



# 安装概述

## Astra Control Center

NetApp  
November 21, 2023

# 目录

安装概述 .....	1
使用标准流程安装 Astra 控制中心 .....	1
使用 OpenShift OperatorHub 安装 Astra 控制中心 .....	31
使用 Cloud Volumes ONTAP 存储后端安装 Astra 控制中心 .....	39
安装后配置Astra控制中心 .....	53

# 安装概述

选择并完成以下 Astra 控制中心安装过程之一：

- "使用标准流程安装 Astra 控制中心"
- "（如果使用 Red Hat OpenShift）使用 OpenShift OperatorHub 安装 Astra 控制中心"
- "使用 Cloud Volumes ONTAP 存储后端安装 Astra 控制中心"

根据您的环境、安装Astra控制中心后可能需要进行其他配置：

- "安装后配置Astra控制中心"

## 使用标准流程安装 Astra 控制中心

要安装Astra控制中心、请从NetApp 支持站点 下载安装包并执行以下步骤。您可以使用此操作在互联网连接或通风环境中安装 Astra 控制中心。

其他安装过程

- 使用**Red Hat OpenShift OperatorHub**安装：使用此 "备用操作步骤" 使用OperatorHub在OpenShift上安装Astra控制中心。
- 使用**Cloud Volumes ONTAP** 后端在公有云中安装：使用 "这些过程" 在带有Cloud Volumes ONTAP 存储后端的Amazon Web Services (AWS)、Google云平台(GCP)或Microsoft Azure中安装Astra控制中心。

有关Astra控制中心安装过程的演示、请参见 "此视频"。

开始之前

- "开始安装之前，请为 Astra Control Center 部署准备您的环境"。
- 如果您已在环境中配置或希望配置POD安全策略、请熟悉POD安全策略及其对Astra Control Center安装的影响。请参见 "了解POD安全策略限制"。
- 确保所有 API 服务均处于运行状况良好且可用：

```
kubectl get apiservices
```

- 确保您计划使用的Astra FQDN可路由到此集群。这意味着您的内部 DNS 服务器中有一个 DNS 条目，或者您正在使用已注册的核心 URL 路由。
- 如果集群中已存在证书管理器、则需要执行某些操作 "前提条件步骤" 这样、Astra控制中心就不会尝试安装自己的证书管理器。默认情况下、Astra控制中心会在安装期间安装自己的证书管理器。



在第三个容错域或二级站点中部署A作用力控制中心。对于应用程序复制和无缝灾难恢复、建议执行此操作。

关于此任务

Astra控制中心安装过程可帮助您执行以下操作：

- 将Astra组件安装到中 `netapp-acc` (或自定义命名的)命名空间。
- 创建默认的Astra Control所有者管理员帐户。
- 建立管理用户电子邮件地址和默认初始设置密码。系统会为此用户分配首次登录到UI所需的所有者角色。
- 确定所有Astra控制中心Pod均正在运行。
- 安装Astra控制中心UI。



请勿删除Astra Control Center运算符(例如、`kubectl delete -f astra_control_center_operator_deploy.yaml`)、以避免删除Pod。

## 步骤

要安装 Astra 控制中心，请执行以下步骤：

- [下载并提取Astra控制中心](#)
- [安装NetApp Astra kubectl插件](#)
- [\[将映像添加到本地注册表\]](#)
- [\[为具有身份验证要求的注册表设置命名空间和密钥\]](#)
- [安装 Astra 控制中心操作员](#)
- [配置 Astra 控制中心](#)
- [完成 Astra 控制中心和操作员安装](#)
- [\[验证系统状态\]](#)
- [\[设置传入以进行负载平衡\]](#)
- [登录到 Astra 控制中心 UI](#)

## 下载并提取Astra控制中心

1. 转至 "[Astra Control Center下载页面](#)" 页面。
2. 下载包含Astra Control Center的软件包 (`astra-control-center-[version].tar.gz`) 。
3. (建议但可选)下载Astra控制中心的证书和签名包 (`astra-control-center-certs-[version].tar.gz`)以验证捆绑包的签名：

```
tar -vxzf astra-control-center-certs-[version].tar.gz
```

```
openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub  
-signature certs/astra-control-center-[version].tar.gz.sig astra-  
control-center-[version].tar.gz
```

此时将显示输出 `Verified OK` 验证成功后。

#### 4. 从Astra Control Center捆绑包中提取映像：

```
tar -vxzf astra-control-center-[version].tar.gz
```

## 安装NetApp Astra kubectl插件

您可以使用NetApp Astra kubectl命令行插件将映像推送到本地Docker存储库。

### 开始之前

NetApp可为不同的CPU架构和操作系统提供插件二进制文件。在执行此任务之前、您需要了解您的CPU和操作系统。

如果您已从先前安装中安装了插件、"[确保您已安装最新版本](#)" 在完成这些步骤之前。

### 步骤

1. 列出可用的NetApp Astra kubectl插件二进制文件、并记下操作系统和CPU架构所需的文件名称：



kubectl插件库是tar包的一部分、并会解压缩到文件夹中 `kubectl-astra`。

```
ls kubectl-astra/
```

2. 将正确的二进制文件移动到当前路径并重命名为 `kubectl-astra`：

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

## 将映像添加到本地注册表

1. 为容器引擎完成相应的步骤顺序：

## Docker

1. 更改为tarball的根目录。您应看到此文件和目录：

```
acc.manifest.bundle.yaml
acc/
```

2. 将Astra Control Center映像目录中的软件包映像推送到本地注册表。在运行之前、请进行以下替换push-images 命令：

- 将<BUNDLE\_FILE> 替换为Astra Control捆绑包文件的名称 (acc.manifest.bundle.yaml) 。
- 将<MY\_FULL\_REGISTRY\_PATH> 替换为Docker存储库的URL；例如 "<a href="https://<docker-registry>" class="bare">https://<docker-registry>"</a>。
- 将<MY\_REGISTRY\_USER> 替换为用户名。
- 将<MY\_REGISTRY\_TOKEN> 替换为注册表的授权令牌。

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

## Podman

1. 更改为tarball的根目录。您应看到此文件和目录：

```
acc.manifest.bundle.yaml
acc/
```

2. 登录到注册表：

```
podman login <YOUR_REGISTRY>
```

3. 准备并运行以下针对您使用的Podman版本自定义的脚本之一。将<MY\_FULL\_REGISTRY\_PATH> 替换为包含任何子目录的存储库的URL。

```
<strong>Podman 4</strong>
```

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

**Podman 3**

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



根据您的注册表配置、此脚本创建的映像路径应类似于以下内容：

```

https://netappdownloads.jfrog.io/docker-astra-control-
prod/netapp/astra/acc/23.04.2-7/image:version

```

## 为具有身份验证要求的注册表设置命名空间和密钥

1. 导出Astra控制中心主机集群的KUBECONFIG：

```
export KUBECONFIG=[file path]
```



在完成安装之前、请确保您的KUBECONFIG指向要安装Astra控制中心的集群。KUBECONFIG只能包含一个上下文。

2. 如果您使用的注册表需要身份验证，则需要执行以下操作：

a. 创建 netapp-acc-operator 命名空间：

```
kubectl create ns netapp-acc-operator
```

响应：

```
namespace/netapp-acc-operator created
```

b. 为创建密钥 netapp-acc-operator 命名空间。添加 Docker 信息并运行以下命令：



占位符 `your_registry_path` 应与您先前上传的映像的位置匹配(例如、`[Registry_URL]/netapp/astra/astracc/23.04.2-7`)。

```
kubectl create secret docker-registry astra-registry-cred -n netapp-acc-operator --docker-server=[your_registry_path] --docker-username=[username] --docker-password=[token]
```

响应示例：

```
secret/astra-registry-cred created
```



如果在生成密钥后删除命名空间、请重新创建命名空间、然后重新生成命名空间的密钥。

c. 创建 netapp-acc (或自定义命名的)命名空间。

```
kubectl create ns [netapp-acc or custom namespace]
```

响应示例：

```
namespace/netapp-acc created
```



- d. 为创建密钥 `netapp-acc` (或自定义命名的)命名空间。添加 Docker 信息并运行以下命令：

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-acc or custom namespace] --docker-server=[your_registry_path] --docker-username=[username] --docker-password=[token]
```

响应

```
secret/astra-registry-cred created
```

## 安装 Astra 控制中心操作员

1. 更改目录：

```
cd manifests
```

2. 编辑Astra控制中心操作员部署YAML (`astra_control_center_operator_deploy.yaml`)以引用您的本地注册表和密钥。

```
vim astra_control_center_operator_deploy.yaml
```



以下步骤将提供一个标注的YAML示例。

- a. 如果您使用的注册表需要身份验证、请替换的默认行 `imagePullSecrets: []` 使用以下命令：

```
imagePullSecrets: [{name: astra-registry-cred}]
```

- b. 更改 `[your_registry_path]`。 `kube-rbac-proxy` 将映像推送到注册表路径中 [上一步](#)。
- c. 更改 `[your_registry_path]`。 `acc-operator-controller-manager` 将映像推送到注册表路径中 [上一步](#)。

```
<strong>astra_control_center_operator_deploy.yaml</strong>
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
```

```

namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
        - args:
            - --secure-listen-address=0.0.0.0:8443
            - --upstream=http://127.0.0.1:8080/
            - --logtostderr=true
            - --v=10
          image: [your_registry_path]/kube-rbac-proxy:v4.8.0
          name: kube-rbac-proxy
          ports:
            - containerPort: 8443
              name: https
        - args:
            - --health-probe-bind-address=:8081
            - --metrics-bind-address=127.0.0.1:8080
            - --leader-elect
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
            - name: ACCOP_HELM_INSTALLTIMEOUT
              value: 5m
          image: [your_registry_path]/acc-operator:23.04.36
          imagePullPolicy: IfNotPresent
          livenessProbe:
            httpGet:
              path: /healthz
              port: 8081
              initialDelaySeconds: 15
              periodSeconds: 20
          name: manager
          readinessProbe:
            httpGet:
              path: /readyz
              port: 8081

```

```
    initialDelaySeconds: 5
    periodSeconds: 10
  resources:
    limits:
      cpu: 300m
      memory: 750Mi
    requests:
      cpu: 100m
      memory: 75Mi
  securityContext:
    allowPrivilegeEscalation: false
imagePullSecrets: []
  securityContext:
    runAsUser: 65532
  terminationGracePeriodSeconds: 10
```

### 3. 安装 Astra 控制中心操作员:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

响应示例:

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io created
role.rbac.authorization.k8s.io/acc-operator-leader-election-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
created
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role created
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding created
configmap/acc-operator-manager-config created
service/acc-operator-controller-manager-metrics-service created
deployment.apps/acc-operator-controller-manager created
```

### 4. 验证Pod是否正在运行:

```
kubectl get pods -n netapp-acc-operator
```

## 配置 Astra 控制中心

1. 编辑Astra Control Center自定义资源(CR)文件 (astra\_control\_center.yaml)进行帐户、支持、注册表和其他必要配置:

```
vim astra_control_center.yaml
```



以下步骤将提供一个标注的YAML示例。

2. 修改或确认以下设置:

**<code>accountName</code>**

正在设置 ...	指导	Type	示例
accountName	更改 accountName 字符串、表示要与Astra Control Center帐户关联的名称。只能有一个accountName。	string	Example

**<code>astraVersion</code>**

正在设置 ...	指导	Type	示例
astraVersion	要部署的Astra控制中心版本。无需对此设置执行任何操作、因为此值将预先填充。	string	23.04.2-7

## <code>astraAddress</code>

正在设置 ...	指导	Type	示例
<code>astraAddress</code>	<p>更改 <code>astraAddress</code> 指向要在浏览器中访问Astra控制中心的FQDN (建议)或IP地址的字符串。此地址用于定义如何在数据中心中找到Astra控制中心、并且与您在完成后从负载均衡器配置的FQDN或IP地址相同 "Astra 控制中心要求"。</p> <p>注意：请勿使用 <code>http://</code> 或 <code>https://</code> 地址中。复制此 FQDN 以在中使用 <a href="#">后续步骤</a>。</p>	string	<code>astra.example.com</code>

## <code>autoSupport</code>

您在本节中的选择将决定您是否要参与NetApp主动支持应用程序NetApp Active IQ 以及数据的发送位置。需要互联网连接(端口442)、所有支持数据均会匿名化。

正在设置 ...	使用 ...	指导	Type	示例
<code>autoSupport.enrolled</code>	两者之一 <code>enrolled</code> 或 <code>url</code> 必须选择字段	更改 <code>enrolled</code> 用于将AutoSupport连接到 <code>false</code> 对于不具有Internet连接或保留的站点 <code>true</code> 对于已连接站点。的设置 <code>true</code> 允许将匿名数据发送到NetApp以获得支持。默认选择为 <code>false</code> 和表示不会向NetApp发送任何支持数据。	布尔值	<code>false</code> (此值为默认值)
<code>autoSupport.url</code>	两者之一 <code>enrolled</code> 或 <code>url</code> 必须选择字段	此URL用于确定匿名数据的发送位置。	string	<a href="https://support.netapp.com/asupprod/post/1.0/postAsup">https://support.netapp.com/asupprod/post/1.0/postAsup</a>

### <code>email</code>

正在设置 ...	指导	Type	示例
email	更改 email 字符串到默认的初始管理员地址。复制此电子邮件地址以在中使用 <a href="#">后续步骤</a> 。此电子邮件地址将用作初始帐户的用户名、用于登录到UI、并在Astra Control中收到事件通知。	string	admin@example.com

### <code>firstName</code>

正在设置 ...	指导	Type	示例
firstName	与Astra帐户关联的默认初始管理员的名字。首次登录后、此处使用的名称将显示在用户界面的标题中。	string	SRE

### <code>LastName</code>

正在设置 ...	指导	Type	示例
lastName	与Astra帐户关联的默认初始管理员的姓氏。首次登录后、此处使用的名称将显示在用户界面的标题中。	string	Admin

## <code>imageRegistry</code>

您在本节中的选择定义了托管Astra应用程序映像、Astra控制中心操作员和Astra控制中心Helm存储库的容器映像注册表。

正在设置 ...	使用 ...	指导	Type	示例
imageRegistry.name	Required	在中推送映像的映像注册表的名称 <a href="#">上一步</a> 。请勿使用 http:// 或 https:// 注册表名称。	string	example.registry.com/astra
imageRegistry.secret	如果您为输入的字符串、则为必填项 imageRegistry.name' requires a secret.  IMPORTANT: If you are using a registry that does not require authorization, you must delete this `secret` 行内 imageRegistry 否则安装将失败。	用于通过映像注册表进行身份验证的Kubernetes密钥的名称。	string	astra-registry-cred

### <code>storageClass</code>

正在设置 ...	指导	Type	示例
storageClass	<p>更改 storageClass 价值来自 ontap-gold 另一个A作用于安装所需的Astra三端存储类资源。运行命令 <code>kubectl get sc</code> 以确定已配置的现有存储类。必须在清单文件中输入一个基于Astra三端的存储类 (astra-control-center-<code>&lt;version&gt;.manifest</code>)、并将用于Astra PV。如果未设置、则会使用默认存储类。</p> <p>注意：如果配置了默认存储类、请确保它是唯一具有默认标注的存储类。</p>	string	ontap-gold

### <code>volumeReclaimPolicy</code>

正在设置 ...	指导	Type	选项
volumeReclaimPolicy	<p>这将为Astra的PV设置回收策略。将此策略设置为 Retain 删除Astra后保留永久性卷。将此策略设置为 Delete 删除Astra后删除永久性卷。如果未设置此值、则会保留PV。</p>	string	<ul style="list-style-type: none"><li>• Retain (这是默认值)</li><li>• Delete</li></ul>



<code>ingressType</code>

正在设置 ...	指导	Type	选项
ingressType	<p>请使用以下入口类型之一：</p> <p><b>Generic</b> (ingressType: "Generic")(默认) 如果您正在使用另一个入口控制器或希望使用您自己的入口控制器、请使用此选项。部署Astra控制中心后、您需要配置 <a href="#">"入口控制器"</a> 以使用URL公开Astra控制中心。</p> <p><b>AccTraefik</b> (ingressType: "AccTraefik") 如果您不希望配置入口控制器、请使用此选项。这将部署Astra控制中心 traefik 网关作为Kubernetes loadbalancer类型的服务。</p> <p>Astra控制中心使用类型为"loadbalancer"的服务 (svc/traefik)、并要求为其分配可访问的外部IP地址。如果您的环境允许使用负载均衡器、但您尚未配置一个平衡器、则可以使用MetalLB或其他外部服务负载均衡器为该服务分配外部IP地址。在内部 DNS 服务器配置中，您应将 Astra 控制中心选择的 DNS 名称指向负载均衡的 IP 地址。</p> <p>注意：有关"load平衡器"和传入服务类型的详细信息、请参见 <a href="#">"要求"</a>。</p>	string	<ul style="list-style-type: none"><li>• Generic (这是默认值)</li><li>• AccTraefik</li></ul>

### <code>scaleSize</code>

正在设置 ...	指导	Type	选项
scaleSize	<p>默认情况下、Astra将使用高可用性(HA) scaleSize 的 Medium ，可在HA中部署大多数服务，并部署多个副本以实现冗余。使用 scaleSize 作为 Small 的作用是减少所有服务的副本数量，但主要服务除外，以减少使用量。</p> <p>提示： Medium 部署包含大约100个Pod (不包括瞬时工作负载) 。100个Pod基于一个三主节点和三个工作节点配置)。请注意您问题描述 的环境中可能存在的每POD网络限制限制、尤其是在考虑灾难恢复方案时。</p>	string	<ul style="list-style-type: none"><li>• Small</li><li>• Medium (这是默认值)</li></ul>

### <code>astraResourcesScaler</code>

正在设置 ...	指导	Type	选项
astraResourcesScaler	<p>AstraControlCenter资源限制的扩展选项。默认情况下、Astra控制中心会进行部署、并为Astra中的大多数组件设置了资源请求。通过这种配置、Astra控制中心软件堆栈可以在应用程序负载和扩展性增加的环境中更好地运行。</p> <p>但是、在使用较小的开发或测试集群的情况下、CR字段为 astraResourcesScaler 可设置为 Off。此操作将禁用资源请求、并允许在较小的集群上部署。</p>	string	<ul style="list-style-type: none"><li>• Default (这是默认值)</li><li>• Off</li></ul>

**<code>additionalValues</code>**

- 对于Astral控制中心和Cloud Insights 通信、默认情况下会禁用TLS证书验证。您可以通过在中添加以下部分来为Cloud Insights 与Astra控制中心主机集群和受管集群之间的通信启用TLS证书验证 additionalValues。

```
additionalValues:
  netapp-monitoring-operator:
    config:
      ciSkipTlsVerify: false
  cloud-insights-service:
    config:
      ciSkipTlsVerify: false
  telemetry-service:
    config:
      ciSkipTlsVerify: false
```

`<code>crds</code>`

您在本节中的选择决定了Astra控制中心应如何处理CRD。

正在设置 ...	指导	Type	示例
<code>crds.externalCertManager</code>	<p>如果使用外部证书管理器、请进行更改 <code>externalCertManager to true</code>。默认值 <code>false</code> 使Astra控制中心在安装期间安装自己的证书管理器CRD。</p> <p>CRD是集群范围的对象、安装它们可能会影响集群的其他部分。您可以使用此标志向Astra控制中心发出信号、指示这些CRD将由Astra控制中心以外的集群管理员安装和管理。</p>	布尔值	False (此值为默认值)
<code>crds.externalTraefik</code>	<p>默认情况下、Astra控制中心将安装所需的Traefik CRD。CRD是集群范围的对象、安装它们可能会影响集群的其他部分。您可以使用此标志向Astra控制中心发出信号、指示这些CRD将由Astra控制中心以外的集群管理员安装和管理。</p>	布尔值	False (此值为默认值)



在完成安装之前、请确保为您的配置选择了正确的存储类和入口类型。

```
astra_control_center.yaml
```

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  volumeReclaimPolicy: "Retain"
  ingressType: "Generic"
  scaleSize: "Medium"
  astraResourcesScaler: "Default"
  additionalValues: {}
  crds:
    externalTraefik: false
    externalCertManager: false
```

## 完成 Astra 控制中心和操作员安装

1. 如果您在上一步中尚未执行此操作、请创建 netapp-acc (或自定义)命名空间:

```
kubectl create ns [netapp-acc or custom namespace]
```

响应示例:

```
namespace/netapp-acc created
```

2. 在中安装Astra控制中心 netapp-acc (或自定义)命名空间:

```
kubectl apply -f astra_control_center.yaml -n [netapp-acc or custom namespace]
```

响应示例:

```
astracontrolcenter.astra.netapp.io/astra created
```



A作用 力控制中心操作员将自动检查环境要求。缺少 "要求" 发生原因 您的安装是否失败或Astra控制中心是否无法正常运行。请参见 [下一节](#) 检查与自动系统检查相关的警告消息。

## 验证系统状态

您可以使用kubectl命令验证系统状态。如果您更喜欢使用 OpenShift ，则可以使用同等的 oc 命令执行验证步骤。

### 步骤

1. 验证安装过程是否未生成与验证检查相关的警告消息：

```
kubectl get acc [astra or custom Astra Control Center CR name] -n  
[netapp-acc or custom namespace] -o yaml
```



A作用 力控制中心操作员日志中还会报告其他警告消息。

2. 更正自动需求检查报告的环境中的任何问题。



您可以通过确保环境满足来更正问题 "要求" A作用 控制中心。

3. 验证是否已成功安装所有系统组件。

```
kubectl get pods -n [netapp-acc or custom namespace]
```

每个POD的状态应为 Running。部署系统 Pod 可能需要几分钟的时间。

响应示例

NAME	READY	STATUS	
RESTARTS	AGE		
acc-helm-repo-6cc7696d8f-pmhm8	1/1	Running	0
9h			
activity-597fb656dc-5rd4l	1/1	Running	0
9h			
activity-597fb656dc-mqmcw	1/1	Running	0
9h			
api-token-authentication-62f84	1/1	Running	0
9h			
api-token-authentication-68nlf	1/1	Running	0
9h			
api-token-authentication-ztgrm	1/1	Running	0
9h			
asup-669d4ddbc4-fnmwp	1/1	Running	1
(9h ago) 9h			
authentication-78789d7549-1k686	1/1	Running	0
9h			
bucket-service-65c7d95496-24x7l	1/1	Running	3
(9h ago) 9h			
cert-manager-c9f9fbf9f-k8zq2	1/1	Running	0
9h			
cert-manager-c9f9fbf9f-qj1zm	1/1	Running	0
9h			
cert-manager-cainjector-dbbbd8447-b5q1l	1/1	Running	0
9h			
cert-manager-cainjector-dbbbd8447-p5whs	1/1	Running	0
9h			
cert-manager-webhook-6f97bb7d84-4722b	1/1	Running	0
9h			
cert-manager-webhook-6f97bb7d84-86kv5	1/1	Running	0
9h			
certificates-59d9f6f4bd-2j899	1/1	Running	0
9h			
certificates-59d9f6f4bd-9d9k6	1/1	Running	0
9h			
certificates-expiry-check-28011180--1-8lkxz	0/1	Completed	0
9h			
cloud-extension-5c9c9958f8-jdhrp	1/1	Running	0
9h			
cloud-insights-service-5cdd5f7f-pp8r5	1/1	Running	0
9h			
composite-compute-66585789f4-hxn5w	1/1	Running	0

9h			
composite-volume-68649f68fd-tb7p4	1/1	Running	0
9h			
credentials-dfc844c57-jsx92	1/1	Running	0
9h			
credentials-dfc844c57-xw26s	1/1	Running	0
9h			
entitlement-7b47769b87-4jb6c	1/1	Running	0
9h			
features-854d8444cc-c24b7	1/1	Running	0
9h			
features-854d8444cc-dv6sm	1/1	Running	0
9h			
fluent-bit-ds-9tlv4	1/1	Running	0
9h			
fluent-bit-ds-bpkcb	1/1	Running	0
9h			
fluent-bit-ds-cxmwx	1/1	Running	0
9h			
fluent-bit-ds-jgnhc	1/1	Running	0
9h			
fluent-bit-ds-vtr6k	1/1	Running	0
9h			
fluent-bit-ds-vxqd5	1/1	Running	0
9h			
graphql-server-7d4b9d44d5-zdbf5	1/1	Running	0
9h			
identity-6655c48769-4pwk8	1/1	Running	0
9h			
influxdb2-0	1/1	Running	0
9h			
keycloak-operator-55479d6fc6-slvmt	1/1	Running	0
9h			
krakend-f487cb465-78679	1/1	Running	0
9h			
krakend-f487cb465-rjsxx	1/1	Running	0
9h			
license-64cbc7cd9c-qxsr8	1/1	Running	0
9h			
login-ui-5db89b5589-ndb96	1/1	Running	0
9h			
loki-0	1/1	Running	0
9h			
metrics-facade-8446f64c94-x8h7b	1/1	Running	0
9h			
monitoring-operator-6b44586965-pvcl4	2/2	Running	0



9h			
nats-0	1/1	Running	0
9h			
nats-1	1/1	Running	0
9h			
nats-2	1/1	Running	0
9h			
nautilus-85754d87d7-756qb	1/1	Running	0
9h			
nautilus-85754d87d7-q8j7d	1/1	Running	0
9h			
openapi-5f9cc76544-7fnjm	1/1	Running	0
9h			
openapi-5f9cc76544-vzr7b	1/1	Running	0
9h			
packages-5db49f8b5-lrzhd	1/1	Running	0
9h			
polaris-consul-consul-server-0	1/1	Running	0
9h			
polaris-consul-consul-server-1	1/1	Running	0
9h			
polaris-consul-consul-server-2	1/1	Running	0
9h			
polaris-keycloak-0	1/1	Running	2
(9h ago) 9h			
polaris-keycloak-1	1/1	Running	0
9h			
polaris-keycloak-2	1/1	Running	0
9h			
polaris-keycloak-db-0	1/1	Running	0
9h			
polaris-keycloak-db-1	1/1	Running	0
9h			
polaris-keycloak-db-2	1/1	Running	0
9h			
polaris-mongodb-0	1/1	Running	0
9h			
polaris-mongodb-1	1/1	Running	0
9h			
polaris-mongodb-2	1/1	Running	0
9h			
polaris-ui-66fb99479-qp9gq	1/1	Running	0
9h			
polaris-vault-0	1/1	Running	0
9h			
polaris-vault-1	1/1	Running	0

9h	polaris-vault-2	1/1	Running	0
9h	public-metrics-76fbf9594d-zmxzw	1/1	Running	0
9h	storage-backend-metrics-7d7fbc9cb9-lmd25	1/1	Running	0
9h	storage-provider-5bdd456c4b-2fftc	1/1	Running	0
9h	task-service-87575df85-dnn2q	1/1	Running	3
(9h ago) 9h	task-service-task-purge-28011720--1-q6w4r	0/1	Completed	0
28m	task-service-task-purge-28011735--1-vk6pd	1/1	Running	0
13m	telegraf-ds-2r2kw	1/1	Running	0
9h	telegraf-ds-6s9d5	1/1	Running	0
9h	telegraf-ds-96jl7	1/1	Running	0
9h	telegraf-ds-hbp84	1/1	Running	0
9h	telegraf-ds-plwzv	1/1	Running	0
9h	telegraf-ds-sr22c	1/1	Running	0
9h	telegraf-rs-4sbg8	1/1	Running	0
9h	telemetry-service-fb9559f7b-mk917	1/1	Running	3
(9h ago) 9h	tenancy-559bbc6b48-5msgg	1/1	Running	0
9h	traefik-d997b8877-7xpf4	1/1	Running	0
9h	traefik-d997b8877-9xv96	1/1	Running	0
9h	trident-svc-585c97548c-d25z5	1/1	Running	0
9h	vault-controller-88484b454-2d6sr	1/1	Running	0
9h	vault-controller-88484b454-fc5cz	1/1	Running	0
9h	vault-controller-88484b454-jktld	1/1	Running	0
9h				

4. (可选)为确保安装完成、您可以观看 `acc-operator` 使用以下命令记录。

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f
```



`accHost` 集群注册是最后一项操作、如果失败、发生原因 部署不会失败。如果日志中指示的集群注册失败、您可以尝试通过重新注册 ["在UI中添加集群工作流"](#) 或 API。

5. 在所有Pod运行时、验证安装是否成功 (READY 为 True)并获取登录到Astra控制中心时要使用的初始设置密码:

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

响应:

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	23.04.2-7	10.111.111.111
True			



复制UUID值。密码为 `ACC-` 后跟UUID值 (`ACC-[UUID]` 或者、在此示例中、`ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`)。

## 设置传入以进行负载平衡

您可以设置一个Kubernetes入口控制器、用于管理对服务的外部访问。如果您使用的是默认值、则以下过程提供了入口控制器的设置示例 `ingressType: "Generic"` 在Astra Control Center自定义资源中 (`astra_control_center.yaml`)。如果指定、则不需要使用此操作步骤 `ingressType: "AccTraefik"` 在Astra Control Center自定义资源中 (`astra_control_center.yaml`)。

部署 Astra 控制中心后,您需要配置入口控制器,以便使用 URL 公开 Astra 控制中心。

设置步骤因所使用的入口控制器类型而异。Astra控制中心支持多种传入控制器类型。这些设置过程提供了以下传入控制器类型的示例步骤:

- Istio入口
- nginx 入口控制器
- OpenShift 入口控制器

开始之前

- 所需 ["入口控制器"](#) 应已部署。
- ["入口类"](#) 应已创建与入口控制器对应的。

## Istio入口的步骤

1. 配置Istio入口。



此操作步骤 假定使用"默认"配置文件部署Istio。

2. 为传入网关收集或创建所需的证书和专用密钥文件。

您可以使用CA签名或自签名证书。公用名必须为Astra地址(FQDN)。

命令示例:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out  
tls.crt
```

3. 创建密钥 `tls secret name` 类型 `kubernetes.io/tls` 中的TLS专用密钥和证书 `istio-system` namespace 如TLS机密中所述。

命令示例:

```
kubectl create secret tls [tls secret name] --key="tls.key"  
--cert="tls.crt" -n istio-system
```



密钥名称应与匹配 `spec.tls.secretName` 在中提供 `istio-ingress.yaml` 文件

4. 在中部署入站资源 `netapp-acc` (或自定义命名的)命名空间 (`istio-Ingress.yaml` 在此示例中使用):

```

apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: istio
  tls:
    - hosts:
      - <ACC address>
      secretName: [tls secret name]
  rules:
    - host: [ACC address]
      http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: traefik
                port:
                  number: 80

```

## 5. 应用更改:

```
kubectl apply -f istio-Ingress.yaml
```

## 6. 检查入口状态:

```
kubectl get ingress -n [netapp-acc or custom namespace]
```

响应:

NAME	CLASS	HOSTS	ADDRESS	PORTS	AGE
ingress	istio	astra.example.com	172.16.103.248	80, 443	1h

## 7. 完成Astra控制中心安装。

### nginx 入口控制器的步骤

1. 创建类型的密钥 `kubernetes.io/tls` 中的TLS专用密钥和证书 `netapp-acc` (或自定义命名的)命名空间、如中所述 "TLS 密钥"。
2. 在中部署传入资源 `netapp-acc` (或自定义命名的)命名空间 (`nginx-Ingress.yaml` 在此示例中使用):

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
    - hosts:
      - <ACC address>
      secretName: [tls secret name]
  rules:
    - host: <ACC address>
      http:
        paths:
          - path:
              backend:
                service:
                  name: traefik
                  port:
                    number: 80
              pathType: ImplementationSpecific
```

### 3. 应用更改:

```
kubectl apply -f nginx-Ingress.yaml
```



NetApp建议将nginx控制器安装为部署、而不是安装 `daemonSet`。

### OpenShift 入口控制器的步骤

1. 获取证书并获取密钥，证书和 CA 文件，以供 OpenShift 路由使用。
2. 创建 OpenShift 路由:

```
oc create route edge --service=traefik --port=web -n [netapp-acc or
custom namespace] --insecure-policy=Redirect --hostname=<ACC address>
--cert=cert.pem --key=key.pem
```

## 登录到 Astra 控制中心 UI

安装 Astra 控制中心后，您将更改默认管理员的密码并登录到 Astra 控制中心 UI 信息板。

### 步骤

1. 在浏览器中、输入FQDN (包括 https:// 前缀) astraAddress 在中 astra\_control\_center.yaml CR时间 [您安装了 Astra 控制中心](#)。
2. 如果出现提示、请接受自签名证书。



您可以在登录后创建自定义证书。

3. 在Astra Control Center登录页面上、输入您用于的值 email 在中 astra\_control\_center.yaml CR时间 [您安装了 Astra 控制中心](#)、后跟初始设置密码 (ACC-[UUID]) 。



如果您输入的密码三次不正确，管理员帐户将锁定 15 分钟。

4. 选择 \* 登录 \* 。
5. 根据提示更改密码。



如果这是您第一次登录、但您忘记了密码、并且尚未创建任何其他管理用户帐户、请联系 ["NetApp 支持"](#) 以获得密码恢复帮助。

6. (可选) 删除现有自签名 TLS 证书并将其替换为 ["由证书颁发机构 \(CA\) 签名的自定义 TLS 证书"](#)。

## 对安装进行故障排除

如果有任何服务位于中 Error 状态、您可以检查日志。查找 400 到 500 范围内的 API 响应代码。这些信息表示发生故障的位置。

### 选项

- 要检查 Astra 控制中心操作员日志，请输入以下内容：

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-
operator -c manager -f
```

- 要检查Asta Control Center CR的输出：

```
kubectl get acc -n [netapp-acc or custom namespace] -o yaml
```

## 下一步行动

- (可选)根据您的环境、完成安装后操作 "配置步骤"。
- 执行以完成部署 "设置任务"。

## 配置外部证书管理器

如果Kubernetes集群中已存在证书管理器、则需要执行一些前提步骤、以使Astra控制中心不会安装自己的证书管理器。

### 步骤

1. 确认已安装证书管理器：

```
kubectl get pods -A | grep 'cert-manager'
```

#### 响应示例：

```
cert-manager    essential-cert-manager-84446f49d5-sf2zd    1/1
Running         0      6d5h
cert-manager    essential-cert-manager-cainjector-66dc99cc56-9ldmt    1/1
Running         0      6d5h
cert-manager    essential-cert-manager-webhook-56b76db9cc-fjqrq    1/1
Running         0      6d5h
```

2. 为创建证书/密钥对 astraAddress FQDN：

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out
tls.crt
```

#### 响应示例：

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'tls.key'
```

3. 使用先前生成的文件创建密钥：

```
kubectl create secret tls selfsigned-tls --key tls.key --cert tls.crt -n
<cert-manager-namespace>
```



响应示例:

```
secret/selfsigned-tls created
```

4. 创建 ClusterIssuer 文件\*精确\*如下、但包含的命名空间位置 cert-manager Pod的安装:

```
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
  name: astra-ca-clusterissuer
  namespace: <cert-manager-namespace>
spec:
  ca:
    secretName: selfsigned-tls
```

```
kubectl apply -f ClusterIssuer.yaml
```

响应示例:

```
clusterissuer.cert-manager.io/astra-ca-clusterissuer created
```

5. 验证是否已 ClusterIssuer 已正确启动。Ready 必须为 True 在继续操作之前:

```
kubectl get ClusterIssuer
```

响应示例:

NAME	READY	AGE
astra-ca-clusterissuer	True	9s

6. 完成 "[Astra 控制中心安装过程](#)"。有一个 "[Astra控制中心集群YAML的所需配置步骤](#)" 其中、您可以更改CRD 值以指示证书管理器是外部安装的。您必须在安装期间完成此步骤、以使Astra控制中心能够识别外部证书管理器。

## 使用 OpenShift OperatorHub 安装 Astra 控制中心

如果您使用的是 Red Hat OpenShift ，则可以使用 Red Hat 认证操作员安装 Astra Control Center 。使用此操作步骤从安装 Astra 控制中心 "[Red Hat 生态系统目录](#)" 或使用 Red Hat OpenShift 容器平台。

完成此操作步骤后，您必须返回到安装操作步骤以完成 **"剩余步骤"** 以验证安装是否成功并登录。

开始之前

- 满足环境前提条件：["开始安装之前，请为 Astra Control Center 部署准备您的环境"](#)。
- 运行状况良好的集群操作员和API服务：
  - 在OpenShift集群中、确保所有集群操作员均处于运行状况良好的状态：

```
oc get clusteroperators
```

- 在OpenShift集群中、确保所有API服务均处于运行状况良好的状态：

```
oc get apiservices
```

- **\* FQDN地址\***：获取数据中心的Astra控制中心的FQDN地址。
- **\* OpenShift权限\***：获取对Red Hat OpenShift容器平台的必要权限和访问权限、以执行所述的安装步骤。
- 已配置证书管理器：如果集群中已存在证书管理器、则需要执行某些操作 **"前提条件步骤"** 这样、Astra控制中心就不会安装自己的证书管理器。默认情况下、Astra控制中心会在安装期间安装自己的证书管理器。
- **\* Kubernetes入口控制器\***：如果您的Kubernetes入口控制器负责管理对服务的外部访问、例如集群中的负载均衡、则需要将其设置为与Astra控制中心配合使用：
  - a. 创建操作员命名空间：

```
oc create namespace netapp-acc-operator
```

- b. **"完成设置"** 适用于您的入口控制器类型。

步骤

- [下载并提取Astra控制中心](#)
- [安装NetApp Astra kubectI插件](#)
- [\[将映像添加到本地注册表\]](#)
- [\[找到操作员安装页面\]](#)
- [\[安装操作员\]](#)
- [安装 Astra 控制中心](#)

下载并提取**Astra**控制中心

1. 转至 ["Astra Control Center下载页面"](#) 页面。
2. 下载包含Astra Control Center的软件包 (astra-control-center-[version].tar.gz) 。
3. (建议但可选)下载Astra控制中心的证书和签名包 (astra-control-center-certs-[version].tar.gz)以验证捆绑包的签名：

```
tar -vxzf astra-control-center-certs-[version].tar.gz
```

```
openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub  
-signature certs/astra-control-center-[version].tar.gz.sig astra-  
control-center-[version].tar.gz
```

此时将显示输出 Verified OK 验证成功后。

#### 4. 从Astra Control Center捆绑包中提取映像：

```
tar -vxzf astra-control-center-[version].tar.gz
```

## 安装NetApp Astra kubectl插件

您可以使用NetApp Astra kubectl命令行插件将映像推送到本地Docker存储库。

开始之前

NetApp可为不同的CPU架构和操作系统提供插件二进制文件。在执行此任务之前、您需要了解您的CPU和操作系统。

步骤

1. 列出可用的NetApp Astra kubectl插件二进制文件、并记下操作系统和CPU架构所需的文件名称：



kubectl插件库是tar包的一部分、并会解压缩到文件夹中 kubectl-astra。

```
ls kubectl-astra/
```

2. 将正确的二进制文件移动到当前路径并重命名为 kubectl-astra：

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

## 将映像添加到本地注册表

1. 为容器引擎完成相应的步骤顺序：

## Docker

1. 更改为tarball的根目录。您应看到此文件和目录：

```
acc.manifest.bundle.yaml
acc/
```

2. 将Astra Control Center映像目录中的软件包映像推送到本地注册表。在运行之前、请进行以下替换push-images 命令：

- 将<BUNDLE\_FILE> 替换为Astra Control捆绑包文件的名称 (acc.manifest.bundle.yaml) 。
- 将<MY\_FULL\_REGISTRY\_PATH> 替换为Docker存储库的URL；例如 "<a href="https://<docker-registry>" class="bare">https://<docker-registry>"</a>。
- 将<MY\_REGISTRY\_USER> 替换为用户名。
- 将<MY\_REGISTRY\_TOKEN> 替换为注册表的授权令牌。

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

## Podman

1. 更改为tarball的根目录。您应看到此文件和目录：

```
acc.manifest.bundle.yaml
acc/
```

2. 登录到注册表：

```
podman login <YOUR_REGISTRY>
```

3. 准备并运行以下针对您使用的Podman版本自定义的脚本之一。将<MY\_FULL\_REGISTRY\_PATH> 替换为包含任何子目录的存储库的URL。

```
<strong>Podman 4</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

<strong>Podman 3</strong>

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```



根据您的注册表配置、此脚本创建的映像路径应类似于以下内容：

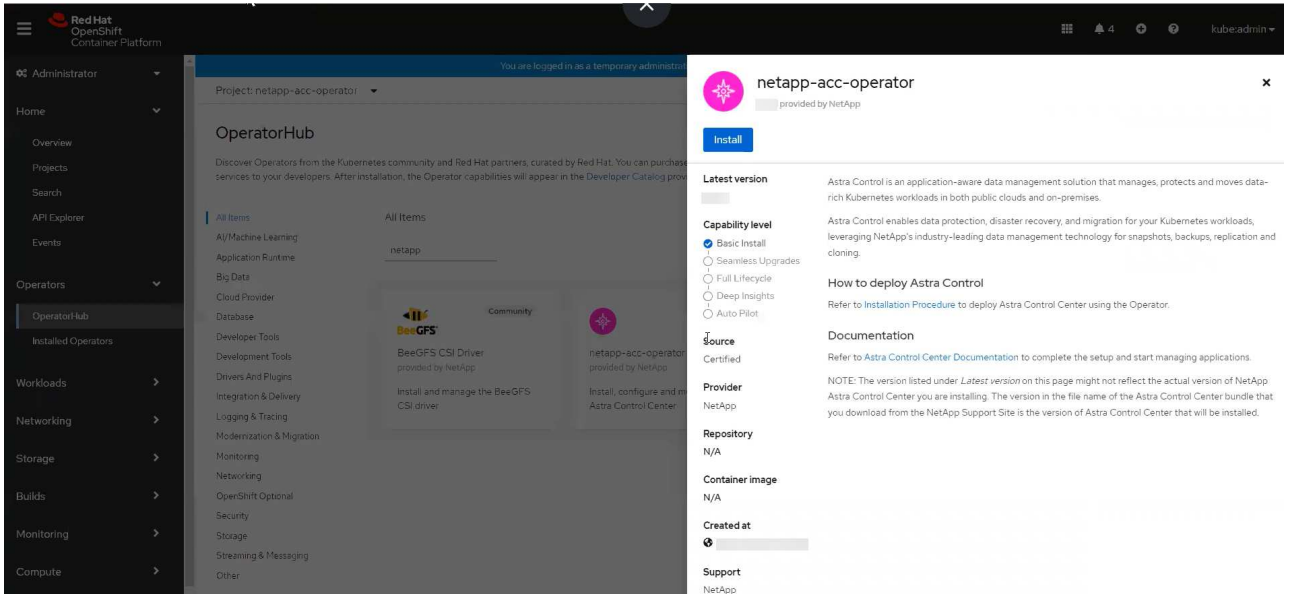
```
https://netappdownloads.jfrog.io/docker-astra-control-
prod/netapp/astra/acc/23.04.2-7/image:version
```

## 找到操作员安装页面

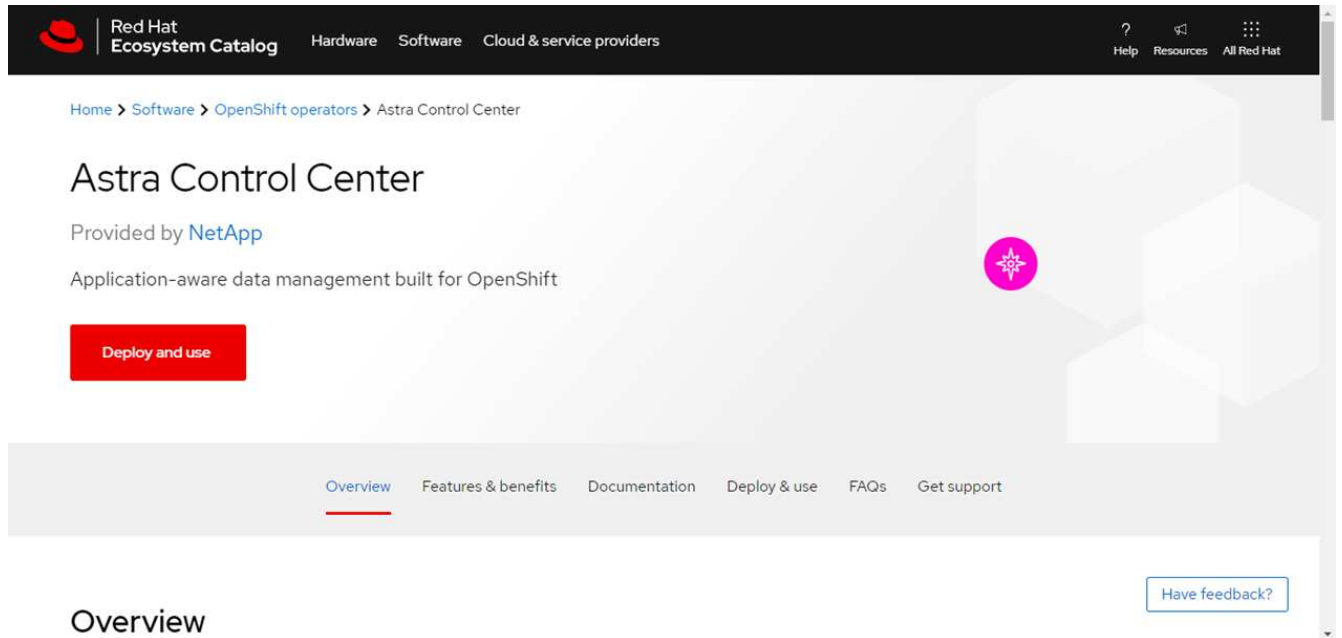
1. 要访问操作员安装页面，请完成以下过程之一：

- 从 Red Hat OpenShift Web 控制台：

- i. 登录到 OpenShift 容器平台 UI。
- ii. 从侧面菜单中，选择 \* 运算符 > OperatorHub \*。
- iii. 搜索并选择 NetApp Astra Control Center 运算符。



- 从 Red Hat 生态系统目录：
  - i. 选择 NetApp Astra 控制中心 "运算符"。
  - ii. 选择 \* 部署并使用 \*。



## 安装操作员

1. 完成 \* 安装操作员 \* 页面并安装操作员：



操作员将在所有集群命名空间中可用。

- a. 选择操作符命名空间或 `netapp-acc-operator` 命名空间将在操作员安装过程中自动创建。
- b. 选择手动或自动批准策略。



建议手动批准。每个集群只能运行一个操作员实例。

- c. 选择 \* 安装 \*。

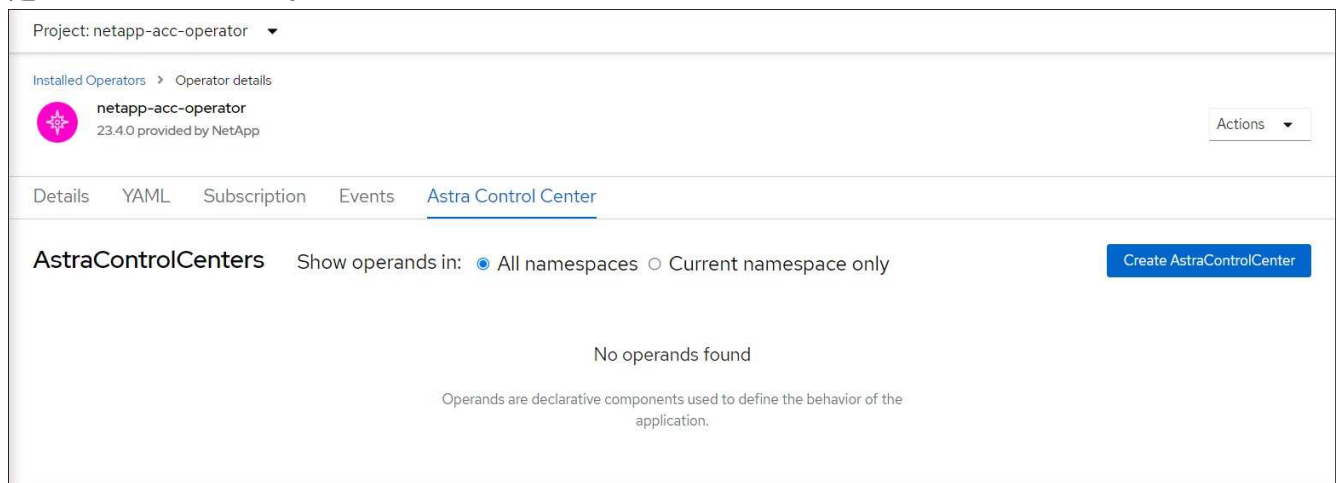


如果您选择了手动批准策略，系统将提示您批准此操作员的手动安装计划。

2. 从控制台中，转到 OperatorHub 菜单并确认操作员已成功安装。

## 安装 Astra 控制中心

1. 从 Astra Control Center 操作员的 \* Astra Control Center\* 选项卡中的控制台中、选择 \* 创建 AstraControlCenter\*。



2. 完成 Create AstraControlCenter 表单字段：

- a. 保留或调整 Astra 控制中心名称。
- b. 为 Astra 控制中心添加标签。
- c. 启用或禁用自动支持。建议保留自动支持功能。
- d. 输入 Astra 控制中心 FQDN 或 IP 地址。请止步 `http://` 或 `https://` 在地址字段中。
- e. 输入 Astra Control Center 版本、例如 23.04.2-7。
- f. 输入帐户名称，电子邮件地址和管理员姓氏。
- g. 选择的卷回收策略 `Retain`，`Recycle`` 或 ``Delete`。默认值为 `Retain`。
- h. 选择安装的可扩展大小。



默认情况下、Astra 将使用高可用性(HA) `scaleSize` 的 `Medium`，可在 HA 中部署大多数服务，并部署多个副本以实现冗余。使用 `scaleSize` 作为 ``Small`` 作用是减少所有服务的副本数量，但主要服务除外，以减少使用量。

- i. 选择入口类型：

- **Generic** (ingressType: "Generic")(默认)

如果您正在使用另一个入口控制器或希望使用您自己的入口控制器、请使用此选项。部署Astra控制中心后、您需要配置 ["入口控制器"](#) 以使用URL公开Astra控制中心。

- **AccTraefik** (ingressType: "AccTraefik")

如果您不希望配置入口控制器、请使用此选项。这将部署Astra控制中心 traefik 网关作为Kubernetes的"loadbalancer"类型服务。

Astra控制中心使用类型为"loadbalancer"的服务 (svc/traefik)、并要求为其分配可访问的外部IP地址。如果您的环境允许使用负载均衡器、但您尚未配置一个平衡器、则可以使用MetalLB或其他外部服务负载均衡器为该服务分配外部IP地址。在内部 DNS 服务器配置中，您应将Astra控制中心选择的DNS名称指向负载均衡的IP地址。



有关"负载均衡器"和传入服务类型的详细信息、请参见 ["要求"](#)。

- a. 在 \* 映像注册表 \* 中，输入本地容器映像注册表路径。请止步 http:// 或 https:// 在地址字段中。
- b. 如果您使用的映像注册表需要身份验证、请输入映像密钥。



如果您使用的注册表需要身份验证、[在集群上创建密钥](#)。

- c. 输入管理员的名字。
- d. 配置资源扩展。
- e. 提供默认存储类。



如果配置了默认存储类、请确保它是唯一具有默认标注的存储类。

- f. 定义 CRD 处理首选项。

3. 选择YAML视图以查看您选择的设置。
4. 选择 ... Create。

## 创建注册表密钥

如果您使用的注册表需要身份验证、请在OpenShift集群上创建一个密钥、然后在 表单字段。

1. 为Astra控制中心操作员创建命名空间：

```
oc create ns [netapp-acc-operator or custom namespace]
```

2. 在此命名空间中创建密钥：



```
oc create secret docker-registry astra-registry-cred n [netapp-acc-operator or custom namespace] --docker-server=[your_registry_path] --docker-username=[username] --docker-password=[token]
```



Astra Control仅支持Docker注册表机密。

3. 完成中的其余字段 [创建AstraControlCenter表单字段](#)。

## 下一步行动

完成 "剩余步骤" 要验证是否已成功安装Astra控制中心、请设置一个入口控制器(可选)并登录到UI。此外、您还需要执行 "设置任务" 完成安装后。

## 使用 Cloud Volumes ONTAP 存储后端安装 Astra 控制中心

借助 Astra 控制中心，您可以使用自管理的 Kubernetes 集群和 Cloud Volumes ONTAP 实例在混合云环境中管理应用程序。您可以在内部 Kubernetes 集群或云环境中的一个自我管理 Kubernetes 集群中部署 Astra Control Center 。

在其中一种部署中，您可以使用 Cloud Volumes ONTAP 作为存储后端来执行应用程序数据管理操作。您还可以将 S3 存储分段配置为备份目标。

要在Amazon Web Services (AWS)、Google云平台(GCP)和Microsoft Azure中使用Cloud Volumes ONTAP 存储后端安装Astra控制中心、请根据您的云环境执行以下步骤。

- [在 Amazon Web Services 中部署 Astra 控制中心](#)
- [在Google Cloud Platform中部署Astra控制中心](#)
- [在 Microsoft Azure 中部署 Astra 控制中心](#)

您可以使用自我管理Kubernetes集群(例如OpenShift容器平台(OCP))在分发版中管理应用程序。只有自我管理的OCP集群才会通过验证来部署Astra控制中心。

## 在 Amazon Web Services 中部署 Astra 控制中心

您可以在 Amazon Web Services (AWS) 公有云上托管的自管理 Kubernetes 集群上部署 Astra 控制中心。

### AWS所需的功能

在 AWS 中部署 Astra 控制中心之前，您需要满足以下条件：

- Astra Control Center 许可证。请参见 "[Astra 控制中心许可要求](#)"。
- "[满足 Astra 控制中心的要求](#)"。
- NetApp Cloud Central account
- 如果使用OCP、则Red Hat OpenShift Container Platform (OCP)权限(在命名空间级别用于创建Pod)
- AWS 凭据，访问 ID 和机密密钥，具有用于创建存储分段和连接器的权限

- AWS 帐户弹性容器注册 (Elastic Container Registry, ECR) 访问和登录
- 要访问 Astra Control UI, 需要 AWS 托管分区和 Route 53 条目

## AWS 的操作环境要求

Astra 控制中心需要以下 AWS 操作环境:

- Red Hat OpenShift 容器平台 4.8



确保您选择托管 Astra 控制中心的操作环境满足环境官方文档中概述的基本资源要求。

除了环境的资源要求之外, Astra 控制中心还需要以下资源:

组件	要求
后端 <b>NetApp Cloud Volumes ONTAP</b> 存储容量	至少 300 GB 可用
工作节点 ( <b>AWS EC2</b> 要求)	总共至少 3 个辅助节点, 每个节点有 4 个 vCPU 核心和 12 GB RAM
负载均衡器	服务类型 "loadbalancer" 可用于将传入流量发送到操作环境集群中的服务
<b>FQDN</b>	一种将 Astra 控制中心的 FQDN 指向负载均衡 IP 地址的方法
<b>Astra Trident</b> (在 <b>NetApp BlueXP</b> 中作为 <b>Kubernetes</b> 集群发现的一部分安装、以前称为 <b>Cloud Manager</b> )	安装并配置了 Astra Trident 21.04 或更高版本, 并将 NetApp ONTAP 9.5 或更高版本作为存储后端
映像注册表	<p>您必须拥有一个现有的私有注册表, 例如 AWS 弹性容器注册表, 您可以将 Astra Control Center 构建映像推送到该注册表。您需要提供要将映像上传到的映像注册表的 URL。</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  Astra 控制中心托管的集群和受管集群必须能够访问同一映像注册表, 才能使用基于 Restic 的映像备份和还原应用程序。 </div>

组件	要求
<b>Astra Trident / ONTAP 配置</b>	<p>Astra 控制中心要求创建一个存储类并将其设置为默认存储类。Astra控制中心支持以下ONTAP Kubernetes存储类、这些存储类是在将Kubernetes集群导入到NetApp BlueXP (以前称为Cloud Manager)时创建的。这些功能由 Astra Trident 提供:</p> <ul style="list-style-type: none"> <li>• vsaworkingenvironment-&lt;&gt;-ha-nas csi.trident.netapp.io</li> <li>• vsaworkingenvironment-&lt;&gt;-ha-san csi.trident.netapp.io</li> <li>• vsaworkingenvironment-&lt;&gt;-single-nas csi.trident.netapp.io</li> <li>• vsaworkingenvironment-&lt;&gt;-single-san csi.trident.netapp.io</li> </ul>



这些要求假定 Astra 控制中心是运行环境中唯一运行的应用程序。如果环境运行的是其他应用程序，请相应地调整这些最低要求。



AWS 注册表令牌将在 12 小时后过期，之后您必须续订 Docker 映像注册表密钥。

## AWS 部署概述

下面简要介绍了将 Cloud Volumes ONTAP 作为存储后端安装适用于 AWS 的 Astra 控制中心的过程。

下面详细介绍了其中每个步骤。

1. [确保您具有足够的 IAM 权限。](#)
2. [在 AWS 上安装 RedHat OpenShift 集群。](#)
3. [配置AWS。](#)
4. [配置适用于AWS的NetApp BlueXP。](#)
5. [安装适用于AWS的Astra控制中心。](#)

确保您具有足够的 **IAM** 权限

确保您具有足够的IAM角色和权限、可以安装RedHat OpenShift集群和NetApp BlueXP (以前称为Cloud Manager) Connector。

请参见 "[初始 AWS 凭据](#)"。

在 **AWS** 上安装 **RedHat OpenShift 集群**

在 AWS 上安装 RedHat OpenShift 容器平台集群。

有关安装说明，请参见 "[在 OpenShift 容器平台中的 AWS 上安装集群](#)"。

## 配置AWS

接下来、将AWS配置为创建虚拟网络、设置EC2计算实例、创建AWS S3存储分段、创建弹性容器注册表(ECR)以托管Astra控制中心映像、并将这些映像推送到此注册表。

按照 AWS 文档完成以下步骤。请参见 "[AWS 安装文档](#)"。

1. 创建AWS虚拟网络。
2. 查看 EC2 计算实例。这可以是 AWS 中的裸机服务器或 VM 。
3. 如果实例类型尚未与主节点和工作节点的 Astra 最低资源要求匹配，请更改 AWS 中的实例类型以满足 Astra 要求。请参见 "[Astra 控制中心要求](#)"。
4. 至少创建一个 AWS S3 存储分段来存储备份。
5. 创建 AWS 弹性容器注册表（ ECR ）以托管所有 AccR 映像。



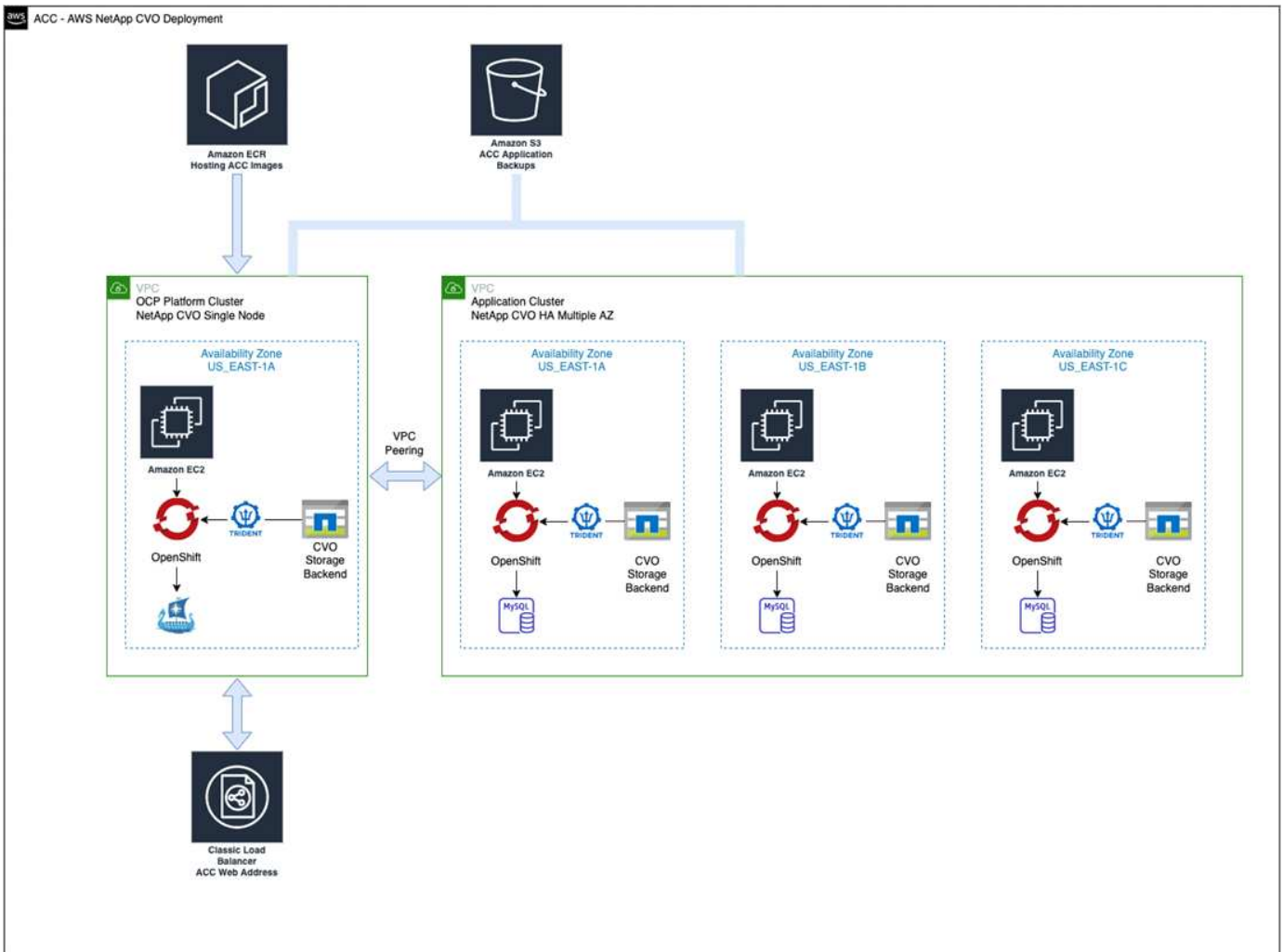
如果不创建ECR、则Astra控制中心无法从包含Cloud Volumes ONTAP 且具有AWS后端的集群访问监控数据。如果您尝试使用 Astra 控制中心发现和管理的集群没有 AWS ECR 访问权限，则会导致出现问题描述 。

6. 将这些 Accc 映像推送到您定义的注册表。



AWS 弹性容器注册表（ ECR ）令牌将在 12 小时后过期，并导致跨集群克隆操作失败。从为AWS配置的Cloud Volumes ONTAP 管理存储后端时会发生此问题描述。要更正此问题描述，请再次向 ECR 进行身份验证，并生成一个新密钥，以便成功恢复克隆操作。

以下是 AWS 部署示例：



## 配置适用于AWS的NetApp BlueXP

使用NetApp BlueXP (以前称为Cloud Manager)创建工作空间、向AWS添加连接器、创建工作环境并导入集群。

按照BlueXP文档完成以下步骤。请参见以下内容：

- ["AWS 中的 Cloud Volumes ONTAP 入门"](#)。
- ["使用BlueXP在AWS中创建连接器"](#)

### 步骤

1. 将凭据添加到BlueXP。
2. 创建工作空间。
3. 为 AWS 添加连接器。选择 AWS 作为提供程序。
4. 为您的云环境创建一个工作环境。
  - a. 位置： "Amazon Web Services (AWS)"
  - b. 类型： Cloud Volumes ONTAP HA
5. 导入 OpenShift 集群。集群将连接到您刚刚创建的工作环境。
  - a. 选择 \* K8s\* > \* 集群列表 \* > \* 集群详细信息 \* ， 查看 NetApp 集群详细信息。

- b. 请注意右上角的Asta三端版本。
- c. 记下显示 NetApp 作为配置程序的 Cloud Volumes ONTAP 集群存储类。

此操作将导入 Red Hat OpenShift 集群并为其分配默认存储类。您可以选择存储类。Asta三项功能会在导入和发现过程中自动安装。

6. 记下此Cloud Volumes ONTAP 部署中的所有永久性卷和卷。



Cloud Volumes ONTAP 可以作为单个节点运行，也可以在高可用性环境下运行。如果已启用 HA，请记下在 AWS 中运行的 HA 状态和节点部署状态。

安装适用于**AWS**的**Astra**控制中心

请遵循标准 "[Astra 控制中心安装说明](#)"。



AWS使用通用S3存储分段类型。

## 在Google Cloud Platform中部署Astra控制中心

您可以在Google云平台(GCP)公有云上托管的自管理Kubernetes集群上部署Astra控制中心。

### GCP所需的功能

在GCP中部署Astra控制中心之前、您需要满足以下条件：

- Astra Control Center 许可证。请参见 "[Astra 控制中心许可要求](#)"。
- "[满足 Astra 控制中心的要求](#)"。
- NetApp Cloud Central account
- 如果使用的是OCP、则为Red Hat OpenShift Container Platform (OCP) 4.10
- 如果使用OCP、则Red Hat OpenShift Container Platform (OCP)权限(在命名空间级别用于创建Pod)
- GCP服务帐户、具有创建存储分段和连接器的权限

### GCP的操作环境要求



确保您选择托管 Astra 控制中心的操作环境满足环境官方文档中概述的基本资源要求。

除了环境的资源要求之外，Astra 控制中心还需要以下资源：

组件	要求
后端 <b>NetApp Cloud Volumes ONTAP</b> 存储容量	至少 300 GB 可用
工作节点( <b>GCP</b> 计算要求)	总共至少 3 个辅助节点，每个节点有 4 个 vCPU 核心和 12 GB RAM
负载均衡器	服务类型 "loadbalancer" 可用于将传入流量发送到操作环境集群中的服务

组件	要求
<b>FQDN (GCP DNS区域)</b>	一种将 Astra 控制中心的 FQDN 指向负载均衡 IP 地址的方法
<b>Astra Trident (在NetApp BlueXP 中作为Kubernetes集群发现的一部分安装、以前称为Cloud Manager)</b>	安装并配置了 Astra Trident 21.04 或更高版本，并将 NetApp ONTAP 9.5 或更高版本作为存储后端
映像注册表	<p>您必须具有现有的专用注册表、例如Google Container Registry、您可以将Astra Control Center构建映像推送到该注册表。您需要提供要将映像上传到的映像注册表的 URL。</p> <p> 您需要启用匿名访问以提取要备份的 Restic 映像。</p>
<b>Astra Trident / ONTAP 配置</b>	<p>Astra 控制中心要求创建一个存储类并将其设置为默认存储类。Astra控制中心支持在将ONTAP Kubernetes集群导入到NetApp BlueXP中时创建的以下Kubernetes存储类。这些功能由 Astra Trident 提供：</p> <ul style="list-style-type: none"> <li>• vsaworkingenvironment-&lt;&gt;-ha-nas csi.trident.netapp.io</li> <li>• vsaworkingenvironment-&lt;&gt;-ha-san csi.trident.netapp.io</li> <li>• vsaworkingenvironment-&lt;&gt;-single-nas csi.trident.netapp.io</li> <li>• vsaworkingenvironment-&lt;&gt;-single-san csi.trident.netapp.io</li> </ul>



这些要求假定 Astra 控制中心是运行环境中唯一运行的应用程序。如果环境运行的是其他应用程序，请相应地调整这些最低要求。

## GCP部署概述

下面概述了在GCP中将Cloud Volumes ONTAP 作为存储后端的自管理OCP集群上安装Astra控制中心的过程。

下面详细介绍了其中每个步骤。

1. [在GCP上安装RedHat OpenShift集群。](#)
2. [创建GCP项目和虚拟私有云。](#)
3. [确保您具有足够的 IAM 权限。](#)
4. [配置GCP。](#)
5. [为GCP配置NetApp BlueXP。](#)
6. [安装适用于GCP的Astra Control Center。](#)

## 在GCP上安装RedHat OpenShift集群

第一步是在GCP上安装RedHat OpenShift集群。

有关安装说明，请参见以下内容：

- ["在GCP中安装OpenShift集群"](#)
- ["创建GCP服务帐户"](#)

### 创建GCP项目和虚拟私有云

至少创建一个GCP项目和虚拟私有云(Virtual Private Cloud、VPC)。



OpenShift 可能会创建自己的资源组。此外、您还应定义GCP VPC。请参见 OpenShift 文档。

您可能需要创建平台集群资源组和目标应用程序 OpenShift 集群资源组。

确保您具有足够的 **IAM** 权限

确保您具有足够的IAM角色和权限、可以安装RedHat OpenShift集群和NetApp BlueXP (以前称为Cloud Manager) Connector。

请参见 ["初始GCP凭据和权限"](#)。

### 配置GCP

接下来、将GCP配置为创建VPC、设置计算实例、创建Google Cloud Object Storage、创建用于托管Astra控制中心映像的Google Container Register并将这些映像推送到此注册表。

按照GCP文档完成以下步骤。请参见在GCP中安装OpenShift集群。

1. 在GCP中创建一个GCP项目和VPC、该项目和VPC计划用于具有CVO后端的OCP集群。
2. 查看计算实例。此服务器可以是GCP中的裸机服务器或VM。
3. 如果实例类型尚未与主节点和工作节点的Astra最低资源要求匹配、请在GCP中更改实例类型以满足Astra要求。请参见 ["Astra 控制中心要求"](#)。
4. 至少创建一个GCP Cloud Storage Bucket以存储备份。
5. 创建存储分段访问所需的密钥。
6. 创建Google容器注册表以托管所有Astra控制中心映像。
7. 为所有Astra控制中心映像设置用于Docker推/拉的Google容器注册表访问权限。

示例：输入以下脚本可将Accc映像推送到此注册表：

```
gcloud auth activate-service-account <service account email address>
--key-file=<GCP Service Account JSON file>
```

此脚本需要一个Astra控制中心清单文件以及您的Google映像注册表位置。



## 示例

```
manifestfile=astra-control-center-<version>.manifest
GCP_CR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image
    docker push $GCP_CR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

### 8. 设置 DNS 区域。

#### 为GCP配置NetApp BlueXP

使用NetApp BlueXP (原Cloud Manager)创建工作空间、向GCP添加连接器、创建工作环境并导入集群。

按照BlueXP文档完成以下步骤。请参见 ["GCP中的Cloud Volumes ONTAP 入门"](#)。

#### 开始之前

- 使用所需的IAM权限和角色访问GCP服务帐户

#### 步骤

1. 将凭据添加到BlueXP。请参见 ["正在添加GCP帐户"](#)。
2. 为GCP添加一个连接器。
  - a. 选择"GCP"作为提供程序。
  - b. 输入GCP凭据。请参见 ["从BlueXP在GCP中创建连接器"](#)。
  - c. 确保连接器正在运行，然后切换到该连接器。
3. 为您的云环境创建一个工作环境。
  - a. 位置: "GCP"
  - b. 类型: Cloud Volumes ONTAP HA
4. 导入 OpenShift 集群。集群将连接到您刚刚创建的工作环境。
  - a. 选择 \* K8s\* > \* 集群列表 \* > \* 集群详细信息 \*，查看 NetApp 集群详细信息。
  - b. 在右上角，记下 Trident 版本。
  - c. 记下显示为"netapp"作为配置程序的Cloud Volumes ONTAP 集群存储类。

此操作将导入 Red Hat OpenShift 集群并为其分配默认存储类。您可以选择存储类。Asta三项功能会在导入和发现过程中自动安装。

5. 记下此Cloud Volumes ONTAP 部署中的所有永久性卷和卷。



Cloud Volumes ONTAP 可以作为单个节点运行、也可以在高可用性(HA)中运行。如果已启用 HA、请记下在GCP中运行的HA状态和节点部署状态。

## 安装适用于GCP的Astra Control Center

请遵循标准 ["Astra 控制中心安装说明"](#)。



GCP使用通用S3存储分段类型。

1. 生成Docker密钥以提取用于Astra控制中心安装的映像：

```
kubectl create secret docker-registry <secret name> --docker
-server=<Registry location> --docker-username=_json_key --docker
-password="$(cat <GCP Service Account JSON file>)" --namespace=pcloud
```

## 在 Microsoft Azure 中部署 Astra 控制中心

您可以在 Microsoft Azure 公有云上托管的自管理 Kubernetes 集群上部署 Astra 控制中心。

### Azure所需的功能

在 Azure 中部署 Astra 控制中心之前，您需要满足以下条件：

- Astra Control Center 许可证。请参见 ["Astra 控制中心许可要求"](#)。
- ["满足 Astra 控制中心的要求"](#)。
- NetApp Cloud Central account
- 如果使用OCP、则为Red Hat OpenShift Container Platform (OCP) 4.8
- 如果使用OCP、则Red Hat OpenShift Container Platform (OCP)权限(在命名空间级别用于创建Pod)
- 具有用于创建存储分段和连接器的权限的 Azure 凭据

### Azure 的操作环境要求

确保您选择托管 Astra 控制中心的操作环境满足环境官方文档中概述的基本资源要求。

除了环境的资源要求之外，Astra 控制中心还需要以下资源：

请参见 ["Astra 控制中心运营环境要求"](#)。

组件	要求
后端 NetApp Cloud Volumes ONTAP 存储容量	至少 300 GB 可用

组件	要求
员工节点（ <b>Azure</b> 计算要求）	总共至少 3 个辅助节点，每个节点有 4 个 vCPU 核心和 12 GB RAM
负载均衡器	服务类型 "loadbalancer" 可用于将传入流量发送到操作环境集群中的服务
<b>FQDN</b> （ <b>Azure DNS</b> 区域）	一种将 Astra 控制中心的 FQDN 指向负载均衡 IP 地址的方法
<b>Astra Trident</b> (在 <b>NetApp BlueXP</b> 中作为 <b>Kubernetes</b> 集群发现的一部分安装)	安装和配置的 Astra Trident 21.04 或更高版本以及 NetApp ONTAP 9.5 或更高版本将用作存储后端
映像注册表	<p>您必须具有一个现有的专用注册表，例如 Azure 容器注册表（ACR），您可以将 Astra Control Center 构建映像推送到该注册表。您需要提供要将映像上传到的映像注册表的 URL。</p> <p> 您需要启用匿名访问以提取要备份的 Restic 映像。</p>
<b>Astra Trident / ONTAP</b> 配置	<p>Astra 控制中心要求创建一个存储类并将其设置为默认存储类。Astra控制中心支持在将ONTAP Kubernetes集群导入到NetApp BlueXP中时创建的以下Kubernetes存储类。这些功能由 Astra Trident 提供：</p> <ul style="list-style-type: none"> <li>• <code>vsaworkingenvironment-&lt;&gt;-ha-nas csi.trident.netapp.io</code></li> <li>• <code>vsaworkingenvironment-&lt;&gt;-ha-san csi.trident.netapp.io</code></li> <li>• <code>vsaworkingenvironment-&lt;&gt;-single-nas csi.trident.netapp.io</code></li> <li>• <code>vsaworkingenvironment-&lt;&gt;-single-san csi.trident.netapp.io</code></li> </ul>



这些要求假定 Astra 控制中心是运行环境中唯一运行的应用程序。如果环境运行的是其他应用程序，请相应地调整这些最低要求。

## Azure 部署概述

下面简要介绍了适用于 Azure 的 Astra 控制中心的安装过程。

下面详细介绍了其中每个步骤。

1. [在 Azure 上安装 RedHat OpenShift 集群。](#)
2. [创建 Azure 资源组。](#)
3. [确保您具有足够的 IAM 权限。](#)
4. [配置 Azure。](#)
5. [为 Azure 配置 NetApp BlueXP \(以前称为 Cloud Manager\)。](#)

## 6. 安装和配置适用于Azure的Astra控制中心。

### 在 Azure 上安装 RedHat OpenShift 集群

第一步是在 Azure 上安装 RedHat OpenShift 集群。

有关安装说明，请参见以下内容：

- ["在 Azure 上安装 OpenShift 集群"](#)。
- ["安装 Azure 帐户"](#)。

### 创建 Azure 资源组

至少创建一个 Azure 资源组。



OpenShift 可能会创建自己的资源组。除了这些之外，您还应定义 Azure 资源组。请参见 OpenShift 文档。

您可能需要创建平台集群资源组和目标应用程序 OpenShift 集群资源组。

确保您具有足够的 IAM 权限

确保您具有足够的IAM角色和权限、可以安装RedHat OpenShift集群和NetApp BlueXP Connector。

请参见 ["Azure 凭据和权限"](#)。

### 配置 Azure

接下来、将Azure配置为创建虚拟网络、设置计算实例、创建Azure Blob容器、创建Azure容器注册表(ACR)以托管Astra控制中心映像、并将这些映像推送到此注册表。

按照 Azure 文档完成以下步骤。请参见 ["在 Azure 上安装 OpenShift 集群"](#)。

1. 创建Azure虚拟网络。
2. 查看计算实例。这可以是 Azure 中的裸机服务器或 VM 。
3. 如果实例类型尚未与主节点和工作节点的 Astra 最低资源要求匹配，请在 Azure 中更改实例类型以满足 Astra 要求。请参见 ["Astra 控制中心要求"](#)。
4. 至少创建一个Azure Blob容器以存储备份。
5. 创建存储帐户。您需要一个存储帐户来创建要用作 Astra 控制中心分段的容器。
6. 创建存储分段访问所需的密钥。
7. 创建 Azure 容器注册表（ACR）以托管所有 Astra 控制中心映像。
8. 为 Docker 推送 / 拉所有 Astra 控制中心映像设置 ACR 访问。
9. 输入以下脚本，将 Accc 映像推送到此注册表：

```
az acr login -n <AZ ACR URL/Location>
This script requires ACC manifest file and your Azure ACR location.
```

◦ 示例 \* :

```
manifestfile=astra-control-center-<version>.manifest
AZ_ACR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

10. 设置 DNS 区域。

为**Azure**配置**NetApp BlueXP** (以前称为**Cloud Manager**)

使用BlueXP (以前称为Cloud Manager)创建工作空间、向Azure添加连接器、创建工作环境并导入集群。

按照BlueXP文档完成以下步骤。请参见 ["Azure中的BlueXP入门"](#)。

开始之前

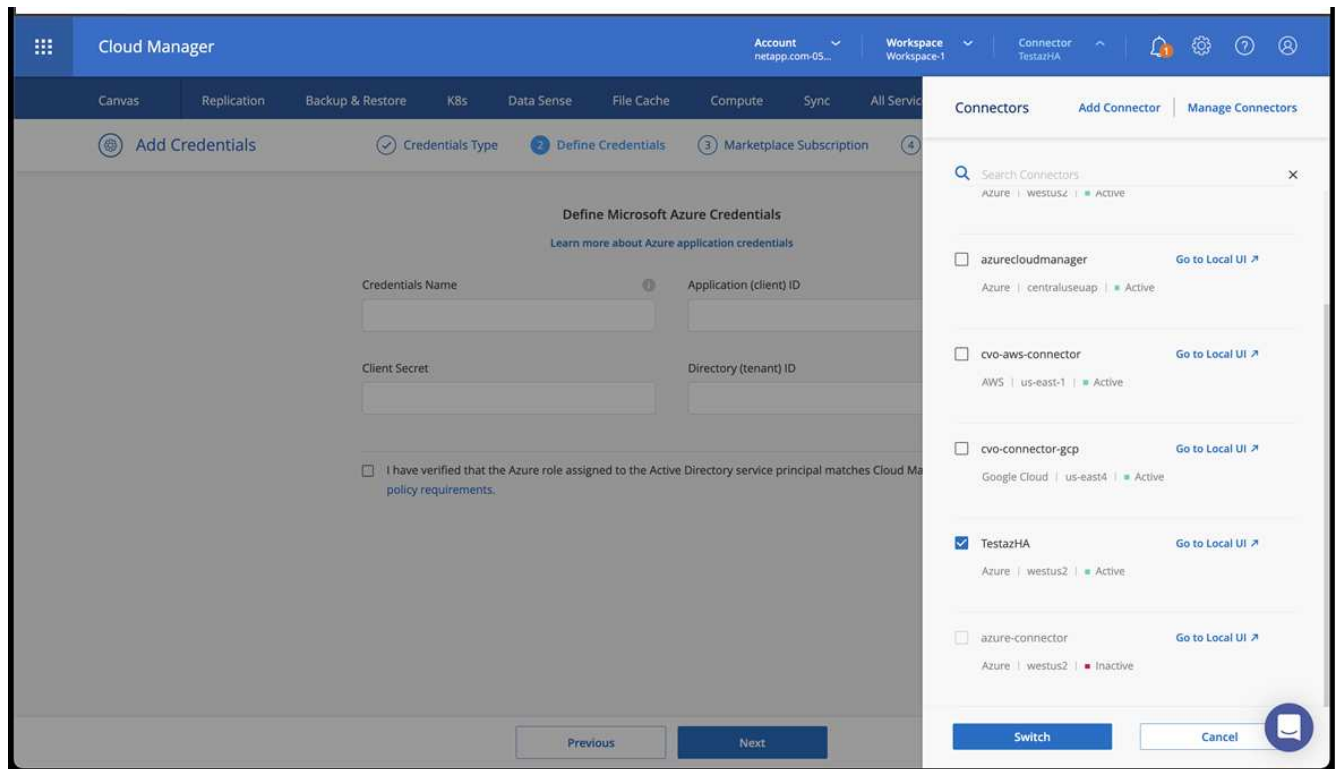
使用所需的 IAM 权限和角色访问 Azure 帐户

步骤

1. 将凭据添加到BlueXP。
2. 添加适用于 Azure 的连接器。请参见 ["BlueXP策略"](#)。
  - a. 选择 \* Azure \* 作为提供程序。
  - b. 输入 Azure 凭据，包括应用程序 ID ， 客户端密钥和目录（租户） ID 。

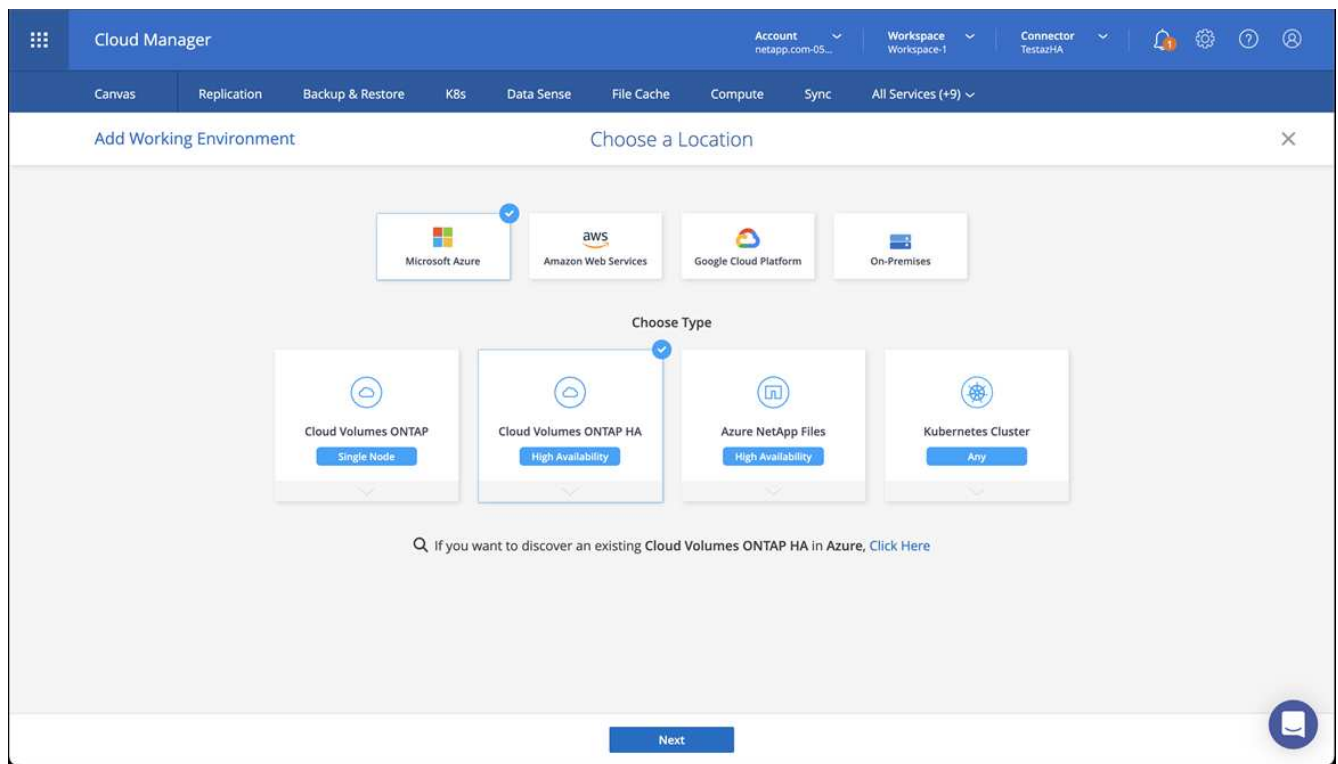
请参见 ["从BlueXP在Azure中创建连接器"](#)。

3. 确保连接器正在运行，然后切换到该连接器。



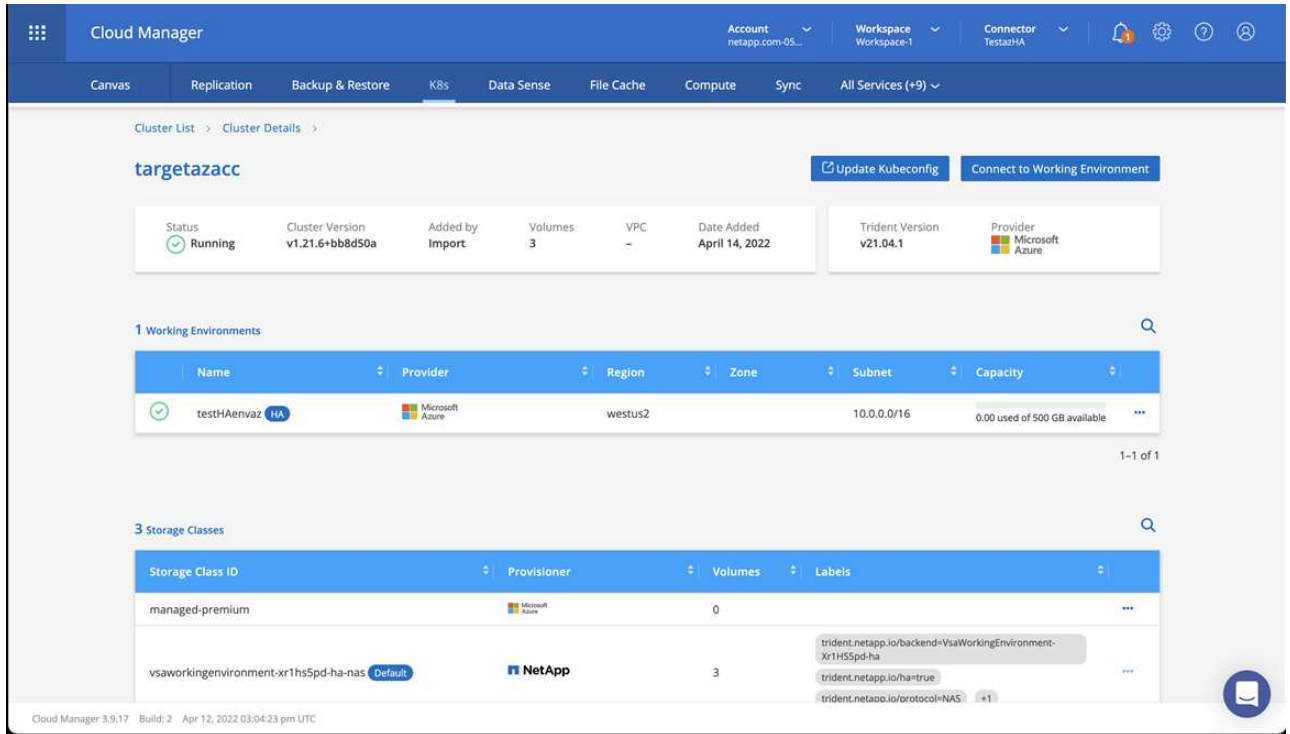
4. 为您的云环境创建一个工作环境。

- a. 位置: "Microsoft Azure"。
- b. 键入: Cloud Volumes ONTAP HA。



5. 导入 OpenShift 集群。集群将连接到您刚刚创建的工作环境。

a. 选择 \* K8s\* > \* 集群列表 \* > \* 集群详细信息 \* ，查看 NetApp 集群详细信息。



b. 请注意右上角的Astra三端版本。

c. 记下显示 NetApp 作为配置程序的 Cloud Volumes ONTAP 集群存储类。

此操作将导入 Red Hat OpenShift 集群并分配默认存储类。您可以选择存储类。Astra三项功能会在导入和发现过程中自动安装。

6. 记下此Cloud Volumes ONTAP 部署中的所有永久性卷和卷。

7. Cloud Volumes ONTAP 可以作为单个节点运行，也可以在高可用性环境下运行。如果已启用 HA ，请记下在 Azure 中运行的 HA 状态和节点部署状态。

安装和配置适用于**Azure**的**Astra**控制中心

按照标准安装 Astra 控制中心 "[安装说明](#)"。

使用 Astra 控制中心添加 Azure 存储分段。请参见 "[设置 Astra 控制中心并添加存储分段](#)"。

## 安装后配置Astra控制中心

根据您的环境、安装Astra控制中心后可能需要进行其他配置。

### 消除资源限制

某些环境使用ResourceQuotas和LimitRanges对象来防止命名空间中的资源占用集群上的所有可用CPU和内存。Astra控制中心未设置最大限制、因此不符合这些资源的要求。如果您的环境采用这种方式配置、则需要从计划安装Astra控制中心的命名空间中删除这些资源。

您可以使用以下步骤检索和删除这些配额和限制。在这些示例中、命令输出会立即显示在命令后面。

## 步骤

1. 在中获取资源配额 netapp-acc (或自定义名称)命名空间:

```
kubectl get quota -n [netapp-acc or custom namespace]
```

响应:

```
NAME          AGE    REQUEST                                     LIMIT
pods-high     16s   requests.cpu: 0/20, requests.memory: 0/100Gi
limits.cpu: 0/200, limits.memory: 0/1000Gi
pods-low      15s   requests.cpu: 0/1, requests.memory: 0/1Gi
limits.cpu: 0/2, limits.memory: 0/2Gi
pods-medium   16s   requests.cpu: 0/10, requests.memory: 0/20Gi
limits.cpu: 0/20, limits.memory: 0/200Gi
```

2. 按名称删除所有资源配额:

```
kubectl delete resourcequota pods-high -n [netapp-acc or custom namespace]
```

```
kubectl delete resourcequota pods-low -n [netapp-acc or custom namespace]
```

```
kubectl delete resourcequota pods-medium -n [netapp-acc or custom namespace]
```

3. 在中获取限制范围 netapp-acc (或自定义名称)命名空间:

```
kubectl get limits -n [netapp-acc or custom namespace]
```

响应:

```
NAME                CREATED AT
cpu-limit-range     2022-06-27T19:01:23Z
```

4. 按名称删除限制范围:



```
kubectl delete limitrange cpu-limit-range -n [netapp-acc or custom namespace]
```

## 在命名空间之间启用网络通信

某些环境使用NetworkPolicy构造来限制命名空间之间的流量。Astra控制中心操作员和Astra控制中心位于不同的命名空间中。这些不同命名空间中的服务需要能够彼此通信。要启用此通信、请执行以下步骤。

### 步骤

1. 删除Astra控制中心命名空间中的任何NetworkPolicy资源：

```
kubectl get networkpolicy -n [netapp-acc or custom namespace]
```

2. 对于上述命令返回的每个NetworkPolicy对象、请使用以下命令将其删除。将[object\_name]替换为返回对象的名称：

```
kubectl delete networkpolicy [OBJECT_NAME] -n [netapp-acc or custom namespace]
```

3. 应用以下资源文件以配置 `acc-avp-network-policy` 允许Asta插件服务向Asta Control Center服务发出请求的对象。将括号<>中的信息替换为您环境中的信息：

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-avp-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: <PLUGIN_NAMESPACE_NAME> #
REPLACE THIS WITH THE ASTRA PLUGIN NAMESPACE NAME
```

4. 应用以下资源文件以配置 `acc-operator-network-policy` 允许Astra控制中心操作员与Astra控制中心服务进行通信的对象。将括号<>中的信息替换为您环境中的信息：

```

apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-operator-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: <NETAPP-ACC-OPERATOR> #
REPLACE THIS WITH THE OPERATOR NAMESPACE NAME

```

## 添加自定义 TLS 证书

默认情况下、Astra控制中心对传入控制器流量(仅在某些配置中)和Web浏览器的Web UI身份验证使用自签名TLS证书。您可以删除现有的自签名 TLS 证书，并将其替换为由证书颁发机构（CA）签名的 TLS 证书。

默认的自签名证书用于两种类型的连接：



- 通过HTTPS连接到Astra控制中心Web UI
- 传入控制器流量(仅当 `ingressType: "AccTraefik"` 属性已在 `astra_control_center.yaml` 在安装Astra Control Center期间生成文件)

替换默认TLS证书将替换用于对这些连接进行身份验证的证书。

### 开始之前

- 安装了 Astra 控制中心的 Kubernetes 集群
- 对集群上要运行的命令Shell的管理访问 `kubectl` 命令
- CA 中的专用密钥和证书文件

### 删除自签名证书

删除现有的自签名 TLS 证书。

1. 使用 SSH ，以管理用户身份登录到托管 Astra 控制中心的 Kubernetes 集群。
2. 使用以下命令替换、查找与当前证书关联的TLS密钥 `<ACC-deployment-namespace>` 使用Astra Control Center部署命名空间：

```
kubectl get certificate -n <ACC-deployment-namespace>
```

3. 使用以下命令删除当前安装的密钥和证书:

```
kubectl delete cert cert-manager-certificates -n <ACC-deployment-namespace>
kubectl delete secret secure-testing-cert -n <ACC-deployment-namespace>
```

## 使用命令行添加新证书

添加一个由 CA 签名的新 TLS 证书。

1. 使用以下命令使用 CA 中的专用密钥和证书文件创建新的 TLS 密钥，并将括号 <> 中的参数替换为相应的信息:

```
kubectl create secret tls <secret-name> --key <private-key-filename>
--cert <certificate-filename> -n <ACC-deployment-namespace>
```

2. 使用以下命令和示例编辑集群自定义资源定义(CRD)文件并更改 `spec.selfSigned` 值为 `spec.ca.secretName` 要引用先前创建的TLS密钥、请执行以下操作:

```
kubectl edit clusterissuers.cert-manager.io/cert-manager-certificates -n
<ACC-deployment-namespace>
....

#spec:
#  selfSigned: {}

spec:
  ca:
    secretName: <secret-name>
```

3. 使用以下命令和示例输出验证所做的更改是否正确以及集群是否已准备好验证证书、然后进行替换 <ACC-deployment-namespace> 使用Astra Control Center部署命名空间:

```
kubectl describe clusterissuers.cert-manager.io/cert-manager-
certificates -n <ACC-deployment-namespace>
....

Status:
  Conditions:
    Last Transition Time: 2021-07-01T23:50:27Z
    Message:             Signing CA verified
    Reason:              KeyPairVerified
    Status:              True
    Type:                Ready
  Events:               <none>
```

4. 创建 `certificate.yaml` file 使用以下示例将括号<>中的占位符值替换为相应的信息:

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: <certificate-name>
  namespace: <ACC-deployment-namespace>
spec:
  secretName: <certificate-secret-name>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  - <astra.dnsname.example.com> #Replace with the correct Astra Control
  Center DNS address
  issuerRef:
    kind: ClusterIssuer
    name: cert-manager-certificates
```

5. 使用以下命令创建证书:

```
kubectl apply -f certificate.yaml
```

6. 使用以下命令和示例输出, 验证是否已正确创建证书以及是否使用您在创建期间指定的参数 (例如名称, 持续时间, 续订截止日期和 DNS 名称)。

```
kubectl describe certificate -n <ACC-deployment-namespace>
....

Spec:
  Dns Names:
    astra.example.com
  Duration: 125h0m0s
  Issuer Ref:
    Kind:      ClusterIssuer
    Name:      cert-manager-certificates
  Renew Before: 61h0m0s
  Secret Name: <certificate-secret-name>
Status:
  Conditions:
    Last Transition Time: 2021-07-02T00:45:41Z
    Message:             Certificate is up to date and has not expired
    Reason:              Ready
    Status:              True
    Type:               Ready
  Not After:           2021-07-07T05:45:41Z
  Not Before:          2021-07-02T00:45:41Z
  Renewal Time:        2021-07-04T16:45:41Z
  Revision:            1
Events:               <none>
```

7. 使用以下命令和示例编辑传入 CRD TLS 选项以指向新的证书密钥，并将括号 <> 中的占位符值替换为相应的信息：

```
kubectl edit ingressroutes.traefik.containo.us -n <ACC-deployment-namespace>
....

# tls:
#   options:
#     name: default
#     secretName: secure-testing-cert
#     store:
#       name: default

tls:
  options:
    name: default
    secretName: <certificate-secret-name>
  store:
    name: default
```

8. 使用 Web 浏览器浏览到 Astra 控制中心的部署 IP 地址。
9. 验证证书详细信息是否与您安装的证书的详细信息匹配。
10. 导出证书并将结果导入到 Web 浏览器中的证书管理器中。

## 版权信息

版权所有 © 2023 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。