OpenShift Container Platform 4.2

安装

安装并配置 OpenShift Container Platform 4.2 集群

Last Updated: 2020-08-21

OpenShift Container Platform 4.2 安装

安装并配置 OpenShift Container Platform 4.2 集群

法律通告

摘要

本文档提供有关安装和配置 OpenShift Container Platform 4.2 的信息。

目录

第 1 章 收集安装日志

为帮助排查 OpenShift Container Platform 安装失败的问题，您可以从 bootstrap 和 control plane 或 master 机器中收集日志。

先决条件

- 已尝试安装 OpenShift Container Platform 集群，但安装失败。
- 您为安装程序提供了 SSH 密钥，且该密钥已加入到正在运行的 **ss-agent** 进程中。

1.1. 从失败安装中收集日志

如果为安装程序提供了 SSH 密钥，则可以收集与失败安装相关的数据。

注意

用于收集失败安装日志的命令与从正在运行的集群收集日志时所用的命令不同。如果需要从正在运行的集群收集日志，请使用 **oc adm must-gather** 命令。

先决条件

- OpenShift Container Platform 安装在 bootstrap 过程完成前失败。bootstrap 节点必须正在运行，并可通过 SSH 访问。
- **ssh-agent** 进程在您的计算机上处于活跃状态，并且为 **ssh-agent** 进程和安装程序提供了相同的 SSH 密钥。
- 如果尝试在您置备的基础架构中安装集群，则一定需要有 control plane 或 master 机器的完全限定域名。

流程

1. 生成从 bootstrap 和 control plane 机器获取安装日志的命令：
   - 如果使用了安装程序置备的基础架构，请运行以下命令：

     ```
     $ ./openshift-install gather bootstrap --dir=<directory> 1
     ```

     1 **installation_directory** 是安装程序所创建的用来保存 OpenShift Container Platform 定义文件的目录。

     对于安装程序置备的基础架构，安装程序会保存有关集群的信息，因此您不用指定主机名或 IP 地址。

   - 如果使用了您置备的基础架构，请运行以下命令：

     ```
     $ ./openshift-install gather bootstrap --dir=<directory> \ 1
       --bootstrap <bootstrap_address> \ 2
       --master <master_1_address> \ 3
       --master <master_2_address> \ 4
       --master <master_3_address>" 5
     ```

1. **installation_directory** 是安装程序所创建的用来保存 OpenShift Container Platform 定义文件的目录。
2. **<bootstrap_address>** 是集群 bootstrap 机器的完全限定域名或 IP 地址。
3. 4. 5. **<master_address>** 是集群中 control plane 或 master 机器的完全限定域名或 IP 地址。

注意

默认集群包含三个 control plane 机器。如所示，列出所有 control plane 机器，无论集群使用了多少个。

命令输出类似以下示例：

```
INFO Pulling debug logs from the bootstrap machine
INFO Bootstrap gather logs captured here "<directory>/log-bundle-<timestamp>.tar.gz"
```

如果需要创建关安装失败的红帽支持问题单，请在问题单中附上压缩日志。

1.2. 通过到主机的 SSH 连接手动收集日志

在 **must-gather** 或自动收集方法无法正常工作的情况下手动收集日志。

先决条件

- 必须有到主机的 SSH 访问权限。

流程

1. 运行以下命令，使用 **journalctl** 命令从 bootstrap 主机收集 **bootkube.service** 服务日志：

```
$ journalctl -b -f -u bootkube.service
```

2. 使用 Podman 的 logs 命令收集 bootstrap 主机的容器日志。以下命令从主机获取所有容器的日志：

```
$ for pod in $(sudo podman ps -a -q); do sudo podman logs $pod; done
```

3. 或者，通过运行以下命令来使用 **tail** 命令收集主机的容器日志：

```
# tail -f /var/lib/containers/storage/overlay-containers/*/userdata/ctr.log
```

4. 运行 **journalctl** 命令从 master 和 worker 主机收集 **kubelet.service** 和 **crio.service** 服务日志：

```
$ journalctl -b -f -u kubelet.service -u crio.service
```

5. 使用 **tail** 命令收集 master 和 worker 主机容器日志：

```
$ sudo tail -f /var/log/containers/*
```

1.3. 在不使用 SSH 连接到主机的情况下手动收集日志

在 **must-gather** 或自动收集方法无法正常工作的情况下手动收集日志。

如果您无法对节点进行 SSH 访问，则可以通过访问系统日志来调查主机上发生的情况。

先决条件

- OpenShift Container Platform 安装已完成。
- API 服务仍然可以正常工作。
- 有系统管理员特权。

流程

1. 通过运行以下命令访问 **/var/log** 中的 **journald** 单元日志：

```
$ oc adm node-logs --role=master -u kubelet
```

2. 通过运行以下命令访问 **/var/log** 中的主机文件路径：

```
$ oc adm node-logs --role=master --path=openshift-apiserver
```

第 2 章 安装配置

2.1. 不同平台的安装方法

您可以在不同的平台上执行不同类型的安装。

表 2.1. 安装程序置备的基础架构选项

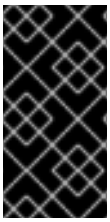
	AWS	Azure	GCP	OpenStack	裸机	vSphere	IBM Z
Default	X	X	X				
Custom	X	X	X	X			
Cluster Network Operator	X	X	X				

表 2.2. 用户置备的基础架构

	AWS	Azure	GCP	OpenStack	裸机	vSphere	IBM Z
Custom	X		X		X	X	X
Cluster Network Operator					X	X	
Restricted network	X				X	X	

2.2. 创建用于在受限网络中安装的镜像 REGISTRY

在受限网络中置备的基础架构上安装集群前，您必须创建镜像 registry。在受限网络中安装仅支持您置备的基础架构，不支持安装程序置备的基础架构。



重要

您必须有权访问互联网，才能获取填充镜像存储库的数据。在这一流程中，您要将镜像 registry 放在可访问您的网络以及互联网的堡垒（bastion）主机上。如果您没有堡垒主机的访问权限，请使用最适合您的限制条件的方法将镜像 registry 的内容提取到受限网络中。

2.2.1. 关于镜像 registry

您可以镜像 OpenShift Container Platform registry 的内容，也可以镜像生成安装程序所需的镜像。

镜像 registry 是一个关键组件，有了它才能在受限网络中完成安装。您可以在堡垒主机上创建此镜像，该主机可同时访问互联网和您的封闭网络，也可以使用满足您的限制条件的其他方法。

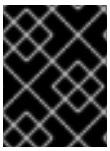
由于 OpenShift Container Platform 验证发行版本有效负载完整性的方式，您的本地 registry 中的镜像引用与红帽在 Quay.io 上托管的镜像相同。在安装的 bootstrap 过程中，不论镜像是从哪个存储库提取的，镜像都必须有相同的摘要。要确保发行版有效负载一致，请将镜像镜像到您的本地存储库。

2.2.2. 准备堡垒主机

在创建镜像 registry 前，您必须准备堡垒主机。

2.2.2.1. 安装 CLI

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



重要

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

流程

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

注意

您可在 Linux、Windows 或 macOS 上安装 **oc**。

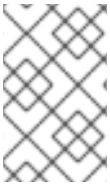
3. 将文件保存到文件系统。
4. 展开压缩文件。
5. 把它放到 **PATH** 中的一个目录下。

安装 CLI 后，就可以使用**oc**命令：

```
$ oc <command>
```

2.2.3. 创建镜像 registry

创建 registry 来托管安装 OpenShift Container Platform 所需的镜像内容。要在受限网络中安装，您必须将镜像放在您的堡垒主机上。



注意

以下流程创建一个简单的 registry，它可在 **/opt/registry** 文件夹中保存数据并在 **podman** 容器中运行。您可以使用不同的 registry 解决方案，例如 Red Hat Quay。检查以下流程以确保 registry 可以正常工作。

先决条件

- 网络上有一个 Red Hat Enterprise Linux (RHEL) 服务器充当 registry 主机。
- registry 主机可以访问互联网。

流程

在堡垒主机上，执行以下操作：

1. 安装所需的软件包：

```
# yum -y install podman httpd-tools
```

podman 软件包提供容器软件包，用于运行 registry。**httpd-tools** 软件包提供 **htpasswd** 实用程序，用于创建用户。

2. 为 registry 创建文件夹：

```
# mkdir -p /opt/registry/{auth,certs,data}
```

这些文件夹挂载到 registry 容器中。

3. 为 registry 提供证书。如果您没有现有的可信证书颁发机构，您可以生成自签名证书：

```
$ cd /opt/registry/certs
# openssl req -newkey rsa:4096 -nodes -sha256 -keyout domain.key -x509 -days 365 -out
domain.crt
```

在提示符处，为证书提供所需的值：

国家/地区名称（双字母代码）	指定您所在位置的双字母 ISO 国家/地区代码。请参见 ISO 3166 国家/地区代码标准。
州或省名称（完整名称）	输入您的州或省的完整名称。
本地名称（例如，城市）	输入您的城市名称。
机构名称（例如，公司）	输入公司的名称。
组织单元名称（例如，部门）	输入您的部门名称。

通用名称（例如，您的名字或服务器主机名）	输入 registry 主机的主机名。确保您的主机名在 DNS 中，并且解析为预期的 IP 地址。
电子邮件地址	输入您的电子邮件地址。如需了解更多信息，请参阅 OpenSSL 文档中的 req 说明。

4. 为 registry 生成使用 **bcrpt** 格式的用户名和密码：

```
# htpasswd -bBc /opt/registry/auth/htpasswd <user_name> <password> 1
```

1 将 **<user_name>** 和 **<password>** 替换为用户名和密码。

5. 创建 **mirror-registry** 容器以托管 registry：

```
# podman run --name mirror-registry -p <local_registry_host_port>:5000 \ 1
    -v /opt/registry/data:/var/lib/registry:z \
    -v /opt/registry/auth:/auth:z \
    -e "REGISTRY_AUTH=htpasswd" \
    -e "REGISTRY_AUTH_HTPASSWD_REALM=Registry Realm" \
    -e REGISTRY_AUTH_HTPASSWD_PATH=/auth/htpasswd \
    -v /opt/registry/certs:/certs:z \
    -e REGISTRY_HTTP_TLS_CERTIFICATE=/certs/domain.crt \
    -e REGISTRY_HTTP_TLS_KEY=/certs/domain.key \
    -e REGISTRY_COMPATIBILITY_SCHEMA1_ENABLED=true \
    -d docker.io/library/registry:2
```

1 对于 **<local_registry_host_port>**，请指定您的镜像 registry 用于提供内容的端口。

6. 为 registry 打开所需的端口：

```
# firewall-cmd --add-port=<local_registry_host_port>/tcp --zone=internal --permanent 1
# firewall-cmd --add-port=<local_registry_host_port>/tcp --zone=public   --permanent 2
# firewall-cmd --reload
```

1 2 对于 **<local_registry_host_port>**，请指定您的镜像 registry 用于提供内容的端口。

7. 将自签名证书添加到您的可信证书列表中：

```
# cp /opt/registry/certs/domain.crt /etc/pki/ca-trust/source/anchors/
# update-ca-trust
```

您必须信任您的证书，才能在镜像过程中登录到 registry。

8. 确认 registry 可用：

```
$ curl -u <user_name>:<password> -k https://<local_registry_host_name>:
<local_registry_host_port>/v2/_catalog 1
```

```
{"repositories":[]}
```

1. 对于 **<user_name>** 和 **<password>**，指定 registry 的用户名和密码。对于 **<local_registry_host_name>**，请指定在您的证书中指定的 registry 域名，如 **registry.example.com**。对于 **<local_registry_host_port>**，请指定您的镜像 registry 用于提供内容的端口。

如果命令输出显示一个空存储库，则您的 registry 已经可用。

2.2.4. 在 pull secret 中添加 registry

在受限网络中安装 OpenShift Container Platform 集群前，需要为 OpenShift Container Platform 集群修改 pull secret 来使用本地 registry。

先决条件

- 配置了一个镜像（mirror） registry 在受限网络中使用。

流程

在堡垒主机上完成以下步骤：

1. 从 Red Hat OpenShift Cluster Manager 站点的 Pull Secret 页面下载 **registry.redhat.io** 的 pull secret。
2. 为您的镜像 registry 生成 base64 编码的用户名和密码或令牌：

```
$ echo -n '<user_name>:<password>' | base64 -w0 1

BGVtbYk3ZHAtqXs=
```

1. 通过 **<user_name>** 和 **<password>** 指定 registry 的用户名和密码。

3. 以 JSON 格式创建您的 pull secret 副本：

```
$ cat ./pull-secret.text | jq .  > <path>/<pull-secret-file> 1
```

1. 指定到存储 pull secret 的文件夹的路径，以及您创建的 JSON 文件的名称。

该文件类似于以下示例：

```
{
  "auths": {
    "cloud.openshift.com": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
    "quay.io": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
    "registry.connect.redhat.com": {
```

```
    "auth": "NTE3Njg5Nj...",
    "email": "you@example.com"
  },
  "registry.redhat.io": {
    "auth": "NTE3Njg5Nj...",
    "email": "you@example.com"
  }
 }
}
```

4. 编辑新文件并添加描述 registry 的部分：

```
 "auths": {
...
   "<local_registry_host_name>:<local_registry_host_port>": {  (1)
    "auth": "<credentials>",  (2)
    "email": "you@example.com"
 },
...
```

(1) 使用 **<local_registry_host_name>** 指定您证书中指定的 registry 域名，使用 **<local_registry_host_port>** 指定镜像 registry 用来提供内容的端口。

(2) 使用 **<credentials>** 为您生成的镜像 registry 指定 base64 编码的用户名和密码。

该文件类似于以下示例：

```
{
 "auths": {
  "cloud.openshift.com": {
   "auth": "b3BlbnNo...",
   "email": "you@example.com"
  },
  "quay.io": {
   "auth": "b3BlbnNo...",
   "email": "you@example.com"
  },
  "registry.connect.redhat.com": {
   "auth": "NTE3Njg5Nj...",
   "email": "you@example.com"
  },
  "<local_registry_host_name>:<local_registry_host_port>": {
   "auth": "<credentials>",
   "email": "you@example.com"
  },
  "registry.redhat.io": {
   "auth": "NTE3Njg5Nj...",
   "email": "you@example.com"
  }
 }
}
```

2.2.5. 镜像 OpenShift Container Platform 镜像存储库

镜像要在集群安装或升级过程中使用的 OpenShift Container Platform 镜像存储库。

先决条件

- 您已将镜像 registry 配置为在受限网络中使用，并可访问您配置的证书和凭证。
- 您已从 Red Hat OpenShift Cluster Manager 站点的 Pull Secret 页面下载了 pull secret，并已修改为包含镜像存储库身份验证信息。

流程

在堡垒主机上完成以下步骤：

1. 查看 OpenShift Container Platform 下载页面，以确定您要安装的 OpenShift Container Platform 版本。
2. 设置所需的环境变量：

```
$ export OCP_RELEASE=<release_version> 1
$ export LOCAL_REGISTRY='<local_registry_host_name>:<local_registry_host_port>' 2
$ export LOCAL_REPOSITORY='<repository_name>' 3
$ export PRODUCT_REPO='openshift-release-dev' 4
$ export LOCAL_SECRET_JSON='<path_to_pull_secret>' 5
$ export RELEASE_NAME="ocp-release" 6
```

1. 对于 **<release_version>**，请指定要安装的 OpenShift Container Platform 版本号，如 **4.2.0**。
2. 对于 **<local_registry_host_name>**，请指定镜像存储库的 registry 域名；对于 **<local_registry_host_port>**，请指定用于提供内容的端口。
3. 对于 **<repository_name>**，请指定要在 registry 中创建的存储库名称，如 **ocp4/openshift4**。
4. 要镜像的存储库。对于生产环境版本，必须指定 **openshift-release-dev**。
5. 对于 **<path_to_pull_secret>**，请指定您创建的镜像 registry 的 pull secret 的绝对路径和文件名。
6. 发行版本镜像。对于生产环境版本，您必须指定 **ocp-release**。

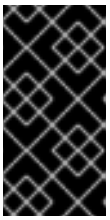
3. 镜像存储库：

```
$ oc adm -a ${LOCAL_SECRET_JSON} release mirror \
    --from=quay.io/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE} \
    --to=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY} \
    --to-release-image=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}
```

该命令将发行信息提取为摘要，其输出包括安装集群时所需的 **imageContentSources** 数据。

4. 记录上一命令输出中的 **imageContentSources** 部分。您的镜像信息与您的镜像存储库相对应，您必须在安装过程中将 **imageContentSources** 部分添加到 **install-config.yaml** 文件中。
5. 要创建基于您镜像内容的安装程序，请提取内容并将其固定到发行版中：

```
$ oc adm -a ${LOCAL_SECRET_JSON} release extract --command=openshift-install
"${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}"
```



重要

要确保将正确的镜像用于您选择的 OpenShift Container Platform 版本，您必须从镜像内容中提取安装程序。

您必须在有活跃互联网连接的机器上执行这个步骤。

2.2.6. 使用带有备用或经过镜像的 registry 的 Samples Operator 镜像流

OpenShift 命名空间中大多数由 Samples Operator 管理的镜像流指向位于 registry.redhat.io 上红帽 registry 中的镜像。镜像功能不适用于这些镜像流。

重要

jenkins、**jenkins-agent-maven** 和 **jenkins-agent-nodejs** 镜像流的确来自安装有效负载，并由 Samples Operator 管理，因此这些镜像流不需要进一步的镜像操作。

将 Sample Operator 配置文件中的 **samplesRegistry** 字段设置为 registry.redhat.io 有很多冗余，因为它已经定向到 registry.redhat.io，只用于 Jenkins 镜像和镜像流。它还会破坏 Jenkins 镜像流的安装有效负载。

Samples Operator 禁止将以下 registry 用于 Jenkins 镜像流：

- docker.io
- registry.redhat.io
- registry.access.redhat.com
- *.quay.io

注意

cli、**installer**、**must-gather** 和 **test** 镜像流虽然属于安装有效负载的一部分，但不由 Samples Operator 管理。此流程中不涉及这些镜像流。

先决条件

- 使用具有 **cluster-admin** 角色的用户访问集群。
- 为您的镜像 registry 创建 pull secret。

流程

1. 访问被镜像（mirror）的特定镜像流的镜像，例如：

```
$ oc get is <imagestream> -n openshift -o json | jq .spec.tags[].from.name | grep
registry.redhat.io
```

2. 将 registry.redhat.io 中与您在受限网络环境中需要的任何镜像流关联的镜像，镜像 (mirror) 成一个定义的镜像 (mirror)：

```
$ oc image mirror registry.redhat.io/rhscl/ruby-25-rhel7:latest ${MIRROR_ADDR}/rhscl/ruby-25-rhel7:latest
```

3. 在集群的镜像配置对象中，为镜像添加所需的可信 CA：

```
$ oc create configmap registry-config --from-file=${MIRROR_ADDR_HOSTNAME}..5000=$path/ca.crt -n openshift-config
$ oc patch image.config.openshift.io/cluster --patch '{"spec":{"additionalTrustedCA":{"name":"registry-config"}}}' --type=merge
```

4. 更新 Samples Operator 配置对象中的 **samplesRegistry** 字段，使其包含镜像配置中定义的镜像位置的 **hostname** 部分：

```
$ oc get configs.samples.operator.openshift.io -n openshift-cluster-samples-operator
```

注意

这是必要的，因为镜像流导入过程在此刻不使用镜像（mirro）或搜索机制。

5. 将所有未镜像的镜像流添加到 Samples Operator 配置对象的 **skippedImagestreams** 字段。或者，如果您不想支持任何示例镜像流，请在 Samples Operator 配置对象中将 Samples Operator 设置为 **Removed**。

注意

镜像流导入失败两小时后，任何没有跳过的未镜像的镜像流，或者如果 Samples Operator 没有更改为 **Removed**，都会导致 Samples Operator 报告 **Degraded** 状态。

OpenShift 命名空间中的多个模板都引用镜像流。因此，使用 **Removed** 清除镜像流和模板，将避免在因为缺少镜像流而导致镜像流和模板无法正常工作时使用它们。

后续步骤

- 在您在受限网络中置备的基础架构上安装集群，如 VMware vSphere、裸机或 Amazon Web Services。

2.3. 可用的集群自定义

大多数集群配置和自定义在 OpenShift Container Platform 集群部署后完成。有若干*配置资源*可用。

注意

如果在 IBM Z 上安装集群，则不是所有功能都可用。详情请查看发行注记 。

您可以修改配置资源来配置集群的主要功能，如镜像 registry、网络配置、镜像构建操作以及用户身份供应商。

如需设置这些资源的当前信息，请使用 **oc explain** 命令，如 **oc explain builds --api-version=config.openshift.io/v1**

2.3.1. 集群配置资源

所有集群配置资源都作用于全局范围（而非命名空间），且命名为 **cluster**。

资源名称	描述
apiserver.config.openshift.io	提供 api-server 配置，如证书和证书颁发机构。
authentication.config.openshift.io	控制集群的用户身份供应商和验证配置。
build.config.openshift.io	控制集群中所有构建的默认和强制配置。
console.config.openshift.io	配置 Web 控制台界面的行为，包括注销行为。
featuregate.config.openshift.io	启用 FeatureGates，以便您能使用技术预览功能。
image.config.openshift.io	配置应如何对待特定的镜像 registry（允许、禁用、不安全、CA 详情）。
ingress.config.openshift.io	与路由相关的配置详情，如路由的默认域。
oauth.config.openshift.io	配置用户身份供应商，以及与内部 OAuth 服务器流程相关的其他行为。
project.config.openshift.io	配置项目的创建方式，包括项目模板。
proxy.config.openshift.io	定义需要外部网络访问的组件要使用的代理。注意：目前不是所有组件都会消耗这个值。
scheduler.config.openshift.io	配置调度程序行为，如策略和默认节点选择器。

2.3.2. Operator 配置资源

这些配置资源是集群范围的实例，即 **cluster**，控制归特定 Operator 所有的特定组件的行为。

资源名称	描述
console.operator.openshift.io	控制控制台外观，如品牌定制

资源名称	描述
config.imageregistry.operator.openshift.io	配置内部镜像 registry 设置，如公共路由、日志级别、代理设置、资源约束、副本数和存储类型。
config.samples.operator.openshift.io	配置 Samples Operator，以控制在集群上安装哪些镜像流和模板示例。

2.3.3. 其他配置资源

这些配置资源代表一个特定组件的单一实例。在有些情况下，您可以通过创建多个资源实例来请求多个实例。在其他情况下，Operator 只消耗指定命名空间中的特定资源实例名称。如需有关如何和何时创建其他资源实例的详情，请参考具体组件的文档。

资源名称	实例名称	命名空间	描述
alertmanager.monitoring.coreos.com	main	openshift-monitoring	控制 alertmanager 部署参数。
ingresscontroller.operator.openshift.io	default	openshift-ingress-operator	配置 Ingress Operator 行为，如域、副本数、证书和控制器放置。

2.3.4. 信息资源

可以使用这些资源检索集群信息。请不要直接编辑这些资源。

资源名称	实例名称	描述
clusterversion.config.openshift.io	version	在 OpenShift Container Platform 4.2 中，不得自定义生产集群的 ClusterVersion 资源，而应遵循相关流程来更新集群。
dns.config.openshift.io	cluster	无法修改集群的 DNS 设置。您可以查看 DNS Operator 状态。
infrastructure.config.openshift.io	cluster	允许集群与其云供应商交互的配置详情。
network.config.openshift.io	cluster	无法在安装后修改集群网络。要自定义您的网络，请遵循相关的流程在安装过程中自定义联网。

2.4. 配置防火墙

如果使用防火墙，您必须进行配置，以便 OpenShift Container Platform 能访问正常运作所需要的网站。您必须始终授予一些站点的访问权限，如果使用 Red Hat Insights、Telemetry 服务、托管集群的云以及某些构建策略，则还要授予更多站点的访问权限。

2.4.1. 为 OpenShift Container Platform 配置防火墙

在安装 OpenShift Container Platform 之前，您必须配置防火墙，以授予 OpenShift Container Platform 所需站点的访问权限。

流程

1. 将以下 registry URL 列入白名单：

URL	功能
registry.redhat.io	提供核心容器镜像
***.quay.io**	提供核心容器镜像
sso.redhat.com	**https://cloud.redhat.com/openshift** 站点使用 **sso.redhat.com** 提供的身份验证

2. 将提供构建所需语言或框架的资源的任何站点列入白名单。

3. 如果不禁用 Telemetry，您必须授予对以下 URL 的访问权限，以便能访问 Red Hat Insights：

URL	功能
cert-api.access.redhat.com	Telemetry 所需
api.access.redhat.com	Telemetry 所需
infogw.api.openshift.com	Telemetry 所需
https://cloud.redhat.com/api/ingress	Telemetry 和 **insights-operator** 需要

4. 如果使用 Amazon Web Services (AWS)、Microsoft Azure 或 Google Cloud Platform (GCP) 来托管您的集群，您必须授予对提供该云的云供应商 API 和 DNS 的 URL 的访问权限：

云	URL	功能
AWS	***.amazonaws.com**	需要此项以访问 AWS 服务和资源。请参阅 AWS 文档中 AWS Service Endpoints，以确定您使用的区域所允许的具体端点。

云	URL	功能
GCP	***.googleapis.com**	需要此项以访问 GCP 服务和资源。请参阅 GCP 文档中的 Cloud Endpoints，以确定您的 API 所允许的端点。
	accounts.google.com	需要此项以访问您的 GCP 帐户。
Azure	**management.azure.com**	需要此项以访问 Azure 服务和资源。请参阅 Azure 文档中的Azure REST API 参考，以确定您的 API 所允许的端点。

5. 将以下 URL 列入白名单：

URL	功能
mirror.openshift.com	需要此项以访问镜像安装内容和镜像
***.apps.<cluster_name>.<base_domain>**	需要此项以访问默认的集群路由，除非您在安装过程中设置了入口通配符
quay-registry.s3.amazonaws.com	需要此项以访问 AWS 中的 Quay 镜像内容
api.openshift.com	需要此项以检查集群是否有可用的更新
art-rhcos-ci.s3.amazonaws.com	需要此项以下载 Red Hat Enterprise Linux CoreOS (RHCOS) 镜像
api.openshift.com	集群令牌所需
cloud.redhat.com/openshift	集群令牌所需