OpenShift Container Platform 4.3

在 OpenStack 上安装

安装 OpenShift Container Platform 4.3 OpenStack 集群

Last Updated: 2020-09-16

OpenShift Container Platform 4.3 在 OpenStack 上安装

安装 OpenShift Container Platform 4.3 OpenStack 集群

法律通告

摘要

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

目录

第 1 章 在 OPENSTACK 上安装

1.1. 使用自定义配置在 OPENSTACK 上安装集群

在 OpenShift Container Platform 版本 4.3 中，您可以在 Red Hat OpenStack Platform (RHOSP) 上安装自定义集群。要自定义安装，请在安装集群前修改 **install-config.yaml** 中的参数。

1.1.1. 先决条件

- 查看有关 OpenShift Container Platform 安装和更新流程的详细信息。
  - 在 *Available platforms* 部分验证 OpenShift Container Platform 4.3 是否与您的 RHOSP 版本兼容。您还可以查看 OpenShift Container Platform 在 RHOSP 中的支持 来比较不同版本的平台支持。
- 在 RHOSP 中启用了元数据服务

1.1.2. 在 RHOSP 上安装 OpenShift Container Platform 的资源指南

您的配额必须满足以下要求，才能在 Red Hat OpenStack Platform (RHOSP) 中运行 OpenShift Container Platform 安装程序：

表 1.1. RHOSP 上默认 OpenShift Container Platform 集群的建议资源

资源	值
浮动 IP 地址	2
端口	15
路由器	1
子网	1
RAM	112 GB
vCPUs	28
卷存储	175 GB
实例	7
安全组	3
安全组规则	60
Swift 容器	2
Swift 对象	1

资源	值
Swift 可用空间	10 MB 或以上

注意

根据 bootstrap Ignition 文件和镜像 registry 的大小，Swift 空间要求会有所不同。

集群或许能使用少于推荐数量的资源来运作，但其性能无法保证。

注意

默认情况下，您的安全组和安全组规则配额可能较低。如果遇到问题，请以 admin 的身份运行 **openstack quota set --secgroups 3 --secgroup-rules 60 <project>** 来提高配额。

OpenShift Container Platform 部署由 control plane 机器、计算机器和 bootstrap 机器组成。

1.1.2.1. control plane 和计算机器

默认情况下，OpenShift Container Platform 安装程序支持三台 control plane 和计算机器。

每台机器都需要：

- 来自 RHOSP 配额的实例
- 来自 RHOSP 配额的端口
- 其类别至少有 16 GB 内存、4 个 vCPU 和 25GB 存储空间

提示

计算机器托管您在 OpenShift Container Platform 上运行的应用程序；运行数量应尽可能多。

1.1.2.2. bootstrap 机器

在安装时，会临时置备 bootstrap 机器来支持 control plane。生产控制平面就绪后，bootstrap 机器会被取消置备。

bootstrap 机器需要：

- 来自 RHOSP 配额的实例
- 来自 RHOSP 配额的端口
- 其类别至少有 16 GB 内存、4 个 vCPU 和 25GB 存储空间

注意

安装程序无法将证书颁发机构捆绑包传递给 control plane 机器上的 Ignition。因此，如果端点使用自签名证书，bootstrap 机器将无法从 Swift 检索 Ignition 配置。

1.1.3. 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。

1.1.4. 在 OpenStack 中启用 Swift

在 Red Hat OpenStack Platform (RHOSP) 上的 OpenShift Container Platform 使用 RHOSP Object Storage (Swift) 来存储和提供用户配置文件。

Swift 由具有 **swiftoperator** 角色的用户帐户操控。

先决条件

- 目标环境中的 RHOSP 管理员帐户
- Ceph RGW 上必须启用 **account in url** 选项

流程

在 RHOSP 上启用 Swift：

1. 在 RHOSP CLI 中以管理员身份，将 **swiftoperator** 角色添加到要访问 Swift 的帐户：

```
$ openstack role add --user <user> --project <project> swiftoperator
```

您的 RHOSP 部署现在可以使用 Swift 来存储和提供文件。

1.1.5. 验证外部网络访问

OpenShift Container Platform 安装程序需要外部网络访问权限。您必须为其提供外部网络值，否则部署会失败。在运行安装程序之前，请验证 Red Hat OpenStack Platform (RHOSP) 中是否存在具有外部路由器类型的网络。

先决条件

- 在 RHOSP 中，必须将 **NeutronDhcpAgentDnsmasqDnsServers** 参数配置为允许 DHCP 代理转发实例的 DNS 查询。设置这个参数的方法之一为：

  a. 在模板目录中创建新环境文件 。

  b. 在文件中提供参数值 。例如：

  ```
  parameter_defaults:
    NeutronDhcpAgentDnsmasqDnsServers:
  ['<DNS_server_address_1>','<DNS_server_address_2']
  ```

  c. 在 Overcloud 部署命令中包括 环境文件。例如：

  ```
  $ openstack overcloud deploy --templates -e neutron-dhcp-agent-dnsmasq-dns-servers.yaml ...
  ```

流程

1. 使用 RHOSP CLI 验证"外部"网络的名称和 ID：

```
$ openstack network list --long -c ID -c Name -c "Router Type"

+--------------------------------------+---------------+-------------+
| ID                                   | Name          | Router Type |
+--------------------------------------+---------------+-------------+
| 148a8023-62a7-4672-b018-003462f8d7dc | public_network | External    |
+--------------------------------------+---------------+-------------+
```

网络列表中会显示具有外部路由器类型的网络。如果最少有一个没有，请参阅 创建默认浮动 IP 网络和创建默认供应商网络。

重要

如果外部网络 CIDR 范围与某一个默认网络范围重叠，您必须在运行安装程序前更改 **install-config.yaml** 文件中匹配的网络范围。

默认的网络范围：

网络	范围
machineCIDR	10.0.0.0/16
serviceNetwork	172.30.0.0/16
clusterNetwork	10.128.0.0/14

小心

如果安装程序找到多个同名的镜像，它会随机设置其中之一。为避免这种行为，请在 RHOSP 中为资源创建唯一名称。

注意

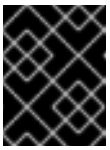
如果启用了 Neutron 中继服务插件，则默认创建中继端口。如需更多信息，请参阅 Neutron 中继端口。

1.1.6. 为安装程序定义参数

OpenShift Container Platform 安装程序依赖于一个名为 **clouds.yaml** 的文件。该文件描述了 Red Hat OpenStack Platform (RHOSP) 配置参数，包括项目名称、登录信息和授权服务 URL。

流程

1. 创建 **clouds.yaml** 文件：
   - 如果您的 RHOSP 发行版包含 Horizon web UI，请在该 UI 中生成 **clouds.yaml** 文件。

     重要

     请记住在 **auth** 字段中添加密码。您也可以把 secret 保存在 **clouds.yaml** 以外的一个独立的文件中。

   - 如果您的 RHOSP 发行版不包含 Horizon Web UI，或者您不想使用 Horizon，请自行创建该文件。如需有关 **clouds.yaml** 的详细信息，请参阅 RHOSP 文档中的配置文件。

```
clouds:
  shiftstack:
    auth:
      auth_url: http://10.10.14.42:5000/v3
      project_name: shiftstack
      username: shiftstack_user
      password: XXX
      user_domain_name: Default
      project_domain_name: Default
  dev-env:
    region_name: RegionOne
    auth:
      username: 'devuser'
      password: XXX
      project_name: 'devonly'
      auth_url: 'https://10.10.14.22:5001/v2.0'
```

2. 将您生成的文件放在以下位置之一：
   a. **OS_CLIENT_CONFIG_FILE** 环境变量的值
   b. 当前目录
   c. 特定于 Unix 的用户配置目录，如 **~/.config/openstack/clouds.yaml**
   d. 特定于 Unix 的站点配置目录，如 **/etc/openstack/clouds.yaml**
   安装程序会按照以上顺序搜索 **clouds.yaml**。

1.1.7. 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。

1.1.8. 创建安装配置文件

您可以自定义 Red Hat OpenStack Platform（RHOSP）上的 OpenShift Container Platform 安装。

先决条件

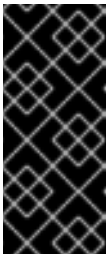
- 获取 OpenShift Container Platform 安装程序以及集群的 pull secret。

流程

1. 创建 **install-config.yaml** 文件。
   a. 运行以下命令：

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

1 对于 **<installation_directory>**，请指定用于保存安装程序所创建的文件的目录名称。



重要

指定一个空目录。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。

b. 在提示符处，提供您的云的配置详情：

   i. 可选：选择用来访问集群机器的 SSH 密钥。

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。

   ii. 选择 **openstack** 作为目标平台。

   iii. 指定用于安装集群的 Red Hat OpenStack Platform (RHOSP) 外部网络名称。

   iv. 指定用于从外部访问 OpenShift API 的浮动 IP 地址。

   v. 指定至少有 16 GB RAM 用于 control plane 和计算节点的 RHOSP 类别。

   vi. 选择集群要部署到的基域。所有 DNS 记录都将是这个基域的子域，并包含集群名称。

   vii. 为集群输入一个名称。名称不能多于 14 个字符。

   viii. 粘贴从 Red Hat OpenShift Cluster Manager 站点的 Pull Secret 页面中获取的 pull secret。

2. 修改 **install-config.yaml** 文件。您可以在**安装配置参数**部分中找到有关可用参数的更多信息。

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

重要

install-config.yaml 文件会在安装过程中消耗掉。如果要重复使用此文件，必须现在备份。

1.1.9. 安装配置参数

在部署 OpenShift Container Platform 集群前，您可以提供参数值，以描述托管集群的云平台的帐户并选择性地自定义集群平台。在创建 **install-config.yaml** 安装配置文件时，您可以通过命令行来提供所需的参数的值。如果要自定义集群，可以修改 **install-config.yaml** 文件来提供关于平台的更多信息。

注意

安装之后，您无法修改 **install-config.yaml** 文件中的这些参数。

表 1.2. 所需的参数

参数	描述	值
baseDomain	云供应商的基域。此值用于创建到 OpenShift Container Platform 集群组件的路由。集群的完整 DNS 名称是 **baseDomain** 和 **metadata.name** 参数值的组合，其格式为 **<metadata.name>.<baseDomain>**。	完全限定域名或子域名，如 **example.com**。
controlPlane.platform	托管 control plane 机器的云供应商。此参数值必须与 **compute.platform** 参数值匹配。	**aws**、**azure**、**gcp**、**openstack** 或 **{}**
compute.platform	托管 worker 机器的云供应商。此参数值必须与 **controlPlane.platform** 参数值匹配。	**aws**、**azure**、**gcp**、**openstack** 或 **{}**
metadata.name	集群的名称。	包含大写字母或小写字母的字符串，如 **dev**。该字符串长度必须为 14 个字符或更少。
platform.<platform>.region	集群要部署到的区域。	云的有效区域，如 AWS 的 **us-east-1**、Azure 的 **centralus** 或 Red Hat OpenStack Platform (RHOSP) 的 **region1**。

pullSecret	从 Red Hat OpenShift Cluster Manager 站点的 Pull Secret 页面中获取的 pull secret。您可以使用此 pull secret 来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。	<pre>{
		  "auths":{
		    "cloud.openshift.com":{
		      "auth":"b3Blb=",
		      "email":"you@example.com"
		    },
		    "quay.io":{
		      "auth":"b3Blb=",
		      "email":"you@example.com"
		    }
		  }
		}</pre>

表 1.3. 可选参数

参数	描述	值

参数	描述	值
sshKey	用于访问集群机器的 SSH 密钥。  **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。	添加到 **ssh-agent** 进程的有效本地公共 SSH 密钥。
fips	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。	**false** 或 **true**
publish	如何发布集群的面向用户的端点。	**Internal** 或 **External**。把 **publish** 设置为 **Internal** 以部署一个私有集群，它不能被互联网访问。默认值为 **External**。
compute.hyperthreading	是否在计算机器上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。  **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。	**Enabled** 或 **Disabled**
compute.replicas	要置备的计算机器数量，也称为 worker 机器。	大于或等于 **2** 的正整数。默认值为 **3**。

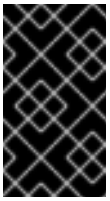
参数	描述	值
controlPlane.hyperthreading	是否在 control plane 机器上启用或禁用并发多线程或**超线程**。默认情况下，启用并发多线程以提高机器内核的性能。  **重要** 如果禁用并发多线程，请确保在容量规划时考虑到机器性能可能会显著降低的问题。	**Enabled** 或 **Disabled**
controlPlane.replicas	要置备的 control plane 机器数量。	大于或等于 **3** 的正整数。默认值为 **3**。

表 1.4. 其他 Red Hat OpenStack Platform (RHOSP) 参数

参数	描述	值
compute.platform.openstack.rootVolume.size	对于计算机器，以 GB 为单位表示的根卷大小。如果您不设置这个值，机器将使用临时存储。	整数，如 **30**。
compute.platform.openstack.rootVolume.type	对于计算机器，根卷的类型。	字符串，如 **performance**。
controlPlane.platform.openstack.rootVolume.size	对于 control plane 机器，以 GB 为单位表示的根卷大小。如果您不设置这个值，机器将使用临时存储。	整数，如 **30**。
controlPlane.platform.openstack.rootVolume.type	对于 control plane 机器，根卷的类型。	字符串，如 **performance**。
platform.openstack.region	在其中创建 RHOSP 集群的区域。	字符串，如 **region1**。
platform.openstack.cloud	要使用的 RHOSP 云的名称，来自于 **clouds.yaml** 文件中的云列表。	字符串，如 **MyCloud**。
platform.openstack.externalDNS	*可选*。集群实例用于进行 DNS 解析的外部 DNS 服务器的 IP 地址。	包括 IP 地址列表的字符串，如 **["8.8.8.8", "192.168.1.12"]**。
platform.openstack.externalNetwork	用于安装的 RHOSP 外部网络名称。	字符串，如 **external**。

参数	描述	值
platform.openstack.computeFlavor	用于 control plane 和计算机器的 RHOSP 类别。	字符串，如 **m1.xlarge**。
platform.openstack.lbFloatingIP	与负载均衡器 API 关联的现有浮动 IP 地址。	IP 地址，如 **128.0.0.1**。
platform.openstack.defaultMachinePlatform	*可选*。默认机器池平台配置。	{ "type": "ml.large", "rootVolume": { "size": 30, "type": "performance" } }

1.1.9.1. RHOSP 的自定义 install-config.yaml 文件示例

此示例 **install-config.yaml** 展示了所有可能的 Red Hat OpenStack Platform (RHOSP) 自定义选项。

重要

此示例文件仅供参考。您必须使用安装程序来获取 **install-config.yaml** 文件。

```
apiVersion: v1
baseDomain: example.com
clusterID: os-test
controlPlane:
  name: master
  platform: {}
  replicas: 3
compute:
- name: worker
  platform:
    openstack:
      type: ml.large
  replicas: 3
metadata:
  name: example
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineCIDR: 10.0.0.0/16
  serviceNetwork:
  - 172.30.0.0/16
  networkType: OpenShiftSDN
platform:
  openstack:
    region: region1
    cloud: mycloud
```

```
    externalNetwork: external
    computeFlavor: m1.xlarge
    lbFloatingIP: 128.0.0.1
fips: false
pullSecret: '{"auths": ...}'
sshKey: ssh-ed25519 AAAA...
```

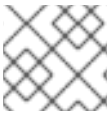
1.1.10. 生成 SSH 私钥并将其添加到代理中

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。

1.1.11. 启用对环境的访问

在部署时，所有 OpenShift Container Platform 机器都是在 Red Hat OpenStack Platform (RHOSP) 租户网络中创建的。因此，大多数 RHOSP 部署中都无法直接访问它们。

您可以配置 OpenShift Container Platform API，以便能使用或不使用浮动 IP 地址来访问。

1.1.11.1. 启用通过浮动 IP 地址进行访问

将两个浮动 IP (FIP) 地址附加到 OpenShift Container Platform API 端点以便可以访问这些端点：一个用于 API 负载均衡器 (**lb FIP**)，另一个用于 OpenShift Container Platform 应用程序 (**apps FIP**)。

重要

install-config.yaml 文件中也会使用负载均衡器 FIP。

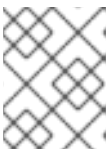
流程

1. 使用 Red Hat OpenStack Platform (RHOSP) CLI，创建一个新的外部网络：

```
$ openstack floating ip create <external network>
```

2. 向您的 DNS 服务器中添加一条符合此模式的记录：

```
api.<cluster name>.<base domain>  IN  A  <lb FIP>
```



注意

如果您不控制 DNS 服务器，可以改为将记录添加到 **/etc/hosts** 文件中。此操作使 API 可供您自己访问，不适合于生产部署。这可用于进行开发和测试的安装。

提示

您可以通过分配浮动 IP 地址并更新防火墙配置，使 OpenShift Container Platform 资源在集群之外可用。

1.1.11.2. 启用不通过浮动 IP 地址进行访问

如果您无法使用浮动 IP 地址，OpenShift Container Platform 安装或许仍然可以完成。不过，安装程序在等待 API 访问超时后会失败。

安装程序超时后，集群或许仍然可以初始化。 bootstrap 过程开始后，它必须完成。但是，您必须在部署后编辑集群网络配置。

1.1.12. 部署集群

您可以在兼容云平台中安装 OpenShift Container Platform。

重要

安装程序的 **create cluster** 命令只能在初始安装过程中运行一次。

先决条件

- 获取 OpenShift Container Platform 安装程序以及集群的 pull secret。

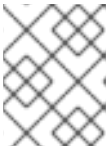
流程

1. 运行安装程序：

```
$ ./openshift-install create cluster --dir=<installation_directory> \ 1
    --log-level=info 2
```

1 对于 **<installation_directory>**，请指定自定义 **./install-config.yaml** 文件的位置。

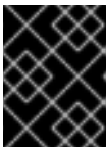
2 要查看不同的安装详情，请指定 **warn**、**debug** 或 **error**，而不要指定 **info**。



注意

如果您在主机上配置的云供应商帐户没有足够的权限来部署集群，安装过程将会停止，并且显示缺少的权限。

集群部署完成后，终端会显示访问集群的信息，包括指向其 Web 控制台的链接和 **kubeadmin** 用户的凭证。



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。

重要

您不得删除安装程序或安装程序所创建的文件。需要这两者才能删除集群。

1.1.13. 验证集群状态

在安装过程中或安装后验证 OpenShift Container Platform 集群的状态：

流程

1. 在集群环境中，导出管理员的 kubeconfig 文件：

```
$ 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。

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。

2. 查看部署后创建的 control plane 和计算机器：

```
$ oc get nodes
```

3. 查看集群的版本：

```
$ oc get clusterversion
```

4. 查看 Operator 的状态：

```
$ oc get clusteroperator
```

5. 查看集群中所有正在运行的 Pod：

```
$ oc get pods -A
```

1.1.14. 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
```

1.1.15. 使用浮动 IP 地址配置应用程序访问

安装 OpenShift Container Platform 后，请配置 Red Hat OpenStack Platform (RHOSP) 以允许应用程序网络流量。

先决条件

- 必须已安装 OpenShift Container Platform 集群
- 已启用浮动 IP 地址，如*启用对环境的访问*中所述。

流程

在安装 OpenShift Container Platform 集群后，将浮动 IP 地址附加到入口端口：

1. 显示端口：

```
$ openstack port show <cluster name>-<clusterID>-ingress-port
```

2. 将端口附加到 IP 地址：

```
$ openstack floating ip set --port <ingress port ID> <apps FIP>
```

3. 在您的 DNS 文件中，为 ***apps.** 添加一条通配符 **A** 记录。

```
*.apps.<cluster name>.<base domain>  IN  A  <apps FIP>
```

注意

如果您不控制 DNS 服务器，但希望为非生产用途启用应用程序访问，您可以将这些主机名添加到 **/etc/hosts**：

```
<apps FIP> console-openshift-console.apps.<cluster name>.<base domain>
<apps FIP> integrated-oauth-server-openshift-authentication.apps.<cluster name>.
<base domain>
<apps FIP> oauth-openshift.apps.<cluster name>.<base domain>
<apps FIP> prometheus-k8s-openshift-monitoring.apps.<cluster name>.<base
domain>
<apps FIP> grafana-openshift-monitoring.apps.<cluster name>.<base domain>
<apps FIP> <app name>.apps.<cluster name>.<base domain>
```

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. 在带有 KURYR 的 OPENSTACK 上安装集群

在 OpenShift Container Platform 版本 4.3 中，您可以在使用 Kuryr SDN 的 Red Hat OpenStack Platform (RHOSP) 上安装自定义集群。要自定义安装，请在安装集群前修改 **install-config.yaml** 中的参数。

1.2.1. 先决条件

- 查看有关 OpenShift Container Platform 安装和更新流程的详细信息。
    - 在 *Available platforms* 部分验证 OpenShift Container Platform 4.3 是否与您的 RHOSP 版本兼容。您还可以查看 OpenShift Container Platform 在 RHOSP 中的支持 来比较不同版本的平台支持。

1.2.2. 关于 Kuryr SDN

Kuryr 是一个容器网络接口（CNI）插件解决方案，它使用 Neutron 和 Octavia Red Hat OpenStack Platform（RHOSP）服务来为 Pod 和服务提供网络。

Kuryr 和 OpenShift Container Platform 的集成主要针对在 RHOSP VM 上运行的 OpenShift Container Platform 集群设计。Kuryr 通过将 OpenShift Container Platform Pod 插入到 RHOSP SDN 来提高网络性能。另外，它还提供 Pod 和 RHOSP 虚拟实例间的互联性。

Kuryr 组件作为 Pod 在 OpenShift Container Platform 中安装，使用 **openshift-kuryr** 命名空间：

- **kuryr-controller** - 在一个 **master** 节点上安装的单个服务实例。这在 OpenShift Container Platform 中建模为一个 **Deployment**。
- **kuryr-cni** - 在每个 OpenShift Container Platform 节点上安装并配置 Kuryr 作为 CNI 驱动的容器。这在 OpenShift Container Platform 中建模为一个 **DaemonSet**。

Kuryr 控制器监控 OpenShift API 服务器中的 Pod、Service 和命名空间创建、更新和删除事件。它将 OpenShift Container Platform API 调用映射到 Neutron 和 Octavia 中的对应对象。这意味着，实现了 Neutron 中继端口功能的每个网络解决方案都可以通过 Kuryr 支持 OpenShift Container Platform。这包括开源解决方案，比如 Open vSwitch (OVS) 和 Open Virtual Network (OVN)，以及 Neutron 兼容的商业 SDN。

建议在封装的 RHOSP 租户网络上部署 OpenShift Container Platform 时使用 Kuryr，以避免出现重复封装，例如通过 RHOSP 网络运行封装的 OpenShift Container Platform SDN。

因此，在以下情况下不建议使用 Kuryr：

- 使用供应商网络或租户 VLAN。
- 您的部署在少数几个 hypervisor 上使用多个服务。每个 OpenShift Service 都会在 OpenStack 中创建了一个 Octavia Amphora 虚拟机，它托管所需的负载均衡器。
- 需要 UDP 服务。

1.2.3. 在带有 Kuryr 的 OpenStack 上安装 OpenShift Container Platform 的资源指南

当使用 Kuryr SDN 时，Pod、Service、命名空间 和网络策略会使用来自 RHOSP 配额的资源，这会增加最低要求。除了默认安装需要满足的要求，Kuryr 还有一些额外的要求。

使用以下配额来满足集群的默认最低要求：

表 1.5. 带有 Kuryr 的 RHOSP 上默认 OpenShift Container Platform 集群的建议资源

资源	值
浮动 IP 地址	3 - 加上预期的 LoadBalancer 类型服务的数量
端口	1500 - 每个 Pod 需要 1 个
路由器	1
子网	250 - 每个命名空间/项目需要 1 个
网络	250 - 每个命名空间/项目需要 1 个
RAM	112 GB

资源	值
vCPUs	28
卷存储	175 GB
实例	7
安全组	250 - 每个服务和每个 NetworkPolicy 需要 1 个
安全组规则	1000
Swift 容器	2
Swift 对象	1
Swift 可用空间	10 MB 或以上
负载均衡器	100 - 每个服务需要 1 个
负载均衡器侦听程序	500 - 每个服务公开端口需要 1 个
负载均衡器池	500 - 每个服务公开端口需要 1 个

集群或许能使用少于推荐数量的资源来运作，但其性能无法保证。

在设置资源时请考虑以下几点：

- 需要的端口数量实际上会大于 Pod 的数量。Kuryr 使用端口池来预创建端口以供 Pod 使用，用于加快 Pod 的启动时间。
- 每个 NetworkPolicy 都映射到一个 RHOSP 安全组，并根据 NetworkPolicy 规格将一个或多个规则添加到安全组中。
- 每个服务都映射到 RHOSP 负载均衡器中。每个负载均衡器都有一个带有用户项目的安全组; 因此，在设置配额时需要考虑所需的安全组数量。
- 根据 bootstrap Ignition 文件和镜像 registry 的大小，Swift 空间要求会有所不同。
- 配额不考虑负载均衡器资源（如 VM 资源），但您必须在决定 RHOSP 部署的大小时考虑这些资源。默认安装将有超过 50 个负载均衡器，集群必须可以容纳它们。

OpenShift Container Platform 部署由 control plane 机器、计算机器和 bootstrap 机器组成。

要启用 Kuryr SDN，您的环境必须满足以下要求：

- 运行 RHOSP 13+。
- 具有 Octavia 的 Overcloud。
- 使用 Neutron Trunk 端口扩展。

- 如果使用 ML2/OVS Neutron 驱动而不是 **ovs-hybrid**，则请使用 **openvswitch** 防火墙驱动。

1.2.3.1. 增加配额

使用 Kuryr SDN 时，您必须提高配额以满足 Pod 、Services 、namespaces 和网络策略所使用的 Red Hat OpenStack Platform（RHOSP）资源要求。

流程

- 运行以下命令为项目增加配额：

```
$ sudo openstack quota set --secgroups 250 --secgroup-rules 1000 --ports 1500 --subnets 250 --networks 250 <project>
```

1.2.3.2. 配置 Neutron

Kuryr CNI 利用 Neutron Trunks 扩展来将容器插入 Red Hat OpenStack Platform（RHOSP）SDN，因此您必须使用 **trunks** 扩展才可以使 Kuryr 正常工作。

另外，如果您使用默认的 ML2/OVS Neutron 驱动程序，防火墙必须设为 **openvswitch** 而不是 **ovs_hybrid** ，以便在中继子端口上强制实施安全组，同时 Kuryr 可以正确处理网络策略。

1.2.3.3. 配置 Octavia

Kuryr SDN 使用 Red Hat OpenStack Platform（RHOSP）的 Octavia LBaaS 来实现 OpenShift Container Platform 服务。因此，您必须在 RHOSP 上安装和配置 Octavia 组件以使用 Kuryr SDN。

要启用 Octavia，您必须在安装 RHOSP Overcloud 的过程中包括 Octavia 服务，如果 Overcloud 已存在则需要升级 Octavia 服务。以下启用 Octavia 的步骤适用于新的 Overcloud 安装或 Overcloud 更新。

注意

以下步骤只包括在部署 RHOSP 时需要处理 Octavia 部分的信息。请注意 registry 可能会不同。

这个示例使用本地的 registry。

流程

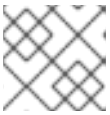
1. 如果您使用本地 registry，请创建一个模板来将镜像上传到 registry。例如：

```
(undercloud) $ openstack overcloud container image prepare \
-e /usr/share/openstack-tripleo-heat-templates/environments/services-docker/octavia.yaml \
--namespace=registry.access.redhat.com/rhosp13 \
--push-destination=<local-ip-from-undercloud.conf>:8787 \
--prefix=openstack- \
--tag-from-label {version}-{release} \
--output-env-file=/home/stack/templates/overcloud_images.yaml \
--output-images-file /home/stack/local_registry_images.yaml
```

2. 验证 **local_registry_images.yaml** 文件是否包含 Octavia 镜像。例如：

```
...
- imagename: registry.access.redhat.com/rhosp13/openstack-octavia-api:13.0-43
```

```
  push_destination: <local-ip-from-undercloud.conf>:8787
- imagename: registry.access.redhat.com/rhosp13/openstack-octavia-health-manager:13.0-
45
  push_destination: <local-ip-from-undercloud.conf>:8787
- imagename: registry.access.redhat.com/rhosp13/openstack-octavia-housekeeping:13.0-45
  push_destination: <local-ip-from-undercloud.conf>:8787
- imagename: registry.access.redhat.com/rhosp13/openstack-octavia-worker:13.0-44
  push_destination: <local-ip-from-undercloud.conf>:8787
```



注意

Octavia 容器版本根据所安装的特定 RHOSP 版本的不同而有所不同。

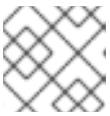
3. 将 registry.redhat.io 中的容器镜像拉取到 Undercloud 节点：

```
(undercloud) $ sudo openstack overcloud container image upload \
  --config-file  /home/stack/local_registry_images.yaml \
  --verbose
```

这可能需要一些时间，具体要看您的网络速度和 Undercloud 使用的磁盘。

4. 因为 Octavia 负载均衡器是用来访问 OpenShift API 的，所以您必须增加它们的监听程序的默认超时时间。默认超时为 50 秒。通过将以下文件传递给 Overcloud deploy 命令，将超时时间增加到 20 分钟：

```
(undercloud) $ cat octavia_timeouts.yaml
parameter_defaults:
  OctaviaTimeoutClientData: 1200000
  OctaviaTimeoutMemberData: 1200000
```



注意

RHOSP 14+ 不需要这一步。

5. 使用 Octavia 安装或更新 overcloud 环境：

```
openstack overcloud deploy --templates \
  -e /usr/share/openstack-tripleo-heat-templates/environments/services-docker/octavia.yaml \
  -e octavia_timeouts.yaml
```

注意

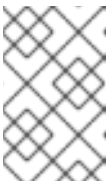
这个命令只包含与 Octavia 相关的文件，它根据您具体的 RHOSP 安装而有所不同。如需更多信息，请参阅 RHOSP 文档。有关自定义 Octavia 安装的详情请参考使用 Director 安装 Octavia。

注意

当利用 Kuryr SDN 时，Overcloud 安装需要 Neutron **trunk** 扩展。这在 Director 部署中默认可用。当 Neutron 后端是 ML2/OVS 时，使用 **openvswitch** 防火墙而不是默认的 **ovs-hybrid**。如果后端为 ML2/OVN，则不需要修改。

6. 在 RHOSP 13 和 15 中，在创建完项目后把项目 ID 添加到 **octavia.conf** 配置文件。

- 要跨服务实施网络策略，比如网络流量会通过 Octavia 负载均衡器时，您必须确保 Octavia 在用户项目中创建 Amphora VM 安全组。
  这可确保所需的 LoadBalancer 安全组属于该项目，并可将其更新为强制实施服务隔离。



注意

在 RHOSP 16 或更高版本中不需要此操作。

Octavia 实施新的 ACL API，限制对负载均衡器 VIP 的访问。

a. 获取项目 ID

```
$ openstack project show <project>
+-------------+----------------------------------+
| Field       | Value                            |
+-------------+----------------------------------+
| description |                                  |
| domain_id   | default                          |
| enabled     | True                             |
| id          | PROJECT_ID                       |
| is_domain   | False                            |
| name        | *<project>*                      |
| parent_id   | default                          |
| tags        | []                               |
+-------------+----------------------------------+
```

b. 将项目 ID 添加到控制器的 **octavia.conf** 中。

i. 列出 Overcloud 控制器。

```
$ source stackrc  # Undercloud credentials
$ openstack server list
+--------------------------------------+-------------+--------+----------------------+-------
---------+------------+
|
| ID                                   | Name        | Status | Networks
| Image          | Flavor     |
|
+--------------------------------------+-------------+--------+----------------------+-------
---------+------------+
|
| 6bef8e73-2ba5-4860-a0b1-3937f8ca7e01 | controller-0 | ACTIVE |
ctlplane=192.168.24.8 | overcloud-full | controller |
|
| dda3173a-ab26-47f8-a2dc-8473b4a67ab9 | compute-0    | ACTIVE |
ctlplane=192.168.24.6 | overcloud-full | compute    |
|
+--------------------------------------+-------------+--------+----------------------+-------
---------+------------+
```

ii. SSH 到控制器。

```
$ ssh heat-admin@192.168.24.8
```

-

iii. 编辑 **octavia.conf** ，将项目添加到 Amphora 安全组存在于用户账户的项目列表中。

```
# List of project IDs that are allowed to have Load balancer security groups
# belonging to them.
amp_secgroup_allowed_projects = PROJECT_ID
```

c. 重启 Octavia worker 以便重新加载配置。

```
controller-0$ sudo docker restart octavia_worker
```

注意

根据您具体的 RHOSP 环境，Octavia 可能不支持 UDP 侦听程序。这意味着，如果使用了 Kuryr SDN，则不支持 UDP 服务。

1.2.3.4. 已知使用 Kuryr 安装的限制

将 OpenShift Container Platform 与 Kuryr SDN 搭配使用有一些已知的限制。

1.2.3.4.1. RHOSP 常规限制

带有 Kuryr SDN 的 OpenShift Container Platform 不支持 NodePort 服务。

RHOSP 资源限制

- 每个 OpenShift Service 部署了一个 Amphora 负载均衡器 VM，并使用默认的 Octavia 负载均衡器驱动（Amphora 驱动）。创建太多的服务会导致您耗尽资源。

RHOSP 版本限制
使用带有 Kuryr SDN 的 OpenShift Container Platform 有一些限制，具体取决于 RHOSP 版本。

- Octavia RHOSP 16 之前的版本不支持 UDP 侦听程序。因此，OpenShift UDP 服务不被支持。
- Octavia RHOSP 16 前的版本无法侦听同一端口上的多个协议。不支持将同一端口暴露给不同协议的服务，比如 TCP 和 UDP。

重要

在任何 RHOSP 版本中，OVN Octavia 驱动程序都不支持使用不同协议的监听程序。

RHOSP 环境限制
使用取决于您的部署环境的 Kuryr SDN 会有一些限制。

由于 Octavia 缺少对 UDP 协议和多个监听器的支持，Kuryr 会强制 Pod 在 DNS 解析中使用 TCP，如果：

- RHOSP 版本早于 16
- 使用 OVN Octavia 驱动

在 Go 版本 1.12 及更早的版本中，通过 CGO 支持被禁用的模式编译的应用程序只使用 UDP。在这种情况下，native Go 解析器无法识别 **resolv.conf** 中的 **use-vc** 选项，它控制 DNS 解析是否强制使用 TCP。因此，UDP 仍会被用来解析 DNS，这将导致失败。

要确保 TCP 强制使用是允许的，在编译应用程序使把环境变量 **CGO_ENABLED** 设定为 **1**（如 **CGO_ENABLED=1**），或者不使用这个变量。

在 Go 版本 1.13 及之后的版本中，如果使用 UDP 的 DNS 解析失败，则会自动使用 TCP。

注意

基于 musl 的容器，包括基于 Alpine 的容器，不支持 **use-vc** 选项。

1.2.3.5. control plane 和计算机器

默认情况下，OpenShift Container Platform 安装程序支持三台 control plane 和计算机器。

每台机器都需要：

- 来自 RHOSP 配额的实例
- 来自 RHOSP 配额的端口
- 其类别至少有 16 GB 内存、4 个 vCPU 和 25GB 存储空间

提示

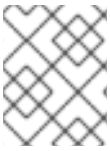
计算机器托管您在 OpenShift Container Platform 上运行的应用程序；运行数量应尽可能多。

1.2.3.6. bootstrap 机器

在安装时，会临时置备 bootstrap 机器来支持 control plane。生产控制平面就绪后，bootstrap 机器会被取消置备。

bootstrap 机器需要：

- 来自 RHOSP 配额的实例
- 来自 RHOSP 配额的端口
- 其类别至少有 16 GB 内存、4 个 vCPU 和 25GB 存储空间



注意

安装程序无法将证书颁发机构捆绑包传递给 control plane 机器上的 Ignition。因此，如果端点使用自签名证书，bootstrap 机器将无法从 Swift 检索 Ignition 配置。

1.2.4. 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。

1.2.5. 在 OpenStack 中启用 Swift

在 Red Hat OpenStack Platform (RHOSP) 上的 OpenShift Container Platform 使用 RHOSP Object Storage (Swift) 来存储和提供用户配置文件。

Swift 由具有 **swiftoperator** 角色的用户帐户操控。

先决条件

- 目标环境中的 RHOSP 管理员帐户
- Ceph RGW 上必须启用 **account in url** 选项

流程

在 RHOSP 上启用 Swift：

1. 在 RHOSP CLI 中以管理员身份，将 **swiftoperator** 角色添加到要访问 Swift 的帐户：

```
$ openstack role add --user <user> --project <project> swiftoperator
```

您的 RHOSP 部署现在可以使用 Swift 来存储和提供文件。

1.2.6. 验证外部网络访问

OpenShift Container Platform 安装程序需要外部网络访问权限。您必须为其提供外部网络值，否则部署会失败。在运行安装程序之前，请验证 Red Hat OpenStack Platform (RHOSP) 中是否存在具有外部路由器类型的网络。

先决条件

- 在 RHOSP 中，必须将 **NeutronDhcpAgentDnsmasqDnsServers** 参数配置为允许 DHCP 代理转发实例的 DNS 查询。设置这个参数的方法之一为：
  a. 在模板目录中创建新环境文件 。
  b. 在文件中提供参数值 。例如：

```
parameter_defaults:
  NeutronDhcpAgentDnsmasqDnsServers:
['<DNS_server_address_1>','<DNS_server_address_2']
```

c. 在 Overcloud 部署命令中包括 环境文件。例如：

```
$ openstack overcloud deploy --templates -e neutron-dhcp-agent-dnsmasq-dns-
servers.yaml ...
```

流程

1. 使用 RHOSP CLI 验证"外部"网络的名称和 ID：

```
$ openstack network list --long -c ID -c Name -c "Router Type"

+--------------------------------------+----------------+-------------+
| ID                                   | Name           | Router Type |
+--------------------------------------+----------------+-------------+
| 148a8023-62a7-4672-b018-003462f8d7dc | public_network | External    |
+--------------------------------------+----------------+-------------+
```

网络列表中会显示具有外部路由器类型的网络。如果最少有一个没有，请参阅 创建默认浮动 IP 网络和创建默认供应商网络。

重要

如果外部网络 CIDR 范围与某一个默认网络范围重叠，您必须在运行安装程序前更改 **install-config.yaml** 文件中匹配的网络范围。

默认的网络范围：

网络	范围
machineCIDR	10.0.0.0/16
serviceNetwork	172.30.0.0/16
clusterNetwork	10.128.0.0/14

小心

如果安装程序找到多个同名的镜像，它会随机设置其中之一。为避免这种行为，请在 RHOSP 中为资源创建唯一名称。

注意

如果启用了 Neutron 中继服务插件，则默认创建中继端口。如需更多信息，请参阅 Neutron 中继端口。

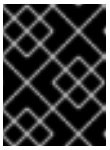
1.2.7. 为安装程序定义参数

OpenShift Container Platform 安装程序依赖于一个名为 **clouds.yaml** 的文件。该文件描述了 Red Hat OpenStack Platform (RHOSP) 配置参数，包括项目名称、登录信息和授权服务 URL。

流程

1. 创建 **clouds.yaml** 文件：

   - 如果您的 RHOSP 发行版包含 Horizon web UI，请在该 UI 中生成 **clouds.yaml** 文件。

     重要

     请记住在 **auth** 字段中添加密码。您也可以把 secret 保存在 **clouds.yaml** 以外的一个独立的文件中。

   - 如果您的 RHOSP 发行版不包含 Horizon Web UI，或者您不想使用 Horizon，请自行创建该文件。如需有关 **clouds.yaml** 的详细信息，请参阅 RHOSP 文档中的配置文件。

     ```
     clouds:
       shiftstack:
         auth:
           auth_url: http://10.10.14.42:5000/v3
           project_name: shiftstack
           username: shiftstack_user
           password: XXX
           user_domain_name: Default
           project_domain_name: Default
       dev-env:
         region_name: RegionOne
         auth:
           username: 'devuser'
           password: XXX
           project_name: 'devonly'
           auth_url: 'https://10.10.14.22:5001/v2.0'
     ```

2. 将您生成的文件放在以下位置之一：

   a. **OS_CLIENT_CONFIG_FILE** 环境变量的值

   b. 当前目录

   c. 特定于 Unix 的用户配置目录，如 **~/.config/openstack/clouds.yaml**

   d. 特定于 Unix 的站点配置目录，如 **/etc/openstack/clouds.yaml**
   安装程序会按照以上顺序搜索 **clouds.yaml**。

1.2.8. 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。

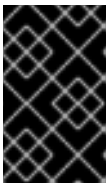
流程

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。

1.2.9. 创建安装配置文件

您可以自定义 Red Hat OpenStack Platform（RHOSP）上的 OpenShift Container Platform 安装。

先决条件

- 获取 OpenShift Container Platform 安装程序以及集群的 pull secret。

流程

1. 创建 **install-config.yaml** 文件。

   a. 运行以下命令：

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

   1 对于 **<installation_directory>**，请指定用于保存安装程序所创建的文件的目录名称。

重要

指定一个空目录。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。

   b. 在提示符处，提供您的云的配置详情：

      i. 可选：选择用来访问集群机器的 SSH 密钥。

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。

ii. 选择 **openstack** 作为目标平台。

iii. 指定用于安装集群的 Red Hat OpenStack Platform (RHOSP) 外部网络名称。

iv. 指定用于从外部访问 OpenShift API 的浮动 IP 地址。

v. 指定至少有 16 GB RAM 用于 control plane 和计算节点的 RHOSP 类别。

vi. 选择集群要部署到的基域。所有 DNS 记录都将是这个基域的子域，并包含集群名称。

vii. 为集群输入一个名称。名称不能多于 14 个字符。

viii. 粘贴从 Red Hat OpenShift Cluster Manager 站点的 Pull Secret 页面中获取的 pull secret。

2. 修改 **install-config.yaml** 文件。您可以在**安装配置参数**部分中找到有关可用参数的更多信息。

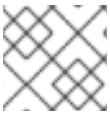
3. 备份 **install-config.yaml** 文件，以便用于安装多个集群。

重要

install-config.yaml 文件会在安装过程中消耗掉。如果要重复使用此文件，必须现在备份。

1.2.10. 安装配置参数

在部署 OpenShift Container Platform 集群前，您可以提供参数值，以描述托管集群的云平台的帐户并选择性地自定义集群平台。在创建 **install-config.yaml** 安装配置文件时，您可以通过命令行来提供所需的参数的值。如果要自定义集群，可以修改 **install-config.yaml** 文件来提供关于平台的更多信息。



注意

安装之后，您无法修改 **install-config.yaml** 文件中的这些参数。

表 1.6. 所需的参数

参数	描述	值
baseDomain	云供应商的基域。此值用于创建到 OpenShift Container Platform 集群组件的路由。集群的完整 DNS 名称是 **baseDomain** 和 **metadata.name** 参数值的组合，其格式为 **<metadata.name>.<baseDomain>**。	完全限定域名或子域名，如 **example.com**。

参数	描述	值
controlPlane.platform	托管 control plane 机器的云供应商。此参数值必须与 **compute.platform** 参数值匹配。	**aws**、**azure**、**gcp**、**openstack** 或 **{}**
compute.platform	托管 worker 机器的云供应商。此参数值必须与 **controlPlane.platform** 参数值匹配。	**aws**、**azure**、**gcp**、**openstack** 或 **{}**
metadata.name	集群的名称。	包含大写字母或小写字母的字符串，如 **dev**。该字符串长度必须为 14 个字符或更少。
platform.<platform>.region	集群要部署到的区域。	云的有效区域，如 AWS 的 **us-east-1**、Azure 的 **centralus** 或 Red Hat OpenStack Platform (RHOSP) 的 **region1**。

pullSecret	从 Red Hat OpenShift Cluster Manager 站点的 Pull Secret 页面中获取的 pull secret。您可以使用此 pull secret 来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。	{
		"auths":{
		"cloud.openshift.com":{
		"auth":"b3Blb=",
		"email":"you@example.com"
		},
		"quay.io":{
		"auth":"b3Blb=",
		"email":"you@example.com"
		}
		}
		}

表 1.7. 可选参数

参数	描述	值
sshKey	用于访问集群机器的 SSH 密钥。 **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。	添加到 **ssh-agent** 进程的有效本地公共 SSH 密钥。

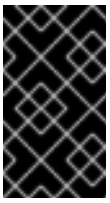
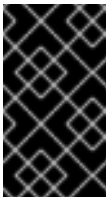
参数	描述	值
fips	是否启用或禁用 FIPS 模式。默认情况下不启用 FIPS 模式。如果启用了 FIPS 模式，运行 OpenShift Container Platform 的 Red Hat Enterprise Linux CoreOS (RHCOS) 机器会绕过默认的 Kubernetes 加密套件，并使用由 RHCOS 提供的加密模块。	**false** 或 **true**
publish	如何发布集群的面向用户的端点。	**Internal** 或 **External**。把 **publish** 设置为 **Internal** 以部署一个私有集群，它不能被互联网访问。默认值为 **External**。
compute.hyperthreading	是否在计算机器上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。  **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。	**Enabled** 或 **Disabled**
compute.replicas	要置备的计算机器数量，也称为 worker 机器。	大于或等于 **2** 的正整数。默认值为 **3**。
controlPlane.hyperthreading	是否在 control plane 机器上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。  **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。	**Enabled** 或 **Disabled**
controlPlane.replicas	要置备的 control plane 机器数量。	大于或等于 **3** 的正整数。默认值为 **3**。

表 1.8. 其他 Red Hat OpenStack Platform (RHOSP) 参数

参数	描述	值
compute.platform.openstack.rootVolume.size	对于计算机器，以 GB 为单位表示的根卷大小。如果您不设置这个值，机器将使用临时存储。	整数，如 **30**。
compute.platform.openstack.rootVolume.type	对于计算机器，根卷的类型。	字符串，如 **performance**。
controlPlane.platform.openstack.rootVolume.size	对于 control plane 机器，以 GB 为单位表示的根卷大小。如果您不设置这个值，机器将使用临时存储。	整数，如 **30**。
controlPlane.platform.openstack.rootVolume.type	对于 control plane 机器，根卷的类型。	字符串，如 **performance**。
platform.openstack.region	在其中创建 RHOSP 集群的区域。	字符串，如 **region1**。
platform.openstack.cloud	要使用的 RHOSP 云的名称，来自于 **clouds.yaml** 文件中的云列表。	字符串，如 **MyCloud**。
platform.openstack.externalDNS	*可选*。集群实例用于进行 DNS 解析的外部 DNS 服务器的 IP 地址。	包括 IP 地址列表的字符串，如 **["8.8.8.8", "192.168.1.12"]**。
platform.openstack.externalNetwork	用于安装的 RHOSP 外部网络名称。	字符串，如 **external**。
platform.openstack.computeFlavor	用于 control plane 和计算机器的 RHOSP 类别。	字符串，如 **m1.xlarge**。
platform.openstack.lbFloatingIP	与负载均衡器 API 关联的现有浮动 IP 地址。	IP 地址，如 **128.0.0.1**。

platform.openstack.defaultMachinePlatform	*可选*。默认机器池平台配置。	<pre>{
		"type": "ml.large",
		"rootVolume": {
		"size": 30,
		"type": "performance"
		}
		}</pre>

1.2.10.1. 使用 Kuryr 的 RHOSP 的自定义 install-config.yaml 文件示例

要使用 Kuryr SDN 而不是默认的 OpenShift SDN 部署，您必须修改 **install-config.yaml** 文件，使其包含 **Kuryr** 作为所需的 **networking.networkType**，然后执行默认的 OpenShift SDN 安装步骤。此示例 **install-config.yaml** 展示了所有可能的 Red Hat OpenStack Platform (RHOSP) 自定义选项。

重要

此示例文件仅供参考。您必须使用安装程序来获取 **install-config.yaml** 文件。

```
apiVersion: v1
baseDomain: example.com
clusterID: os-test
controlPlane:
  name: master
  platform: {}
  replicas: 3
compute:
- name: worker
  platform:
    openstack:
      type: ml.large
  replicas: 3
metadata:
  name: example
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineCIDR: 10.0.0.0/16
  serviceNetwork:
  - 172.30.0.0/16
  networkType: Kuryr
platform:
  openstack:
    region: region1
    cloud: mycloud
    externalNetwork: external
    computeFlavor: m1.xlarge
    lbFloatingIP: 128.0.0.1
    trunkSupport: true
    octaviaSupport: true
pullSecret: '{"auths": ...}'
sshKey: ssh-ed25519 AAAA...
```

注意

安装程序会自动发现 **trunkSupport** 和 **octaviaSupport**，因此无需设置它们。但是，如果您的环境不满足这两个要求，Kuryr SDN 将无法正常工作。需要使用中继来把 Pod 连接到 RHOSP 网络，并且需要 Octavia 来创建 OpenShift 服务。

1.2.11. 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。

1.2.12. 启用对环境的访问

在部署时，所有 OpenShift Container Platform 机器都是在 Red Hat OpenStack Platform (RHOSP) 租户网络中创建的。因此，大多数 RHOSP 部署中都无法直接访问它们。

您可以配置 OpenShift Container Platform API，以便能使用或不使用浮动 IP 地址来访问。

1.2.12.1. 启用通过浮动 IP 地址进行访问

将两个浮动 IP (FIP) 地址附加到 OpenShift Container Platform API 端点以便可以访问这些端点：一个用于 API 负载均衡器 (**lb FIP**)，另一个用于 OpenShift Container Platform 应用程序 (**apps FIP**)。

重要

install-config.yaml 文件中也会使用负载均衡器 FIP。

流程

1. 使用 Red Hat OpenStack Platform (RHOSP) CLI，创建一个新的外部网络：

```
$ openstack floating ip create <external network>
```

2. 向您的 DNS 服务器中添加一条符合此模式的记录：

```
api.<cluster name>.<base domain>  IN  A  <lb FIP>
```

注意

如果您不控制 DNS 服务器，可以改为将记录添加到 **/etc/hosts** 文件中。此操作使 API 可供您自己访问，不适合于生产部署。这可用于进行开发和测试的安装。

提示

您可以通过分配浮动 IP 地址并更新防火墙配置，使 OpenShift Container Platform 资源在集群之外可用。

1.2.12.2. 启用不通过浮动 IP 地址进行访问

如果您无法使用浮动 IP 地址，OpenShift Container Platform 安装或许仍然可以完成。不过，安装程序在等待 API 访问超时后会失败。

安装程序超时后，集群或许仍然可以初始化。 bootstrap 过程开始后，它必须完成。但是，您必须在部署后编辑集群网络配置。

1.2.13. 部署集群

您可以在兼容云平台中安装 OpenShift Container Platform。

重要

安装程序的 **create cluster** 命令只能在初始安装过程中运行一次。

先决条件

- 获取 OpenShift Container Platform 安装程序以及集群的 pull secret。

流程

1. 运行安装程序：

```
$ ./openshift-install create cluster --dir=<installation_directory> \ 1
    --log-level=info 2
```

1 对于 **<installation_directory>**，请指定自定义 **./install-config.yaml** 文件的位置。

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

注意

如果您在主机上配置的云供应商帐户没有足够的权限来部署集群，安装过程将会停止，并且显示缺少的权限。

集群部署完成后，终端会显示访问集群的信息，包括指向其 Web 控制台的链接和 **kubeadmin** 用户的凭证。

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。

重要

您不得删除安装程序或安装程序所创建的文件。需要这两者才能删除集群。

1.2.14. 验证集群状态

在安装过程中或安装后验证 OpenShift Container Platform 集群的状态：

流程

1. 在集群环境中，导出管理员的 kubeconfig 文件：

```
$ 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。

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。

2. 查看部署后创建的 control plane 和计算机器：

```
$ oc get nodes
```

3. 查看集群的版本：

```
$ oc get clusterversion
```

4. 查看 Operator 的状态：

```
$ oc get clusteroperator
```

5. 查看集群中所有正在运行的 Pod：

```
$ oc get pods -A
```

1.2.15. 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
```

1.2.16. 使用浮动 IP 地址配置应用程序访问

安装 OpenShift Container Platform 后，请配置 Red Hat OpenStack Platform (RHOSP) 以允许应用程序网络流量。

先决条件

- 必须已安装 OpenShift Container Platform 集群
- 已启用浮动 IP 地址，如*启用对环境的访问*中所述。

流程

在安装 OpenShift Container Platform 集群后，将浮动 IP 地址附加到入口端口：

1. 显示端口：

```
$ openstack port show <cluster name>-<clusterID>-ingress-port
```

2. 将端口附加到 IP 地址：

```
$ openstack floating ip set --port <ingress port ID> <apps FIP>
```

3. 在您的 DNS 文件中，为 ***apps.** 添加一条通配符 **A** 记录。

```
*.apps.<cluster name>.<base domain>  IN  A  <apps FIP>
```

注意

如果您不控制 DNS 服务器，但希望为非生产用途启用应用程序访问，您可以将这些主机名添加到 **/etc/hosts**：

```
<apps FIP> console-openshift-console.apps.<cluster name>.<base domain>
<apps FIP> integrated-oauth-server-openshift-authentication.apps.<cluster name>.
<base domain>
<apps FIP> oauth-openshift.apps.<cluster name>.<base domain>
<apps FIP> prometheus-k8s-openshift-monitoring.apps.<cluster name>.<base
domain>
<apps FIP> grafana-openshift-monitoring.apps.<cluster name>.<base domain>
<apps FIP> <app name>.apps.<cluster name>.<base domain>
```

1.2.17. 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。

1.3. 在 OPENSTACK 上卸载集群

您可以删除部署到 Red Hat OpenStack Platform (RHOSP) 的集群。

1.3.1. 删除使用安装程序置备的基础架构的集群

您可以从云中删除使用安装程序置备的基础架构的集群。

先决条件

- 有部署集群时所用的安装程序副本。
- 有创建集群时安装程序所生成的文件。

流程

1. 在用来安装集群的计算机中运行以下命令：

```
$ ./openshift-install destroy cluster \
--dir=<installation_directory> --log-level=info 1 2
```

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

注意

您必须为集群指定包含集群定义文件的目录。安装程序需要此目录中的 **metadata.json** 文件来删除集群。

2. 可选：删除 **<installation_directory>** 目录和 OpenShift Container Platform 安装程序。