OpenShift Container Platform 4.2

在 Azure 上安装

安装 OpenShift Container Platform 4.2 Azure 集群

Last Updated: 2020-08-21

OpenShift Container Platform 4.2 在 Azure 上安装

安装 OpenShift Container Platform 4.2 Azure 集群

法律通告

摘要

本文档提供在 Microsoft Azure 上安装和卸载 OpenShift Container Platform 4.2 集群的说明。

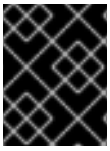
目录

第 1 章 在 AZURE 上安装 **3**
1.1. 配置 AZURE 帐户 3
1.2. 在 AZURE 上快速安装集群 10
1.3. 使用自定义在 AZURE 上安装集群 15
1.4. 使用网络自定义在 AZURE 上安装集群 25
1.5. 在 AZURE 上卸载集群 39

第 1 章 在 AZURE 上安装

1.1. 配置 AZURE 帐户

在安装 OpenShift Container Platform 之前，您必须配置 Microsoft Azure 帐户。

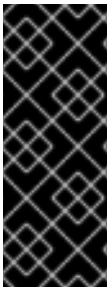


重要

所有通过公共端点提供的 Azure 资源均存在资源名称的限制，您无法创建使用某些名称的资源。如需 Azure 限制词语列表，请参阅 Azure 文档中的解决保留资源名称错误。

1.1.1. Azure 帐户限值

OpenShift Container Platform 集群使用诸多 Microsoft Azure 组件，默认的 Azure 订阅和服务限值、配额和约束会影响您安装 OpenShift Container Platform 集群的能力。



重要

默认的限制因服务类别的不同（如 Free Trial 或 Pay-As-You-Go）以及系列的不同（如 Dv2、F 或 G）而有所不同。例如，对于 Enterprise Agreement 订阅的默认限制是 350 个内核。

在 Azure 上安装默认集群前，请检查您的订阅类型的限制，如有必要，请提高帐户的配额限制。

下表总结了 Azure 组件，它们的限值会影响您安装和运行 OpenShift Container Platform 集群的能力。

组件	默认所需的组件数	默认 Azure 限值	描述

组件	默认所需的组件数	默认 Azure 限值	描述
vCPU	34	每个区域 20 个	默认集群需要 34 个 vCPU，因此您必须提高帐户限值。 默认情况下，每个集群创建以下实例： ● 一台 Bootstrap 机器，在安装后删除 ● 三个 control plane 机器 ● 三个计算（compute）机器 由于 Bootstrap 机器使用 **Standard_D4s_v3** 机器（使用 4 个 vCPU），control plane 机器使用 **Standard_D8s_v3** 虚拟机（8 个 vCPU），并且 worker 机器使用 **Standard_D2s_v3** 虚拟机（2 个 vCPU），因此默认集群需要 34 个 vCPU。 若要部署更多 worker 节点、启用自动扩展、部署大型工作负载或使用不同的实例类型，您必须进一步提高帐户的 vCPU 限值，以确保集群可以部署您需要的机器。 默认情况下，安装程序将 control plane 和 compute 机器分布到一个区域中的所有可用区。要确保集群的高可用性，请选择至少含有三个可用区的区域。如果您的区域包含的可用区少于三个，安装程序将在可用区中放置多台 control plane 机器。
VNet	1	每个区域 1000 个	每个默认集群都需要一个虚拟网络 (VNet)，此网络包括两个子网。
网络接口	6	每个区域 65,536 个	每个默认集群都需要六个网络接口。如果您要创建更多机器或者您部署的工作负载要创建负载均衡器，则集群会使用更多的网络接口。
网络安全组	2	5000	每个默认集群为 VNet 中的每个子网创建网络安全组。默认集群为 control plane 和计算节点子网创建网络安全组： **controlplane**：允许从任何位置通过端口 6443 访问 control plane 机器 **node**：允许从互联网通过端口 80 和 443 访问 worker 节点

组件	默认所需的组件数	默认 Azure 限值	描述
网络负载均衡器	3	每个区域 1000 个	每个集群都会创建以下负载均衡器： **default** 用于在 worker 机器之间对端口 80 和 443 的请求进行负载均衡的公共 IP 地址 **internal** 用于在 control plane 机器之间对端口 6443 和 22623 的请求进行负载均衡的专用 IP 地址 **external** 用于在 control plane 机器之间对端口 6443 的请求进行负载均衡的公共 IP 地址 如果您的应用程序创建了更多的 Kubernetes LoadBalancer Service 对象，您的集群会使用更多的负载均衡器。
公共 IP 地址	3		两个公共负载均衡器各自使用一个公共 IP 地址。bootstrap 机器也使用一个公共 IP 地址，以便您可以在安装期间通过 SSH 连接到该机器来进行故障排除。bootstrap 节点的 IP 地址仅在安装过程中使用。
专用 IP 地址	7		内部负载均衡器、三台 control plane 机器中的每一台以及三台 worker 机器中的每一台各自使用一个专用 IP 地址。

1.1.2. 在 Azure 中配置公共 DNS 区

要安装 OpenShift Container Platform，您使用的 Microsoft Azure 帐户必须在帐户中具有一个专用的公共托管 DNS 区。此区域必须对域具有权威。此服务为集群外部连接提供集群 DNS 解析和名称查询。

流程

1. 标识您的域或子域，以及注册商（registrar）。您可以转移现有的域和注册商，或通过 Azure 或其他来源获取新的域和注册商。

注意

如需通过 Azure 购买域的更多信息，请参阅 Azure 文档中的购买 Azure 应用服务的自定义域名。

2. 如果您使用现有的域和注册商，请将其 DNS 迁移到 Azure。请参阅 Azure 文档中的将活动 DNS 名称迁移到 Azure 应用服务。

3. 为您的域配置 DNS。按照 Azure 文档中教程：在 Azure DNS 中托管域部分里的步骤，为您的域或子域创建一个公共托管区，提取新的权威名称服务器，并更新您的域使用的名称服务器的注册商记录。
使用合适的根域（如 **openshiftcorp.com**）或子域（如 **clusters.openshiftcorp.com**）。

4. 如果您使用子域，请按照您公司的流程将其委派记录添加到父域。

1.1.3. 提高 Azure 帐户限值

要提高帐户限值，请在 Azure 门户上提交支持请求。

注意

每一支持请求只能提高一种类型的配额。

流程

1. 从 Azure 门户，点击左下角的 **Help + suport**。
2. 点击 **New support request**，然后选择所需的值：
   a. 从 **Issue type** 列表中，选择 **Service and subscription limits (quotas)**。
   b. 从 **Subscription** 列表中，选择要修改的订阅。
   c. 从 **Quota type** 列表中，选择要提高的配额。例如，选择 **Compute-VM (cores-vCPUs) subscription limit increases** 以增加 vCPU 的数量，这是安装集群所必须的。
   d. 点击 **Next: Solutions**。
3. 在 PROBLEM DETAILS 页面中，为您要提高的配额提供必要的信息：
   a. 点击 **Provide details**，然后在“Quota details”窗口中提供所需的详情。
   b. 在 SUPPORT METHOD 和 CONTACT INFO 部分中，提供问题严重性和您的联系详情。
4. 点击 **Next: Review + create**，然后点击 **Create**。

1.1.4. 所需的 Azure 角色

Microsoft Azure 帐户必须具有您所用订阅的以下角色：

- **User Access Administrator**

要在 Azure 门户上设置角色，请参阅 Azure 文档中的使用 RBAC 和 Azure 门户管理对 Azure 资源的访问。

1.1.5. 创建服务主体

由于 OpenShift Container Platform 及其安装程序必须通过 Azure Resource Manager 创建 Microsoft Azure 资源，因此您必须创建一个能代表它的服务主体。

先决条件

- 安装或更新 Azure CLI。
- 安装**jq**软件包。
- 您的 Azure 帐户具有您所用订阅所需的角色。

流程

1. 登录 Azure CLI：

```
$ az login
```

在 Web 控制台中，使用您的凭证登录 Azure。

2. 如果您的 Azure 帐户使用订阅，请确保使用正确的订阅。

a. 查看可用帐户列表并记录您要用于集群的订阅的 **tenantId** 值：

```
$ az account list --refresh
[
  {
    "cloudName": "AzureCloud",
    "id": "9bab1460-96d5-40b3-a78e-17b15e978a80",
    "isDefault": true,
    "name": "Subscription Name",
    "state": "Enabled",
    "tenantId": "6057c7e9-b3ae-489d-a54e-de3f6bf6a8ee",
    "user": {
      "name": "you@example.com",
      "type": "user"
    }
  }
]
```

b. 查看您的活跃帐户详情，确认 **tenantId** 与您要使用的订阅匹配：

```
$ az account show
{
  "environmentName": "AzureCloud",
  "id": "9bab1460-96d5-40b3-a78e-17b15e978a80",
  "isDefault": true,
  "name": "Subscription Name",
  "state": "Enabled",
  "tenantId": "6057c7e9-b3ae-489d-a54e-de3f6bf6a8ee", (1)
  "user": {
    "name": "you@example.com",
    "type": "user"
  }
}
```

(1) 确定 **tenantId** 参数的值是正确订阅的 UUID。

c. 如果您使用的订阅不正确，请更改活跃的订阅：

```
$ az account set -s <id> (1)
```

(1) 替换您要用于 **<id>** 的订阅的 **id** 值。

d. 如果您更改了活跃订阅，请重新显示您的帐户信息：

-

```
$ az account show

{
  "environmentName": "AzureCloud",
  "id": "33212d16-bdf6-45cb-b038-f6565b61edda",
  "isDefault": true,
  "name": "Subscription Name",
  "state": "Enabled",
  "tenantId": "8049c7e9-c3de-762d-a54e-dc3f6be6a7ee",
  "user": {
    "name": "you@example.com",
    "type": "user"
  }
}
```

3. 记录前面输出中 **tenantId** 和 **id** 参数的值。OpenShift Container Platform 安装过程中需要这些值。

4. 为您的帐户创建服务主体：

```
$ az ad sp create-for-rbac --role Contributor --name <service_principal> (1)
Changing "<service_principal>" to a valid URI of "http://<service_principal>", which is the
required format used for service principal names
Retrying role assignment creation: 1/36
Retrying role assignment creation: 2/36
Retrying role assignment creation: 3/36
Retrying role assignment creation: 4/36
{
  "appId": "8bd0d04d-0ac2-43a8-928d-705c598c6956",
  "displayName": "<service_principal>",
  "name": "http://<service_principal>",
  "password": "ac461d78-bf4b-4387-ad16-7e32e328aec6",
  "tenant": "6048c7e9-b2ad-488d-a54e-dc3f6be6a7ee"
}
```

(1) 将 **<service_principal>** 替换要您要分配给服务主体的名称。

5. 记录前面输出中 **appId** 和 **password** 参数的值。OpenShift Container Platform 安装过程中需要这些值。

6. 为服务主体授予额外权限。服务主体需要传统的 **Azure Active Directory Graph → Application.ReadWrite.OwnedBy** 权限以及集群的 **User Access Administrator** 角色，以便为其组件分配凭证。

   a. 要分配 **User Access Administrator** 角色，请运行以下命令：

```
$ az role assignment create --role "User Access Administrator" \
    --assignee-object-id $(az ad sp list --filter "appId eq '<appId>'" \ (1)
      | jq '.[0].objectId' -r)
```

(1) 将 **<appId>** 替换为服务器主体的 **appId** 参数值。

   b. 要分配 **Azure Active Directory Graph** 权限，请运行以下命令：

```
$ az ad app permission add --id <appId> \ 1
    --api 00000002-0000-0000-c000-000000000000 \
    --api-permissions 824c81eb-e3f8-4ee6-8f6d-de7f50d565b7=Role

    Invoking "az ad app permission grant --id 46d33abc-b8a3-46d8-8c84-f0fd58177435 --
api 00000002-0000-0000-c000-000000000000" is needed to make the change effective
```

1 将 **<appId>** 替换为服务器主体的 **appId** 参数值。

如需进一步了解可通过此命令授予的具体权限，请参阅 Windows Azure Active Directory 权限的 GUID 表。

c. 批准权限请求。如果您的帐户没有 Azure Active Directory 租户管理员角色，请按照您的组织的准则请租户管理员批准您的权限请求。

```
$ az ad app permission grant --id <appId> \ 1
    --api 00000002-0000-0000-c000-000000000000
```

1 将 **<appId>** 替换为服务器主体的 **appId** 参数值。

1.1.6. 支持的 Azure 区域

安装程序会根据您的订阅动态地生成可用的 Microsoft Azure 区域列表。OpenShift Container Platform 4.2.0 中已测试并验证了以下 Azure 区域：

- centralus (Central US)
- eastus (East US)
- eastus2 (East US 2)
- northcentralus (North Central US)
- southcentralus (South Central US)
- westcentralus (West Central US)
- westus (West US)
- westus2 (West US 2)
- uksouth (UK South)
- ukwest (UK West)
- francecentral (France Central)
- northeurope (North Europe)
- westeurope (West Europe)
- japaneast (Japan East)
- japanwest (Japan West)

- koreacentral (Korea Central)
- koreasouth (Korea South)
- eastasia (East Asia)
- southeastasia (Southeast Asia)
- southindia (South India)
- centralindia (Central India)
- westindia (West India)
- uaenorth (UAE North)

后续步骤

- 在 Azure 上安装 OpenShift Container Platform 集群。您可以安装自定义集群，或使用默认选项快速安装集群。

1.2. 在 AZURE 上快速安装集群

在 OpenShift Container Platform 版本 4.2 中，您可以使用默认配置选项在 Microsoft Azure 上安装集群。

先决条件

- 查看有关 OpenShift Container Platform 安装和更新流程的详细信息。
- 配置一个 Azure 帐户以托管集群，并决定要将集群部署到的已测试和验证的区域。
- 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。

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

在 OpenShift Container Platform 4.2 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：

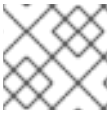
- 访问 Red Hat OpenShift Cluster Manager 页面，以下载安装程序并执行订阅管理。如果集群可以访问互联网，并且没有禁用 Telemetry，该服务会自动授权您的集群。
- 访问 Quay.io，以获取安装集群所需的软件包。
- 获取执行集群更新所需的软件包。

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。

1.2.2. 生成 SSH 私钥并将其添加到代理中

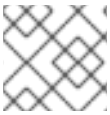
如果要在集群上执行安装调试或灾难恢复，则必须为 **ssh-agent** 和安装程序提供 SSH 密钥。



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**。

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。

1.2.3. 获取安装程序

在安装 OpenShift Container Platform 之前，将安装文件下载到

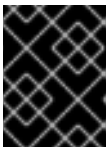
本地计算机。

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。

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。

1.2.4. 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

- 配置托管集群的云平台的帐户。
- 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
```

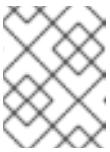
1. 对于 **<installation_directory>**，请指定用于保存安装程序所创建的文件的目录名称。
2. 要查看不同的安装详情，请指定 **warn**、**debug** 或 **error**，而不要指定 **info**。

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。

在提示符处提供值：

a. 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。

b. 选择 **azure** 作为目标平台。

c. 如果计算机上没有 Microsoft Azure 配置集，请为您的订阅和服务主体指定以下 Azure 参数值：

- **azure subscription id**：要用于集群的订阅 ID。指定帐户输出中的 **id** 值。
- **azure tenant id**：租户 ID。指定帐户输出中的 **tenantId** 值。
- **azure service principal client id**：服务主体的 **appId** 参数值。
- **azure service principal client secret**：服务主体的 **password** 参数值。

d. 选择要在其中部署集群的区域。

e. 选择集群要部署到的基域。基域与您为集群创建的 Azure DNS 区对应。

f. 为集群输入一个描述性名称。

重要

所有通过公共端点提供的 Azure 资源均存在资源名称的限制，您无法创建使用某些名称的资源。如需 Azure 限制词语列表，请参阅 Azure 文档中的解决保留资源名称错误。

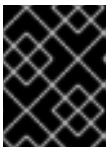
g. 粘贴从 Red Hat OpenShift Cluster Manager 站点的 Pull Secret 页面中获取的 pull secret。

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

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

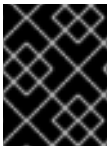
安装程序生成的 Ignition 配置文件中所含的证书会在 24 小时后过期。您必须以非降级状态持续运行集群 24 小时，以确保完成第一次证书轮转。

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。

1.2.5. 安装 CLI

为了可以使用命令行界面与 OpenShift Container Platform 进行交互，您需要安装 CLI。

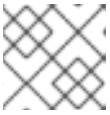


重要

如果安装了旧版本的 **oc**，则无法使用 OpenShift Container Platform 4.2 中的所有命令。下载并安装新版本的 **oc**。

流程

1. 在 Red Hat OpenShift Cluster Manager 站点的 Infrastructure Provider 页面中导航至您的安装类型页面，并点击 **Download Command-line Tools**。
2. 点您的操作系统和系统架构的文件夹，然后点压缩文件。



注意

您可在 Linux、Windows 或 macOS 上安装 **oc**。

3. 将文件保存到文件系统。
4. 展开压缩文件。
5. 把它放到 **PATH** 中的一个目录下。

安装 CLI 后，就可以使用**oc**命令：

```
$ oc <command>
```

1.2.6. 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
```

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. 使用自定义在 AZURE 上安装集群

在 OpenShift Container Platform 版本 4.2 中，您可以在安装程序在 Microsoft Azure 上置备的基础架构上安装自定义的集群。要自定义安装，请在安装集群前修改 **install-config.yaml** 文件中的参数。

先决条件

- 查看有关 OpenShift Container Platform 安装和更新流程的详细信息。
- 配置一个 Azure 帐户以托管集群，并决定要将集群部署到的已测试和验证的区域。
- 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。

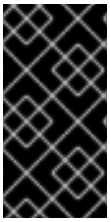
1.3.1. OpenShift Container Platform 对互联网和 Telemetry 的访问

在 OpenShift Container Platform 4.2 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。

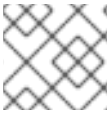


重要

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。

1.3.2. 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**。

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。

1.3.3. 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。

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。

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。

1.3.4. 创建安装配置文件

您可以自定义 Microsoft Azure 上的 OpenShift Container Platform 安装。

先决条件

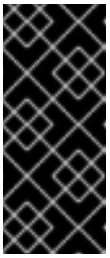
- 获取 OpenShift Container Platform 安装程序以及集群的 pull secret。

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 **azure** 作为目标平台。

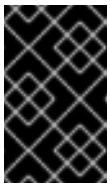
iii. 如果计算机上没有 Microsoft Azure 配置集，请为您的订阅和服务主体指定以下 Azure 参数值：

- **azure subscription id**：要用于集群的订阅 ID。指定帐户输出中的 **id** 值。
- **azure tenant id**：租户 ID。指定帐户输出中的 **tenantId** 值。
- **azure service principal client id**：服务主体的 **appId** 参数值。
- **azure service principal client secret**：服务主体的 **password** 参数值。

iv. 选择要在其中部署集群的区域。

v. 选择集群要部署到的基域。基域与您为集群创建的 Azure DNS 区对应。

vi. 为集群输入一个描述性名称。



重要

所有通过公共端点提供的 Azure 资源均存在资源名称的限制，您无法创建使用某些名称的资源。如需 Azure 限制词语列表，请参阅 Azure 文档中的解决保留资源名称错误。

vii. 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。

1.3.4.1. 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 1.1. 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**。
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**。

参数	描述	值

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 1.2. 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。
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**。

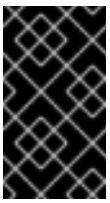
参数	描述	值
controlPlane.hyperthreading	是否在 control plane 机器上启用或禁用并发多线程或**超线程**。默认情况下，启用并发多线程以提高机器内核的性能。  **重要** 如果禁用并发多线程，请确保在容量规划时考虑到机器性能可能会显著降低的问题。	**Enabled** 或 **Disabled**
controlPlane.replicas	要置备的 control plane 机器数量。	大于或等于 **3** 的正整数。默认值为 **3**。

表 1.3. 其他 Azure 参数

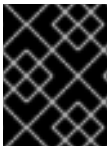
参数	描述	值
machines.platform.azure.type	Azure 虚拟机实例类型。	使用 Windows 或 Linux 作为操作系统的虚拟机。请参阅 Azure 文档中的 Azure Stack 上支持的客户端操作系统。
machines.platform.azure.osDisk.diskSizeGB	虚拟机的 Azure 磁盘大小。	以 GB 为单位表示磁盘大小的整数，如 **512**。支持的最小磁盘大小为 **120**。
platform.azure.baseDomainResourceGroupName	包含基域的 DNS 区的资源组的名称。	字符串，如 **production_cluster**。
platform.azure.region	托管集群的 Azure 区域名称。	任何有效的区域名称。
platform.azure.zone	可在其中放入机器的可用区的列表。如需高可用性，请至少指定两个区域。	区域列表，如 **["1", "2", "3"]**

注意

您无法自定义 Azure 可用区，也不能使用标签来整理用于 Azure 集群的 Azure 资源。

1.3.4.2. Azure 的自定义 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。



重要

此示例 YAML 文件仅供参考。您必须使用安装程序来获取 **install-config.yaml** 文件，并且修改该文件。

```
apiVersion: v1
baseDomain: example.com (1)
controlPlane: (2)
  hyperthreading: Enabled (3) (4)
  name: master
  platform:
    azure:
      osDisk:
        diskSizeGB: 512 (5)
      type: Standard_D8s_v3
  replicas: 3
compute: (6)
- hyperthreading: Enabled (7)
  name: worker
  platform:
    azure:
      type: Standard_D2s_v3
      osDisk:
        diskSizeGB: 512 (8)
      zones: (9)
      - "1"
      - "2"
      - "3"
  replicas: 5
metadata:
  name: test-cluster (10)
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineCIDR: 10.0.0.0/16
  networkType: OpenShiftSDN
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    region: centralus (11)
    baseDomainResourceGroupName: resource-group (12)
pullSecret: '{"auths": ...}' (13)
sshKey: ssh-ed25519 AAAA... (14)
```

(1) (10) (11) (13) 必需。安装程序会提示您输入这个值。

(2) (6) 如果没有提供这些参数和值，安装程序会提供默认值。

(3) (7) **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。

4 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

重要

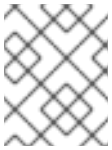
如果禁用并发多线程，请确保在容量规划时考虑到机器性能可能会显著降低的问题。如果禁用并发多线程，请使用较大的虚拟机类型，如 **Standard_D8s_v3**。

5 8 可以 GB 为单位指定要使用的磁盘大小。

9 指定要将机器部署到的区域列表。如需高可用性，请至少指定两个区域。

12 指定包含基域的 DNS 区的资源组的名称。

14 您可以选择提供您用来访问集群中机器的 **sshKey** 值。



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。

1.3.5. 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

- 配置托管集群的云平台的帐户。
- 获取 OpenShift Container Platform 安装程序以及集群的 pull secret。

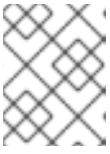
流程

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。

1.3.6. 安装 CLI

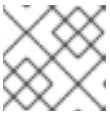
为了可以使用命令行界面与 OpenShift Container Platform 进行交互，您需要安装 CLI。

重要

如果安装了旧版本的 **oc**，则无法使用 OpenShift Container Platform 4.2 中的所有命令。下载并安装新版本的 **oc**。

流程

1. 在 Red Hat OpenShift Cluster Manager 站点的 Infrastructure Provider 页面中导航至您的安装类型页面，并点击 **Download Command-line Tools**。
2. 点您的操作系统和系统架构的文件夹，然后点压缩文件。



注意

您可在 Linux、Windows 或 macOS 上安装 **oc**。

3. 将文件保存到文件系统。
4. 展开压缩文件。
5. 把它放到 **PATH** 中的一个目录下。

安装 CLI 后，就可以使用**oc**命令：

```
$ oc <command>
```

1.3.7. 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
```

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。

1.4. 使用网络自定义在 AZURE 上安装集群

在 OpenShift Container Platform 版本 4.2 中，您可以使用自定义的网络配置在安装程序在 Microsoft Azure 上置备的基础架构上安装集群。通过自定义网络配置，您的集群可以与环境中现有的 IP 地址分配共存，并与现有的 MTU 和 VXLAN 配置集成。

大部分网络配置参数必须在安装过程中设置，只有 **kubeProxy** 配置参数可以在运行的集群中修改。

先决条件

- 查看有关 OpenShift Container Platform 安装和更新流程的详细信息。
- 配置一个 Azure 帐户以托管集群，并决定要将集群部署到的已测试和验证的区域。
- 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。

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

在 OpenShift Container Platform 4.2 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。

1.4.2. 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**。

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。

1.4.3. 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。

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。

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。

1.4.4. 创建安装配置文件

您可以自定义 Microsoft Azure 上的 OpenShift Container Platform 安装。

先决条件

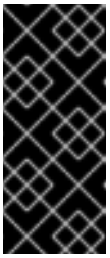
- 获取 OpenShift Container Platform 安装程序以及集群的 pull secret。

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 **azure** 作为目标平台。

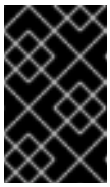
iii. 如果计算机上没有 Microsoft Azure 配置集，请为您的订阅和服务主体指定以下 Azure 参数值：

- **azure subscription id**：要用于集群的订阅 ID。指定帐户输出中的 **id** 值。
- **azure tenant id**：租户 ID。指定帐户输出中的 **tenantId** 值。
- **azure service principal client id**：服务主体的 **appId** 参数值。
- **azure service principal client secret**：服务主体的 **password** 参数值。

iv. 选择要在其中部署集群的区域。

v. 选择集群要部署到的基域。基域与您为集群创建的 Azure DNS 区对应。

vi. 为集群输入一个描述性名称。



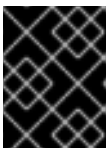
重要

所有通过公共端点提供的 Azure 资源均存在资源名称的限制，您无法创建使用某些名称的资源。如需 Azure 限制词语列表，请参阅 Azure 文档中的解决保留资源名称错误。

vii. 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。

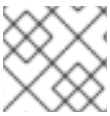


重要

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。

1.4.4.1. 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 1.4. 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**。
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**。

参数	描述	值

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 1.5. 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。
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 1.6. 其他 Azure 参数

参数	描述	值
machines.platform.azure.type	Azure 虚拟机实例类型。	使用 Windows 或 Linux 作为操作系统的虚拟机。请参阅 Azure 文档中的 Azure Stack 上支持的客户端操作系统。
machines.platform.azure.osDisk.diskSizeGB	虚拟机的 Azure 磁盘大小。	以 GB 为单位表示磁盘大小的整数，如 **512**。支持的最小磁盘大小为 **120**。
platform.azure.baseDomainResourceGroupName	包含基域的 DNS 区的资源组的名称。	字符串，如 **production_cluster**。
platform.azure.region	托管集群的 Azure 区域名称。	任何有效的区域名称。
platform.azure.zone	可在其中放入机器的可用区的列表。如需高可用性，请至少指定两个区域。	区域列表，如 **["1", "2", "3"]**

注意

您无法自定义 Azure 可用区，也不能使用标签来整理用于 Azure 集群的 Azure 资源。

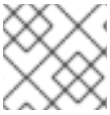
重要

Open Virtual Networking (OVN) Kubernetes 网络插件只是技术预览功能。技术预览功能不被红帽产品服务等级协议 (SLA) 支持，且可能在功能方面有缺陷。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

如需 OVN 技术预览支持范围的更多信息，请参阅 https://access.redhat.com/articles/4380121。

1.4.4.2. 网络配置参数

您可以在 **install-config.yaml** 配置文件中修改集群网络配置参数。下表描述了这些参数。



注意

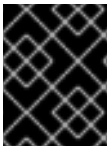
安装之后，您无法修改 **install-config.yaml** 文件中的这些参数。

表 1.7. 所需的网络参数

参数	描述	值
networking.networkType	要部署的网络插件。**OpenShiftSDN** 插件是 OpenShift Container Platform 4.2 中唯一支持的插件。**OVNKubernetes** 插件在 OpenShift Container Platform 4.2 中仅以技术预览提供。	**OpenShiftSDN** 或 **OVNKubernetes**。默认值为 **OpenShiftSDN**。
networking.clusterNetwork.cidr	从中分配 Pod IP 地址的 IP 地址块。**OpenShiftSDN** 网络插件支持多个集群网络。多个集群网络的地址块不得互相重叠。请选择足够大的地址池，以适配预期的工作负载。	CIDR 格式的 IP 地址分配。默认值为 **10.128.0.0/14**。
networking.clusterNetwork.hostPrefix	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。	子网前缀。默认值为 **23**。
networking.serviceNetwork	服务的 IP 地址块。**OpenShiftSDN** 只允许一个 **serviceNetwork** 块。该地址块不得与任何其他网络块重叠。	CIDR 格式的 IP 地址分配。默认值为 **172.30.0.0/16**。
networking.machineCIDR	OpenShift Container Platform 安装程序在安装集群时使用的 IP 地址块。该地址块不得与任何其他网络块重叠。	CIDR 格式的 IP 地址分配。默认值为 **10.0.0.0/16**。

1.4.4.3. Azure 的自定义 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。



重要

此示例 YAML 文件仅供参考。您必须使用安装程序来获取 **install-config.yaml** 文件，并且修改该文件。

```
apiVersion: v1
baseDomain: example.com (1)
controlPlane: (2)
  hyperthreading: Enabled (3) (4)
  name: master
  platform:
    azure:
      osDisk:
        diskSizeGB: 512 (5)
      type: Standard_D8s_v3
  replicas: 3
compute: (6)
- hyperthreading: Enabled (7)
  name: worker
  platform:
    azure:
      type: Standard_D2s_v3
      osDisk:
        diskSizeGB: 512 (8)
      zones: (9)
      - "1"
      - "2"
      - "3"
  replicas: 5
metadata:
  name: test-cluster (10)
networking: (11)
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineCIDR: 10.0.0.0/16
  networkType: OpenShiftSDN
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    region: centralus (12)
    baseDomainResourceGroupName: resource-group (13)
pullSecret: '{"auths": ...}' (14)
sshKey: ssh-ed25519 AAAA... (15)
```

(1) (10) (12) (14) 必需。安装程序会提示您输入这个值。

(2) (6) (11) 如果没有提供这些参数和值，安装程序会提供默认值。

(3) (7) **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。

4 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

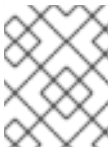
如果禁用并发多线程，请确保在容量规划时考虑到机器性能可能会显著降低的问题。如果禁用并发多线程，请使用较大的虚拟机类型，如 **Standard_D8s_v3**。

5 8 可以 GB 为单位指定要使用的磁盘大小。

9 指定要将机器部署到的区域列表。如需高可用性，请至少指定两个区域。

13 指定包含基域的 DNS 区的资源组的名称。

15 您可以选择提供您用来访问集群中机器的 **sshKey** 值。



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。

1.4.5. 修改高级网络配置参数

您只能在安装集群前修改高级网络配置参数。通过自定义高级配置，您可以指定 MTU 或 VXLAN 端口，允许自定义 kube-proxy 设置，以及为 **openshiftSDNConfig** 参数指定不同的 **mode**，从而将集群整合到现有的网络环境中。

重要

不支持直接修改 OpenShift Container Platform 清单文件。

先决条件

- 创建 **install-config.yaml** 文件并完成对其所做的任何修改。

流程

1. 使用以下命令来创建清单：

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

1 对于 **<installation_directory>**，请指定含有集群的 **install-config.yaml** 文件的目录的名称。

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 **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。

3. 在 **<installation_directory>/manifests/** 目录下，创建一个名为 **cluster-network-03-config.yml** 的文件：

```
$ touch <installation_directory>/manifests/cluster-network-03-config.yml 1
```

1 对于 **<installation_directory>**，请指定包含集群的 **manifests/** 目录的目录名称。

创建该文件后，**manifests/** 目录中会包含多个网络配置文件，如下所示：

```
$ ls <installation_directory>/manifests/cluster-network-*
cluster-network-01-crd.yml
cluster-network-02-config.yml
cluster-network-03-config.yml
```

4. 在编辑器中打开 **cluster-network-03-config.yml** 文件，然后输入描述您想要的 Operator 配置的 CR：

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec: 1
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  serviceNetwork:
  - 172.30.0.0/16
  defaultNetwork:
    type: OpenShiftSDN
    openshiftSDNConfig:
      mode: NetworkPolicy
      mtu: 1450
      vxlanPort: 4789
```

1 **spec** 参数的参数仅作示例。在 CR 中为 Cluster Network Operator 指定配置。

CNO 为 CR 中的参数提供默认值，因此您必须只指定要更改的参数。

5. 保存 **cluster-network-03-config.yml** 文件，再退出文本编辑器。

6. 可选：备份 **manifests/cluster-network-03-config.yml** 文件。创建集群时，安装程序会删除 **manifests/** 目录。

1.4.6. Cluster Network Operator 自定义资源 (CR)

Network.operator.openshift.io 自定义资源 (CR) 中的集群网络配置存储 Cluster Network Operator (CNO) 的配置设置。Operator 管理集群网络。

您可以通过在 CNO CR 中设置 **defaultNetwork** 参数的参数，为 OpenShift Container Platform 集群指定集群网络配置。以下 CR 显示了 CNO 的默认配置，并且说明了您可以配置的参数和有效的参数值：

Cluster Network Operator CR

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  clusterNetwork: 1
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  serviceNetwork: 2
  - 172.30.0.0/16
  defaultNetwork: 3
    ...
  kubeProxyConfig: 4
    iptablesSyncPeriod: 30s 5
    proxyArguments:
      iptables-min-sync-period: 6
      - 30s
```

1 2 在 **install-config.yaml** 文件中指定。

3 为集群网络配置软件定义型网络 (SDN)。

4 此对象的参数指定 **kube-proxy** 配置。如果没有指定参数值，Network Operator 会使用显示的默认参数值。

5 **iptables** 规则的刷新周期。默认值为 **30s**。有效的后缀包括 **s**、**m**和 **h**，具体参见 Go 时间包文档。

6 刷新 **iptables** 规则前的最短时长。此参数确保刷新的频率不会过于频繁。有效的后缀包括 **s**、**m**和 **h**，具体参见 Go 时间包。

1.4.6.1. OpenShift SDN 的配置参数

以下 YAML 对象描述了 OpenShift SDN 的配置参数：

```
defaultNetwork:
  type: OpenShiftSDN 1
  openshiftSDNConfig: 2
    mode: NetworkPolicy 3
    mtu: 1450 4
    vxlanPort: 4789 5
```

1 在 **install-config.yaml** 文件中指定。

2 只有您要覆盖部分 OpenShift SDN 配置时才需要指定。

3 配置 **OpenShiftSDN** 的网络隔离模式。允许的值有 **Multitenant**、**Subnet** 或 **NetworkPolicy**。默认值为 **NetworkPolicy**。

4 用于 VXLAN 覆盖网络的 MTU。这个值通常是自动配置的；但是，如果集群中的节点没有全部使用相同的 MTU，那么您必须将此值明确设置为比最小节点 MTU 的值小 50。

5 用于所有 VXLAN 数据包的端口。默认值为 **4789**。如果您在虚拟环境中运行，并且现有节点是另一个 VXLAN 网络的一部分，那么可能需要更改此值。例如，当在 VMware NSX-T 上运行 OpenShift SDN 覆盖时，您必须为 VXLAN 选择一个备用端口，因为两个 SDN 都使用相同的默认 VXLAN 端口号。

在 Amazon Web Services (AWS) 上，您可以在端口 **9000** 和端口 **9999** 之间为 VXLAN 选择一个备用端口。

1.4.6.2. Open Virtual Network (OVN) SDN 的配置参数

OVN SDN 在 OpenShift Container Platform 4.2 中没有任何配置参数。

1.4.6.3. Cluster Network Operator 示例 CR

下例中显示了 CNO 的完整 CR：

Cluster Network Operator 示例 CR

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  serviceNetwork:
  - 172.30.0.0/16
  defaultNetwork:
    type: OpenShiftSDN
    openshiftSDNConfig:
      mode: NetworkPolicy
      mtu: 1450
      vxlanPort: 4789
  kubeProxyConfig:
    iptablesSyncPeriod: 30s
    proxyArguments:
      iptables-min-sync-period:
      - 30s
```

1.4.7. 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

- 配置托管集群的云平台的帐户。
- 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
```

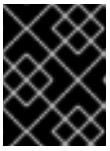
1 对于 **<installation_directory>**，请指定自定义 **./install-config.yaml** 文件的位置。

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。

1.4.8. 安装 CLI

为了可以使用命令行界面与 OpenShift Container Platform 进行交互，您需要安装 CLI。

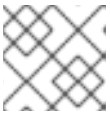
重要

如果安装了旧版本的 **oc**，则无法使用 OpenShift Container Platform 4.2 中的所有命令。下载并安装新版本的 **oc**。

流程

1. 在 Red Hat OpenShift Cluster Manager 站点的 Infrastructure Provider 页面中导航至您的安装类型页面，并点击 **Download Command-line Tools**。

2. 点您的操作系统和系统架构的文件夹，然后点压缩文件。



注意

您可在 Linux 、Windows 或 macOS 上安装 **oc**。

3. 将文件保存到文件系统。
4. 展开压缩文件。
5. 把它放到 **PATH** 中的一个目录下。

安装 CLI 后，就可以使用**oc**命令：

```
$ oc <command>
```

1.4.9. 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
```

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。

1.5. 在 AZURE 上卸载集群

您可以删除部署到 Microsoft Azure 的集群。

1.5.1. 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。