须满足下列网络拓扑要求。

负载均衡器

在安装 OpenShift Container Platform 前，您必须置备两个满足以下要求的负载均衡器：

1. **API 负载均衡器**：提供一个通用端点，供用户（包括人和机器）与平台交互和配置。配置以下条件：
 - 只适用于第 4 层负载均衡。这可被称为 Raw TCP、SSL Passthrough 或者 SSL 桥接模式。如果使用 SSL Bridge 模式，必须为 API 路由启用 Server Name Indication (SNI)。
 - 无状态负载平衡算法。这些选项根据负载均衡器的实现而有所不同。



注意

API 负载均衡器正常工作不需要会话持久性。

在负载均衡器的前端和后台配置以下端口：

表 1.8. API 负载均衡器

端口	后端机器（池成员）	内部	外部	描述
6443	Bootstrap 和 control plane.bootstrap 机器初始化集群 control plane 后，您要从负载均衡器中删除 bootstrap 机器。您必须为 API 服务器健康检查探测配置 /readyz 端点。	X	X	Kubernetes API 服务器
22623	Bootstrap 和 control plane.bootstrap 机器初始化集群 control plane 后，您要从负载均衡器中删除 bootstrap 机器。	X		机器配置服务器



注意

负载均衡器必须配置为，从 API 服务器关闭 `/readyz` 端点到从池中删除 API 服务器实例时最多需要 30 秒。在 `/readyz` 返回错误或处于健康状态后的时间范围内，端点必须被删除或添加。每 5 秒或 10 秒探测一次，有两个成功请求处于健康状态，三个成为不健康的请求经过测试。

2. **应用程序入口负载均衡器**:提供来自集群外部的应用程序流量流量的 Ingress 点。配置以下条件：

- 只适用于第 4 层负载均衡。这可被称为 Raw TCP、SSL Passthrough 或者 SSL 桥接模式。如果使用 SSL Bridge 模式，您必须为 Ingress 路由启用 Server Name Indication (SNI)。
- 建议根据可用选项以及平台上托管的应用程序类型，使用基于连接的或者基于会话的持久性。

在负载均衡器的前端和后台配置以下端口：

表 1.9. 应用程序入口负载均衡器

端口	后端机器 (池成员)	内部	外部	描述
443	默认运行入口路由器 Pod、计算或 worker 的机器。	X	X	HTTPS 流量
80	默认运行入口路由器 Pod、计算或 worker 的机器。	X	X	HTTP 流量

提示

如果负载均衡器可以看到客户端的真实 IP 地址，启用基于 IP 的会话持久性可提高使用端到端 TLS 加密的应用程序的性能。



注意

OpenShift Container Platform 集群需要正确配置入口路由器。control plane 初始化后，您必须配置入口路由器。

1.2.4.2. 用户置备 DNS 要求

采用用户置备的基础架构的 OpenShift Container Platform 集群需要以下 DNS 记录。在每一记录中，`<cluster_name>` 是集群名称，`<base_domain>` 则是您在 `install-config.yaml` 文件中指定的集群基域。完整的 DNS 记录采用如下格式：`<component>.<cluster_name>.<base_domain>.`

表 1.10. 所需的 DNS 记录

组件	记录	描述
Kubernetes API	<code>api.<cluster_name>.<base_domain>.</code>	此 DNS A/AAAA 或 CNAME 记录必须指向 control plane 机器的负载均衡器。此记录必须能由集群外的客户端和集群内的所有节点解析。

组件	记录	描述
	api-int.<cluster_name>.<base_domain>.	<p>此 DNS A/AAAA 或 CNAME 记录必须指向 control plane 机器的负载均衡器。此记录必须可从集群内的所有节点解析。</p> <div data-bbox="1038 409 1145 786" style="background-color: black; color: white; padding: 5px; display: inline-block;"> <p>重要</p> <p>API 服务器必须能够根据在 Kubernetes 中记录的主机名解析 worker 节点。如果无法解析节点名称，代理的 API 调用会失败，而且您无法从 Pod 检索日志。</p> </div>
Routes	*.apps.<cluster_name>.<base_domain>.	<p>通配符 DNS A/AAAA 或 CNAME 记录，指向以运行入口路由器 Pod 的机器（默认为 worker 节点）为目标的负载均衡器。此记录必须能由集群外的客户端和集群内的所有节点解析。</p>
etcd	etcd-<index>.<cluster_name>.<base_domain>.	<p>OpenShift Container Platform 要求每个 etcd 实例的 DNS A/AAAA 记录指向托管实例的 control plane 机器。etcd 实例通过 <index> 值来区分，值的范围为 0 到 n-1，其中 n 是集群中 control plane 机器的数量。DNS 记录必须解析到 control plane 机器的单播 IPv4 地址，并且这些记录必须可以从集群中的所有节点解析。</p>

组件	记录	描述
	<code>_etcd-server-ssl._tcp.<cluster_name>.<base_domain></code>	<p>对于每台 control plane 机器，OpenShift Container Platform 还需要该机器上具有 etcd 服务器的 SRV DNS 记录，其优先级为 0，权重为 10，端口则为 2380。使用三台 control plane 机器的集群需要以下记录：</p> <pre># _service._proto.name. TTL class SRV priority weight port target. _etcd-server-ssl._tcp. <cluster_name>. <base_domain>. 86400 IN SRV 0 10 2380 etcd- 0.<cluster_name>. <base_domain> _etcd-server-ssl._tcp. <cluster_name>. <base_domain>. 86400 IN SRV 0 10 2380 etcd- 1.<cluster_name>. <base_domain> _etcd-server-ssl._tcp. <cluster_name>. <base_domain>. 86400 IN SRV 0 10 2380 etcd- 2.<cluster_name>. <base_domain></pre>

1.2.5. 生成 SSH 私钥并将其添加到代理中

如果要在集群上执行安装调试或灾难恢复，则必须为 **ssh-agent** 和安装程序提供 SSH 密钥。



注意

在生产环境中，您需要进行灾难恢复和调试。

您可以使用此密钥以 **core** 用户身份通过 SSH 连接到 master 节点。在部署集群时，此密钥会添加到 **core** 用户的 `~/.ssh/authorized_keys` 列表中。



注意

您必须使用一个本地密钥，而不要使用在特定平台上配置的密钥，如 [AWS 密钥对](#)。

流程

1. 如果还没有为计算机上免密码身份验证而配置的 SSH 密钥，请创建一个。例如，在使用 Linux 操作系统的计算机上运行以下命令：

```
$ ssh-keygen -t rsa -b 4096 -N "" \
-f <path>/<file_name> 1
```

- 1 指定 SSH 密钥的路径和文件名，如 `~/.ssh/id_rsa`。不要指定已存在的 SSH 密钥，因为它会被覆盖。

运行此命令会在指定的位置生成不需要密码的 SSH 密钥。

2. 作为后台任务启动 `ssh-agent` 进程：

```
$ eval "$(ssh-agent -s)"
Agent pid 31874
```

3. 将 SSH 私钥添加到 `ssh-agent`：

```
$ ssh-add <path>/<file_name> 1
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

- 1 指定 SSH 私钥的路径和文件名，如 `~/.ssh/id_rsa`

后续步骤

- 在安装 OpenShift Container Platform 时，为安装程序提供 SSH 公钥。

1.2.6. 手动创建安装配置文件

对于使用用户自备的基础架构的 OpenShift Container Platform 安装，您必须手动生成安装配置文件。

先决条件

- 获取 OpenShift Container Platform 安装程序和集群的访问令牌。

流程

1. 创建用来存储您所需的安装资产的安装目录：

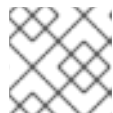
```
$ mkdir <installation_directory>
```



重要

您必须创建目录。一些安装信息，如 bootstrap X.509 证书，有较短的过期间隔，因此不要重复使用安装目录。如果要重复使用另一个集群安装中的个别文件，可以将其复制到您的目录中。但是，一些安装数据的文件名可能会在发行版本之间有所改变。从 OpenShift Container Platform 老版本中复制安装文件时要格外小心。

2. 自定义以下 `install-config.yaml` 文件模板，并将它保存到 `<installation_directory>` 中。

**注意**

此配置文件必须命名为 `install-config.yaml`。

3. 备份 `install-config.yaml` 文件，以便用于安装多个集群。

**重要**

`install-config.yaml` 文件会在安装过程的下一步骤中消耗掉。现在必须备份它。

1.2.6.1. 裸机 `install-config.yaml` 文件示例

1.2.6.2. IBM Power 的 `install-config.yaml` 文件示例

您可以自定义 `install-config.yaml` 文件，以指定有关 OpenShift Container Platform 集群平台的更多信息，或修改所需参数的值。

```

apiVersion: v1
baseDomain: example.com 1
compute:
- hyperthreading: Enabled 2 3
  name: worker
  replicas: 0 4
controlPlane:
  hyperthreading: Enabled 5 6
  name: master 7
  replicas: 3 8
metadata:
  name: test 9
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14 10
    hostPrefix: 23 11
  networkType: OpenShiftSDN
  serviceNetwork: 12
  - 172.30.0.0/16
platform:
  none: {} 13
fips: false 14
pullSecret: '{"auths": ...}' 15
sshKey: 'ssh-ed25519 AAAA...' 16

```

1 集群的基域。所有 DNS 记录都必须是这个基域的子域，并包含集群名称。

2 5 `controlPlane` 部分是一个单映射，但 `compute` 部分是一系列映射。为满足不同数据结构的要求，`compute` 部分的第一行必须以连字符 - 开头，`controlPlane` 部分的第一行则不可以连字符开头。虽然这两个部分目前都定义单个机器池，但未来的 OpenShift Container Platform 版本可能会支持在安装过程中定义多个计算池。只使用一个 control plane 池。

3 6 7 是否要启用或禁用并发多线程或超线程。默认情况下，启用并发多线程以提高机器内核的性能。您可以通过将参数值设为 **Disabled** 来禁用。如果您在某些集群机器上禁用并发多线程，则必须在所有集群机器上禁用。



重要

如果禁用并发多线程，请确保在容量规划时考虑到机器性能可能会显著降低的问题。

- 4 **replicas** 参数的值必须设置为 **0**。此参数控制集群为您创建和管理的 worker 数量，使用户置备的基础架构时集群不会执行这些功能。在完成 OpenShift Container Platform 安装前，您必须手动为集群部署 worker 机器。
- 8 您添加到集群的 control plane 机器数量。由于集群将这个值用作集群中 etcd 端点的数量，因此该值必须与您部署的 control plane 机器数量匹配。
- 9 您在 DNS 记录中指定的集群名称。
- 10 从中分配 Pod IP 地址的 IP 地址块。此块不得与现有的物理网络重叠。这些 IP 地址用于 Pod 网络。如果您需要从外部网络访问 Pod，请配置负载均衡器和路由器来管理流量。
- 11 分配给每个单独节点的子网前缀长度。例如，如果 **hostPrefix** 设为 **23**，则每个节点从所给的 **cidr** 中分配一个 **/23** 子网，这样就能有 510 ($2^{(32 - 23)} - 2$) 个 Pod IP 地址。如果您需要从外部网络访问节点，请配置负载均衡器和路由器来管理流量。
- 12 用于服务 IP 地址的 IP 地址池。您只能输入一个 IP 地址池。如果您需要从外部网络访问服务，请配置负载均衡器和路由器来管理流量。
- 13 您必须将平台设置为 **none**。您无法为 IBM Power 基础架构提供额外的平台配置变量。
- 14 是否启用或禁用 FIPS 模式。默认情况下不启用 FIPS 模式。如果启用了 FIPS 模式，运行 OpenShift Container Platform 的 Red Hat Enterprise Linux CoreOS (RHCOS) 机器会绕过默认的 Kubernetes 加密套件，并使用由 RHCOS 提供的加密模块。
- 15 从 Red Hat OpenShift Cluster Manager 站点的 [Pull Secret](#) 页面中获取的 pull secret。通过此 pull secret，您可以进行所含授权机构提供的服务的身份验证，这些服务包括为 OpenShift Container Platform 组件提供容器镜像的 Quay.io。
- 16 Red Hat Enterprise Linux CoreOS (RHCOS) 中 **core** 用户的默认 SSH 密钥的公钥部分。



注意

对于您要在其上执行安装调试或灾难恢复的生产环境 OpenShift Container Platform 集群，请指定 **ssh-agent** 进程使用的 SSH 密钥。

1.2.6.3. 在安装过程中配置集群范围代理

生产环境可能会拒绝直接访问互联网，而是提供 HTTP 或 HTTPS 代理。您可以通过在 **install-config.yaml** 文件中配置代理设置，将新的 OpenShift Container Platform 集群配置为使用代理。

先决条件

- 现有的 **install-config.yaml** 文件。
- 查看集群需要访问的站点，并决定是否需要绕过代理。默认情况下代理所有集群出口流量，包括对托管云供应商 API 的调用。若有需要，将站点添加到 Proxy 对象的 **spec.noProxy** 字段来绕过代理服务器。



注意

Proxy 对象的 **status.noProxy** 字段默认填充实例元数据端点 (169.254.169.254), 以及您的安装配置中 **networking.machineCIDR**、**networking.clusterNetwork.cidr** 和 **networking.serviceNetwork[]** 字段的值。

流程

1. 编辑 **install-config.yaml** 文件并添加代理设置。例如：

```
apiVersion: v1
baseDomain: my.domain.com
proxy:
  httpProxy: http://<username>:<pswd>@<ip>:<port> 1
  httpsProxy: http://<username>:<pswd>@<ip>:<port> 2
  noProxy: example.com 3
  additionalTrustBundle: | 4
    -----BEGIN CERTIFICATE-----
    <MY_TRUSTED_CA_CERT>
    -----END CERTIFICATE-----
...

```

- 1 用于创建集群外 HTTP 连接的代理 URL。URL 必须是 **http**。如果您使用不要求额外代理配置但需要额外 CA 的 MITM 透明代理网络，则不得指定 **httpProxy** 值。
- 2 用于创建集群外 HTTPS 连接的代理 URL。如果未指定此字段，**httpProxy** 会同时用于 HTTP 和 HTTPS 连接。如果您使用不要求额外代理配置但需要额外 CA 的 MITM 透明代理网络，则不得指定 **httpsProxy** 值。
- 3 要排除代理的目标域名、域、IP 地址或其他网络 CIDR 的逗号分隔列表。域之前加上前缀。可包含该域的所有子域。使用 * 可对所有目的地绕过所有代理。
- 4 如果提供，安装程序会在 **openshift-config** 命名空间中生成名为 **user-ca-bundle** 的 ConfigMap，其包含代理 HTTPS 连接所需的一个或多个额外 CA 证书。然后，Cluster Network Operator 会创建 **trusted-ca-bundle** ConfigMap，将这些内容与 Red Hat Enterprise Linux CoreOS (RHCOS) 信任捆绑包合并，Proxy 对象的 **trustedCA** 字段中也会引用此 ConfigMap。**additionalTrustBundle** 字段是必需的，除非代理的身份证书由来自 RHCOS 信任捆绑包的颁发机构签名。如果您使用不要求额外代理配置但需要额外 CA 的 MITM 透明代理网络，您必须提供 MITM CA 证书。



注意

安装程序不支持代理的 **readinessEndpoints** 字段。

2. 保存该文件，并在安装 OpenShift Container Platform 时引用。

安装程序会创建一个名为 **cluster** 的集群范围代理，该代理使用提供的 **install-config.yaml** 文件中的代理设置。如果没有提供代理设置，仍然会创建 **cluster** Proxy 对象，但它会有一个零 **spec**。



注意

只支持名为 **cluster** 的 Proxy 对象，且无法创建额外的代理。

1.2.7. 创建 Kubernetes 清单和 Ignition 配置文件

由于您必须修改一些集群定义文件并要手动启动集群机器，因此您必须生成 Kubernetes 清单和 Ignition 配置文件，集群需要这两项来创建其机器。



重要

安装程序生成的 Ignition 配置文件中所含的证书会在 24 小时后过期。您必须完成集群安装，并使集群以非降级状态运行 24 小时，以确保完成第一次证书轮转。

先决条件

- 获取 OpenShift Container Platform 安装程序。
- 创建 **install-config.yaml** 安装配置文件。

流程

1. 为集群生成 Kubernetes 清单：

```
$ ./openshift-install create manifests --dir=<installation_directory> 1
INFO Consuming Install Config from target directory
WARNING Making control-plane schedulable by setting MastersSchedulable to true for
Scheduler cluster settings
```

- 1** 对于 **<installation_directory>**，请指定含有您创建的 **install-config.yaml** 文件的安装目录。

由于您稍后会在安装过程中自行创建计算机器，因此可以忽略这个警告。

2. 修改 **<installation_directory>/manifests/cluster-scheduler-02-config.yml** Kubernetes 清单文件，以防止在 control plane 机器上调度 Pod：
 - a. 打开 **<installation_directory>/manifests/cluster-scheduler-02-config.yml** 文件。
 - b. 找到 **mastersSchedulable** 参数，并将其值设为 **False**。
 - c. 保存并退出文件。



注意

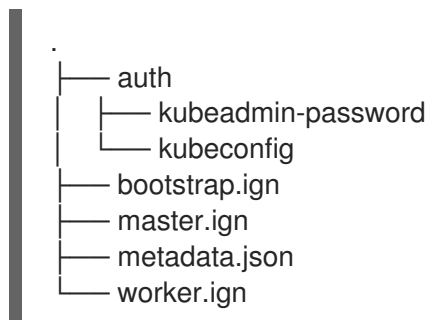
目前，由于 [Kubernetes 限制](#)，入口负载均衡器将无法访问在 control plane 机器上运行的路由器 Pod。以后的 OpenShift Container Platform 次要版本中可能不需要这一步骤。

3. 获取 Ignition 配置文件：

```
$ ./openshift-install create ignition-configs --dir=<installation_directory> 1
```

- 1** 对于 **<installation_directory>**，请指定相同的安装目录。

该目录中将生成以下文件：



1.2.8. 创建 Red Hat Enterprise Linux CoreOS (RHCOS) 机器

在您置备的 IBM Power 基础架构上安装集群前，必须先创建 RHCOS 机器供其使用。按照相应的步骤，使用 ISO 镜像或网络 PXE 启动来创建机器。

1.2.8.1. 使用 ISO 镜像创建 Red Hat Enterprise Linux CoreOS (RHCOS) 机器

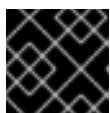
在您置备的 IBM Power 基础架构上安装集群前，必须先创建 RHCOS 机器供其使用。您可以使用 ISO 镜像来创建这些机器。

先决条件

- 获取集群的 Ignition 配置文件。
- 具有 HTTP 服务器的访问权限，以便您可从计算机进行访问，并且您创建的机器也可访问此服务器。

流程

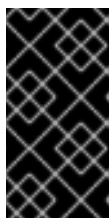
1. 将安装程序创建的 control plane、计算和 bootstrap Ignition 配置文件上传到 HTTP 服务器。记下这些文件的 URL。



重要

如果您计划在安装完成后在集群中添加更多计算机，请不要删除这些文件。

2. 从红帽客户门户上的[产品下载](#)页面或 [RHCOS 镜像](#) 页面，获取您选择的操作系统实例安装方法所需的 RHCOS 镜像。

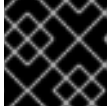


重要

RHCOS 镜像可能不会随着 OpenShift Container Platform 的每一发行版本都有改变。您必须下载最高版本的镜像，其版本号应小于或等于您安装的 OpenShift Container Platform 版本。如果可用，请使用与 OpenShift Container Platform 版本匹配的镜像版本。

您必须下载 ISO 文件和 RAW 磁盘文件。这些文件的名称类似以下示例：

- ISO: `rhcos-<version>-installer.<architecture>.iso`
 - 压缩的裸机 RAW: `rhcos-<version>-metal.<architecture>.raw.gz`
3. 将 RAW RHCOS 镜像文件上传到 HTTP 服务器并记录它的 URL。



重要

如果您计划在安装完成后在集群中添加更多计算机器，请不要删除这些文件。

4. 使用 ISO 启动 RHCOS 安装。使用如下安装选项之一：

- 将 ISO 镜像刻录到磁盘并直接启动。
- 通过 LOM 接口使用 ISO 重定向。

5. 实例启动后，按 **TAB** 或 **E** 键编辑内核命令行。

6. 将参数添加到内核命令行：

```
coreos.inst=yes
coreos.inst.install_dev=sda ①
coreos.inst.image_url=<image_URL> ②
coreos.inst.ignition_url=http://example.com/config.ign ③
ip=<dhcp or static IP address> ④ ⑤
```

- ① 指定要安装到的系统块设备。
- ② 指定您上传到服务器的 RAW 镜像的 URL。
- ③ 指定此机器类型的 Ignition 配置文件的 URL。
- ④ 在每个节点中设置 **ip=dhcp** 或者设置单独的静态 IP 地址 (**ip=**) 和 DNS 服务器 (**nameserver=**)。For example, setting **ip=10.10.10.2::10.10.10.254:255.255.255.0:core0.example.com:enp1s0:none nameserver=4.4.4.41** sets:
 - 节点的 IP 地址为 **10.10.10.2**
 - 网关地址为 **10.10.10.254**
 - 子网掩码为 **255.255.255.0**
 - 主机名为 **core0.example.com**
 - DNS 服务器地址为 **4.4.4.41**
- ⑤ 如果使用多个网络接口或 DNS 服务器，您可以使用以下方法进一步自定义 IP 地址配置：
 - 如果您的系统有多个网络接口，您可以通过指定多个 **ip=** 条目来添加多个 IP 地址配置。
 - 如果您的系统有多个网络接口，您可以使用 DHCP 和静态 IP 配置的组合。您需要指定要使用的接口，例如 **ip=enp1s0:dhcp ip=10.10.10.2::10.10.10.254:255.255.255.0:core0.example.com:enp2s0:none**。
 - 您可以为每个服务器添加一个 **nameserver=** 条目来提供多个 DNS 服务器，如 **nameserver=1.1.1.1 nameserver=8.8.8.8**。

7. 按 Enter 键完成安装。安装 RHCOS 后，系统会重启。系统重启后，它会应用您指定的 Ignition 配置文件。

8. 继续为集群创建机器。

**重要**

此刻您必须创建 bootstrap 和 control plane 机器。由于计算机器中已默认部署了一些 Pod，因此在安装集群前，还要创建至少两台计算机器。

1.2.8.2. 通过 PXE 引导来创建 Red Hat Enterprise Linux CoreOS (RHCOS) 机器

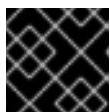
在您置备的裸机 IBM Power 基础架构上安装集群前，必须先创建 RHCOS 机器供其使用。您可以使用 PXE 引导来创建机器。

先决条件

- 获取集群的 Ignition 配置文件。
- 配置适用的 PXE 基础架构。
- 具有 HTTP 服务器的访问权限，以便您可从计算机进行访问。

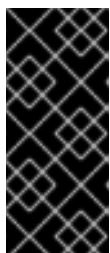
流程

1. 将安装程序创建的 master、worker 和 bootstrap Ignition 配置文件上传到 HTTP 服务器。记下这些文件的 URL。

**重要**

如果您计划在安装完成后在集群中添加更多计算机器，请不要删除这些文件。

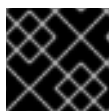
2. 从红帽客户门户上的[产品下载页面](#)或[RHCOS 镜像镜像 RHCOS 镜像镜像](#)页，获取压缩的裸机 RAW 镜像、**kernel** 和 **initramfs** 文件。

**重要**

RHCOS 镜像可能不会随着 OpenShift Container Platform 的每一发行版本都有改变。您必须下载最高版本的镜像，其版本号应小于或等于您安装的 OpenShift Container Platform 版本。如果可用，请使用与 OpenShift Container Platform 版本匹配的镜像版本。此流程只使用 RAW 镜像。对于裸机安装，RHCOS qcow2 镜像不被支持。

文件名包含 OpenShift Container Platform 版本号。它们类似以下示例：

- 压缩的裸机 RAW 镜像: **rhcos-<version>metal.<architecture>.raw.gz**
 - **kernel: rhcos-<version>-installer-kernel-<architecture>**
 - **initramfs: rhcos-<version>-installer-initramfs.<architecture>.img**
3. 将裸机 RAW 镜像以及 **kernel** 和 **initramfs** 文件上传到 HTTP 服务器。

**重要**

如果您计划在安装完成后在集群中添加更多计算机器，请不要删除这些文件。

4. 配置网络启动基础架构，以便在安装 RHCOS 后机器可从本地磁盘启动。
 5. 为 RHCOS 镜像配置 PXE 安装。
针对您的环境修改以下示例菜单条目之一，并验证能否正确访问镜像和 Ignition 文件：
- 对于 PXE：

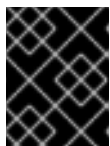
```

DEFAULT pxeboot
TIMEOUT 20
PROMPT 0
LABEL pxeboot
  KERNEL http://<HTTP_server>/rhcos-<version>-installer-kernel-<architecture> 1
  APPEND ip=dhcp rd.neednet=1 initrd=http://<HTTP_server>/rhcos-<version>-installer-
initramfs.<architecture>.img console=tty0 console=ttyS0 coreos.inst=yes
coreos.inst.install_dev=sda coreos.inst.image_url=http://<HTTP_server>/rhcos-
<version>-metal.<architecture>.raw.gz
coreos.inst.ignition_url=http://<HTTP_server>/bootstrap.ign 2 3

```

- 1** 指定上传到 HTTP 服务器的 **kernel** 文件位置。
- 2** 如果您使用多个 NIC，请在 **ip** 选项中指定一个接口。例如，要在名为 **eno1** 的 NIC 上使用 DHCP，请设置 **ip=eno1:dhcp**。
- 3** 指定上传到 HTTP 服务器的 RHCOS 文件的位置。**initrd** 参数值是 **initramfs** 文件的位置，**coreos.inst.image_url** 参数值是压缩的裸机 RAW 镜像的位置，**coreos.inst.ignition_url** 参数值则是 bootstrap Ignition 配置文件的位置。

6. 继续为集群创建机器。



重要

此刻您必须创建 bootstrap 和 control plane 机器。由于计算机上已默认部署了一些 Pod，因此在安装集群前，还要创建至少两台计算机。

1.2.9. 创建集群

要创建 OpenShift Container Platform 集群，请等待您通过安装程序生成的 Ignition 配置文件所置备的机器上完成 bootstrap 过程。

先决条件

- 为集群创建所需的基础架构。
- 已获得安装程序并为集群生成了 Ignition 配置文件。
- 已使用 Ignition 配置文件为集群创建 RHCOS 机器。

流程

1. 监控 bootstrap 过程：

```

$ ./openshift-install --dir=<installation_directory> wait-for bootstrap-complete \ 1
--log-level=info 2

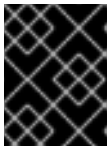
```

```
INFO Waiting up to 30m0s for the Kubernetes API at https://api.test.example.com...
INFO API v1.16.2 up
INFO Waiting up to 30m0s for bootstrapping to complete...
INFO It is now safe to remove the bootstrap resources
```

- 1 对于 `<installation_directory>`，请指定安装文件保存到的目录的路径。
- 2 要查看不同的安装详情，请指定 `warn`、`debug` 或 `error`，而不要指定 `info`。

Kubernetes API 服务器提示已在 control plane 机器上完成 bootstrap 时，命令运行成功。

2. bootstrap 过程完成后，请从负载均衡器中删除 bootstrap 机器。



重要

此时您必须从负载均衡器中删除 bootstrap 机器。您还可以删除或重新格式化机器本身。

1.2.10. 登录集群

您可以通过导出集群 `kubeconfig` 文件，以默认系统用户身份登录集群。`kubeconfig` 文件包含关于集群的信息，供 CLI 用于将客户端连接到正确集群和 API 服务器。该文件特只适用于一个特定的集群，在 OpenShift Container Platform 安装过程中创建。

先决条件

- 部署 OpenShift Container Platform 集群。
- 安装 `oc` CLI。

流程

1. 导出 `kubeadmin` 凭证：

```
$ export KUBECONFIG=<installation_directory>/auth/kubeconfig 1
```

- 1 对于 `<installation_directory>`，请指定安装文件保存到的目录的路径。

2. 使用导出的配置，验证能否成功运行 `oc` 命令：

```
$ oc whoami
system:admin
```

1.2.11. 批准机器的 CSR

将机器添加到集群时，会为您添加的每台机器生成两个待处理证书签名请求（CSR）。您必须确认这些 CSR 已获得批准，或根据需要自行批准。

先决条件

- 您已将机器添加到集群中。

流程

1. 确认集群可以识别这些机器：

```
$ oc get nodes

NAME      STATUS    ROLES    AGE   VERSION
master-0  Ready     master   63m   v1.16.2
master-1  Ready     master   63m   v1.16.2
master-2  Ready     master   64m   v1.16.2
worker-0  NotReady  worker   76s   v1.16.2
worker-1  NotReady  worker   70s   v1.16.2
```

输出将列出您创建的所有机器。

2. 检查待处理的 CSR，并确保添加到集群中的每台机器都有 **Pending** 或 **Approved** 状态的客户端和服务器请求：

```
$ oc get csr

NAME      AGE   REQUESTOR                                     CONDITION
csr-8b2br  15m   system:serviceaccount:openshift-machine-config-operator:node-
bootstrapper Pending 1
csr-8vnps  15m   system:serviceaccount:openshift-machine-config-operator:node-
bootstrapper Pending
csr-bfd72  5m26s system:node:ip-10-0-50-126.us-east-2.compute.internal
Pending 2
csr-c57lv  5m26s system:node:ip-10-0-95-157.us-east-2.compute.internal
Pending
...
```

1 客户端请求 CSR。

2 服务器请求 CSR。

在本例中，两台机器加入了集群。您可能在列表中看到更多已批准的 CSR。

3. 如果 CSR 没有获得批准，请在所添加机器的所有待处理 CSR 都处于 **Pending** 状态后，为您的集群机器批准这些 CSR：



注意

由于 CSR 会自动轮转，因此请在将机器添加到集群后一小时内批准您的 CSR。如果没有在一小时内批准，证书将会轮转，每个节点将会存在多个证书。您必须批准所有这些证书。批准初始 CSR 后，集群的 **kube-controller-manager** 会自动批准后续的节点客户端 CSR。您必须实施一个方法来自动批准 kubelet 提供的证书请求。

- 若要单独批准，请对每个有效的 CSR 运行以下命令：

```
$ oc adm certificate approve <csr_name> 1
```

1 **<csr_name>** 是当前 CSR 列表中 CSR 的名称。

- 要批准所有待处理的 CSR，请运行以下命令：

```
$ oc get csr -o go-template='{{range .items}}{{if not .status}}{{.metadata.name}}{\n"}\n{{end}}' | xargs oc adm certificate approve
```

其他信息

- 如需有关 CSR 的更多信息，请参阅[证书签名请求](#)。

1.2.12. 初始 Operator 配置

在 control plane 初始化后，您必须立即配置一些 Operator 以便它们都可用。

先决条件

- 您的 control plane 已初始化。

流程

1. 观察集群组件上线：

```
$ watch -n5 oc get clusteroperators
```

NAME	VERSION	AVAILABLE	PROGRESSING	DEGRADED	SINCE
authentication	4.3.0	True	False	False	69s
cloud-credential	4.3.0	True	False	False	12m
cluster-autoscaler	4.3.0	True	False	False	11m
console	4.3.0	True	False	False	46s
dns	4.3.0	True	False	False	11m
image-registry	4.3.0	True	False	False	5m26s
ingress	4.3.0	True	False	False	5m36s
kube-apiserver	4.3.0	True	False	False	8m53s
kube-controller-manager	4.3.0	True	False	False	7m24s
kube-scheduler	4.3.0	True	False	False	12m
machine-api	4.3.0	True	False	False	12m
machine-config	4.3.0	True	False	False	7m36s
marketplace	4.3.0	True	False	False	7m54m
monitoring	4.3.0	True	False	False	7h54s
network	4.3.0	True	False	False	5m9s
node-tuning	4.3.0	True	False	False	11m
openshift-apiserver	4.3.0	True	False	False	11m
openshift-controller-manager	4.3.0	True	False	False	5m943s
openshift-samples	4.3.0	True	False	False	3m55s
operator-lifecycle-manager	4.3.0	True	False	False	11m
operator-lifecycle-manager-catalog	4.3.0	True	False	False	11m
service-ca	4.3.0	True	False	False	11m
service-catalog-apiserver	4.3.0	True	False	False	5m26s
service-catalog-controller-manager	4.3.0	True	False	False	5m25s
storage	4.3.0	True	False	False	5m30s

2. 配置不可用的 Operator。

1.2.12.1. 镜像 registry 存储配置

对于不提供默认存储的平台，**Image-registry** Operator 最初将不可用。安装后，您必须配置 registry 使用的存储，这样 Registry Operator 才可用。

提供了配置 PersistentVolume 的说明，这是生产集群所需要的；也提供了将空目录配置为存储位置的说明，这仅适用于非生产集群。

1.2.12.1.1. 为裸机配置 registry 存储

1.2.12.1.2. 为 IBM Power 配置 registry 存储

作为集群管理员，在安装后需要配置 registry 来使用存储。

先决条件

- 具有 Cluster Administrator 权限
- 在裸机上有一个集群。IBM Power。
- 为集群置备持久性存储，如 Red Hat OpenShift Container Storage。若要部署私有镜像 registry，您的存储必须提供 ReadWriteMany 访问模式。
- 必须有“100Gi”容量。

流程

1. 为了配置 registry 使用存储，需要修改 **configs.imageregistry/cluster** 资源中的 **spec.storage.pvc**。



注意

当使用类似 NFS 的共享存储时，强烈建议使用 **supplementalGroups** 策略，即指明安全性上下文的允许补充组，而不是 **fsGroup** ID。详情请参考 NFS 组 ID 文档。

2. 验证您没有 registry Pod：

```
$ oc get pod -n openshift-image-registry
```



注意

- 如果存储类型为 **emptyDIR**，则副本数不能超过 1。
- 如果存储类型是 **NFS**，您必须启用 **no_wdelay** 和 **root_squash** 挂载选项。例如：

```
# cat /etc/exports
/mnt/data *(rw,sync,no_wdelay,root_squash,insecure,fsid=0)
sh-4.3# exportfs -rv
exporting */mnt/data
```

3. 检查 registry 配置：

```
$ oc edit configs.imageregistry.operator.openshift.io
```

```
storage:
  pvc:
    claim:
```

将 **claim** 字段留空以允许自动创建一个 **image-registry-storage** PVC。

4. 检查 **clusteroperator** 的状态：

```
$ oc get clusteroperator image-registry
```

1.2.12.1.3. 在非生产集群中配置镜像 registry 存储

您必须为 Image Registry Operator 配置存储。对于非生产集群，您可以将镜像 registry 设置为空目录。如果您这样做，重启 registry 后会丢失所有镜像。

流程

- 将镜像 registry 存储设置为空目录：

```
$ oc patch configs.imageregistry.operator.openshift.io cluster --type merge --patch '{"spec": {"storage":{"emptyDir":{}}}'
```



警告

仅可为非生产集群配置这个选项。

如果在 Image Registry Operator 初始化其组件前运行此命令，**oc patch** 命令会失败并显示以下错误：

```
Error from server (NotFound): configs.imageregistry.operator.openshift.io "cluster" not found
```

等待几分钟，然后再次运行该命令。

1.2.13. 在用户自备的基础架构上完成安装

完成 Operator 配置后，可以在您提供的基础架构上完成集群安装。

先决条件

- 您的 control plane 已初始化。
- 已完成初始 Operator 配置。

流程

1. 确认所有集群组件都已上线：

```
$ watch -n5 oc get clusteroperators
```

NAME	VERSION	AVAILABLE	PROGRESSING	DEGRADED	SINCE
authentication	4.3.0	True	False	False	10m
cloud-credential	4.3.0	True	False	False	22m
cluster-autoscaler	4.3.0	True	False	False	21m
console	4.3.0	True	False	False	10m
dns	4.3.0	True	False	False	21m
image-registry	4.3.0	True	False	False	16m
ingress	4.3.0	True	False	False	16m
kube-apiserver	4.3.0	True	False	False	19m
kube-controller-manager	4.3.0	True	False	False	18m
kube-scheduler	4.3.0	True	False	False	22m
machine-api	4.3.0	True	False	False	22m
machine-config	4.3.0	True	False	False	18m
marketplace	4.3.0	True	False	False	18m
monitoring	4.3.0	True	False	False	18m
network	4.3.0	True	False	False	16m
node-tuning	4.3.0	True	False	False	21m
openshift-apiserver	4.3.0	True	False	False	21m
openshift-controller-manager	4.3.0	True	False	False	17m
openshift-samples	4.3.0	True	False	False	14m
operator-lifecycle-manager	4.3.0	True	False	False	21m
operator-lifecycle-manager-catalog	4.3.0	True	False	False	21m
service-ca	4.3.0	True	False	False	21m
service-catalog-apiserver	4.3.0	True	False	False	16m
service-catalog-controller-manager	4.3.0	True	False	False	16m
storage	4.3.0	True	False	False	16m

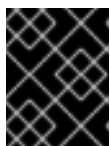
当所有集群 Operator 状态都是 **AVAILABLE** 时，您可以完成安装。

2. 监控集群完成：

```
$ ./openshift-install --dir=<installation_directory> wait-for install-complete 1
INFO Waiting up to 30m0s for the cluster to initialize...
```

1 对于 **<installation_directory>**，请指定安装文件保存到的目录的路径。

Cluster Version Operator 完成从 Kubernetes API 服务器部署 OpenShift Container Platform 集群时，命令运行成功。



重要

安装程序生成的 Ignition 配置文件中所含的证书会在 24 小时后过期。您必须以非降级状态持续运行集群 24 小时，以确保完成第一次证书轮转。

3. 确认 Kubernetes API 服务器正在与 Pod 通信。

a. 要查看所有 Pod 的列表，请使用以下命令：

```
$ oc get pods --all-namespaces
```

NAMESPACE	NAME	READY	STATUS
-----------	------	-------	--------

```

RESTARTS  AGE
openshift-apiserver-operator  openshift-apiserver-operator-85cb746d55-zqhs8  1/1
Running  1      9m
openshift-apiserver           apiserver-67b9g                               1/1  Running  0
3m
openshift-apiserver           apiserver-ljcmx                               1/1  Running  0
1m
openshift-apiserver           apiserver-z25h4                               1/1  Running  0
2m
openshift-authentication-operator authentication-operator-69d5d8bf84-vh2n8  1/1
Running  0      5m
...

```

- b. 使用以下命令，查看上一命令的输出中所列 Pod 的日志：

```
$ oc logs <pod_name> -n <namespace> ①
```

- ① 指定 Pod 名称和命名空间，如上一命令的输出中所示。

如果 Pod 日志显示，Kubernetes API 服务器可以与集群机器通信。

1.2.14. 后续步骤

- [自定义集群](#)。