OpenShift Container Platform 4.14

在 Alibaba 上安装

在 Alibaba Cloud 上安装 OpenShift Container Platform

Last Updated: 2025-12-08

OpenShift Container Platform 4.14 在 Alibaba 上安装

在 Alibaba Cloud 上安装 OpenShift Container Platform

Legal Notice

Abstract

本文档论述了如何在 Alibaba Cloud 上安装 OpenShift Container Platform。

Table of Contents

第 1 章 准备在 ALIBABA CLOUD 上安装

重要

OpenShift Container Platform 上的 Alibaba Cloud 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。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。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

1.1. 先决条件

- 您可以参阅有关 OpenShift Container Platform 安装和更新 流程的详细信息。
- 您可以阅读选择集群安装方法并为用户准备它的文档。

1.2. 在 ALIBABA CLOUD 上安装 OPENSHIFT CONTAINER PLATFORM 的要求

在 Alibaba Cloud 上安装 OpenShift Container Platform 前，您必须配置并注册您的域，为安装创建 Resource Access Management(RAM)用户，并查看支持的 Alibaba Cloud 数据中心区域和区。

1.3. 注册和配置 ALIBABA CLOUD 域

要安装 OpenShift Container Platform，您使用的 Alibaba Cloud 帐户必须在帐户中有一个专用的公共托管区。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 Alibaba Cloud 或其他来源获取新的域和注册商。

注意

如果您通过 Alibaba Cloud 购买了一个新域，则需要时间来传播相关的 DNS 更改。有关通过 Alibaba Cloud 购买域的更多信息，请参阅 Alibaba Cloud 域。

2. 如果您使用现有的域和注册商，请将其 DNS 迁移到 Alibaba Cloud。请参阅 Alibaba Cloud 文档中的 域名传输 部分。
3. 为您的域配置 DNS。这包括：
   - 注册通用域名。
   - 为您的域名完成实际的验证。
   - 为互联网内容提供程序(ICP)填充应用.
   - 启用域名解析.
     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托记录添加到父域中。

1.4. 支持的 ALIBABA 区域

您可以将 OpenShift Container Platform 集群部署到 Alibaba *Regions and zones* 文档中列出的区域。

1.5. 后续步骤

- 创建所需的 Alibaba 云资源。

第 2 章 创建所需的 ALIBABA 云资源

在安装 OpenShift Container Platform 前，您必须使用 Alibaba Cloud 控制台创建一个资源访问管理(RAM)用户，该用户有足够的权限将 OpenShift Container Platform 安装到 Alibaba Cloud 中。此用户还必须具有创建新 RAM 用户的权限。您还可以配置和使用 **ccoctl** 工具为 OpenShift Container Platform 组件创建新凭证，及其所需的权限。

重要

OpenShift Container Platform 上的 Alibaba Cloud 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。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。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

2.1. 创建所需的 RAM 用户

您必须有一个 Alibaba Cloud Resource Access Management(RAM)用户才能进行安装具有足够权限。您可以使用 Alibaba Cloud Resource Access Management 控制台来创建新用户或修改现有用户。之后，您可以根据用户的权限在 OpenShift Container Platform 中创建凭证。

当您配置 RAM 用户时，请确定考虑以下要求：

- 用户必须具有 Alibaba Cloud AccessKey ID 和 AccessKey secret 对。
  - 对于新用户，您可以在创建用户时为 Access Mode 选择 **Open API Access**。这个模式会生成所需的 AccessKey 对。
  - 对于现有用户，您可以添加 AccessKey 对，或者您可以获取该用户的 AccessKey 对。

注意

创建后，AccessKey secret 仅显示一次。您必须立即保存 AccessKey 对，因为 API 调用需要 accessKey 对。

- 将 AccessKey ID 和 secret 添加到本地计算机上的 **~/.alibabacloud/credentials** 文件中。在登录到控制台时，Alibaba Cloud 会自动创建此文件。Cloud Credential Operator(CCO)实用程序 ccoutil 在处理凭证**请求对象**时使用这些凭证。
  例如：

```
[default]                    # Default client
type = access_key            # Certification type: access_key
access_key_id = LTAI5t8cefXKmt          # Key (1)
access_key_secret = wYx56mszAN4Uunfh    # Secret
```

(1) 在这里添加您的 AccessKeyID 和 AccessKeySecret。

- RAM 用户必须具有 **AdministratorAccess** 策略，以确保帐户有充足的权限来创建 OpenShift Container Platform 集群。此策略授予管理所有 Alibaba Cloud 资源的权限。
  将 **AdministratorAccess** 策略附加到 RAM 用户时，您可以授予用户对所有 Alibaba Cloud 服务和资源的完整访问权限。如果您不想创建具有完全访问权限的用户，请创建自定义策略，使其包含可添加到 RAM 用户以进行安装的以下操作。这些操作足以安装 OpenShift Container

Platform。

提示

您可以将以下 JSON 代码复制并粘贴到 Alibaba Cloud 控制台中，以创建自定义策略。有关创建自定义策略的详情，请参考 Alibaba Cloud 文档中的创建自定义策略。

例 2.1. 自定义策略 JSON 文件示例

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "tag:ListTagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DeleteVpc",
        "vpc:DescribeVSwitches",
        "vpc:DeleteVSwitch",
        "vpc:DescribeEipAddresses",
        "vpc:DescribeNatGateways",
        "vpc:ReleaseEipAddress",
        "vpc:DeleteNatGateway",
        "vpc:DescribeSnatTableEntries",
        "vpc:CreateSnatEntry",
        "vpc:AssociateEipAddress",
        "vpc:ListTagResources",
        "vpc:TagResources",
        "vpc:DescribeVSwitchAttributes",
        "vpc:CreateVSwitch",
        "vpc:CreateNatGateway",
        "vpc:DescribeRouteTableList",
        "vpc:CreateVpc",
        "vpc:AllocateEipAddress",
        "vpc:ListEnhanhcedNatGatewayAvailableZones"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:ModifyInstanceAttribute",
        "ecs:DescribeSecurityGroups",
        "ecs:DeleteSecurityGroup",
        "ecs:DescribeSecurityGroupReferences",
        "ecs:DescribeSecurityGroupAttribute",
        "ecs:RevokeSecurityGroup",
        "ecs:DescribeInstances",
```

```
        "ecs:DeleteInstances",
        "ecs:DescribeNetworkInterfaces",
        "ecs:DescribeInstanceRamRole",
        "ecs:DescribeUserData",
        "ecs:DescribeDisks",
        "ecs:ListTagResources",
        "ecs:AuthorizeSecurityGroup",
        "ecs:RunInstances",
        "ecs:TagResources",
        "ecs:ModifySecurityGroupPolicy",
        "ecs:CreateSecurityGroup",
        "ecs:DescribeAvailableResource",
        "ecs:DescribeRegions",
        "ecs:AttachInstanceRamRole"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "pvtz:DescribeRegions",
        "pvtz:DescribeZones",
        "pvtz:DeleteZone",
        "pvtz:DeleteZoneRecord",
        "pvtz:BindZoneVpc",
        "pvtz:DescribeZoneRecords",
        "pvtz:AddZoneRecord",
        "pvtz:SetZoneRecordStatus",
        "pvtz:DescribeZoneInfo",
        "pvtz:DescribeSyncEcsHostTask",
        "pvtz:AddZone"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "slb:DescribeLoadBalancers",
        "slb:SetLoadBalancerDeleteProtection",
        "slb:DeleteLoadBalancer",
        "slb:SetLoadBalancerModificationProtection",
        "slb:DescribeLoadBalancerAttribute",
        "slb:AddBackendServers",
        "slb:DescribeLoadBalancerTCPListenerAttribute",
        "slb:SetLoadBalancerTCPListenerAttribute",
        "slb:StartLoadBalancerListener",
        "slb:CreateLoadBalancerTCPListener",
        "slb:ListTagResources",
        "slb:TagResources",
        "slb:CreateLoadBalancer"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
```

```
      "ram:ListResourceGroups",
      "ram:DeleteResourceGroup",
      "ram:ListPolicyAttachments",
      "ram:DetachPolicy",
      "ram:GetResourceGroup",
      "ram:CreateResourceGroup",
      "ram:DeleteRole",
      "ram:GetPolicy",
      "ram:DeletePolicy",
      "ram:ListPoliciesForRole",
      "ram:CreateRole",
      "ram:AttachPolicyToRole",
      "ram:GetRole",
      "ram:CreatePolicy",
      "ram:CreateUser",
      "ram:DetachPolicyFromRole",
      "ram:CreatePolicyVersion",
      "ram:DetachPolicyFromUser",
      "ram:ListPoliciesForUser",
      "ram:AttachPolicyToUser",
      "ram:CreateUser",
      "ram:GetUser",
      "ram:DeleteUser",
      "ram:CreateAccessKey",
      "ram:ListAccessKeys",
      "ram:DeleteAccessKey",
      "ram:ListUsers",
      "ram:ListPolicyVersions"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "oss:DeleteBucket",
      "oss:DeleteBucketTagging",
      "oss:GetBucketTagging",
      "oss:GetBucketCors",
      "oss:GetBucketPolicy",
      "oss:GetBucketLifecycle",
      "oss:GetBucketReferer",
      "oss:GetBucketTransferAcceleration",
      "oss:GetBucketLog",
      "oss:GetBucketWebSite",
      "oss:GetBucketInfo",
      "oss:PutBucketTagging",
      "oss:PutBucket",
      "oss:OpenOssService",
      "oss:ListBuckets",
      "oss:GetService",
      "oss:PutBucketACL",
      "oss:GetBucketLogging",
      "oss:ListObjects",
      "oss:GetObject",
      "oss:PutObject",
      "oss:DeleteObject"
```

```
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "alidns:DescribeDomainRecords",
        "alidns:DeleteDomainRecord",
        "alidns:DescribeDomains",
        "alidns:DescribeDomainRecordInfo",
        "alidns:AddDomainRecord",
        "alidns:SetDomainRecordStatus"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "bssapi:CreateInstance",
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:PassRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "acs:Service": "ecs.aliyuncs.com"
        }
      }
    }
  ]
}
```


有关创建 RAM 用户和授予权限的更多信息，请参阅 Alibaba Cloud 文档中的 创建 RAM 用户 和 Grant 权限。

2.2. 配置 CLOUD CREDENTIAL OPERATOR 工具

要分配为每个集群组件提供长期 RAM 访问密钥(AK)的 RAM 用户和策略，请提取并准备 Cloud Credential Operator (CCO) 实用程序 (**ccoctl**) 二进制文件。

注意

ccoctl 工具是在 Linux 环境中运行的 Linux 二进制文件。

先决条件

- 您可以访问具有集群管理员权限的 OpenShift Container Platform 帐户。
- 已安装 OpenShift CLI(**oc**)。

流程

1. 运行以下命令，为 OpenShift Container Platform 发行镜像设置变量：

```
$ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
```

2. 运行以下命令，从 OpenShift Container Platform 发行镜像获取 CCO 容器镜像：

```
$ CCO_IMAGE=$(oc adm release info --image-for='cloud-credential-operator'
$RELEASE_IMAGE -a ~/.pull-secret)
```

注意

确保 **$RELEASE_IMAGE** 的架构与将使用 **ccoctl** 工具的环境架构相匹配。

3. 运行以下命令，将 CCO 容器镜像中的 **ccoctl** 二进制文件提取到 OpenShift Container Platform 发行镜像中：

```
$ oc image extract $CCO_IMAGE --file="/usr/bin/ccoctl" -a ~/.pull-secret
```

4. 运行以下命令更改权限以使 **ccoctl** 可执行：

```
$ chmod 775 ccoctl
```

验证

- 要验证 **ccoctl** 是否准备就绪，可以尝试显示帮助文件。运行命令时使用相对文件名，例如：

```
$ ./ccoctl.rhel9
```

输出示例

```
OpenShift credentials provisioning tool

Usage:
  ccoctl [command]

Available Commands:
  alibabacloud Manage credentials objects for alibaba cloud
  aws          Manage credentials objects for AWS cloud
  azure        Manage credentials objects for Azure
  gcp          Manage credentials objects for Google cloud
  help         Help about any command
  ibmcloud     Manage credentials objects for IBM Cloud
  nutanix      Manage credentials objects for Nutanix

Flags:
  -h, --help   help for ccoctl

Use "ccoctl [command] --help" for more information about a command.
```

其他资源

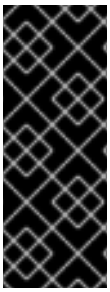
- 准备使用手动维护的凭证更新集群

2.3. 后续步骤

- 您可以使用以下方法之一在 OpenShift Container Platform 安装程序置备的 Alibaba Cloud 基础架构上安装集群：
  - **在 Alibaba Cloud 上快速安装集群**：您可以使用默认配置选项快速安装集群。
  - **在 Alibaba Cloud 上安装自定义集群**：安装程序允许在安装阶段应用一些自定义。其它自定义选项可在安装后使用。

第 3 章 在 ALIBABA CLOUD 上快速安装集群

在 OpenShift Container Platform 版本 4.14 中，您可以使用默认配置选项在 Alibaba Cloud 上安装集群。



重要

OpenShift Container Platform 上的 Alibaba Cloud 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。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。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

3.1. 先决条件

- 您可以参阅有关 OpenShift Container Platform 安装和更新 流程的详细信息。
- 您可以阅读选择集群安装方法并为用户准备它的文档。
- 您已注册了域。
- 如果使用防火墙，将其配置为允许集群需要访问的站点。
- 您已创建了所需的 Alibaba 云资源。
- 如果环境中无法访问云资源访问(RAM)API，或者不想将管理员级别的凭证 secret 存储在 kube-system 命名空间中，您可以手动创建和维护资源访问管理(RAM)凭证。

3.2. OPENSHIFT CONTAINER PLATFORM 互联网访问

在 OpenShift Container Platform 4.14 中，您需要访问互联网来安装集群。

您必须具有以下互联网访问权限：

- 访问 OpenShift Cluster Manager 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型的基础架构上执行受限网络安装。在此过程中，您可以下载所需的内容，并使用它为镜像 registry 填充安装软件包。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。在更新集群前，您要更新镜像 registry 的内容。

3.3. 为集群节点 SSH 访问生成密钥对

在 OpenShift Container Platform 安装过程中，您可以为安装程序提供 SSH 公钥。密钥通过它们的 Ignition 配置文件传递给 Red Hat Enterprise Linux CoreOS(RHCOS)节点，用于验证对节点的 SSH 访问。密钥添加到每个节点上 **core** 用户的 **~/.ssh/authorized_keys** 列表中，这将启用免密码身份验证。

将密钥传递给节点后，您可以使用密钥对作为用户 **核心** 通过 SSH 连接到 RHCOS 节点。若要通过 SSH 访问节点，必须由 SSH 为您的本地用户管理私钥身份。

如果要通过 SSH 连接到集群节点来执行安装调试或灾难恢复，则必须在安装过程中提供 SSH 公钥。**./openshift-install gather** 命令还需要在集群节点上设置 SSH 公钥。

重要

不要在生产环境中跳过这个过程，在生产环境中需要灾难恢复和调试。

注意

您必须使用本地密钥，而不是使用特定平台方法配置 的密钥，如 AWS 密钥对。

流程

1. 如果您在本地计算机上没有可用于在集群节点上进行身份验证的现有 SSH 密钥对，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 ed25519 -N '' -f <path>/<file_name> 1
```

1 指定新 SSH 密钥的路径和文件名，如 **~/.ssh/id_ed25519**。如果您已有密钥对，请确保您的公钥位于 **~/.ssh** 目录中。

注意

如果您计划在 **x86_64**、**ppc64le** 和 **s390x** 架构上安装使用 RHEL 加密库（这些加密库已提交给 NIST 用于 FIPS 140-2/140-3 验证）的 OpenShift Container Platform 集群，则不要创建使用 **ed25519** 算法的密钥。相反，创建一个使用 **rsa** 或 **ecdsa** 算法的密钥。

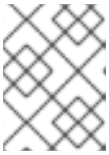
2. 查看公共 SSH 密钥：

```
$ cat <path>/<file_name>.pub
```

例如，运行以下命令来查看 **~/.ssh/id_ed25519.pub** 公钥：

```
$ cat ~/.ssh/id_ed25519.pub
```

3. 将 SSH 私钥身份添加到本地用户的 SSH 代理（如果尚未添加）。在集群节点上，或者要使用 **./openshift-install gather** 命令，需要对该密钥进行 SSH 代理管理，才能在集群节点上进行免密码 SSH 身份验证。



注意

在某些发行版中，自动管理默认 SSH 私钥身份，如 **~/.ssh/id_rsa** 和 **~/.ssh/id_dsa**。

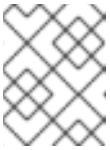
a. 如果 **ssh-agent** 进程尚未为您的本地用户运行，请将其作为后台任务启动：

```
$ eval "$(ssh-agent -s)"
```

-

输出示例

```
Agent pid 31874
```



注意

如果集群处于 FIPS 模式，则只使用 FIPS 兼容算法来生成 SSH 密钥。密钥必须是 RSA 或 ECDSA。

4. 将 SSH 私钥添加到 **ssh-agent** ：

```
$ ssh-add <path>/<file_name> 1
```

1 指定 SSH 私钥的路径和文件名，如 **~/.ssh/id_ed25519.pub**

输出示例

```
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

后续步骤

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

3.4. 获取安装程序

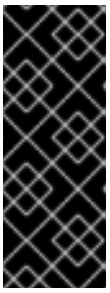
在安装 OpenShift Container Platform 前，将安装文件下载到您用于安装的主机上。

先决条件

- 您有一台运行 Linux 或 macOS 的计算机，至少有 1.2 GB 本地磁盘空间。

流程

1. 进入 Red Hat Hybrid Cloud Console 上的 Cluster Type 页。如果您有红帽帐户，请使用您的凭证登录。如果没有，请创建一个帐户。
2. 在页的 **Run it yourself** 部分中选择您的基础架构供应商。
3. 从 **OpenShift 安装程序**下的下拉菜单中选择您的主机操作系统和架构，然后点**下载安装程序**。
4. 将下载的文件保存在要存储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几个文件。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。删除集群需要这两个文件。
- 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。要删除集群，请为特定云供应商完成 OpenShift Container Platform 卸载流程。

5. 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 openshift-install-linux.tar.gz
```

6. 从 Red Hat OpenShift Cluster Manager 下载安装 pull secret 。此 pull secret 允许您与所含授权机构提供的服务进行身份验证，这些服务包括为 OpenShift Container Platform 组件提供容器镜像的 Quay.io。

提示

另外，您还可以从红帽客户门户网站检索安装程序，您可以在其中指定要下载的安装程序版本。但是，您需要有一个有效的订阅才能访问此页。

3.5. 创建安装配置文件

您可以自定义在 Alibaba Cloud 上安装的 OpenShift Container Platform 集群。

先决条件

- 您有 OpenShift Container Platform 安装程序和集群的 pull secret。

流程

1. 创建 **install-config.yaml** 文件。
   a. 进入包含安装程序的目录并运行以下命令：

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

1 对于 **<installation_directory>**，请指定要存储安装程序创建的文件的目录名称。

在指定目录时：

- 验证该目录是否具有**执行**权限。在安装目录中运行 Terraform 二进制文件需要这个权限。
- 使用空目录。有些安装资产，如 bootstrap X.509 证书的过期间隔较短，因此不得重复使用安装目录。如果要重复使用另一个集群安装中的单个文件，您可以将它们复制到您的目录中。但是，安装资产的文件名可能会在发行版本间有所变化。从以前的 OpenShift Container Platform 版本中复制安装文件时请小心。

注意

始终删除 **~/.powervs** 目录，以避免重复使用过时的配置。运行以下命令:

```
$ rm -rf ~/.powervs
```

   b. 在提示符处，提供云的配置详情：
      i. 可选： 选择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。

ii. 选择 **alibabacloud** 作为目标平台。

iii. 选择要将集群部署到的区域。

iv. 选择集群要部署到的基域。基域与您为集群创建的公共 DNS 区对应。

v. 为集群提供一个描述性名称。

2. 将集群安装到 Alibaba Cloud 中需要 Cloud Credential Operator(CCO)以手动模式运行。修改 **install-config.yaml** 文件，将 **credentialsMode** 参数设置为 **Manual** ：

带有 credentialsMode 被设置为 Manual 的 install-config.yaml 配置文件示例

```
apiVersion: v1
baseDomain: cluster1.example.com
credentialsMode: Manual 1
compute:
- architecture: amd64
  hyperthreading: Enabled
...
```

1 添加此行，将 **credentialsMode** 设置为 **Manual**。

3. 备份 **install-config.yaml** 文件，以便您可以使用它安装多个集群。

重要

install-config.yaml 文件会在安装过程中消耗掉。如果要重复使用该文件，您必须立即备份该文件。

3.6. 生成所需的安装清单

您必须生成 Kubernetes 清单和 Ignition 配置文件，集群需要配置机器。

流程

1. 从包含安装程序的目录中运行以下命令来生成清单：

```
$ openshift-install create manifests --dir <installation_directory>
```

其中：

<installation_directory>

指定安装程序在其中创建文件的目录。

3.7. 使用 CCOCTL 工具为 OPENSHIFT CONTAINER PLATFORM 组件创建凭证

您可以使用 OpenShift Container Platform Cloud Credential Operator(CCO)实用程序自动为每个集群组件创建 Alibaba Cloud RAM 用户和策略。

注意

默认情况下，**ccoctl** 在运行命令的目录中创建对象。要在其他目录中创建对象，请使用 **--output-dir** 标志。此流程使用 **<path_to_ccoctl_output_dir>** 来引用这个目录。

先决条件

您必须：

- 提取并准备好 **ccoctl** 二进制文件。
- 创建具有足够权限来创建 OpenShift Container Platform 集群的 RAM 用户。
- 将 RAM 用户的 AccessKeyID(**access_key_id**)和 AccessKeySecret(**access_key_secret**)添加到本地计算机上的 **~/.alibabacloud/credentials** 文件中。

流程

1. 运行以下命令，使用安装文件中的发行镜像设置 **$RELEASE_IMAGE** 变量：

```
$ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
```

2. 运行以下命令，从 OpenShift Container Platform 发行镜像中提取 **CredentialsRequest** 对象列表：

```
$ oc adm release extract \
  --from=$RELEASE_IMAGE \
  --credentials-requests \
  --included \ 1
  --install-config=<path_to_directory_with_installation_configuration>/install-config.yaml \ 2
  --to=<path_to_directory_for_credentials_requests> 3
```

1. **--included** 参数仅包含特定集群配置所需的清单。
2. 指定 **install-config.yaml** 文件的位置。
3. 指定要存储 **CredentialsRequest** 对象的目录的路径。如果指定的目录不存在，这个命令会创建它。

注意

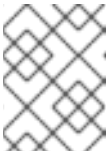
此命令可能需要一些时间才能运行。

3. 运行以下命令，使用 **ccoctl** 工具处理所有 **CredentialsRequest** 对象：

   a. 运行以下命令使用该工具：

```
$ ccoctl alibabacloud create-ram-users \
  --name <name> \1
  --region=<alibaba_region> \2
  --credentials-requests-dir=<path_to_credentials_requests_directory> \3
  --output-dir=<path_to_ccoctl_output_dir> 4
```

1. 指定用于标记创建用于跟踪的任何云资源的名称。
2. 指定在其中创建云资源的 Alibaba Cloud 区域。
3. 指定包含组件 **CredentialsRequest** 对象文件的目录。
4. 指定要放置生成组件凭证 secret 的目录。

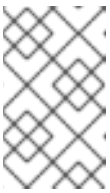


注意

如果您的集群使用 **TechPreviewNoUpgrade** 功能集启用的技术预览功能，则必须包含 **--enable-tech-preview** 参数。

输出示例

```
2022/02/11 16:18:26 Created RAM User: user1-alicloud-openshift-machine-api-alibabacloud-credentials
2022/02/11 16:18:27 Ready for creating new ram policy user1-alicloud-openshift-machine-api-alibabacloud-credentials-policy-policy
2022/02/11 16:18:27 RAM policy user1-alicloud-openshift-machine-api-alibabacloud-credentials-policy-policy has created
2022/02/11 16:18:28 Policy user1-alicloud-openshift-machine-api-alibabacloud-credentials-policy-policy has attached on user user1-alicloud-openshift-machine-api-alibabacloud-credentials
2022/02/11 16:18:29 Created access keys for RAM User: user1-alicloud-openshift-machine-api-alibabacloud-credentials
2022/02/11 16:18:29 Saved credentials configuration to: user1-alicloud/manifests/openshift-machine-api-alibabacloud-credentials-credentials.yaml
...
```



注意

RAM 用户可以同时具有两个 accessKeys。如果您运行 **ccoctl alibabacloud create-ram-users** 两次，则之前生成的 manifests secret 将变为过时，您必须重新应用新生成的 secret。

b. 验证 OpenShift Container Platform secret 是否已创建：

```
$ ls <path_to_ccoctl_output_dir>/manifests
```

输出示例

```
openshift-cluster-csi-drivers-alibaba-disk-credentials-credentials.yaml
openshift-image-registry-installer-cloud-credentials-credentials.yaml
openshift-ingress-operator-cloud-credentials-credentials.yaml
```

```
openshift-machine-api-alibabacloud-credentials-credentials.yaml
```

您可以通过查询 Alibaba Cloud 来验证是否创建了 RAM 用户和策略。如需更多信息，请参阅 Alibaba Cloud 文档中有关列出 RAM 用户和策略的内容。

4. 将生成的凭证文件复制到目标清单目录中：

```
$ cp ./<path_to_ccoctl_output_dir>/manifests/*credentials.yaml
./<path_to_installation>dir>/manifests/
```

其中：

<path_to_ccoctl_output_dir>

指定 **ccoctl alibabacloud create-ram-users** 命令创建的目录。

<path_to_installation_dir>

指定安装程序在其中创建文件的目录。

3.8. 部署集群

您可以在兼容云平台上安装 OpenShift Container Platform。

重要

在初始安装过程中，您只能运行安装程序的 **create cluster** 命令一次。

先决条件

- 您已使用托管集群的云平台配置了帐户。
- 您有 OpenShift Container Platform 安装程序和集群的 pull secret。
- 已确认主机上的云供应商帐户具有部署集群的正确权限。权限不正确的帐户会导致安装过程失败，并显示包括缺失权限的错误消息。

流程

- 进入包含安装程序的目录并初始化集群部署：

```
$ ./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**，而不是 **info**。

验证

当集群部署成功完成时：

- 终端会显示用于访问集群的说明，包括指向 Web 控制台和 **kubeadmin** 用户的凭证的链接。
- 凭证信息还会输出到 **<installation_directory>/.openshift_install.log**.

重要

不要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。

输出示例

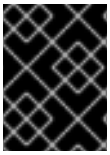
```
...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/home/myuser/install_dir/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-
console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password: "password"
INFO Time elapsed: 36m22s
```

重要

- 安装程序生成的 Ignition 配置文件包含在 24 小时后过期的证书，然后在过期时进行续订。如果在更新证书前关闭集群，且集群在 24 小时后重启，集群会自动恢复过期的证书。一个例外是，您必须手动批准待处理的 **node-bootstrapper** 证书签名请求(CSR)来恢复 kubelet 证书。如需更多信息，*请参阅从过期的 control plane 证书* 中恢复的文档。
- 建议您在 Ignition 配置文件生成后的 12 小时内使用它们，因为 24 小时的证书会在集群安装后的 16 小时到 22 小时间进行轮转。通过在 12 小时内使用 Ignition 配置文件，您可以避免在安装过程中因为执行了证书更新而导致安装失败的问题。

3.9. 通过下载二进制文件安装 OPENSHIFT CLI

您可以安装 OpenShift CLI(**oc**)来使用命令行界面与 OpenShift Container Platform 进行交互。您可以在 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 4.14 中的所有命令。下载并安装新版本的 **oc**。

在 Linux 上安装 OpenShift 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. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **产品变体** 下拉列表中选择架构。
3. 从 **版本** 下拉列表中选择适当的版本。
4. 点 **OpenShift v4.14 Linux Client** 条目旁的 **Download Now** 来保存文件。
5. 解包存档：

```
$ tar xvf <file>
```

6. 将 **oc** 二进制文件放到 **PATH 中的目录中**。
   要查看您的 **PATH**，请执行以下命令：

```
$ echo $PATH
```

验证

- 安装 OpenShift CLI 后，可以使用 **oc** 命令：

```
$ oc <command>
```

在 Windows 上安装 OpenShift CLI

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

流程

1. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **版本** 下拉列表中选择适当的版本。
3. 点 **OpenShift v4.14 Windows Client** 条目旁的 **Download Now** 来保存文件。
4. 使用 ZIP 程序解压存档。
5. 将 **oc** 二进制文件移到 **PATH 中的目录中**。
   要查看您的 **PATH**，请打开命令提示并执行以下命令：

```
C:\> path
```

验证

- 安装 OpenShift CLI 后，可以使用 **oc** 命令：

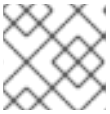
```
C:\> oc <command>
```

在 macOS 上安装 OpenShift CLI

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

流程

1. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **版本** 下拉列表中选择适当的版本。
3. 点 **OpenShift v4.14 macOS Client** 条目旁的 **Download Now** 来保存文件。



注意

对于 macOS arm64，请选择 **OpenShift v4.14 macOS arm64 Client** 条目。

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**，请打开终端并执行以下命令：

```
$ echo $PATH
```

验证

- 使用 **oc** 命令验证安装：

```
$ oc <command>
```

3.10. 使用 CLI 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** 文件包含有关集群的信息，供 CLI 用于将客户端连接到正确的集群和 API 服务器。该文件特定于集群，在 OpenShift Container Platform 安装过程中创建。

先决条件

- 已部署 OpenShift Container Platform 集群。
- 已安装 **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. 验证您可以使用导出的配置成功运行 **oc** 命令：

```
$ oc whoami
```

输出示例

```
system:admin
```

/validating-an-installation.adoc

3.11. 使用 WEB 控制台登录到集群

kubeadmin 用户默认在 OpenShift Container Platform 安装后存在。您可以使用 OpenShift Container Platform Web 控制台以 **kubeadmin** 用户身份登录集群。

先决条件

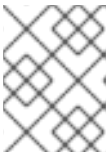
- 有访问安装主机的访问权限。

- 您完成了集群安装，所有集群 Operator 都可用。

流程

1. 从安装主机上的 **kubeadmin -password** 文件中获取 kubeadmin 用户的密码：

```
$ cat <installation_directory>/auth/kubeadmin-password
```

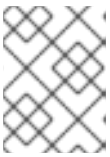


注意

另外，您还可以从安装主机上的 **<installation_directory>/.openshift_install.log** 日志文件获取 **kubeadmin** 密码。

2. 列出 OpenShift Container Platform Web 控制台路由：

```
$ oc get routes -n openshift-console | grep 'console-openshift'
```



注意

另外，您还可以从安装主机上的 **<installation_directory>/.openshift_install.log 日志** 文件获取 OpenShift Container Platform 路由。

输出示例

```
console     console-openshift-console.apps.<cluster_name>.<base_domain>          console
https   reencrypt/Redirect   None
```

3. 在 Web 浏览器中导航到上一命令输出中包括的路由，以 **kubeadmin** 用户身份登录。

3.12. OPENSHIFT CONTAINER PLATFORM 的 TELEMETRY 访问

在 OpenShift Container Platform 4.14 中，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，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 OpenShift Cluster Manager。

确认 OpenShift Cluster Manager 清单正确后，可以由 Telemetry 自动维护，也可以使用 OpenShift Cluster Manager 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。

其他资源

- 如需有关 访问和了解 OpenShift Container Platform Web 控制台的更多详情，请参阅 访问 Web 控制台。
- 有关 Telemetry 服务的更多信息，请参阅关于 远程健康监控

3.13. 后续步骤

- 验证安装.
- 自定义集群。

- 如果需要，您可以选择不使用远程健康报告。

第 4 章 使用自定义在 ALIBABA CLOUD 上安装集群

在 OpenShift Container Platform 版本 4.14 中，您可以在安装程序在 Alibaba Cloud 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。

注意

OpenShift Container Platform 安装配置的作用范围被特意设计为较小。它旨在简化操作并确保成功。在安装完成后，您可以进行更多的 OpenShift Container Platform 配置任务。

重要

OpenShift Container Platform 上的 Alibaba Cloud 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。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。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

4.1. 先决条件

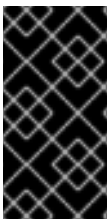
- 您可以参阅有关 OpenShift Container Platform 安装和更新 流程的详细信息。
- 您可以阅读选择集群安装方法并为用户准备它的文档。
- 您已注册了域。
- 如果使用防火墙，将其配置为允许集群需要访问的站点。
- 如果您的环境无法访问云的资源访问管理(RAM)API，或者不想将管理员级别的凭证 secret 存储在 **kube-system** 命名空间中，您可以手动创建和维护资源访问管理(RAM)凭证。

4.2. OPENSHIFT CONTAINER PLATFORM 互联网访问

在 OpenShift Container Platform 4.14 中，您需要访问互联网来安装集群。

您必须具有以下互联网访问权限：

- 访问 OpenShift Cluster Manager 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型的基础架构上执行受限网络安装。在此过程中，您可以下载所需的内容，并使用它为镜像 registry 填充安装软件包。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。在更新集群前，您要更新镜像 registry 的内容。

4.3. 为集群节点 SSH 访问生成密钥对

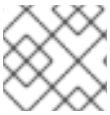
在 OpenShift Container Platform 安装过程中，您可以为安装程序提供 SSH 公钥。密钥通过它们的 Ignition 配置文件传递给 Red Hat Enterprise Linux CoreOS(RHCOS)节点，用于验证对节点的 SSH 访问。密钥添加到每个节点上 **core** 用户的 **~/.ssh/authorized_keys** 列表中，这将启用免密码身份验证。

将密钥传递给节点后，您可以使用密钥对作为用户 **核心** 通过 SSH 连接到 RHCOS 节点。若要通过 SSH 访问节点，必须由 SSH 为您的本地用户管理私钥身份。

如果要通过 SSH 连接到集群节点来执行安装调试或灾难恢复，则必须在安装过程中提供 SSH 公钥。**./openshift-install gather** 命令还需要在集群节点上设置 SSH 公钥。

重要

不要在生产环境中跳过这个过程，在生产环境中需要灾难恢复和调试。



注意

您必须使用本地密钥，而不是使用特定平台方法配置 的密钥，如 AWS 密钥对。

流程

1. 如果您在本地计算机上没有可用于在集群节点上进行身份验证的现有 SSH 密钥对，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 ed25519 -N '' -f <path>/<file_name> 1
```

1 指定新 SSH 密钥的路径和文件名，如 **~/.ssh/id_ed25519**。如果您已有密钥对，请确保您的公钥位于 **~/.ssh** 目录中。

注意

如果您计划在 **x86_64**、**ppc64le** 和 **s390x** 架构上安装使用 RHEL 加密库（这些加密库已提交给 NIST 用于 FIPS 140-2/140-3 验证）的 OpenShift Container Platform 集群，则不要创建使用 **ed25519** 算法的密钥。相反，创建一个使用 **rsa** 或 **ecdsa** 算法的密钥。

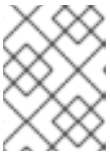
2. 查看公共 SSH 密钥：

```
$ cat <path>/<file_name>.pub
```

例如，运行以下命令来查看 **~/.ssh/id_ed25519.pub** 公钥：

```
$ cat ~/.ssh/id_ed25519.pub
```

3. 将 SSH 私钥身份添加到本地用户的 SSH 代理（如果尚未添加）。在集群节点上，或者要使用 **./openshift-install gather** 命令，需要对该密钥进行 SSH 代理管理，才能在集群节点上进行免密码 SSH 身份验证。



注意

在某些发行版中，自动管理默认 SSH 私钥身份，如 **~/.ssh/id_rsa** 和 **~/.ssh/id_dsa**。

a. 如果 **ssh-agent** 进程尚未为您的本地用户运行，请将其作为后台任务启动：

```
$ eval "$(ssh-agent -s)"
```

输出示例

```
Agent pid 31874
```

注意

如果集群处于 FIPS 模式，则只使用 FIPS 兼容算法来生成 SSH 密钥。密钥必须是 RSA 或 ECDSA。

4. 将 SSH 私钥添加到 **ssh-agent** ：

```
$ ssh-add <path>/<file_name> 1
```

1 指定 SSH 私钥的路径和文件名，如 **~/.ssh/id_ed25519.pub**

输出示例

```
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

后续步骤

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

4.4. 获取安装程序

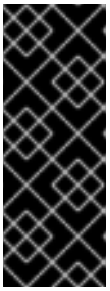
在安装 OpenShift Container Platform 前，将安装文件下载到您用于安装的主机上。

先决条件

- 您有一台运行 Linux 或 macOS 的计算机，至少有 1.2 GB 本地磁盘空间。

流程

1. 进入 Red Hat Hybrid Cloud Console 上的 Cluster Type 页。如果您有红帽帐户，请使用您的凭证登录。如果没有，请创建一个帐户。
2. 在页的 **Run it yourself** 部分中选择您的基础架构供应商。
3. 从 **OpenShift 安装程序**下的下拉菜单中选择您的主机操作系统和架构，然后点**下载安装程序**。
4. 将下载的文件保存在要存储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几个文件。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。删除集群需要这两个文件。
- 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。要删除集群，请为特定云供应商完成 OpenShift Container Platform 卸载流程。

5. 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 openshift-install-linux.tar.gz
```

6. 从 Red Hat OpenShift Cluster Manager 下载安装 pull secret 。此 pull secret 允许您与所含授权机构提供的服务进行身份验证，这些服务包括为 OpenShift Container Platform 组件提供容器镜像的 Quay.io。

提示

另外，您还可以从红帽客户门户网站检索安装程序，您可以在其中指定要下载的安装程序版本。但是，您需要有一个有效的订阅才能访问此页。

4.4.1. 创建安装配置文件

您可以自定义在 Alibaba Cloud 上安装的 OpenShift Container Platform 集群。

先决条件

- 您有 OpenShift Container Platform 安装程序和集群的 pull secret。

流程

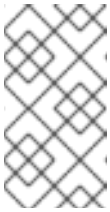
1. 创建 **install-config.yaml** 文件。
   a. 进入包含安装程序的目录并运行以下命令：

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

1 对于 **<installation_directory>**，请指定要存储安装程序创建的文件的目录名称。

在指定目录时：

- 验证该目录是否具有**执行**权限。在安装目录中运行 Terraform 二进制文件需要这个权限。
- 使用空目录。有些安装资产，如 bootstrap X.509 证书的过期间隔较短，因此不得重复使用安装目录。如果要重复使用另一个集群安装中的单个文件，您可以将它们复制到您的目录中。但是，安装资产的文件名可能会在发行版本间有所变化。从以前的 OpenShift Container Platform 版本中复制安装文件时请小心。



注意

始终删除 ~/**.powervs** 目录，以避免重复使用过时的配置。运行以下命令:

```
$ rm -rf ~/.powervs
```

b. 在提示符处，提供云的配置详情：

i. 可选： 选择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。

ii. 选择 **alibabacloud** 作为目标平台。

iii. 选择要将集群部署到的区域。

iv. 选择集群要部署到的基域。基域与您为集群创建的公共 DNS 区对应。

v. 为集群提供一个描述性名称。

2. 将集群安装到 Alibaba Cloud 中需要 Cloud Credential Operator(CCO)以手动模式运行。修改 **install-config.yaml** 文件，将 **credentialsMode** 参数设置为 **Manual** ：

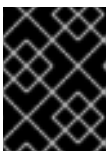
带有 credentialsMode 被设置为 Manual 的 install-config.yaml 配置文件示例

```
apiVersion: v1
baseDomain: cluster1.example.com
credentialsMode: Manual 1
compute:
- architecture: amd64
  hyperthreading: Enabled
 ...
```

1 添加此行，将 **credentialsMode** 设置为 **Manual**。

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

4. 备份 **install-config.yaml** 文件，以便您可以使用它安装多个集群。



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。

其他资源

- Alibaba Cloud 的安装配置参数

4.4.2. 生成所需的安装清单

您必须生成 Kubernetes 清单和 Ignition 配置文件，集群需要配置机器。

流程

1. 从包含安装程序的目录中运行以下命令来生成清单：

```
$ openshift-install create manifests --dir <installation_directory>
```

其中：

<installation_directory>

指定安装程序在其中创建文件的目录。

4.4.3. 使用 ccoctl 工具为 OpenShift Container Platform 组件创建凭证

您可以使用 OpenShift Container Platform Cloud Credential Operator(CCO)实用程序自动为每个集群组件创建 Alibaba Cloud RAM 用户和策略。

注意

默认情况下，**ccoctl** 在运行命令的目录中创建对象。要在其他目录中创建对象，请使用 **--output-dir** 标志。此流程使用 **<path_to_ccoctl_output_dir>** 来引用这个目录。

先决条件

您必须：

- 提取并准备好 **ccoctl** 二进制文件。
- 创建具有足够权限来创建 OpenShift Container Platform 集群的 RAM 用户。
- 将 RAM 用户的 AccessKeyID(**access_key_id**)和 AccessKeySecret(**access_key_secret**)添加到本地计算机上的 **~/.alibabacloud/credentials** 文件中。

流程

1. 运行以下命令，使用安装文件中的发行镜像设置 **$RELEASE_IMAGE** 变量：

```
$ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
```

2. 运行以下命令，从 OpenShift Container Platform 发行镜像中提取 **CredentialsRequest** 对象列表：

```
$ oc adm release extract \
  --from=$RELEASE_IMAGE \
  --credentials-requests \
  --included \ 1
  --install-config=<path_to_directory_with_installation_configuration>/install-config.yaml \ 2
  --to=<path_to_directory_for_credentials_requests> 3
```

1. **--included** 参数仅包含特定集群配置所需的清单。
2. 指定 **install-config.yaml** 文件的位置。

3 指定要存储 **CredentialsRequest** 对象的目录的路径。如果指定的目录不存在，这个命令会创建它。

注意

此命令可能需要一些时间才能运行。

3. 运行以下命令，使用 **ccoctl** 工具处理所有 **CredentialsRequest** 对象：

   a. 运行以下命令使用该工具：

```
$ ccoctl alibabacloud create-ram-users \
  --name <name> \1
  --region=<alibaba_region> \2
  --credentials-requests-dir=<path_to_credentials_requests_directory> \3
  --output-dir=<path_to_ccoctl_output_dir> 4
```

1 指定用于标记创建用于跟踪的任何云资源的名称。

2 指定在其中创建云资源的 Alibaba Cloud 区域。

3 指定包含组件 **CredentialsRequest** 对象文件的目录。

4 指定要放置生成组件凭证 secret 的目录。

注意

如果您的集群使用 **TechPreviewNoUpgrade** 功能集启用的技术预览功能，则必须包含 **--enable-tech-preview** 参数。

输出示例

```
2022/02/11 16:18:26 Created RAM User: user1-alicloud-openshift-machine-api-alibabacloud-credentials
2022/02/11 16:18:27 Ready for creating new ram policy user1-alicloud-openshift-machine-api-alibabacloud-credentials-policy-policy
2022/02/11 16:18:27 RAM policy user1-alicloud-openshift-machine-api-alibabacloud-credentials-policy-policy has created
2022/02/11 16:18:28 Policy user1-alicloud-openshift-machine-api-alibabacloud-credentials-policy-policy has attached on user user1-alicloud-openshift-machine-api-alibabacloud-credentials
2022/02/11 16:18:29 Created access keys for RAM User: user1-alicloud-openshift-machine-api-alibabacloud-credentials
2022/02/11 16:18:29 Saved credentials configuration to: user1-alicloud/manifests/openshift-machine-api-alibabacloud-credentials-credentials.yaml
...
```

注意

RAM 用户可以同时具有两个 accessKeys。如果您运行 **ccoctl alibabacloud create-ram-users** 两次，则之前生成的 manifests secret 将变为过时，您必须重新应用新生成的 secret。

b. 验证 OpenShift Container Platform secret 是否已创建：

```
$ ls <path_to_ccoctl_output_dir>/manifests
```

输出示例

```
openshift-cluster-csi-drivers-alibaba-disk-credentials-credentials.yaml
openshift-image-registry-installer-cloud-credentials-credentials.yaml
openshift-ingress-operator-cloud-credentials-credentials.yaml
openshift-machine-api-alibabacloud-credentials-credentials.yaml
```

您可以通过查询 Alibaba Cloud 来验证是否创建了 RAM 用户和策略。如需更多信息，请参阅 Alibaba Cloud 文档中有关列出 RAM 用户和策略的内容。

4. 将生成的凭证文件复制到目标清单目录中：

```
$ cp ./<path_to_ccoctl_output_dir>/manifests/*credentials.yaml
./<path_to_installation>dir>/manifests/
```

其中：

<path_to_ccoctl_output_dir>

指定 **ccoctl alibabacloud create-ram-users** 命令创建的目录。

<path_to_installation_dir>

指定安装程序在其中创建文件的目录。

4.4.4. Alibaba Cloud 的自定义 install-config.yaml 文件示例

您可以自定义安装配置文件(**install-config.yaml**)，以指定集群平台的更多详情，或修改所需参数的值。

```
apiVersion: v1
baseDomain: alicloud-dev.devcluster.openshift.com
credentialsMode: Manual
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform: {}
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform: {}
  replicas: 3
metadata:
  creationTimestamp: null
```

```
  name: test-cluster (1)
 networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes (2)
  serviceNetwork:
  - 172.30.0.0/16
platform:
  alibabacloud:
    defaultMachinePlatform: (3)
      instanceType: ecs.g6.xlarge
      systemDiskCategory: cloud_efficiency
      systemDiskSize: 200
    region: ap-southeast-1 (4)
    resourceGroupID: rg-acfnw6j3hyai (5)
    vpcID: vpc-0xifdjerdibmaqvtjob2b (6)
    vswitchIDs: (7)
    - vsw-0xi8ycgwc8wv5rhviwdq5
    - vsw-0xiy6v3z2tedv009b4pz2
publish: External
pullSecret: '{"auths": {"cloud.openshift.com": {"auth": ... }' (8)
sshKey: |
  ssh-rsa AAAA... (9)
```

(1) 必需。安装程序会提示您输入集群名称。

(2) 要安装的集群网络插件。支持的值有 **OVNKubernetes** 和 **OpenShiftSDN**。默认值为 **OVNKubernetes**。

(3) 可选。为没有定义自身平台配置的机器池指定参数。

(4) 必需。安装程序会提示您输入要将集群部署到的区域。

(5) 可选。指定应该安装集群的现有资源组。

(8) 必需。安装程序会提示您输入 pull secret。

(9) 可选。安装程序会提示您输入用于访问集群中机器的 SSH 密钥值。

(6) (7) 可选。这些是 vswitchID 值示例。

4.4.5. 在安装过程中配置集群范围的代理

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

- 您有一个现有的 **install-config.yaml** 文件。

- 您检查了集群需要访问的站点，并确定它们中的任何站点是否需要绕过代理。默认情况下，所有集群出口流量都经过代理，包括对托管云供应商 API 的调用。如果需要，您将在 **Proxy** 对象的 **spec.noProxy** 字段中添加站点来绕过代理。

注意

Proxy 对象 **status.noProxy** 字段使用安装配置中的 **networking.machineNetwork[].cidr**、**networking.clusterNetwork[].cidr** 和 **networking.serviceNetwork[]** 字段的值填充。

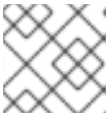
对于在 Amazon Web Services(AWS)、Google Cloud Platform(GCP)、Microsoft Azure 和 Red Hat OpenStack Platform(RHOSP)上安装，**Proxy** 对象 **status.noProxy** 字段也会使用实例元数据端点填充(**169.254.169.254**)。

流程

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

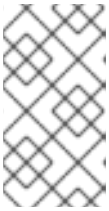
```
apiVersion: v1
baseDomain: my.domain.com
proxy:
  httpProxy: http://<username>:<pswd>@<ip>:<port> 1
  httpsProxy: https://<username>:<pswd>@<ip>:<port> 2
  noProxy: example.com 3
additionalTrustBundle: | 4
    -----BEGIN CERTIFICATE-----
    <MY_TRUSTED_CA_CERT>
    -----END CERTIFICATE-----
additionalTrustBundlePolicy: <policy_to_add_additionalTrustBundle> 5
```

1. 用于创建集群外 HTTP 连接的代理 URL。URL 方案必须是 **http**。
2. 用于创建集群外 HTTPS 连接的代理 URL。
3. 要从代理中排除的目标域名、IP 地址或其他网络 CIDR 的逗号分隔列表。在域前面加上 **.** 以仅匹配子域。例如，**.y.com** 匹配 **x.y.com**，但不匹配 **y.com**。使用 * 绕过所有目的地的代理。
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** 的配置映射，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** 配置映射，将这些内容与 Red Hat Enterprise Linux CoreOS（RHCOS）信任捆绑包合并， **Proxy** 对象的 **trustedCA** 字段中也会引用此配置映射。**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。
5. 可选：决定 **Proxy** 对象的配置以引用 **trustedCA** 字段中 **user-ca-bundle** 配置映射的策略。允许的值是 **Proxyonly** 和 **Always**。仅在配置了 **http/https** 代理时，使用 **Proxyonly** 引用 **user-ca-bundle** 配置映射。使用 **Always** 始终引用 **user-ca-bundle** 配置映射。默认值为 **Proxyonly**。



注意

安装程序不支持代理的 **readinessEndpoints** 字段。



注意

如果安装程序超时，重启并使用安装程序的 **wait-for** 命令完成部署。例如：

```
$ ./openshift-install wait-for install-complete --log-level debug
```

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

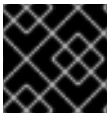
安装程序会创建一个名为 cluster 的集群范围代理，该代理 **使用** 提供的 **install-config.yaml** 文件中的代理设置。如果没有提供代理设置，仍然会创建一个 **cluster Proxy** 对象，但它会有一个空 **spec**。

注意

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

4.5. 部署集群

您可以在兼容云平台上安装 OpenShift Container Platform。



重要

在初始安装过程中，您只能运行安装程序的 **create cluster** 命令一次。

先决条件

- 您已使用托管集群的云平台配置了帐户。
- 您有 OpenShift Container Platform 安装程序和集群的 pull secret。
- 已确认主机上的云供应商帐户具有部署集群的正确权限。权限不正确的帐户会导致安装过程失败，并显示包括缺失权限的错误消息。

流程

- 进入包含安装程序的目录并初始化集群部署：

```
$ ./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**，而不是 **info**。

验证

当集群部署成功完成时：

- 终端会显示用于访问集群的说明，包括指向 Web 控制台和 **kubeadmin** 用户的凭证的链接。

- 凭证信息还会输出到 **<installation_directory>/.openshift_install.log**.

重要

不要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。

输出示例

```
...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/home/myuser/install_dir/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-
console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password: "password"
INFO Time elapsed: 36m22s
```

重要

- 安装程序生成的 Ignition 配置文件包含在 24 小时后过期的证书，然后在过期时进行续订。如果在更新证书前关闭集群，且集群在 24 小时后重启，集群会自动恢复过期的证书。一个例外是，您必须手动批准待处理的 **node-bootstrapper** 证书签名请求(CSR)来恢复 kubelet 证书。如需更多信息，*请参阅从过期的 control plane 证书* 中恢复的文档。
- 建议您在 Ignition 配置文件生成后的 12 小时内使用它们，因为 24 小时的证书会在集群安装后的 16 小时到 22 小时间进行轮转。通过在 12 小时内使用 Ignition 配置文件，您可以避免在安装过程中因为执行了证书更新而导致安装失败的问题。

4.6. 通过下载二进制文件安装 OPENSHIFT CLI

您可以安装 OpenShift CLI(**oc**)来使用命令行界面与 OpenShift Container Platform 进行交互。您可以在 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 4.14 中的所有命令。下载并安装新版本的 **oc**。

在 Linux 上安装 OpenShift 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. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **产品变体** 下拉列表中选择架构。
3. 从 **版本** 下拉列表中选择适当的版本。
4. 点 **OpenShift v4.14 Linux Client** 条目旁的 **Download Now** 来保存文件。

5. 解包存档：

```
$ tar xvf <file>
```

6. 将 **oc** 二进制文件放到 **PATH 中的目录中**。
要查看您的 **PATH**，请执行以下命令：

```
$ echo $PATH
```

验证

- 安装 OpenShift CLI 后，可以使用 **oc** 命令：

```
$ oc <command>
```

在 Windows 上安装 OpenShift CLI

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

流程

1. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **版本** 下拉列表中选择适当的版本。
3. 点 **OpenShift v4.14 Windows Client** 条目旁的 **Download Now** 来保存文件。
4. 使用 ZIP 程序解压存档。
5. 将 **oc** 二进制文件移到 **PATH 中的目录中**。
要查看您的 **PATH**，请打开命令提示并执行以下命令：

```
C:\> path
```

验证

- 安装 OpenShift CLI 后，可以使用 **oc** 命令：

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

在 macOS 上安装 OpenShift CLI

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

流程

1. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **版本** 下拉列表中选择适当的版本。
3. 点 **OpenShift v4.14 macOS Client** 条目旁的 **Download Now** 来保存文件。

注意

对于 macOS arm64，请选择 **OpenShift v4.14 macOS arm64 Client** 条目。

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**，请打开终端并执行以下命令：

```
$ echo $PATH
```

验证

- 使用 **oc** 命令验证安装：

```
$ oc <command>
```

4.7. 使用 CLI 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** 文件包含有关集群的信息，供 CLI 用于将客户端连接到正确的集群和 API 服务器。该文件特定于集群，在 OpenShift Container Platform 安装过程中创建。

先决条件

- 已部署 OpenShift Container Platform 集群。
- 已安装 **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. 验证您可以使用导出的配置成功运行 **oc** 命令：

```
$ oc whoami
```

输出示例

```
system:admin
```

/validating-an-installation.adoc

4.8. 使用 WEB 控制台登录到集群

kubeadmin 用户默认在 OpenShift Container Platform 安装后存在。您可以使用 OpenShift Container Platform Web 控制台以 **kubeadmin** 用户身份登录集群。

先决条件

- 有访问安装主机的访问权限。
- 您完成了集群安装，所有集群 Operator 都可用。

流程

1. 从安装主机上的 **kubeadmin -password** 文件中获取 kubeadmin 用户的密码：

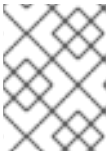
```
$ cat <installation_directory>/auth/kubeadmin-password
```

注意

另外，您还可以从安装主机上的 **<installation_directory>/.openshift_install.log** 日志文件获取 **kubeadmin** 密码。

2. 列出 OpenShift Container Platform Web 控制台路由：

```
$ oc get routes -n openshift-console | grep 'console-openshift'
```



注意

另外，您还可以从安装主机上的 **<installation_directory>/.openshift_install.log 日志** 文件获取 OpenShift Container Platform 路由。

输出示例

```
console     console-openshift-console.apps.<cluster_name>.<base_domain>          console
https   reencrypt/Redirect   None
```

3. 在 Web 浏览器中导航到上一命令输出中包括的路由，以 **kubeadmin** 用户身份登录。

4.9. OPENSHIFT CONTAINER PLATFORM 的 TELEMETRY 访问

在 OpenShift Container Platform 4.14 中，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，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 OpenShift Cluster Manager。

确认 OpenShift Cluster Manager 清单正确后，可以由 Telemetry 自动维护，也可以使用 OpenShift Cluster Manager 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。

其他资源

- 有关 Telemetry 服务的更多信息，请参阅关于远程健康监控。

- 如需有关访问和了解 OpenShift Container Platform Web 控制台的更多信息，请参阅访问 Web 控制台
- 如需有关 访问和了解 OpenShift Container Platform Web 控制台的更多详情，请参阅 访问 Web 控制台。

4.10. 后续步骤

- 验证安装.
- 自定义集群。
- 如果需要，您可以选择 不使用远程健康报告。

第 5 章 使用网络自定义在 ALIBABA CLOUD 上安装集群

在 OpenShift Container Platform 4.14 中，您可以使用自定义的网络配置选项在 Alibaba Cloud 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。

您必须在安装过程中设置大多数网络配置参数，且您只能在正在运行的集群中修改 **kubeProxy** 配置参数。

重要

OpenShift Container Platform 上的 Alibaba Cloud 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。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。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

5.1. 先决条件

- 您可以参阅有关 OpenShift Container Platform 安装和更新 流程的详细信息。
- 您可以阅读选择集群安装方法并为用户准备它的文档。
- 您已注册了域。
- 如果使用防火墙，将其配置为允许集群需要访问的站点。
- 如果您的环境无法访问云的资源访问管理(RAM)API，或者不想将管理员级别的凭证 secret 存储在 **kube-system** 命名空间中，您可以手动创建和维护资源访问管理(RAM)凭证。

5.2. OPENSHIFT CONTAINER PLATFORM 互联网访问

在 OpenShift Container Platform 4.14 中，您需要访问互联网来安装集群。

您必须具有以下互联网访问权限：

- 访问 OpenShift Cluster Manager 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型的基础架构上执行受限网络安装。在此过程中，您可以下载所需的内容，并使用它为镜像 registry 填充安装软件包。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。在更新集群前，您要更新镜像 registry 的内容。

5.3. 为集群节点 SSH 访问生成密钥对

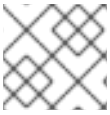
在 OpenShift Container Platform 安装过程中，您可以为安装程序提供 SSH 公钥。密钥通过它们的 Ignition 配置文件传递给 Red Hat Enterprise Linux CoreOS(RHCOS)节点，用于验证对节点的 SSH 访问。密钥添加到每个节点上 **core** 用户的 **~/.ssh/authorized_keys** 列表中，这将启用免密码身份验证。

将密钥传递给节点后，您可以使用密钥对作为用户 **核心** 通过 SSH 连接到 RHCOS 节点。若要通过 SSH 访问节点，必须由 SSH 为您的本地用户管理私钥身份。

如果要通过 SSH 连接到集群节点来执行安装调试或灾难恢复，则必须在安装过程中提供 SSH 公钥。**./openshift-install gather** 命令还需要在集群节点上设置 SSH 公钥。

重要

不要在生产环境中跳过这个过程，在生产环境中需要灾难恢复和调试。



注意

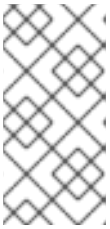
您必须使用本地密钥，而不是使用特定平台方法配置 的密钥，如 AWS 密钥对。

流程

1. 如果您在本地计算机上没有可用于在集群节点上进行身份验证的现有 SSH 密钥对，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 ed25519 -N '' -f <path>/<file_name> 1
```

1 指定新 SSH 密钥的路径和文件名，如 **~/.ssh/id_ed25519**。如果您已有密钥对，请确保您的公钥位于 **~/.ssh** 目录中。



注意

如果您计划在 **x86_64**、**ppc64le** 和 **s390x** 架构上安装使用 RHEL 加密库（这些加密库已提交给 NIST 用于 FIPS 140-2/140-3 验证）的 OpenShift Container Platform 集群，则不要创建使用 **ed25519** 算法的密钥。相反，创建一个使用 **rsa** 或 **ecdsa** 算法的密钥。

2. 查看公共 SSH 密钥：

```
$ cat <path>/<file_name>.pub
```

例如，运行以下命令来查看 **~/.ssh/id_ed25519.pub** 公钥：

```
$ cat ~/.ssh/id_ed25519.pub
```

3. 将 SSH 私钥身份添加到本地用户的 SSH 代理（如果尚未添加）。在集群节点上，或者要使用 **./openshift-install gather** 命令，需要对该密钥进行 SSH 代理管理，才能在集群节点上进行免密码 SSH 身份验证。

注意

在某些发行版中，自动管理默认 SSH 私钥身份，如 **~/.ssh/id_rsa** 和 **~/.ssh/id_dsa**。

a. 如果 **ssh-agent** 进程尚未为您的本地用户运行，请将其作为后台任务启动：

```
$ eval "$(ssh-agent -s)"
```

输出示例

```
Agent pid 31874
```

注意

如果集群处于 FIPS 模式，则只使用 FIPS 兼容算法来生成 SSH 密钥。密钥必须是 RSA 或 ECDSA。

4. 将 SSH 私钥添加到 **ssh-agent** ：

```
$ ssh-add <path>/<file_name> 1
```

1 指定 SSH 私钥的路径和文件名，如 **~/.ssh/id_ed25519.pub**

输出示例

```
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

后续步骤

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

5.4. 获取安装程序

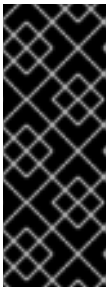
在安装 OpenShift Container Platform 前，将安装文件下载到您用于安装的主机上。

先决条件

- 您有一台运行 Linux 或 macOS 的计算机，至少有 1.2 GB 本地磁盘空间。

流程

1. 进入 Red Hat Hybrid Cloud Console 上的 Cluster Type 页。如果您有红帽帐户，请使用您的凭证登录。如果没有，请创建一个帐户。
2. 在页的 **Run it yourself** 部分中选择您的基础架构供应商。
3. 从 **OpenShift 安装程序**下的下拉菜单中选择您的主机操作系统和架构，然后点**下载安装程序**。
4. 将下载的文件保存在要存储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几个文件。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。删除集群需要这两个文件。
- 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。要删除集群，请为特定云供应商完成 OpenShift Container Platform 卸载流程。

5. 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 openshift-install-linux.tar.gz
```

6. 从 Red Hat OpenShift Cluster Manager 下载安装 pull secret 。此 pull secret 允许您与所含授权机构提供的服务进行身份验证，这些服务包括为 OpenShift Container Platform 组件提供容器镜像的 Quay.io。

提示

另外，您还可以从红帽客户门户网站检索安装程序，您可以在其中指定要下载的安装程序版本。但是，您需要有一个有效的订阅才能访问此页。

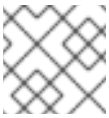
5.5. 网络配置阶段

OpenShift Container Platform 安装前有两个阶段，您可以在其中自定义网络配置。

第 1 阶段

在创建清单文件前，您可以自定义 **install-config.yaml** 文件中的以下与网络相关的字段：

- **networking.networkType**
- **networking.clusterNetwork**
- **networking.serviceNetwork**
- **networking.machineNetwork**
  有关这些字段的更多信息，请参阅 *安装配置参数*。



注意

将 **networking.machineNetwork** 设置为与首选 NIC 所在的 CIDR 匹配。

重要

CIDR 范围 **172.17.0.0/16** 由 libVirt 保留。对于集群中的任何网络，您无法使用此范围或与这个范围重叠的范围。

第 2 阶段

运行 **openshift-install create 清单创建** 清单文件后，您可以只使用您要修改的字段定义自定义 Cluster Network Operator 清单。您可以使用 清单指定高级网络配置。

您不能覆盖在 stage 2 阶段 1 中在 **install-config.yaml** 文件中指定的值。但是，您可以在第 2 阶段进一步自定义网络插件。

5.5.1. 创建安装配置文件

您可以自定义 OpenShift Container Platform 集群。

先决条件

- 您有 OpenShift Container Platform 安装程序和集群的 pull secret。

流程

1. 创建 **install-config.yaml** 文件。
   a. 进入包含安装程序的目录并运行以下命令：

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

   1 对于 **<installation_directory>**，请指定要存储安装程序创建的文件的目录名称。

   在指定目录时：

   - 验证该目录是否具有**执行**权限。在安装目录中运行 Terraform 二进制文件需要这个权限。
   - 使用空目录。有些安装资产，如 bootstrap X.509 证书的过期间隔较短，因此不得重复使用安装目录。如果要重复使用另一个集群安装中的单个文件，您可以将它们复制到您的目录中。但是，安装资产的文件名可能会在发行版本间有所变化。从以前的 OpenShift Container Platform 版本中复制安装文件时请小心。

注意

始终删除 **~/.powervs** 目录，以避免重复使用过时的配置。运行以下命令:

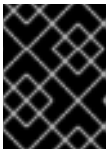
```
$ rm -rf ~/.powervs
```

   b. 在提示符处，提供云的配置详情：
      i. 可选： 选择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。

      ii. 为集群输入描述性名称。
2. 修改 **install-config.yaml** 文件。您可以在"安装配置参数"部分找到有关可用参数的更多信息。
3. 备份 **install-config.yaml** 文件，以便您可以使用它安装多个集群。



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。

其他资源

- Alibaba Cloud 的安装配置参数

5.5.2. 生成所需的安装清单

您必须生成 Kubernetes 清单和 Ignition 配置文件，集群需要配置机器。

流程

1. 从包含安装程序的目录中运行以下命令来生成清单：

```
$ openshift-install create manifests --dir <installation_directory>
```

其中：

<installation_directory>
指定安装程序在其中创建文件的目录。

注意

默认情况下，**ccoctl** 在运行命令的目录中创建对象。要在其他目录中创建对象，请使用 **--output-dir** 标志。此流程使用 **<path_to_ccoctl_output_dir>** 来引用这个目录。

先决条件

您必须：

- 提取并准备好 **ccoctl** 二进制文件。

流程

1. 运行以下命令，使用安装文件中的发行镜像设置 **$RELEASE_IMAGE** 变量：

```
$ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
```

2. 运行以下命令，从 OpenShift Container Platform 发行镜像中提取 **CredentialsRequest** 对象列表：

```
$ oc adm release extract \
  --from=$RELEASE_IMAGE \
  --credentials-requests \
  --included \ 1
  --install-config=<path_to_directory_with_installation_configuration>/install-config.yaml \ 2
  --to=<path_to_directory_for_credentials_requests> 3
```

1 **--included** 参数仅包含特定集群配置所需的清单。

2 指定 **install-config.yaml** 文件的位置。

3 指定要存储 **CredentialsRequest** 对象的目录的路径。如果指定的目录不存在，这个命令会创建它。

注意

此命令可能需要一些时间才能运行。

5.5.3. Alibaba Cloud 的自定义 install-config.yaml 文件示例

您可以自定义安装配置文件(**install-config.yaml**)，以指定集群平台的更多详情，或修改所需参数的值。

```
apiVersion: v1
baseDomain: alicloud-dev.devcluster.openshift.com
credentialsMode: Manual
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform: {}
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform: {}
  replicas: 3
metadata:
  creationTimestamp: null
  name: test-cluster 1
 networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes 2
  serviceNetwork:
  - 172.30.0.0/16
platform:
  alibabacloud:
    defaultMachinePlatform: 3
      instanceType: ecs.g6.xlarge
      systemDiskCategory: cloud_efficiency
      systemDiskSize: 200
    region: ap-southeast-1 4
    resourceGroupID: rg-acfnw6j3hyai 5
    vpcID: vpc-0xifdjerdibmaqvtjob2b 6
    vswitchIDs: 7
    - vsw-0xi8ycgwc8wv5rhviwdq5
    - vsw-0xiy6v3z2tedv009b4pz2
publish: External
```

```
pullSecret: '{"auths": {"cloud.openshift.com": {"auth": ... }' 8
sshKey: |
  ssh-rsa AAAA... 9
```

1 必需。安装程序会提示您输入集群名称。

2 要安装的集群网络插件。支持的值有 **OVNKubernetes** 和 **OpenShiftSDN**。默认值为 **OVNKubernetes**。

3 可选。为没有定义自身平台配置的机器池指定参数。

4 必需。安装程序会提示您输入要将集群部署到的区域。

5 可选。指定应该安装集群的现有资源组。

8 必需。安装程序会提示您输入 pull secret。

9 可选。安装程序会提示您输入用于访问集群中机器的 SSH 密钥值。

6 7 可选。这些是 vswitchID 值示例。

5.5.4. 在安装过程中配置集群范围的代理

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

- 您有一个现有的 **install-config.yaml** 文件。
- 您检查了集群需要访问的站点，并确定它们中的任何站点是否需要绕过代理。默认情况下，所有集群出口流量都经过代理，包括对托管云供应商 API 的调用。如果需要，您将在 **Proxy** 对象的 **spec.noProxy** 字段中添加站点来绕过代理。

注意

Proxy 对象 **status.noProxy** 字段使用安装配置中的 **networking.machineNetwork[].cidr**、**networking.clusterNetwork[].cidr** 和 **networking.serviceNetwork[]** 字段的值填充。

对于在 Amazon Web Services(AWS)、Google Cloud Platform(GCP)、Microsoft Azure 和 Red Hat OpenStack Platform(RHOSP)上安装，**Proxy** 对象 **status.noProxy** 字段也会使用实例元数据端点填充(**169.254.169.254**)。

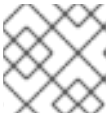
流程

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: https://<username>:<pswd>@<ip>:<port> 2
```

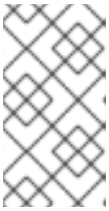
```
  noProxy: example.com 3
additionalTrustBundle: | 4
    -----BEGIN CERTIFICATE-----
    <MY_TRUSTED_CA_CERT>
    -----END CERTIFICATE-----
additionalTrustBundlePolicy: <policy_to_add_additionalTrustBundle> 5
```

1. 用于创建集群外 HTTP 连接的代理 URL。URL 方案必须是 **http**。
2. 用于创建集群外 HTTPS 连接的代理 URL。
3. 要从代理中排除的目标域名、IP 地址或其他网络 CIDR 的逗号分隔列表。在域前面加上 **.** 以仅匹配子域。例如，**.y.com** 匹配 **x.y.com**，但不匹配 **y.com**。使用 * 绕过所有目的地的代理。
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** 的配置映射，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** 配置映射，将这些内容与 Red Hat Enterprise Linux CoreOS（RHCOS）信任捆绑包合并， **Proxy** 对象的 **trustedCA** 字段中也会引用此配置映射。**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。
5. 可选：决定 **Proxy** 对象的配置以引用 **trustedCA** 字段中 **user-ca-bundle** 配置映射的策略。允许的值是 **Proxyonly** 和 **Always**。仅在配置了 **http/https** 代理时，使用 **Proxyonly** 引用 **user-ca-bundle** 配置映射。使用 **Always** 始终引用 **user-ca-bundle** 配置映射。默认值为 **Proxyonly**。



注意

安装程序不支持代理的 **readinessEndpoints** 字段。



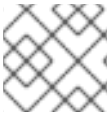
注意

如果安装程序超时，重启并使用安装程序的 **wait-for** 命令完成部署。例如：

```
$ ./openshift-install wait-for install-complete --log-level debug
```

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，仍然会创建一个 **cluster Proxy** 对象，但它会有一个空 **spec**。



注意

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

5.6. CLUSTER NETWORK OPERATOR 配置

集群网络的配置作为 Cluster Network Operator(CNO)配置的一部分指定，并存储在名为 **cluster** 的自定义资源(CR)对象中。CR 指定 **operator.openshift.io** API 组中的 **Network** API 的字段。

CNO 配置在集群安装过程中从 **Network.config.openshift.io** API 组中的 **Network** API 继承以下字段：

clusterNetwork

从中分配 Pod IP 地址的 IP 地址池。

serviceNetwork

服务的 IP 地址池.

defaultNetwork.type

集群网络插件，如 OpenShift SDN 或 OVN-Kubernetes。

您可以通过在名为 **cluster** 的 CNO 对象中设置 **defaultNetwork** 对象的字段来为集群指定集群网络插件配置。

5.6.1. Cluster Network Operator 配置对象

下表中描述了 Cluster Network Operator(CNO)的字段：

表 5.1. Cluster Network Operator 配置对象

字段	类型	描述
metadata.name	**字符串**	CNO 对象的名称。这个名称始终是 **集群**。

spec.clusterNetwork	**array**	用于指定从哪些 IP 地址块分配 Pod IP 地址以及集群中每个节点的子网前缀长度的列表。例如：
		`spec:`
		`  clusterNetwork:`
		`  - cidr: 10.128.0.0/19`
		`  hostPrefix: 23`
		`  - cidr: 10.128.32.0/19`
		`  hostPrefix: 23`

spec.serviceNetwork	**array**	服务的 IP 地址块。OpenShift SDN 和 OVN-Kubernetes 网络插件只支持服务网络的一个 IP 地址块。例如：
		`spec:`
		`  serviceNetwork:`
		`  - 172.30.0.0/14`
		您只能在创建清单前在 **install-config.yaml** 文件中自定义此字段。该值在清单文件中是只读的。

spec.defaultNetwork	**object**	为集群网络配置网络插件。
spec.kubeProxyConfig	**object**	此对象的字段指定 kube-proxy 配置。如果使用 OVN-Kubernetes 集群网络供应商，则 kube-proxy 配置不会起作用。

defaultNetwork 对象配置
下表列出了 **defaultNetwork** 对象的值：

表 5.2. **defaultNetwork** 对象

字段	类型	描述
type	**字符串**	**OpenShiftSDN** 或 **OVNKubernetes**。Red Hat OpenShift Networking 网络插件在安装过程中被选择。您可以通过从 OpenShift SDN 迁移到 OVN-Kubernetes 来更改这个值。  **注意** OpenShift Container Platform 默认使用 OVN-Kubernetes 网络插件。
openshiftSDNConfig	**object**	此对象仅对 OpenShift SDN 网络插件有效。
ovnKubernetesConfig	**object**	此对象仅对 OVN-Kubernetes 网络插件有效。

配置 **OpenShift SDN** 网络插件
下表描述了 OpenShift SDN 网络插件的配置字段：

表 5.3. **openshiftSDNConfig** object

字段	类型	描述
模式	**字符串**	配置 OpenShift SDN 的网络隔离模式。默认值为 **NetworkPolicy**。 **Multitenant** 和 **Subnet** 值可用于向后兼容 OpenShift Container Platform 3.x，但不建议使用。此值在集群安装后无法更改。
mtu	**integer**	VXLAN 覆盖网络的最大传输单元(MTU)。这根据主网络接口的 MTU 自动探测。您通常不需要覆盖检测到的 MTU。 如果自动探测的值不是您期望的值，请确认节点上主网络接口上的 MTU 是否正确。您不能使用这个选项更改节点上主网络接口的 MTU 值。 如果集群中不同节点需要不同的 MTU 值，则必须将此值设置为比集群中的最低 MTU 值小 **50**。例如，如果集群中的某些节点的 MTU 为 **9001**，而某些节点的 MTU 为 **1500**，则必须将此值设置为 **1450**。 此值在集群安装后无法更改。

字段	类型	描述
vxlanPort	**integer**	用于所有 VXLAN 数据包的端口。默认值为 **4789**。此值在集群安装后无法更改。 如果您在虚拟环境中运行，且现有节点是另一个 VXLAN 网络的一部分，则可能需要更改此设置。例如，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。

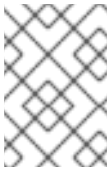
OpenShift SDN 配置示例

```
defaultNetwork:
  type: OpenShiftSDN
  openshiftSDNConfig:
    mode: NetworkPolicy
    mtu: 1450
    vxlanPort: 4789
```

配置 OVN-Kubernetes 网络插件
下表描述了 OVN-Kubernetes 网络插件的配置字段：

表 5.4. ovnKubernetesConfig object

字段	类型	描述
mtu	**integer**	Geneve（通用网络虚拟化封装）覆盖网络的最大传输单元 (MTU)。这根据主网络接口的 MTU 自动探测。您通常不需要覆盖检测到的 MTU。 如果自动探测的值不是您期望的值，请确认节点上主网络接口上的 MTU 是否正确。您不能使用这个选项更改节点上主网络接口的 MTU 值。 如果集群中不同节点需要不同的 MTU 值，则必须将此值设置为 **比** 集群中的最低 MTU 值小 100。例如，如果集群中的某些节点的 MTU 为 **9001**，而某些节点的 MTU 为 **1500**，则必须将此值设置为 **1400**。
genevePort	**integer**	用于所有 Geneve 数据包的端口。默认值为 **6081**。此值在集群安装后无法更改。
ipsecConfig	**object**	指定一个空对象来启用 IPsec 加密。
policyAuditConfig	**object**	指定用于自定义网络策略审计日志的配置对象。如果未设置，则使用默认的审计日志设置。

字段	类型	描述
gatewayConfig	**object**	可选：指定一个配置对象来自定义如何将出口流量发送到节点网关。  **注意** 在迁移出口流量时，工作负载和服务流量会受到一定影响，直到 Cluster Network Operator (CNO) 成功推出更改。
v4InternalSubnet	如果您的现有网络基础架构与 **100.64.0.0/16** IPv4 子网重叠，您可以指定不同的 IP 地址范围供 OVN-Kubernetes 使用。您必须确保 IP 地址范围没有与 OpenShift Container Platform 安装使用的任何其他子网重叠。IP 地址范围必须大于可添加到集群的最大节点数。例如，如果 **clusterNetwork.cidr** 值为 **10.128.0.0/14**，并且 **clusterNetwork.hostPrefix** 值为 **/23**，则最大节点数量为 **2^(23-14)=512**。 在安装后无法更改此字段。	默认值为 **100.64.0.0/16**。

字段	类型	描述
v6InternalSubnet	如果您的现有网络基础架构与 **fd98::/48** IPv6 子网重叠，您可以指定不同的 IP 地址范围供 OVN-Kubernetes 使用。您必须确保 IP 地址范围没有与 OpenShift Container Platform 安装使用的任何其他子网重叠。IP 地址范围必须大于可添加到集群的最大节点数。 在安装后无法更改此字段。	默认值为 **fd98::/48**。

表 5.5. **policyAuditConfig** object

字段	类型	描述
rateLimit	整数	每个节点每秒生成一次的消息数量上限。默认值为每秒 **20** 条消息。
maxFileSize	整数	审计日志的最大大小，以字节为单位。默认值为 **50000000** 或 50 MB。
maxLogFiles	整数	保留的日志文件的最大数量。
目的地	字符串	以下附加审计日志目标之一： **libc** 主机上的 journald 进程的 libc **syslog（）** 函数。 **UDP:<host>:<port>** 一个 syslog 服务器。将 **<host>:<port>** 替换为 **syslog 服务器的主机** 和端口。 **Unix:<file>** 由 **<file>** 指定的 Unix 域套接字文件。 **null** 不要将审计日志发送到任何其他目标。
syslogFacility	字符串	syslog 工具，如 as **kern**，如 RFC5424 定义。默认值为 **local0**。

表 5.6. **gatewayConfig** object

字段	类型	描述
routingViaHost	**布尔值**	将此字段设置为 **true**，将来自 pod 的出口流量发送到主机网络堆栈。对于依赖于在内核路由表中手动配置路由的高级别安装和应用程序，您可能需要将出口流量路由到主机网络堆栈。默认情况下，出口流量在 OVN 中进行处理以退出集群，不受内核路由表中的特殊路由的影响。默认值为 **false**。 此字段与 Open vSwitch 硬件卸载功能有交互。如果将此字段设置为 **true**，则不会获得卸载的性能优势，因为主机网络堆栈会处理出口流量。
ipForwarding	**object**	您可以使用 **Network** 资源中的 **ipForwarding** 规格来控制 OVN-Kubernetes 管理接口上所有流量的 IP 转发。指定 **Restricted** 只允许 Kubernetes 相关流量的 IP 转发。指定 **Global** 以允许转发所有 IP 流量。对于新安装，默认值为 **Restricted**。对于 OpenShift Container Platform 4.14 的更新，默认值为 **Global**。

启用 IPSec 的 OVN-Kubernetes 配置示例

```
defaultNetwork:
  type: OVNKubernetes
  ovnKubernetesConfig:
    mtu: 1400
    genevePort: 6081
    ipsecConfig: {}
```

kubeProxyConfig 对象配置（仅限 **OpenShiftSDN** 容器网络接口）
kubeProxyConfig 对象的值在下表中定义：

表 5.7. **kubeProxyConfig** object

字段	类型	描述
iptablesSyncPeriod	**字符串**	**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。 **注意** 由于 OpenShift Container Platform 4.3 及更高版本中引进了性能改进，不再需要调整 **iptablesSyncPeriod** 参数。

字段	类型	描述
proxyArguments.iptables-min-sync-period	**array**	刷新 **iptables** 规则前的最短持续时间。此字段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 **time** 软件包。默认值为： kubeProxyConfig: proxyArguments: iptables-min-sync-period: - 0s

5.7. 指定高级网络配置

您可以使用网络插件的高级网络配置将集群集成到现有网络环境中。您只能在安装集群前指定高级网络配置。

重要

不支持通过修改安装程序创建的 OpenShift Container Platform 清单文件来自定义网络配置。支持应用您创建的清单文件，如以下流程中所示。

先决条件

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

流程

1. 进入包含安装程序的目录并创建清单：

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

1 **<installation_directory>** 指定包含集群的 **install-config.yaml** 文件的目录名称。

2. 在 **<installation_directory>/manifests/** 目录中 为**高级网络配置创建一个名为 cluster-network-03-config.yml** 的 stub 清单文件：

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
```

3. 在 **cluster-network-03-config.yml** 文件中指定集群的高级网络配置，如下例所示：

为 OpenShift SDN 网络供应商指定不同的 VXLAN 端口

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
```

```
  name: cluster
spec:
  defaultNetwork:
    openshiftSDNConfig:
      vxlanPort: 4800
```

为 OVN-Kubernetes 网络供应商启用 IPsec

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  defaultNetwork:
    ovnKubernetesConfig:
      ipsecConfig: {}
```

4. 可选：备份 **manifests/cluster-network-03-config.yml** 文件。创建 Ignition 配置文件时，安装程序会使用 **manifests/** 目录。

5.8. 使用 OVN-KUBERNETES 配置混合网络

您可以将集群配置为使用 OVN-Kubernetes 网络插件的混合网络。这允许支持不同节点网络配置的混合集群。

注意

此配置是在同一集群中同时运行 Linux 和 Windows 节点所必需的。

先决条件

- 您在 **install-config.yaml** 文件中为 **networking.networkType** 参数定义了 **OVNKubernetes**。如需更多信息，请参阅有关在所选云供应商上配置 OpenShift Container Platform 网络自定义的安装文档。

流程

1. 进入包含安装程序的目录并创建清单：

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

其中：

<installation_directory>

指定包含集群的 **install-config.yaml** 文件的目录名称。

2. 在 **<installation_directory>/manifests/** 目录中为高级网络配置创建一个名为 **cluster-network-03-config.yml** 的 stub 清单文件：

```
$ cat <<EOF > <installation_directory>/manifests/cluster-network-03-config.yml
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
```

```
  name: cluster
spec:
EOF
```

其中：

<installation_directory>

指定包含集群的 **manifests/** 目录的目录名称。

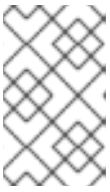
3. 在编辑器中打开 **cluster-network-03-config.yml** 文件，并使用混合网络配置 OVN-Kubernetes，如下例所示：

指定混合网络配置

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  defaultNetwork:
    ovnKubernetesConfig:
      hybridOverlayConfig:
        hybridClusterNetwork: 1
        - cidr: 10.132.0.0/14
          hostPrefix: 23
        hybridOverlayVXLANPort: 9898 2
```

1 指定用于额外覆盖网络上节点的 CIDR 配置。**hybridClusterNetwork** CIDR 不能与 **clusterNetwork** CIDR 重叠。

2 为额外覆盖网络指定自定义 VXLAN 端口。这是在 vSphere 上安装的集群中运行 Windows 节点所需要的，且不得为任何其他云供应商配置。自定义端口可以是除默认 **4789** 端口外的任何打开的端口。有关此要求的更多信息，请参阅 Microsoft 文档中的 Pod 到主机间的 pod 连接性。



注意

Windows Server Long-Term Servicing Channel（LTSC）：Windows Server 2019 在带有自定义 **hybridOverlayVXLANPort** 值的集群中不被支持，因为这个 Windows server 版本不支持选择使用自定义的 VXLAN 端口。

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

5. 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。

5.9. 部署集群

您可以在兼容云平台上安装 OpenShift Container Platform。

重要

在初始安装过程中，您只能运行安装程序的 **create cluster** 命令一次。

先决条件

- 您已使用托管集群的云平台配置了帐户。
- 您有 OpenShift Container Platform 安装程序和集群的 pull secret。
- 已确认主机上的云供应商帐户具有部署集群的正确权限。权限不正确的帐户会导致安装过程失败，并显示包括缺失权限的错误消息。

流程

- 进入包含安装程序的目录并初始化集群部署：

```
$ ./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**，而不是 **info**。

验证

当集群部署成功完成时：

- 终端会显示用于访问集群的说明，包括指向 Web 控制台和 **kubeadmin** 用户的凭证的链接。
- 凭证信息还会输出到 **<installation_directory>/.openshift_install.log**.

重要

不要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。

输出示例

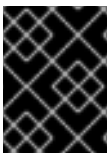
```
...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/home/myuser/install_dir/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-
console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password: "password"
INFO Time elapsed: 36m22s
```

重要

- 安装程序生成的 Ignition 配置文件包含在 24 小时后过期的证书，然后在过期时进行续订。如果在更新证书前关闭集群，且集群在 24 小时后重启，集群会自动恢复过期的证书。一个例外是，您必须手动批准待处理的 **node-bootstrapper** 证书签名请求(CSR)来恢复 kubelet 证书。如需更多信息，*请参阅从过期的 control plane 证书* 中恢复的文档。
- 建议您在 Ignition 配置文件生成后的 12 小时内使用它们，因为 24 小时的证书会在集群安装后的 16 小时到 22 小时间进行轮转。通过在 12 小时内使用 Ignition 配置文件，您可以避免在安装过程中因为执行了证书更新而导致安装失败的问题。

5.10. 通过下载二进制文件安装 OPENSHIFT CLI

您可以安装 OpenShift CLI(**oc**)来使用命令行界面与 OpenShift Container Platform 进行交互。您可以在 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 4.14 中的所有命令。下载并安装新版本的 **oc**。

在 Linux 上安装 OpenShift 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. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **产品变体** 下拉列表中选择架构。
3. 从 **版本** 下拉列表中选择适当的版本。
4. 点 **OpenShift v4.14 Linux Client** 条目旁的 **Download Now** 来保存文件。
5. 解包存档：

```
$ tar xvf <file>
```

6. 将 **oc** 二进制文件放到 **PATH** 中的目录中。
   要查看您的 **PATH**，请执行以下命令：

```
$ echo $PATH
```

验证

- 安装 OpenShift CLI 后，可以使用 **oc** 命令：

```
$ oc <command>
```

在 Windows 上安装 OpenShift CLI

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

流程

1. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **版本** 下拉列表中选择适当的版本。
3. 点 **OpenShift v4.14 Windows Client** 条目旁的 **Download Now** 来保存文件。
4. 使用 ZIP 程序解压存档。
5. 将 **oc** 二进制文件移到 **PATH 中的目录中**。
   要查看您的 **PATH**，请打开命令提示并执行以下命令：

```
C:\> path
```

验证

- 安装 OpenShift CLI 后，可以使用 **oc** 命令：

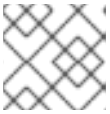
```
C:\> oc <command>
```

在 macOS 上安装 OpenShift CLI

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

流程

1. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **版本** 下拉列表中选择适当的版本。
3. 点 **OpenShift v4.14 macOS Client** 条目旁的 **Download Now** 来保存文件。



注意

对于 macOS arm64，请选择 **OpenShift v4.14 macOS arm64 Client** 条目。

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**，请打开终端并执行以下命令：

```
$ echo $PATH
```

验证

- 使用 **oc** 命令验证安装：

```
$ oc <command>
```

5.11. 使用 CLI 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** 文件包含有关集群的信息，供 CLI 用于将客户端连接到正确的集群和 API 服务器。该文件特定于集群，在 OpenShift Container Platform 安装过程中创建。

先决条件

- 已部署 OpenShift Container Platform 集群。
- 已安装 **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. 验证您可以使用导出的配置成功运行 **oc** 命令：

```
$ oc whoami
```

输出示例

```
system:admin
```

/validating-an-installation.adoc

5.12. 使用 WEB 控制台登录到集群

kubeadmin 用户默认在 OpenShift Container Platform 安装后存在。您可以使用 OpenShift Container Platform Web 控制台以 **kubeadmin** 用户身份登录集群。

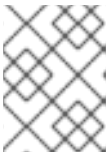
先决条件

- 有访问安装主机的访问权限。
- 您完成了集群安装，所有集群 Operator 都可用。

流程

1. 从安装主机上的 **kubeadmin -password** 文件中获取 kubeadmin 用户的密码：

```
$ cat <installation_directory>/auth/kubeadmin-password
```

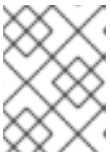


注意

另外，您还可以从安装主机上的 **<installation_directory>/.openshift_install.log** 日志文件获取 **kubeadmin** 密码。

2. 列出 OpenShift Container Platform Web 控制台路由：

```
$ oc get routes -n openshift-console | grep 'console-openshift'
```



注意

另外，您还可以从安装主机上的 **<installation_directory>/.openshift_install.log 日志** 文件获取 OpenShift Container Platform 路由。

输出示例

```
console     console-openshift-console.apps.<cluster_name>.<base_domain>          console
https   reencrypt/Redirect   None
```

3. 在 Web 浏览器中导航到上一命令输出中包括的路由，以 **kubeadmin** 用户身份登录。

5.13. OPENSHIFT CONTAINER PLATFORM 的 TELEMETRY 访问

在 OpenShift Container Platform 4.14 中，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，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 OpenShift Cluster Manager。

确认 OpenShift Cluster Manager 清单正确后，可以由 Telemetry 自动维护，也可以使用 OpenShift Cluster Manager 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。

其他资源

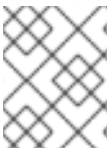
- 有关 Telemetry 服务的更多信息，请参阅关于远程健康监控。
- 如需有关访问和了解 OpenShift Container Platform Web 控制台的更多信息，请参阅访问 Web 控制台
- 如需有关 访问和了解 OpenShift Container Platform Web 控制台的更多详情，请参阅 访问 Web 控制台。

5.14. 后续步骤

- 验证安装。
- 自定义集群。
- 如果需要，您可以选择 不使用远程健康报告。

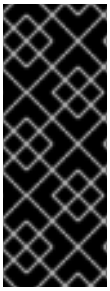
第 6 章 在 ALIBABA CLOUD 上安装集群到现有的 VPC 中

在 OpenShift Container Platform 版本 4.14 中，您可以在 Alibaba Cloud Services 上将集群安装到现有的 Alibaba Virtual Private Cloud (VPC) 中。安装程序置备所需的基础架构，然后可以自定义该基础架构。要自定义 VPC 安装，请在安装集群前修改 'install-config.yaml' 文件中的参数。



注意

OpenShift Container Platform 安装配置的作用范围被特意设计为较小。它旨在简化操作并确保成功。在安装完成后，您可以进行更多的 OpenShift Container Platform 配置任务。



重要

OpenShift Container Platform 上的 Alibaba Cloud 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。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。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

6.1. 先决条件

- 您可以参阅有关 OpenShift Container Platform 安装和更新 流程的详细信息。
- 您可以阅读选择集群安装方法并为用户准备它的文档。
- 您已注册了域。
- 如果使用防火墙，将其配置为允许集群需要访问的站点。
- 如果您的环境无法访问云的资源访问管理(RAM)API，或者不想将管理员级别的凭证 secret 存储在 **kube-system** 命名空间中，您可以手动创建和维护资源访问管理(RAM)凭证。

6.2. 使用自定义 VPC

在 OpenShift Container Platform 4.14 中，您可以在 Alibaba Cloud Platform 的现有 Virtual Private Cloud (VPC) 中将集群部署到现有子网中。通过将 OpenShift Container Platform 部署到现有的 Alibaba VPC 中，您可以避免限制新帐户中的限制，并更轻松地遵循组织的操作限制。如果您无法获得您自己创建 VPC 所需的基础架构创建权限，请使用这个安装选项。您必须使用 vSwitches 配置网络。

6.2.1. 使用 VPC 的要求

VPC CIDR 块的 union，机器网络 CIDR 不能为空。vSwitch 必须在机器网络中。

安装程序不会创建以下组件：

- VPC
- vSwitches
- 路由表
- NAT 网关

注意

安装程序要求您使用由云提供的 DNS 服务器。不支持使用自定义 DNS 服务器，并导致安装失败。

6.2.2. VPC 验证

要确保您提供的 vSwitch 是适当的，安装程序会确认以下数据：

- 您指定的所有 vSwitch 都必须存在。
- 您已为控制平面机器和计算机器提供了一个或多个 vSwitches。
- vSwitches 的 CIDR 属于您指定的机器 CIDR。

6.2.3. 权限划分

有些个人可以在您的云中创建不同的资源。例如，您可以创建特定于应用程序的项目，如实例、存储桶和负载均衡器，但不能创建与网络相关的组件，如 VPC 或 vSwitches。

6.2.4. 集群间隔离

如果您将 OpenShift Container Platform 部署到现有网络中，集群服务的隔离将在以下方面减少：

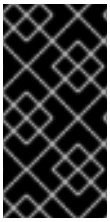
- 您可以在同一 VPC 中安装多个 OpenShift Container Platform 集群。
- 整个网络允许 ICMP 入站流量。
- 整个网络都允许 TCP 22 入站流量 (SSH)。
- 整个网络都允许 control plane TCP 6443 入站流量 (Kubernetes API)。
- 整个网络都允许 control plane TCP 22623 入站流量 (MCS) 。

6.3. OPENSHIFT CONTAINER PLATFORM 互联网访问

在 OpenShift Container Platform 4.14 中，您需要访问互联网来安装集群。

您必须具有以下互联网访问权限：

- 访问 OpenShift Cluster Manager 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型的基础架构上执行受限网络安装。在此过程中，您可以下载所需的内容，并使用它为镜像 registry 填充安装软件包。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。在更新集群前，您要更新镜像 registry 的内容。

6.4. 为集群节点 SSH 访问生成密钥对

在 OpenShift Container Platform 安装过程中，您可以为安装程序提供 SSH 公钥。密钥通过它们的 Ignition 配置文件传递给 Red Hat Enterprise Linux CoreOS(RHCOS)节点，用于验证对节点的 SSH 访问。密钥添加到每个节点上 **core** 用户的 **~/.ssh/authorized_keys** 列表中，这将启用免密码身份验证。

将密钥传递给节点后，您可以使用密钥对作为用户 **核心** 通过 SSH 连接到 RHCOS 节点。若要通过 SSH 访问节点，必须由 SSH 为您的本地用户管理私钥身份。

如果要通过 SSH 连接到集群节点来执行安装调试或灾难恢复，则必须在安装过程中提供 SSH 公钥。**./openshift-install gather** 命令还需要在集群节点上设置 SSH 公钥。

重要

不要在生产环境中跳过这个过程，在生产环境中需要灾难恢复和调试。

注意

您必须使用本地密钥，而不是使用特定平台方法配置 的密钥，如 AWS 密钥对。

流程

1. 如果您在本地计算机上没有可用于在集群节点上进行身份验证的现有 SSH 密钥对，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 ed25519 -N '' -f <path>/<file_name> 1
```

1 指定新 SSH 密钥的路径和文件名，如 **~/.ssh/id_ed25519**。如果您已有密钥对，请确保您的公钥位于 **~/.ssh** 目录中。

注意

如果您计划在 **x86_64**、**ppc64le** 和 **s390x** 架构上安装使用 RHEL 加密库（这些加密库已提交给 NIST 用于 FIPS 140-2/140-3 验证）的 OpenShift Container Platform 集群，则不要创建使用 **ed25519** 算法的密钥。相反，创建一个使用 **rsa** 或 **ecdsa** 算法的密钥。

2. 查看公共 SSH 密钥：

```
$ cat <path>/<file_name>.pub
```

例如，运行以下命令来查看 **~/.ssh/id_ed25519.pub** 公钥：

```
$ cat ~/.ssh/id_ed25519.pub
```

3. 将 SSH 私钥身份添加到本地用户的 SSH 代理（如果尚未添加）。在集群节点上，或者要使用 **./openshift-install gather** 命令，需要对该密钥进行 SSH 代理管理，才能在集群节点上进行免密码 SSH 身份验证。

注意

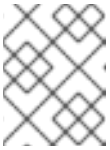
在某些发行版中，自动管理默认 SSH 私钥身份，如 ~/**.ssh/id_rsa** 和 ~/**.ssh/id_dsa**。

a. 如果 **ssh-agent** 进程尚未为您的本地用户运行，请将其作为后台任务启动：

```
$ eval "$(ssh-agent -s)"
```

输出示例

```
Agent pid 31874
```



注意

如果集群处于 FIPS 模式，则只使用 FIPS 兼容算法来生成 SSH 密钥。密钥必须是 RSA 或 ECDSA。

4. 将 SSH 私钥添加到 **ssh-agent** ：

```
$ ssh-add <path>/<file_name> 1
```

1 指定 SSH 私钥的路径和文件名，如 ~/**.ssh/id_ed25519.pub**

输出示例

```
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

后续步骤

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

6.5. 获取安装程序

在安装 OpenShift Container Platform 前，将安装文件下载到您用于安装的主机上。

先决条件

- 您有一台运行 Linux 或 macOS 的计算机，至少有 1.2 GB 本地磁盘空间。

流程

1. 进入 Red Hat Hybrid Cloud Console 上的 Cluster Type 页。如果您有红帽帐户，请使用您的凭证登录。如果没有，请创建一个帐户。
2. 在页的 **Run it yourself** 部分中选择您的基础架构供应商。
3. 从 **OpenShift 安装程序**下的下拉菜单中选择您的主机操作系统和架构，然后点**下载安装程序**。
4. 将下载的文件保存在要存储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几个文件。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。删除集群需要这两个文件。
- 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。要删除集群，请为特定云供应商完成 OpenShift Container Platform 卸载流程。

5. 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 openshift-install-linux.tar.gz
```

6. 从 Red Hat OpenShift Cluster Manager 下载安装 pull secret 。此 pull secret 允许您与所含授权机构提供的服务进行身份验证，这些服务包括为 OpenShift Container Platform 组件提供容器镜像的 Quay.io。

提示

另外，您还可以从红帽客户门户网站检索安装程序，您可以在其中指定要下载的安装程序版本。但是，您需要有一个有效的订阅才能访问此页。

6.5.1. 创建安装配置文件

您可以自定义在 Alibaba Cloud 上安装的 OpenShift Container Platform 集群。

先决条件

- 您有 OpenShift Container Platform 安装程序和集群的 pull secret。

流程

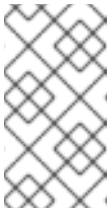
1. 创建 **install-config.yaml** 文件。
   a. 进入包含安装程序的目录并运行以下命令：

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

1 对于 **<installation_directory>**，请指定要存储安装程序创建的文件的目录名称。

在指定目录时：

- 验证该目录是否具有**执行**权限。在安装目录中运行 Terraform 二进制文件需要这个权限。
- 使用空目录。有些安装资产，如 bootstrap X.509 证书的过期间隔较短，因此不得重复使用安装目录。如果要重复使用另一个集群安装中的单个文件，您可以将它们复制到您的目录中。但是，安装资产的文件名可能会在发行版本间有所变化。从以前的 OpenShift Container Platform 版本中复制安装文件时请小心。



注意

始终删除 ~/**.powervs** 目录，以避免重复使用过时的配置。运行以下命令:

```
$ rm -rf ~/.powervs
```

b. 在提示符处，提供云的配置详情：

i. 可选： 选择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。

ii. 选择 **alibabacloud** 作为目标平台。

iii. 选择要将集群部署到的区域。

iv. 选择集群要部署到的基域。基域与您为集群创建的公共 DNS 区对应。

v. 为集群提供一个描述性名称。

2. 将集群安装到 Alibaba Cloud 中需要 Cloud Credential Operator(CCO)以手动模式运行。修改 **install-config.yaml** 文件，将 **credentialsMode** 参数设置为 **Manual** ：

带有 credentialsMode 被设置为 Manual 的 install-config.yaml 配置文件示例

```
apiVersion: v1
baseDomain: cluster1.example.com
credentialsMode: Manual 1
compute:
- architecture: amd64
  hyperthreading: Enabled
 ...
```

1 添加此行，将 **credentialsMode** 设置为 **Manual**。

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

4. 备份 **install-config.yaml** 文件，以便您可以使用它安装多个集群。

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。

其他资源

- Alibaba Cloud 的安装配置参数

6.5.2. Alibaba Cloud 的自定义 install-config.yaml 文件示例

您可以自定义安装配置文件(**install-config.yaml**)，以指定集群平台的更多详情，或修改所需参数的值。

```
apiVersion: v1
baseDomain: alicloud-dev.devcluster.openshift.com
credentialsMode: Manual
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform: {}
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform: {}
  replicas: 3
metadata:
  creationTimestamp: null
  name: test-cluster 1
 networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes 2
  serviceNetwork:
  - 172.30.0.0/16
platform:
  alibabacloud:
    defaultMachinePlatform: 3
      instanceType: ecs.g6.xlarge
      systemDiskCategory: cloud_efficiency
      systemDiskSize: 200
    region: ap-southeast-1 4
    resourceGroupID: rg-acfnw6j3hyai 5
    vpcID: vpc-0xifdjerdibmaqvtjob2b 6
    vswitchIDs: 7
    - vsw-0xi8ycgwc8wv5rhviwdq5
    - vsw-0xiy6v3z2tedv009b4pz2
publish: External
pullSecret: '{"auths": {"cloud.openshift.com": {"auth": ... }' 8
sshKey: |
  ssh-rsa AAAA... 9
```

1. 必需。安装程序会提示您输入集群名称。
2. 要安装的集群网络插件。支持的值有 **OVNKubernetes** 和 **OpenShiftSDN**。默认值为 **OVNKubernetes**。
3. 可选。为没有定义自身平台配置的机器池指定参数。
4. 必需。安装程序会提示您输入要将集群部署到的区域。

5 可选。指定应该安装集群的现有资源组。

8 必需。安装程序会提示您输入 pull secret。

9 可选。安装程序会提示您输入用于访问集群中机器的 SSH 密钥值。

6 7 可选。这些是 vswitchID 值示例。

6.5.3. 生成所需的安装清单

您必须生成 Kubernetes 清单和 Ignition 配置文件，集群需要配置机器。

流程

1. 从包含安装程序的目录中运行以下命令来生成清单：

```
$ openshift-install create manifests --dir <installation_directory>
```

其中：

<installation_directory>
指定安装程序在其中创建文件的目录。

6.5.4. 配置 Cloud Credential Operator 工具

当 Cloud Credential Operator(CCO)以手动模式运行时，要从集群外部创建和管理云凭证，提取并准备 CCO 实用程序(**ccoctl**)二进制文件。

注意

ccoctl 工具是在 Linux 环境中运行的 Linux 二进制文件。

先决条件

- 您可以访问具有集群管理员权限的 OpenShift Container Platform 帐户。
- 已安装 OpenShift CLI(**oc**)。

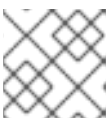
流程

1. 运行以下命令，为 OpenShift Container Platform 发行镜像设置变量：

```
$ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
```

2. 运行以下命令，从 OpenShift Container Platform 发行镜像获取 CCO 容器镜像：

```
$ CCO_IMAGE=$(oc adm release info --image-for='cloud-credential-operator'
$RELEASE_IMAGE -a ~/.pull-secret)
```



注意

确保 **$RELEASE_IMAGE** 的架构与将使用 **ccoctl** 工具的环境架构相匹配。

3. 运行以下命令，将 CCO 容器镜像中的 **ccoctl** 二进制文件提取到 OpenShift Container Platform 发行镜像中：

```
$ oc image extract $CCO_IMAGE --file="/usr/bin/ccoctl" -a ~/.pull-secret
```

4. 运行以下命令更改权限以使 **ccoctl** 可执行：

```
$ chmod 775 ccoctl
```

验证

- 要验证 **ccoctl** 是否准备就绪，可以尝试显示帮助文件。运行命令时使用相对文件名，例如：

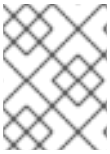
```
$ ./ccoctl.rhel9
```

输出示例

```
OpenShift credentials provisioning tool

Usage:
  ccoctl [command]

Available Commands:
  alibabacloud Manage credentials objects for alibaba cloud
  aws          Manage credentials objects for AWS cloud
  azure        Manage credentials objects for Azure
  gcp          Manage credentials objects for Google cloud
  help         Help about any command
  ibmcloud     Manage credentials objects for IBM Cloud
  nutanix      Manage credentials objects for Nutanix

Flags:
  -h, --help   help for ccoctl

Use "ccoctl [command] --help" for more information about a command.
```

6.5.5. 使用 ccoctl 工具为 OpenShift Container Platform 组件创建凭证

您可以使用 OpenShift Container Platform Cloud Credential Operator(CCO)实用程序自动为每个集群组件创建 Alibaba Cloud RAM 用户和策略。



注意

默认情况下，**ccoctl** 在运行命令的目录中创建对象。要在其他目录中创建对象，请使用 **--output-dir** 标志。此流程使用 **<path_to_ccoctl_output_dir>** 来引用这个目录。

先决条件

您必须：

- 提取并准备好 **ccoctl** 二进制文件。
- 创建具有足够权限来创建 OpenShift Container Platform 集群的 RAM 用户。

- 将 RAM 用户的 AccessKeyID(**access_key_id**)和 AccessKeySecret(**access_key_secret**)添加到本地计算机上的 **~/.alibabacloud/credentials** 文件中。

流程

1. 运行以下命令，使用安装文件中的发行镜像设置 **$RELEASE_IMAGE** 变量：

```
$ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
```

2. 运行以下命令，从 OpenShift Container Platform 发行镜像中提取 **CredentialsRequest** 对象列表：

```
$ oc adm release extract \
  --from=$RELEASE_IMAGE \
  --credentials-requests \
  --included \(1)
  --install-config=<path_to_directory_with_installation_configuration>/install-config.yaml \(2)
  --to=<path_to_directory_for_credentials_requests> (3)
```

(1) **--included** 参数仅包含特定集群配置所需的清单。

(2) 指定 **install-config.yaml** 文件的位置。

(3) 指定要存储 **CredentialsRequest** 对象的目录的路径。如果指定的目录不存在，这个命令会创建它。

注意

此命令可能需要一些时间才能运行。

3. 运行以下命令，使用 **ccoctl** 工具处理所有 **CredentialsRequest** 对象：

a. 运行以下命令使用该工具：

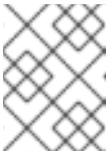
```
$ ccoctl alibabacloud create-ram-users \
  --name <name> \(1)
  --region=<alibaba_region> \(2)
  --credentials-requests-dir=<path_to_credentials_requests_directory> \(3)
  --output-dir=<path_to_ccoctl_output_dir> (4)
```

(1) 指定用于标记创建用于跟踪的任何云资源的名称。

(2) 指定在其中创建云资源的 Alibaba Cloud 区域。

(3) 指定包含组件 **CredentialsRequest** 对象文件的目录。

(4) 指定要放置生成组件凭证 secret 的目录。



注意

如果您的集群使用 **TechPreviewNoUpgrade** 功能集启用的技术预览功能，则必须包含 **--enable-tech-preview** 参数。

输出示例

```
2022/02/11 16:18:26 Created RAM User: user1-alicloud-openshift-machine-api-alibabacloud-credentials
2022/02/11 16:18:27 Ready for creating new ram policy user1-alicloud-openshift-machine-api-alibabacloud-credentials-policy-policy
2022/02/11 16:18:27 RAM policy user1-alicloud-openshift-machine-api-alibabacloud-credentials-policy-policy has created
2022/02/11 16:18:28 Policy user1-alicloud-openshift-machine-api-alibabacloud-credentials-policy-policy has attached on user user1-alicloud-openshift-machine-api-alibabacloud-credentials
2022/02/11 16:18:29 Created access keys for RAM User: user1-alicloud-openshift-machine-api-alibabacloud-credentials
2022/02/11 16:18:29 Saved credentials configuration to: user1-alicloud/manifests/openshift-machine-api-alibabacloud-credentials-credentials.yaml
...
```

注意

RAM 用户可以同时具有两个 accessKeys。如果您运行 **ccoctl alibabacloud create-ram-users** 两次，则之前生成的 manifests secret 将变为过时，您必须重新应用新生成的 secret。

b. 验证 OpenShift Container Platform secret 是否已创建：

```
$ ls <path_to_ccoctl_output_dir>/manifests
```

输出示例

```
openshift-cluster-csi-drivers-alibaba-disk-credentials-credentials.yaml
openshift-image-registry-installer-cloud-credentials-credentials.yaml
openshift-ingress-operator-cloud-credentials-credentials.yaml
openshift-machine-api-alibabacloud-credentials-credentials.yaml
```

您可以通过查询 Alibaba Cloud 来验证是否创建了 RAM 用户和策略。如需更多信息，请参阅 Alibaba Cloud 文档中有关列出 RAM 用户和策略的内容。

4. 将生成的凭证文件复制到目标清单目录中：

```
$ cp ./<path_to_ccoctl_output_dir>/manifests/*credentials.yaml ./<path_to_installation>dir>/manifests/
```

其中：

<path_to_ccoctl_output_dir>

指定 **ccoctl alibabacloud create-ram-users** 命令创建的目录。

<path_to_installation_dir>

指定安装程序在其中创建文件的目录。

6.6. 部署集群

您可以在兼容云平台上安装 OpenShift Container Platform。

重要

在初始安装过程中，您只能运行安装程序的 **create cluster** 命令一次。

先决条件

- 您已使用托管集群的云平台配置了帐户。
- 您有 OpenShift Container Platform 安装程序和集群的 pull secret。
- 已确认主机上的云供应商帐户具有部署集群的正确权限。权限不正确的帐户会导致安装过程失败，并显示包括缺失权限的错误消息。

流程

- 进入包含安装程序的目录并初始化集群部署：

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

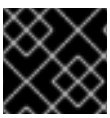
1 对于 **<installation_directory>**，请指定自定义 **./install-config.yaml** 文件的位置。

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

验证

当集群部署成功完成时：

- 终端会显示用于访问集群的说明，包括指向 Web 控制台和 **kubeadmin** 用户的凭证的链接。
- 凭证信息还会输出到 **<installation_directory>/.openshift_install.log**.



重要

不要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。

输出示例

```
...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/home/myuser/install_dir/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-
console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password: "password"
INFO Time elapsed: 36m22s
```

重要

- 安装程序生成的 Ignition 配置文件包含在 24 小时后过期的证书，然后在过期时进行续订。如果在更新证书前关闭集群，且集群在 24 小时后重启，集群会自动恢复过期的证书。一个例外是，您必须手动批准待处理的 **node-bootstrapper** 证书签名请求(CSR)来恢复 kubelet 证书。如需更多信息，*请参阅从过期的 control plane 证书* 中恢复的文档。
- 建议您在 Ignition 配置文件生成后的 12 小时内使用它们，因为 24 小时的证书会在集群安装后的 16 小时到 22 小时间进行轮转。通过在 12 小时内使用 Ignition 配置文件，您可以避免在安装过程中因为执行了证书更新而导致安装失败的问题。

6.7. 通过下载二进制文件安装 OPENSHIFT CLI

您可以安装 OpenShift CLI(**oc**)来使用命令行界面与 OpenShift Container Platform 进行交互。您可以在 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 4.14 中的所有命令。下载并安装新版本的 **oc**。

在 Linux 上安装 OpenShift 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. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **产品变体** 下拉列表中选择架构。
3. 从 **版本** 下拉列表中选择适当的版本。
4. 点 **OpenShift v4.14 Linux Client** 条目旁的 **Download Now** 来保存文件。
5. 解包存档：

```
$ tar xvf <file>
```

6. 将 **oc** 二进制文件放到 **PATH 中的目录中**。
   要查看您的 **PATH**，请执行以下命令：

```
$ echo $PATH
```

验证

- 安装 OpenShift CLI 后，可以使用 **oc** 命令：

```
$ oc <command>
```

在 Windows 上安装 OpenShift CLI

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

流程

1. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **版本** 下拉列表中选择适当的版本。
3. 点 **OpenShift v4.14 Windows Client** 条目旁的 **Download Now** 来保存文件。
4. 使用 ZIP 程序解压存档。
5. 将 **oc** 二进制文件移到 **PATH 中的目录中**。
   要查看您的 **PATH**，请打开命令提示并执行以下命令：

```
C:\> path
```

验证

- 安装 OpenShift CLI 后，可以使用 **oc** 命令：

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

在 macOS 上安装 OpenShift CLI

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

流程

1. 导航到红帽客户门户网站上的 OpenShift Container Platform 下载页面。
2. 从 **版本** 下拉列表中选择适当的版本。
3. 点 **OpenShift v4.14 macOS Client** 条目旁的 **Download Now** 来保存文件。

注意

对于 macOS arm64，请选择 **OpenShift v4.14 macOS arm64 Client** 条目。

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**，请打开终端并执行以下命令：

```
$ echo $PATH
```

验证

- 使用 **oc** 命令验证安装：

```
$ oc <command>
```

6.8. 使用 CLI 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** 文件包含有关集群的信息，供 CLI 用于将客户端连接到正确的集群和 API 服务器。该文件特定于集群，在 OpenShift Container Platform 安装过程中创建。

先决条件

- 已部署 OpenShift Container Platform 集群。
- 已安装 **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. 验证您可以使用导出的配置成功运行 **oc** 命令：

```
$ oc whoami
```

输出示例

```
system:admin
```

/validating-an-installation.adoc

6.9. 使用 WEB 控制台登录到集群

kubeadmin 用户默认在 OpenShift Container Platform 安装后存在。您可以使用 OpenShift Container Platform Web 控制台以 **kubeadmin** 用户身份登录集群。

先决条件

- 有访问安装主机的访问权限。
- 您完成了集群安装，所有集群 Operator 都可用。

流程

1. 从安装主机上的 **kubeadmin -password** 文件中获取 kubeadmin 用户的密码：

```
$ cat <installation_directory>/auth/kubeadmin-password
```

注意

另外，您还可以从安装主机上的 **<installation_directory>/.openshift_install.log** 日志文件获取 **kubeadmin** 密码。

2. 列出 OpenShift Container Platform Web 控制台路由：

```
$ oc get routes -n openshift-console | grep 'console-openshift'
```

注意

另外，您还可以从安装主机上的 **<installation_directory>/.openshift_install.log 日志** 文件获取 OpenShift Container Platform 路由。

输出示例

```
console     console-openshift-console.apps.<cluster_name>.<base_domain>          console
https   reencrypt/Redirect   None
```

3. 在 Web 浏览器中导航到上一命令输出中包括的路由，以 **kubeadmin** 用户身份登录。

6.10. OPENSHIFT CONTAINER PLATFORM 的 TELEMETRY 访问

在 OpenShift Container Platform 4.14 中，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，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 OpenShift Cluster Manager。

确认 OpenShift Cluster Manager 清单正确后，可以由 Telemetry 自动维护，也可以使用 OpenShift Cluster Manager 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。

其他资源

- 有关 Telemetry 服务的更多信息，请参阅关于远程健康监控。
- 如需有关访问和了解 OpenShift Container Platform Web 控制台的更多信息，请参阅访问 Web 控制台

6.11. 后续步骤

- 验证安装.
- 自定义集群。
- 如果需要，您可以选择 不使用远程健康报告。

第 7 章 ALIBABA CLOUD 的安装配置参数

在 Alibaba Cloud 上部署 OpenShift Container Platform 集群前，您可以提供参数来自定义集群和托管它的平台。在创建 **install-config.yaml** 文件时，您可以通过命令行为所需参数提供值。然后，您可以修改 **install-config.yaml** 文件以进一步自定义集群。

7.1. ALIBABA CLOUD 可用的安装配置参数

下表指定您可以在安装过程中设置所需的、可选和特定于 Alibaba Cloud 的安装配置参数。

注意

安装后，您无法在 **install-config.yaml** 文件中修改这些参数。

7.1.1. 所需的配置参数

下表描述了所需的安装配置参数：

表 7.1. 所需的参数

参数	描述	值
apiVersion:	**install-config.yaml** 内容的 API 版本。当前版本为 **v1**。安装程序可能还支持旧的 API 版本。	字符串
baseDomain:	云供应商的基域。基域用于创建到 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**。
metadata:	Kubernetes 资源 **ObjectMeta**，其中只消耗 **name** 参数。	对象
metadata: name:	集群的名称。集群的 DNS 记录是 **{{.metadata.name}}.{{.baseDomain}}** 的子域。	小写字母、连字符(**-**)和句点(**.**)字符串，如 **dev**。

参数	描述	值
platform:	要执行安装的具体平台配置：**alibabacloud**, **aws**, **baremetal**, **azure**, **gcp**, **ibmcloud**, **nutanix**, **openstack**, **powervs**, **vsphere**, or **{}**。有关 **platform.<platform>** 参数的更多信息，请参考下表中您的特定平台。	对象
pullSecret:	从 Red Hat OpenShift Cluster Manager 获取 pull secret，验证从 Quay.io 等服务中下载 OpenShift Container Platform 组件的容器镜像。	`{ "auths":{ "cloud.openshift.com":{ "auth":"b3Blb=", "email":"you@example.com" }, "quay.io":{ "auth":"b3Blb=", "email":"you@example.com" } } }`

7.1.2. 网络配置参数

您可以根据现有网络基础架构的要求自定义安装配置。例如，您可以扩展集群网络的 IP 地址块，或者提供不同于默认值的不同 IP 地址块。

仅支持 IPv4 地址。

注意

Red Hat OpenShift Data Foundation 灾难恢复解决方案不支持 Globalnet。对于区域灾难恢复场景，请确保为每个集群中的集群和服务网络使用非重叠的专用 IP 地址。

表 7.2. 网络参数

参数	描述	值
networking:	集群网络的配置。	对象  **注意** 您无法在安装后修改 **网络** 对象指定的参数。

参数	描述	值
networking: networkType:	要安装的 Red Hat OpenShift Networking 网络插件。	**OpenShiftSDN** 或 **OVNKubernetes**。**OpenShiftSDN** 是 all-Linux 网络的 CNI 插件。**OVNKubernetes** 是 Linux 网络和包含 Linux 和 Windows 服务器的混合网络的 CNI 插件。默认值为 **OVNKubernetes**。
networking: clusterNetwork:	pod 的 IP 地址块。 默认值为 **10.128.0.0/14**，主机前缀为 **/23**。 如果您指定了多个 IP 地址块，块不得重叠。	对象数组。例如： networking: clusterNetwork: - cidr: 10.128.0.0/14 hostPrefix: 23
networking: clusterNetwork: cidr:	使用 **networking.clusterNetwork** 时需要此项。IP 地址块。 IPv4 网络。	无类别域间路由(CIDR)表示法中的 IP 地址块。IPv4 块的前缀长度介于 **0 到 32** 之间。
networking: clusterNetwork: hostPrefix:	分配给每个节点的子网前缀长度。例如，如果 **hostPrefix** 设为 **23**，则每个节点从 given **cidr** 中分配 a **/23** 子网。**hostPrefix** 值 **23** 提供 510（2^(32 - 23)- 2）pod IP 地址。	子网前缀。 默认值为 **23**。
networking: serviceNetwork:	服务的 IP 地址块。默认值为 **172.30.0.0/16**。 OpenShift SDN 和 OVN-Kubernetes 网络插件只支持服务网络的一个 IP 地址块。	CIDR 格式具有 IP 地址块的数组。例如： networking: serviceNetwork: - 172.30.0.0/16
networking: machineNetwork:	机器的 IP 地址块。 如果您指定了多个 IP 地址块，块不得重叠。	对象数组。例如： networking: machineNetwork: - cidr: 10.0.0.0/16

参数	描述	值
networking: machineNetwork: cidr:	使用 **networking.machineNetwork** 时需要此项。IP 地址块。对于 libvirt 和 IBM Power® Virtual Server 以外的所有平台，默认值为 **10.0.0.0/16**。对于 libvirt，默认值 为 **192.168.126.0/24**。对于 IBM Power® Virtual Server，默认值为 **192.168.0.0/24**。	CIDR 表示法中的 IP 网络块。 例如： **10.0.0.0/16**。  **注意** 将 **networking.machineNetwork** 设置为与首选 NIC 所在的 CIDR 匹配。

7.1.3. 可选的配置参数

下表描述了可选的安装配置参数：

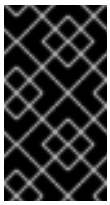
表 7.3. 可选参数

参数	描述	值
additionalTrustBundle:	添加到节点可信证书存储中的 PEM 编码 X.509 证书捆绑包。配置了代理时，也可以使用此信任捆绑包。	字符串
capabilities:	控制可选核心组件的安装。您可以通过禁用可选组件来减少 OpenShift Container Platform 集群的空间。如需更多信息，请参阅 *安装*中的"集群功能"页面。	字符串数组
capabilities: baselineCapabilitySet:	选择要启用的一组初始可选功能。有效值为 **None**、**v4.11**、**v4.12** 和 **vCurrent**。默认值为 **vCurrent**。	字符串
capabilities: additionalEnabledCapabilities:	将可选功能集合扩展到您在 **baselineCapabilitySet** 中指定的范围。您可以在此参数中指定多个功能。	字符串数组

参数	描述	值
cpuPartitioningMode:	启用工作负载分区，它会隔离 OpenShift Container Platform 服务、集群管理工作负载和基础架构 pod，以便在保留的一组 CPU 上运行。工作负载分区只能在安装过程中启用，且在安装后无法禁用。虽然此字段启用工作负载分区，但它不会将工作负载配置为使用特定的 CPU。如需更多信息，请参阅 *Scalability and Performance* 部分中的 *Workload partitioning* 页面。	**None** 或 **AllNodes**。**None** 是默认值。
compute:	组成计算节点的机器的配置。	**MachinePool** 对象的数组。
compute: architecture:	决定池中机器的指令集合架构。目前，不支持具有不同架构的集群。所有池都必须指定相同的架构。有效值为 **amd64**（默认值）。	字符串
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** 如果您禁用并发多线程，请确保您的容量规划考虑机器性能显著降低的情况。	**enabled** 或 **Disabled**
compute: name:	使用 **compute** 时需要此项。机器池的名称。	**worker**
compute: platform:	使用 **compute** 时需要此项。使用此参数指定托管 worker 机器的云供应商。此参数值必须与 **controlPlane.platform** 参数值匹配。	**alibabacloud**, **aws**, **azure**, **gcp**, **ibmcloud**, **nutanix**, **openstack**, **powervs**, **vsphere**, 或 **{}**
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
featureSet:	为功能集启用集群。功能集是 OpenShift Container Platform 功能的集合，默认情况下不启用。有关在安装过程中启用功能集的更多信息，请参阅"使用功能门启用功能"。	字符串.要启用的功能集的名称，如 **TechPreviewNoUpgrade**。
controlPlane:	组成 control plane 的机器的配置。	**MachinePool** 对象的数组。
controlPlane: architecture:	决定池中机器的指令集合架构。目前，不支持具有不同架构的集群。所有池都必须指定相同的架构。有效值为 **amd64** （默认值）。	字符串
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** 如果您禁用并发多线程，请确保您的容量规划考虑机器性能显著降低的情况。	**enabled** 或 **Disabled**
controlPlane: name:	使用 **controlPlane** 时需要此项。机器池的名称。	**master**
controlPlane: platform:	使用 **controlPlane** 时需要此项。使用此参数指定托管 control plane 机器的云供应商。此参数值必须与 **compute.platform** 参数值匹配。	**alibabacloud**, **aws**, **azure**, **gcp**, **ibmcloud**, **nutanix**, **openstack**, **powervs**, **vsphere**, 或 **{}**
controlPlane: replicas:	要置备的 control plane 机器数量。	部署单节点 OpenShift 时支持的值为 **3** 或 **1**。
credentialsMode:	Cloud Credential Operator(CCO)模式。如果没有指定模式，CCO 会动态尝试决定提供的凭证的功能，在支持多个模式的平台上首选 mint 模式。	**Mint**、**Passthrough**、**Manual** 或空字符串(**""**)。[1]

参数	描述	值
fips:	启用或禁用 FIPS 模式。默认值为 **false**（禁用）。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。  **重要** 要为集群启用 FIPS 模式，您必须从配置为以 FIPS 模式操作的 Red Hat Enterprise Linux (RHEL) 计算机运行安装程序。有关在 RHEL 中配置 FIPS 模式的更多信息，请参阅在 FIPS 模式中安装该系统。当以 FIPS 模式运行 Red Hat Enterprise Linux (RHEL) 或 Red Hat Enterprise Linux CoreOS (RHCOS) 时，OpenShift Container Platform 核心组件使用 RHEL 加密库，在 x86_64、ppc64le 和 s390x 架构上提交到 NIST FIPS 140-2/140-3 Validation。  **注意** 如果使用 Azure File 存储，则无法启用 FIPS 模式。	**false** 或 **true**

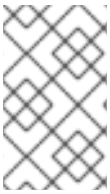
参数	描述	值
imageContentSources:	release-image 内容的源和存储库。	对象数组。包括一个 **source** 以及可选的 **mirrors**，如本表的以下行所述。
imageContentSources: source:	使用 **imageContentSources** 时需要此项。指定用户在镜像拉取规格中引用的存储库。	字符串
imageContentSources: mirrors:	指定可能还包含同一镜像的一个或多个仓库。	字符串数组
publish:	如何发布或公开集群的面向用户的端点，如 Kubernetes API、OpenShift 路由。	**内部或外部 .**默认值为 **External**。 在非云平台上不支持将此字段设置为 **Internal**。  **重要** 如果将字段的值设为 **Internal**，集群将无法运行。如需更多信息，请参阅 BZ#1953035。
sshKey:	用于验证对集群机器的访问的 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。	例如，**sshKey: ssh-ed25519 AAAA..**。

1. 不是所有 CCO 模式都支持所有云供应商。有关 CCO 模式的更多信息，请参阅*身份验证和授权*内容中的"管理云供应商凭证"条目。

7.1.4. 其他 Alibaba Cloud 配置参数

下表描述了其他 Alibaba Cloud 配置参数。**alibabacloud** 参数是在 Alibaba Cloud 上安装时使用的配置。**defaultMachinePlatform** 参数是在 Alibaba Cloud 上安装用于不定义自身平台配置的机器池时使用的默认配置。

这些参数适用于指定的机器和控制平面机器。



注意

如果定义，则参数 **compute.platform.alibabacloud** 和 **controlPlane.platform.alibabacloud** 将分别覆盖计算机器和控制平面机器的 **platform.alibabacloud.defaultMachinePlatform** 设置。

表 7.4. 可选的 Alibaba Cloud 参数

参数	描述	值

compute:
  platform:
 	
alibabacloud:
  imageID:
	用于创建 ECS 实例的 imageID。imageID 必须与集群属于同一区域。	字符串.

compute: platform: alibabacloud: instanceType:	InstanceType 定义 ECS 实例类型。示例： **ecs.g6.large**	字符串.
compute: platform: alibabacloud: systemDiskCategory:	定义系统磁盘的类别。示例： **cloud_efficiency**,**cloud_essd**	字符串.
compute: platform: alibabacloud: systemDisksize:	以 KB (GiB) 为单位定义系统磁盘大小。	整数.

参数	描述	值
compute: platform: alibabacloud: zones:	可以使用的可用区列表。示例： **cn-hangzhou-h**,**cn-hangzhou-j**	字符串列表。
controlPlane: platform: alibabacloud: imageID:	用于创建 ECS 实例的 imageID。imageID 必须与集群属于同一区域。	字符串.
controlPlane: platform: alibabacloud: instanceType:	InstanceType 定义 ECS 实例类型。示例： **ecs.g6.xlarge**	字符串.
controlPlane: platform: alibabacloud: systemDiskCategory:	定义系统磁盘的类别。示例： **cloud_efficiency**,**cloud_essd**	字符串.
controlPlane: platform: alibabacloud: systemDisksize:	以 KB (GiB) 为单位定义系统磁盘大小。	整数.
controlPlane: platform: alibabacloud: zones:	可以使用的可用区列表。示例： **cn-hangzhou-h**,**cn-hangzhou-j**	字符串列表。

参数	描述	值
platform: alibabacloud: region:	必需。创建集群的 Alibaba Cloud 区域。	字符串.
platform: alibabacloud: resourceGroupID:	安装集群的现有资源组的 ID。如果为空，安装程序会为集群创建新资源组。	字符串.
platform: alibabacloud: tags:	应用到为集群创建的所有 Alibaba Cloud 资源的额外键和值。	对象。
platform: alibabacloud: vpcID:	应该安装集群的现有 VPC 的 ID。如果为空，安装程序会为集群创建新 VPC。	字符串.
platform: alibabacloud: vswitchIDs:	创建集群资源的现有 VSwitches 的 ID 列表。现有的 VSwitches 只能在使用现有的 VPC 时使用。如果为空，安装程序会为集群创建新的 VSwitches。	字符串列表。
platform: alibabacloud: defaultMachinePlatform: imageID:	对于计算机器和控制平面机器，应用于创建 ECS 实例的镜像 ID。如果设置，镜像 ID 应该属于与集群相同的区域。	字符串.

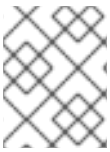
参数	描述	值
platform: alibabacloud: defaultMachinePlatform: instanceType:	对于计算机器和控制平面机器，用于创建 ECS 实例的 ECS 实例类型。示例：**ecs.g6.xlarge**	字符串.
platform: alibabacloud: defaultMachinePlatform: systemDiskCategory:	对于计算机器和控制平面机器，系统磁盘的类别。示例：**cloud_efficiency**,**cloud_essd**.	字符串，如 "", **cloud_efficiency**, **cloud_essd**。
platform: alibabacloud: defaultMachinePlatform: systemDiskSize:	对于计算机器和控制平面机器，以 KB (GiB) 为单位的系统磁盘大小。最小值为 **120**。	整数.
platform: alibabacloud: defaultMachinePlatform: zones:	对于计算机器和控制平面机器，可以使用的可用区列表。示例： **cn-hangzhou-h**,**cn-hangzhou-j**	字符串列表。
platform: alibabacloud: privateZoneID:	现有私有区的 ID，在其中为集群的内部 API 添加 DNS 记录。只有同时使用现有的 VPC 时，才可以使用现有私有区。私有区必须与包含子网的 VPC 关联。将私有区保留为不设置，让安装程序代表您创建私有区。	字符串.

第 8 章 在 ALIBABA CLOUD 上卸载集群

您可以删除部署到 Alibaba Cloud 的集群。

8.1. 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。



注意

卸载后，检查云供应商是否有未正确删除的资源，特别是在用户置备基础架构(UPI)集群中。可能存在安装程序未创建或安装程序无法访问的资源。

先决条件

- 有用于部署集群的安装程序副本。
- 有创建集群时安装程序生成的文件。

流程

1. 在用来安装集群的计算机中包含安装程序的目录中，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**，而不是 **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。