



開始使用

Astra Control Center

NetApp
November 21, 2023

目錄

開始使用	1
Astra Control Center需求	1
Astra Control Center快速入門	5
安裝總覽	6
設定Astra控制中心	55
Astra Control Center的常見問題集	68

開始使用

= :allow-uri-read:

Astra Control Center需求

開始驗證作業環境、應用程式叢集、應用程式、授權和網頁瀏覽器的整備度。

- [\[營運環境需求\]](#)
- [\[支援的儲存後端\]](#)
- [\[存取網際網路\]](#)
- [\[授權\]](#)
- [內部部署Kubernetes叢集的入口](#)
- [\[網路需求\]](#)
- [\[支援的網頁瀏覽器\]](#)
- [\[應用程式叢集的其他需求\]](#)
- [Google Anthos叢集需求](#)
- [VMware Tanzu Kubernetes Grid叢集需求](#)

營運環境需求

Astra Control Center已在下列類型的作業環境中通過驗證：

- Cisco IKS搭配Kubernetes 1.22
- Google Anthos 1.11或1.12（請參閱 [Google Anthos叢集需求](#)）
- Rancher Kubernetes Engine（RKE）：
 - RKE 1.3.12搭配Rancher 2.6.5和2.6.6
 - RKE 1.3.13搭配Rancher 2.6.8
 - RKE 2（v1.23.6+ rke2r1）搭配Rancher 2.6.5和2.6.6
 - RKE 2（v1.24.x）搭配Rancher 2.6.8
- Red Hat OpenShift Container Platform 4.8至4.11
- 上游Kubernetes 1.23至1.25（Kubernetes 1.25需要Astra Trident 22.10或更新版本）
- VMware Tanzu Kubernetes Grid：（請參閱 [VMware Tanzu Kubernetes Grid叢集需求](#)）
 - VMware Tanzu Kubernetes Grid 1.5
 - VMware Tanzu Kubernetes Grid整合版1.13和1.14

確保您選擇裝載Astra Control Center的作業環境符合環境正式文件中所述的基本資源需求。除了環境的資源需求之外、Astra Control Center還需要下列資源：

元件	需求
CPU擴充	託管環境中所有節點的CPU都必須啟用AVX擴充功能。
儲存後端容量	至少可提供500GB容量
工作節點	總共至少3個工作節點、每個節點有4個CPU核心和12GB RAM
FQDN位址	Astra Control Center的FQDN位址
Astra Trident	Astra Trident 22.01或更新版本已安裝並設定Astra Trident 22.07或更新版本、以供SnapMirror型應用程式複寫Astra Trident 22.10或更新版本安裝於Kubernetes 1.25叢集（您必須在升級至Kubernetes之前升級至Astra Trident 22.10）



這些需求假設Astra Control Center是營運環境中唯一執行的應用程式。如果環境正在執行其他應用程式、請相應調整這些最低需求。

- 映像登錄：您必須擁有現有的私有Docker映像檔登錄、才能將Astra Control Center建置映像推入其中。您需要提供映像登錄的URL、以便上傳映像。
- * Astra Trident / ONTAP S161* :
 - 您需要在叢集上設定至少一個Astra Trident儲存類別。如果已設定預設儲存類別、請確定它是唯一具有預設指定的儲存類別。
 - 確保叢集中的工作節點已設定適當的儲存驅動程式、以便Pod與後端儲存設備互動。Astra Control Center支援ONTAP Astra Trident提供的下列支援資訊驅動程式：
 - ONTAP-NAS
 - ONTAP-SAN
 - ONTAP-san經濟型（不支援應用程式複寫）

支援的儲存後端

Astra Control Center支援下列儲存後端。

- NetApp ONTAP S9.5或更新AFF 版本的功能、包括ASA FAS
- 適用於ONTAP SnapMirror應用程式複寫的NetApp支援9.8或更新AFF 版本的功能、FAS 功能、功能及ASA 功能
- NetApp ONTAP Select S9.5或更新版本
- 適用於ONTAP Select SnapMirror型應用程式複寫的NetApp更新版本9.8
- NetApp Cloud Volumes ONTAP S9.5或更新版本

若要使用Astra Control Center、請視ONTAP 您需要完成的工作而定、確認您擁有下列各項的版次授權：

- FlexClone
- SnapMirror：選用。僅使用SnapMirror技術複寫至遠端系統時才需要。請參閱 "[SnapMirror授權資訊](#)"。

- S3授權：選用。僅適用於SS3鏟斗ONTAP

若要檢查ONTAP 您的不實系統是否有必要的授權、請參閱 ["管理ONTAP 不需購買的授權"](#)。

存取網際網路

您應該判斷是否有外部網際網路存取權。如果您沒有、部分功能可能會受到限制、例如從NetApp Cloud Insights接收監控和數據資料、或是將支援組合傳送至 ["NetApp 支援網站"](#)。

授權

Astra Control Center需要Astra Control Center授權才能提供完整功能。向NetApp取得評估授權或完整授權。您需要授權來保護應用程式和資料。請參閱 ["Astra Control Center功能"](#) 以取得詳細資料。

您可以使用Astra Control Center試用試用版授權、從下載授權之日起90天內即可使用Astra Control Center。您可以註冊以免費試用 ["請按這裡"](#)。

若要設定授權、請參閱 ["使用90天試用版授權"](#)。

若要深入瞭解授權的運作方式、請參閱 ["授權"](#)。

如需ONTAP 有關支援不支援的詳細資訊、請參閱 ["支援的儲存後端"](#)。

內部部署Kubernetes叢集的入口

您可以選擇網路入侵Astra控制中心的用途類型。依預設、Astra Control Center會將Astra Control Center閘道（服務/網路）部署為整個叢集的資源。Astra Control Center也支援使用服務負載平衡器（如果環境允許）。如果您想要使用服務負載平衡器、但尚未設定一個、則可以使用MetalLB負載平衡器自動將外部IP位址指派給服務。在內部DNS伺服器組態中、您應該將Astra Control Center所選的DNS名稱指向負載平衡的IP位址。



負載平衡器應使用與Astra Control Center工作節點IP位址位於同一子網路中的IP位址。



如果您要在Tanzu Kubernetes Grid叢集上裝載Astra Control Center、請使用 `kubectl get nsxlbmonitors -A` 命令以查看您是否已設定服務監視器以接受入口流量。如果存在、則不應安裝MetalLB、因為現有的服務監視器將會覆寫任何新的負載平衡器組態。

如需詳細資訊、請參閱 ["設定入口以進行負載平衡"](#)。

網路需求

裝載Astra Control Center的作業環境會使用下列TCP連接埠進行通訊。您應確保這些連接埠可透過任何防火牆、並設定防火牆、以允許來自Astra網路的任何HTTPS輸出流量。有些連接埠需要在裝載Astra Control Center的環境與每個託管叢集之間進行連線（視情況而定）。



您可以在雙堆疊Kubernetes叢集中部署Astra Control Center、Astra Control Center則可管理已設定為雙堆疊作業的應用程式和儲存後端。如需雙堆疊叢集需求的詳細資訊、請參閱 ["Kubernetes 文件"](#)。

來源	目的地	連接埠	傳輸協定	目的
用戶端PC	Astra控制中心	443..	HTTPS	UI / API存取：確保此連接埠在裝載Astra Control Center的叢集與每個受管理叢集之間都開啟
度量使用者	Astra Control Center工作節點	9090	HTTPS	度量資料通訊：確保每個託管叢集都能存取裝載Astra Control Center的叢集上的此連接埠（需要雙向通訊）
Astra控制中心	託管Cloud Insights版的服務	443..	HTTPS	通訊Cloud Insights
Astra控制中心	Amazon S3儲存貯體供應商	443..	HTTPS	Amazon S3儲存通訊
Astra控制中心	NetApp AutoSupport	443..	HTTPS	NetApp AutoSupport通訊

支援的網頁瀏覽器

Astra Control Center支援最新版本的Firefox、Safari和Chrome、最低解析度為1280 x 720。

應用程式叢集的其他需求

如果您打算使用這些Astra Control Center功能、請謹記以下要求：

- 應用程式叢集需求：["叢集管理需求"](#)
 - 受管理的應用程式需求：["應用程式管理需求"](#)
 - 應用程式複寫的其他需求：["複寫先決條件"](#)

Google Anthos叢集需求

在Google Anthos叢集上裝載Astra Control Center時、請注意、Google Anthos預設包含MetalLB負載平衡器和Istio入口閘道服務、讓您在安裝期間只需使用Astra Control Center的一般入口功能即可。請參閱["設定Astra控制中心"](#)以取得詳細資料。

VMware Tanzu Kubernetes Grid叢集需求

在VMware Tanzu Kubernetes Grid (TKG) 或Tanzu Kubernetes Grid整合版 (TKGi) 叢集上裝載Astra Control Center時、請謹記下列考量事項。

- 停用要由Astra Control管理的任何應用程式叢集上的TKG或TKGi預設儲存類別強制。您可以編輯來執行此作業 `TanzuKubernetesCluster` 命名空間叢集上的資源。
- 在TKG或TKGi環境中部署Astra Control Center時、請注意Astra Trident的特定需求。如需詳細資訊、請參閱["Astra Trident文件"](#)。



預設的VMware TKG和TKGi組態檔案權杖會在部署後10小時內過期。如果您使用Tanzu產品組合產品、則必須產生一個含有非過期權杖的Tanzu Kubernetes叢集組態檔、以避免Astra Control Center與託管應用程式叢集之間發生連線問題。如需相關指示、請造訪 ["VMware NSxT-T資料中心產品文件"](#)。

下一步

檢視 ["快速入門"](#) 總覽：

Astra Control Center快速入門

以下是使用Astra Control Center所需的步驟總覽。每個步驟中的連結都會帶您前往提供更多詳細資料的頁面。

1

檢閱Kubernetes叢集需求

確保您的環境符合這些要求。

- [Kubernetes叢集*](#)
- ["確保您的環境符合作業環境需求"](#)
- ["設定內部部署Kubernetes叢集的負載平衡入口"](#)

儲存整合

- ["確保您的環境包含Astra Trident支援的版本"](#)
- ["準備工作節點"](#)
- ["設定Astra Trident儲存後端"](#)
- ["設定Astra Trident儲存類別"](#)
- ["安裝Astra Trident Volume Snapshot控制器"](#)
- ["建立Volume Snapshot類別"](#)

不包含認證資料 ONTAP

- ["設定ONTAP 驗證資料"](#)

2

下載並安裝Astra Control Center

完成這些安裝工作。

- ["請從NetApp 支援網站 《The》 《The》 《The》 《The》 《The》 《The》 《The》 《The》 《The》"](#)
- 取得NetApp授權檔案：
 - ["如果您正在評估Astra Control Center、請下載試用版授權檔案"](#)
 - ["如果您已購買Astra Control Center、請產生授權檔案"](#)

- ["安裝Astra Control Center"](#)
- ["執行其他選用的組態步驟"](#)

3

完成一些初始設定工作

完成一些基本工作以開始使用。

- ["新增授權"](#)
- ["為叢集管理做好準備"](#)
- ["新增叢集"](#)
- ["新增儲存後端"](#)
- ["新增儲存庫"](#)

4

使用Astra控制中心

完成Astra Control Center的設定之後、接下來您可以做什麼。您可以使用Astra Control使用者介面 (UI) 或 ["Astra Control API"](#)。

- ["管理應用程式"](#)
- ["保護應用程式"](#)：設定保護原則、並複寫、複製及移轉應用程式。
- ["管理帳戶"](#)：使用者、角色、LDAP、認證等
- ["也可以連接Cloud Insights 到"](#)：查看系統健全狀況的指標。

以取得更多資訊

- ["Astra Control API"](#)
- ["升級Astra Control Center"](#)
- ["取得Astra Control的協助"](#)

安裝總覽

選擇並完成下列其中一個Astra Control Center安裝程序：

- ["使用標準程序安裝Astra Control Center"](#)
- ["（如果您使用Red Hat OpenShift）使用OpenShift作業系統集線器安裝Astra Control Center"](#)
- ["安裝Astra Control Center搭配Cloud Volumes ONTAP 一套功能性儲存後端"](#)

視您的環境而定、安裝Astra Control Center之後可能需要額外的組態：

- ["安裝後設定Astra Control Center"](#)

使用標準程序安裝Astra Control Center

若要安裝Astra Control Center、請從NetApp 支援網站 下列網址下載安裝套件、並執行下列步驟。您可以使用此程序、在連線網際網路或無線環境中安裝Astra Control Center。

其他安裝程序

- *使用RedHat OpenShift操作員中樞*安裝：請使用此功能 ["替代程序"](#) 使用作業系統集線器在OpenShift上安裝Astra Control Center。
- 以**Cloud Volumes ONTAP** 支援功能的方式在公有雲上安裝：使用 ["這些程序"](#) 若要在Amazon Web Services (AWS)、Google Cloud Platform (GCP) 或Microsoft Azure中安裝Astra Control Center、並提供Cloud Volumes ONTAP 一套支援整合式儲存後端的功能。

如需Astra Control Center安裝程序的示範、請參閱 ["這段影片"](#)。

您需要的產品

- ["開始安裝之前、請先準備好環境以進行Astra Control Center部署"](#)。
- 如果您已設定或想要在環境中設定Pod安全性原則、請熟悉Pod安全性原則、以及這些原則如何影響Astra Control Center安裝。請參閱 ["瞭解Pod安全性原則限制"](#)。
- 確保所有API服務均處於健全狀態且可供使用：

```
kubectl get apiservices
```

- 確保您打算使用的Astra FQDN可路由傳送至此叢集。這表示您在內部DNS伺服器中有DNS項目、或是使用已註冊的核心URL路由。
- 如果叢集中已存在憑證管理程式、您需要執行某些作業 ["必要步驟"](#) 因此Astra Control Center不會嘗試安裝自己的憑證管理程式。依預設、Astra Control Center會在安裝期間安裝自己的憑證管理程式。

關於這項工作

Astra Control Center安裝程序可協助您執行下列作業：

- 將Astra元件安裝至 `netapp-acc` (或自訂命名) 命名空間。
- 建立預設的Astra Control擁有者管理帳戶。
- 建立管理使用者電子郵件地址和預設初始設定密碼。此使用者會被指派第一次登入UI時所需的擁有者角色。
- 確定所有Astra Control Center Pod都在執行中。
- 安裝Astra Control Center UI。



請勿刪除Astra Control Center運算子 (例如、`kubectl delete -f astra_control_center_operator_deploy.yaml`) 在Astra Control Center安裝或操作期間、隨時避免刪除Pod。

步驟

若要安裝Astra Control Center、請執行下列步驟：

- [下載並擷取Astra Control Center](#)
- [安裝NetApp Astra kubectl外掛程式](#)
- [\[將映像新增至本機登錄\]](#)
- [\[設定具有驗證需求之登錄的命名空間和機密\]](#)
- [安裝Astra Control Center操作員](#)
- [設定Astra控制中心](#)
- [完整的Astra控制中心和操作員安裝](#)
- [\[驗證系統狀態\]](#)
- [\[設定入口以進行負載平衡\]](#)
- [登入Astra Control Center UI](#)

下載並擷取Astra Control Center

1. 前往 "[Astra Control Center評估下載頁面](#)" 於 NetApp 支援網站。
2. 下載包含Astra Control Center的套裝組合 (astra-control-center-[version].tar.gz) 。
3. (建議但可選) 下載Astra Control Center的憑證與簽名套件 (astra-control-center-certs-[version].tar.gz) 若要驗證套件的簽名：

```
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
```

隨即顯示輸出 Verified OK 驗證成功之後。

4. 從Astra Control Center套裝組合擷取映像：

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

安裝NetApp Astra kubectl外掛程式

NetApp Astra kubectl命令列外掛程式可在執行與部署及升級Astra Control Center相關的一般工作時節省時間。

您需要的產品

NetApp為不同的CPU架構和作業系統提供外掛程式二進位檔。執行此工作之前、您必須先瞭解您的CPU和作業系統。

步驟

1. 列出可用的NetApp Astra kubectl外掛程式二進位檔、並記下作業系統和CPU架構所需的檔案名稱：



KECBECTI外掛程式庫是tar套件的一部分、會擷取到資料夾中 `kubectl-astra`。

```
ls kubectl-astra/
```

2. 將正確的二進位檔移至目前路徑、並將其重新命名為 `kubectl-astra`：

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

將映像新增至本機登錄

1. 為您的Container引擎完成適當的步驟順序：

Docker

1. 切換到tar檔案的根目錄。您應該會看到這個檔案和目錄：

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

2. 將Astra Control Center映像目錄中的套件映像推送到本機登錄。執行之前、請先進行下列替換 `push-images` 命令：
 - 以<BUNDLE_FILE> Astra Control套裝組合檔案的名稱取代 (`acc.manifest.bundle.yaml`)。
 - 以<MY_FULL_REGISTRY_PATH> Docker儲存庫的URL取代支援；例如 "`<a href="https://<docker-registry>"; class="bare">https://<docker-registry>;`"。
 - 以<MY_REGISTRY_USER> 使用者名稱取代。
 - 以<MY_REGISTRY_TOKEN> 登錄的授權權杖取代。

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

Podman

1. 切換到tar檔案的根目錄。您應該會看到這個檔案和目錄：

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

2. 登入您的登錄：

```
podman login <YOUR_REGISTRY>
```

3. 針對您使用的Podman版本、準備並執行下列其中一個自訂指令碼。以包含任何子目錄的儲存庫URL取代<MY_FULL_REGISTRY_PATH>。

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

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
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=22.11.0-82
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

```



指令碼所建立的映像路徑應如下所示、視登錄組態而定：

<https://netappdownloads.jfrog.io/docker-astra-control-prod/netapp/astra/acc/22.11.0-82/image:version>

設定具有驗證需求之登錄的命名空間和機密

1. 匯出Astra Control Center主機叢集的KUBECONFIG：

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



完成安裝之前、請確定KUBECONFIG指向您要安裝Astra Control Center的叢集。KUBECONFIG只能包含一個內容。

2. 如果您使用需要驗證的登錄、則需要執行下列動作：

a. 建立 netapp-acc-operator 命名空間：

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

回應：

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

b. 為建立秘密 netapp-acc-operator 命名空間。新增Docker資訊並執行下列命令：



預留位置 `your_registry_path` 應與您先前上傳的影像位置相符（例如、`[Registry_URL]/netapp/astra/astracc/22.11.0-82`）。

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

回應範例：

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



如果在產生機密之後刪除命名空間、請重新建立命名空間、然後重新產生命名空間的機密。

c. 建立 netapp-acc （或自訂命名）命名空間。

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

回應範例：

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

d. 為建立秘密 netapp-acc （或自訂命名）命名空間。新增Docker資訊並執行下列命令：

```
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]
```

回應

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

安裝Astra Control Center操作員

1. 變更目錄：

```
cd manifests
```

2. 編輯Astra Control Center營運者部署Yaml (astra_control_center_operator_deploy.yaml) 以參考您的本機登錄和機密。

```
vim astra_control_center_operator_deploy.yaml
```



附註的Y反 洗錢範例遵循下列步驟。

a. 如果您使用需要驗證的登錄、請取代的預設行 `imagePullSecrets: []` 提供下列功能：

```
imagePullSecrets:  
- name: astra-registry-cred
```

- b. 變更 `[your_registry_path]` 適用於 `kube-rbac-proxy` 映像到您在中推入映像的登錄路徑 [上一步](#)。
- c. 變更 `[your_registry_path]` 適用於 `acc-operator-controller-manager` 映像到您在中推入映像的登錄路徑 [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:[version x.y.z]
          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. 安裝Astra Control Center操作員：

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

回應範例：

```
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. 確認Pod正在執行：

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

設定Astra控制中心

1. 編輯Astra Control Center自訂資源 (CR) 檔案 (astra_control_center.yaml) 進行帳戶、支援、登錄及其他必要設定：

```
vim astra_control_center.yaml
```



附註的Y反洗錢範例遵循下列步驟。

2. 修改或確認下列設定：

`accountName`

設定	指導	類型	範例
accountName	變更 accountName 字串至您要與Astra Control Center帳戶建立關聯的名稱。只能有一個帳戶名稱。	字串	Example

`astraVersion`

設定	指導	類型	範例
astraVersion	要部署的Astra Control Center版本。此設定不需要任何動作、因為此值將預先填入。	字串	22.11.0-82

<code>astraAddress</code>

設定	指導	類型	範例
<code>astraAddress</code>	變更 <code>astraAddress</code> 字串至您要在瀏覽器中使用的FQDN (建議) 或IP位址、以存取Astra Control Center。此位址定義Astra Control Center在資料中心的找到方式、以及當您完成配置時、從負載平衡器配置的相同FQDN或IP位址 " Astra Control Center需求 "。附註：請勿使用 <code>http://</code> 或 <code>https://</code> 地址中。複製此FQDN以供在中使用 後續步驟 。	字串	<code>astra.example.com</code>

<code>autoSupport</code>

您在本節中的選擇決定您是否會參與NetApp主動式支援應用程式NetApp Active IQ 功能、以及資料的傳送位置。需要網際網路連線 (連接埠4442)、所有支援資料都會匿名。

設定	使用	指導	類型	範例
<code>autoSupport.enrolled</code>	也可以 <code>enrolled</code> 或 <code>url</code> 必須選取欄位	變更 <code>enrolled for</code> 解決方案AutoSupport <code>false</code> 適用於沒有網際網路連線或無法保留的網站 <code>true</code> 適用於連線站台。的設定 <code>true</code> 可將匿名資料傳送至NetApp以供支援之用。預設選項為 <code>false</code> 並表示不會將任何支援資料傳送給NetApp。	布林值	<code>false</code> (此值為預設值)
<code>autoSupport.url</code>	也可以 <code>enrolled</code> 或 <code>url</code> 必須選取欄位	此URL決定匿名資料的傳送位置。	字串	https://support.netapp.com/asupprod/post/1.0/postAsup

<code>email</code>

設定	指導	類型	範例
email	變更 email 字串至預設的初始系統管理員位址。複製此電子郵件地址以供在中使用 後續步驟 。此電子郵件地址將作為初始帳戶登入UI的使用者名稱、並會收到Astra Control中事件的通知。	字串	admin@example.com

<code>firstName</code>

設定	指導	類型	範例
firstName	與Astra帳戶相關聯的預設初始系統管理員的名字。第一次登入後、此處使用的名稱會顯示在UI的標題中。	字串	SRE

<code>lastName</code>

設定	指導	類型	範例
lastName	與Astra帳戶相關聯的預設初始管理員姓氏。第一次登入後、此處使用的名稱會顯示在UI的標題中。	字串	Admin

<code>imageRegistry</code>

您在本節中的選擇定義了裝載Astra應用程式映像、Astra Control Center運算子和Astra Control Center Helm儲存庫的容器映像登錄。

設定	使用	指導	類型	範例
<code>imageRegistry.name</code>	必要	您在中推入映像的映像登錄名稱 上一步 。請勿使用 <code>http://</code> 或 <code>https://</code> 在登錄名稱中。	字串	<code>example.registry.com/astra</code>
<code>imageRegistry.secret</code>	如果您輸入的字串則為必要 <code>imageRegistry.name</code> requires a secret. IMPORTANT: If you are using a registry that does not require authorization, you must delete this <code>secret</code> 行內 <code>imageRegistry</code> 否則安裝將會失敗。	用來驗證映像登錄的Kubernetes機密名稱。	字串	<code>astra-registry-cred</code>

<code>storageClass</code>

設定	指導	類型	範例
storageClass	變更 storageClass 價值來源 ontap-gold 安裝所需的另一個Trident storageClass資源。執行命令 kubectl get sc 以判斷您現有的已設定儲存類別。必須在資訊清單檔案中輸入其中一個Trident型儲存類別 (astra-control-center-<version>.manifest) 、並將用於Astra PV。如果未設定、則會使用預設的儲存類別。附註：如果已設定預設儲存類別、請確定它是唯一具有預設附註的儲存類別。	字串	ontap-gold

<code>volumeReclaimPolicy</code>

設定	指導	類型	選項
volumeReclaimPolicy	這為Astra的PV設定回收原則。將此原則設定為 Retain 刪除Astra後保留持續磁碟區。將此原則設定為 Delete 刪除Astra後刪除持續磁碟區。如果未設定此值、則會保留PV。	字串	<ul style="list-style-type: none">• Retain (這是預設值)• Delete

`<code>ingressType</code>`

設定	指導	類型	選項
ingressType	<p>使用下列其中一種入口類型：Generic (ingressType: "Generic") (預設) 當您使用另一個入口控制器、或偏好使用自己的入口控制器時、請使用此選項。部署Astra Control Center之後、您需要設定 "入口控制器" 使用URL公開Astra Control Center</p> <ul style="list-style-type: none">◦ AccTraefik (ingressType: "AccTraefik") 如果您不想設定入口控制器、請使用此選項。這會部署Astra控制中心 traefik 作為Kubernetes負載平衡器類型服務的閘道。Astra Control Center使用「負載平衡器」類型的服務 (svc/traefik (在Astra Control Center命名空間中)、並要求指派可存取的外部IP位址。如果您的環境允許負載平衡器、但您尚未設定負載平衡器、則可以使用MetalLB或其他外部服務負載平衡器、將外部IP位址指派給服務。在內部DNS伺服器組態中、您應該將Astra Control Center所選的DNS名稱指向負載平衡的IP位址。附註：如需有關「負載平衡器」和入口的服務類型詳細資訊、請參閱 "需求"。	字串	<ul style="list-style-type: none">• Generic (這是預設值)• AccTraefik

`<code>astraResourcesScaler</code>`

設定	指導	類型	選項
<code>astraResourcesScaler</code>	<p>適用的擴充選項適用於適用的適用範圍。依預設、Astra Control Center會針對Astra內的大部分元件設定資源要求來進行部署。此組態可讓Astra Control Center軟體堆疊在應用程式負載和擴充性增加的環境中、發揮更佳效能。不過、在使用較小開發或測試叢集的案例中、則是使用「CR」欄位</p> <p><code>astraResourcesScaler</code> 可能設為 <code>Off</code>。這會停用資源要求、並允許在較小的叢集上部署。</p>	字串	<ul style="list-style-type: none">• Default (這是預設值)• Off

`<code>crds</code>`

您在本節中的選擇決定Astra Control Center應如何處理客戶需求日。

設定	指導	類型	範例
<code>crds.externalCertManager</code>	如果您使用外部憑證管理程式、請變更 <code>externalCertManager</code> 至 <code>true</code> 。預設值 <code>false</code> 讓Astra Control Center在安裝期間安裝自己的憑證管理程式客戶檔案。CRD是整個叢集的物件、安裝這些物件可能會影響叢集的其他部分。您可以使用此旗標向Astra控制中心發出訊號、表示這些客戶需求日將由Astra控制中心外部的叢集管理員安裝及管理。	布林值	<code>False</code> (此值為預設值)
<code>crds.externalTraefik</code>	依預設、Astra Control Center會安裝必要的Traefik客戶需求日。CRD是整個叢集的物件、安裝這些物件可能會影響叢集的其他部分。您可以使用此旗標向Astra控制中心發出訊號、表示這些客戶需求日將由Astra控制中心外部的叢集管理員安裝及管理。	布林值	<code>False</code> (此值為預設值)

`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"
  astraResourcesScaler: "Default"
  additionalValues: {}
  crds:
    externalTraefik: false
    externalCertManager: false
```

完整的Astra控制中心和操作員安裝

1. 如果您尚未在上一步中執行此動作、請建立 netapp-acc (或自訂) 命名空間：

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

回應範例：

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

2. 在中安裝Astra Control Center netapp-acc (或自訂) 命名空間：

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

回應範例：

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

驗證系統狀態

您可以使用kubect命令來驗證系統狀態。如果您偏好使用OpenShift、您可以使用相似的相關命令來進行驗證步驟。

步驟

1. 驗證是否已成功安裝所有系統元件。

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

每個Pod的狀態應為 Running。部署系統Pod可能需要幾分鐘的時間。

回應範例

NAME	READY	STATUS	
RESTARTS			AGE
acc-helm-repo-76d8d845c9-ggds2	1/1	Running	0
14m			
activity-6cc67ff9f4-z48mr	1/1	Running	2
(8m32s ago)			9m
api-token-authentication-7s67v	1/1	Running	0
8m56s			
api-token-authentication-bplb4	1/1	Running	0
8m56s			
api-token-authentication-p2c9z	1/1	Running	0
8m56s			
asup-6cdfbc6795-md8vn	1/1	Running	0
9m14s			
authentication-9477567db-8hnc9	1/1	Running	0
7m4s			
bucket-service-f4dbdfcd6-wqzkw	1/1	Running	0
8m48s			
cert-manager-bb756c7c4-wm2cv	1/1	Running	0
14m			
cert-manager-cainjector-c9bb86786-8wrf5	1/1	Running	0
14m			
cert-manager-webhook-dd465db99-j2w4x	1/1	Running	0
14m			
certificates-68dff9cdd6-kcvml	1/1	Running	2
(8m43s ago)			9m2s
certificates-68dff9cdd6-rsnsb	1/1	Running	0
9m2s			
cloud-extension-69d48c956c-2s8dt	1/1	Running	3
(8m43s ago)			9m24s
cloud-insights-service-7c4f48b978-7gvlh	1/1	Running	3
(8m50s ago)			9m28s
composite-compute-7d9ff5f68-nxbhl	1/1	Running	0
8m51s			
composite-volume-57b4756d64-nl66d	1/1	Running	0
9m13s			
credentials-6dbc55f89f-qpzff	1/1	Running	0
11m			
entitlement-67bfb6d7-gl6kp	1/1	Running	4
(8m33s ago)			9m38s
features-856cc4dccc-mxbdb	1/1	Running	0
9m20s			
fluent-bit-ds-4rtsp	1/1	Running	0

6m54s			
fluent-bit-ds-9rq1l	1/1	Running	0
6m54s			
fluent-bit-ds-w5mp7	1/1	Running	0
6m54s			
graphql-server-7c7cc49776-jz2kn	1/1	Running	0
2m29s			
identity-87c59c975-9jpnf	1/1	Running	0
9m6s			
influxdb2-0	1/1	Running	0
13m			
keycloak-operator-84ff6d59d4-qcnmc	1/1	Running	0
7m1s			
krakend-cbf6c7df9-mdtzv	1/1	Running	0
2m30s			
license-5b888b78bf-plj6j	1/1	Running	0
9m32s			
login-ui-846b4664dd-fz8hv	1/1	Running	0
2m24s			
loki-0	1/1	Running	0
13m			
metrics-facade-779cc9774-n26rw	1/1	Running	0
9m18s			
monitoring-operator-974db78f-pkspq	2/2	Running	0
6m58s			
nats-0	1/1	Running	0
13m			
nats-1	1/1	Running	0
13m			
nats-2	1/1	Running	0
13m			
nautilus-7bdc7ddc54-49tfn	1/1	Running	0
7m50s			
nautilus-7bdc7ddc54-cwc79	1/1	Running	0
9m36s			
openapi-5584ff9f46-gbrdj	1/1	Running	0
9m17s			
openapi-5584ff9f46-z9mzk	1/1	Running	0
9m17s			
packages-bfc58cc98-lpxq9	1/1	Running	0
8m58s			
polaris-consul-consul-server-0	1/1	Running	0
13m			
polaris-consul-consul-server-1	1/1	Running	0
13m			
polaris-consul-consul-server-2	1/1	Running	0

13m			
polaris-keycloak-0	1/1	Running	3
(6m15s ago) 6m56s			
polaris-keycloak-1	1/1	Running	0
4m22s			
polaris-keycloak-2	1/1	Running	0
3m41s			
polaris-keycloak-db-0	1/1	Running	0
6m56s			
polaris-keycloak-db-1	1/1	Running	0
4m23s			
polaris-keycloak-db-2	1/1	Running	0
3m36s			
polaris-mongodb-0	2/2	Running	0
13m			
polaris-mongodb-1	2/2	Running	0
13m			
polaris-mongodb-2	2/2	Running	0
12m			
polaris-ui-5ccff47897-8rzgh	1/1	Running	0
2m33s			
polaris-vault-0	1/1	Running	0
13m			
polaris-vault-1	1/1	Running	0
13m			
polaris-vault-2	1/1	Running	0
13m			
public-metrics-6cb7bfc49b-p54xm	1/1	Running	1
(8m29s ago) 9m31s			
storage-backend-metrics-5c77994586-kjn48	1/1	Running	0
8m52s			
storage-provider-769fdc858c-62w54	1/1	Running	0
8m54s			
task-service-9ffc484c5-kx9f4	1/1	Running	3
(8m44s ago) 9m34s			
telegraf-ds-bphb9	1/1	Running	0
6m54s			
telegraf-ds-rtsm2	1/1	Running	0
6m54s			
telegraf-ds-s9h5h	1/1	Running	0
6m54s			
telegraf-rs-lbpv7	1/1	Running	0
6m54s			
telemetry-service-57cfb998db-zjx78	1/1	Running	1
(8m40s ago) 9m26s			
tenancy-5d5dfbcf9f-vmbxh	1/1	Running	0

```

9m5s
traefik-7b87c4c474-jmgrp2      1/1      Running   0
2m24s
traefik-7b87c4c474-t9k8x      1/1      Running   0
2m24s
trident-svc-c78f5b6bd-nwdsq   1/1      Running   0
9m22s
vault-controller-55bbc96668-c6425 1/1      Running   0
11m
vault-controller-55bbc96668-lq9n9 1/1      Running   0
11m
vault-controller-55bbc96668-rfkgg 1/1      Running   0
11m

```

- (選用) 若要確保安裝完成、您可以觀看 `acc-operator` 使用下列命令記錄。

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



`accHost` 叢集登錄是最後一項作業、如果失敗、也不會導致部署失敗。如果記錄中指出叢集登錄失敗、您可以透過再次嘗試登錄 ["在UI中新增叢集工作流程"](#) 或API。

- 當所有Pod都在執行時、請確認安裝成功 (READY 是 True) 並取得您登入Astra Control Center時所使用的初始設定密碼：

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

回應：

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	22.11.0-82	10.111.111.111
True			



複製UUID值。密碼是 ACC- 接著是UUID值 (ACC-[UUID] 或者、在此範例中、ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f)。

設定入口以進行負載平衡

您可以設定Kubernetes入口控制器來管理外部服務存取。如果您使用的預設值、這些程序會提供入口控制器的設定範例 `ingressType: "Generic"` Astra Control Center自訂資源 (`astra_control_center.yaml`)。如果您指定、則不需要使用此程序 `ingressType: "AccTraefik"` Astra Control Center自訂資源

(astra_control_center.yaml)。

部署Astra Control Center之後、您需要設定入口控制器、以URL顯示Astra Control Center。

設定步驟視您使用的入口控制器類型而有所不同。Astra Control Center支援多種入站控制器類型。這些設定程序提供下列入口控制器類型的範例步驟：

- Istio入口
- Nginx入口控制器
- OpenShift入口控制器

您需要的產品

- 必要的 "入口控制器" 應已部署。
- "入口等級" 應已建立對應於入口控制器的。

Istio入侵步驟

1. 設定Istio入口。



此程序假設使用「預設」組態設定檔來部署Istio。

2. 收集或建立Ingress閘道所需的憑證和私密金鑰檔案。

您可以使用CA簽署或自我簽署的憑證。一般名稱必須是Astra位址 (FQDN)。

命令範例：

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

3. 建立秘密 `tls secret name` 類型 `kubernetes.io/tls` 中的TLS私密金鑰和憑證 `istio-system namespace` 如TLS機密所述。

命令範例：

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



機密名稱應與相符 `spec.tls.secretName` 提供於 `istio-ingress.yaml` 檔案：

4. 在中部署入口資源 `netapp-acc` (或自訂命名) 命名空間、使用v1資源類型作為架構 (`istio-ingress.yaml` 在本例中使用)：


```

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. 套用變更：

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

6. 檢查入侵狀態：

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

回應：

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

7. 完成Astra Control Center安裝。

適用於Nginx像 控制器的步驟

1. 建立類型的秘密 kubernetes.io/tls 中的TLS私密金鑰和憑證 netapp-acc （或自訂命名）命名空間、如所述 "TLS機密"。
2. 在中部署入口資源 netapp-acc （或自訂命名）命名空間、使用v1資源類型作為架構 (nginx-Ingress.yaml 在本例中使用) ：

```
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. 套用變更：

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



NetApp建議將Nginx像 控制器安裝為部署、而非 daemonSet。

OpenShift入口控制器的步驟

1. 取得您的憑證、取得可供OpenShift路由使用的金鑰、憑證和CA檔案。
2. 建立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
```

登入Astra Control Center UI

安裝Astra Control Center之後、您將變更預設管理員的密碼、並登入Astra Control Center UI儀表板。

步驟

1. 在瀏覽器中、輸入 FQDN (包括 `https://` 字首) `astraAddress` 在中 `astra_control_center.yaml` 請於何時進行 [您安裝了Astra Control Center](#)。
2. 收到提示時、請接受自我簽署的憑證。



您可以在登入後建立自訂憑證。

3. 在Astra Control Center登入頁面、輸入您使用的值 `email` 在中 `astra_control_center.yaml` 請於何時進行 [您安裝了Astra Control Center](#)，然後輸入初始設定密碼 (`ACC-[UUID]`)。



如果您輸入錯誤密碼三次、系統將鎖定管理員帳戶15分鐘。

4. 選擇*登入*。
5. 出現提示時變更密碼。



如果這是您第一次登入、但您忘記密碼、而且尚未建立其他管理使用者帳戶、請聯絡 ["NetApp支援"](#) 以取得密碼恢復協助。

6. (選用) 移除現有的自我簽署TLS憑證、並以取代 ["由憑證授權單位 \(CA\) 簽署的自訂TLS憑證"](#)。

疑難排解安裝

如果有任何服務存在 `ERROR` 狀態、您可以檢查記錄。尋找400到500範圍內的API回應代碼。這些都表示發生故障的地點。

步驟

1. 若要檢查Astra控制中心的操作員記錄、請輸入下列內容：

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

下一步

- (選用) 視您的環境而定、請在安裝後完成 ["組態步驟"](#)。
- 執行以完成部署 ["設定工作"](#)。

=
:allow-uri-read:

使用OpenShift作業系統集線器安裝Astra Control Center

如果您使用Red Hat OpenShift、可以使用Red Hat認證的操作員來安裝Astra Control Center。請使用此程序從安裝Astra Control Center ["Red Hat生態系統目錄"](#) 或使用Red Hat OpenShift Container Platform。

完成此程序之後、您必須返回安裝程序、才能完成 ["剩餘步驟"](#) 以驗證安裝是否成功並登入。

您需要的產品

- 符合環境先決條件：["開始安裝之前、請先準備好環境以進行Astra Control Center部署"](#)。
- 健全的叢集運算子與API服務：
 - 從OpenShift叢集確保所有叢集操作員都處於健全狀態：

```
oc get clusteroperators
```

- 從OpenShift叢集、確保所有API服務都處於健全狀態：

```
oc get apiservices
```

- * FQDN位址*：取得資料中心Astra Control Center的FQDN位址。
- * OpenShift權限*：取得必要的權限並存取Red Hat OpenShift Container Platform、以執行所述的安裝步驟。
- 已設定的憑證管理程式：如果叢集中已存在憑證管理程式、您需要執行某些作業 ["必要步驟"](#) 因此Astra Control Center不會安裝自己的憑證管理程式。依預設、Astra Control Center會在安裝期間安裝自己的憑證管理程式。
- * Kubernetes入口控制器*：如果您有一個Kubernetes入口控制器來管理外部服務存取、例如叢集中的負載平衡、您就需要將其設定為與Astra Control Center搭配使用：
 - a. 建立運算子命名空間：

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

- b. ["完成設定"](#) 適用於您的入口控制器類型。

步驟

- [下載並擷取Astra Control Center](#)
- [安裝NetApp Astra kubecl外掛程式](#)
- [\[將映像新增至本機登錄\]](#)
- [\[尋找操作員安裝頁面\]](#)

- [\[安裝操作員\]](#)
- [安裝Astra Control Center](#)

下載並擷取Astra Control Center

1. 前往 "[Astra Control Center評估下載頁面](#)" 於 NetApp 支援網站。
2. 下載包含Astra Control Center的套裝組合 (astra-control-center-[version].tar.gz) 。
3. (建議但可選) 下載Astra Control Center的憑證與簽名套件 (astra-control-center-certs-[version].tar.gz) 若要驗證套件的簽名：

```
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
```

隨即顯示輸出 Verified OK 驗證成功之後。

4. 從Astra Control Center套裝組合擷取映像：

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

安裝NetApp Astra kubectl外掛程式

NetApp Astra kubectl命令列外掛程式可在執行與部署及升級Astra Control Center相關的一般工作時節省時間。

您需要的產品

NetApp為不同的CPU架構和作業系統提供外掛程式二進位檔。執行此工作之前、您必須先瞭解您的CPU和作業系統。

步驟

1. 列出可用的NetApp Astra kubectl外掛程式二進位檔、並記下作業系統和CPU架構所需的檔案名稱：



KECBECTI外掛程式庫是tar套件的一部分、會擷取到資料夾中 kubectl-astra 。

```
ls kubectl-astra/
```

2. 將正確的二進位檔移至目前路徑、並將其重新命名為 kubectl-astra：

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

將映像新增至本機登錄

1. 為您的Container引擎完成適當的步驟順序：

Docker

1. 切換到tar檔案的根目錄。您應該會看到這個檔案和目錄：

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

2. 將Astra Control Center映像目錄中的套件映像推送到本機登錄。執行之前、請先進行下列替換 `push-images` 命令：
 - 以<BUNDLE_FILE> Astra Control套裝組合檔案的名稱取代 (`acc.manifest.bundle.yaml`)。
 - 以<MY_FULL_REGISTRY_PATH> Docker儲存庫的URL取代支援；例如 "`<a href="https://<docker-registry>"; class="bare">https://<docker-registry>;`"。
 - 以<MY_REGISTRY_USER> 使用者名稱取代。
 - 以<MY_REGISTRY_TOKEN> 登錄的授權權杖取代。

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

Podman

1. 切換到tar檔案的根目錄。您應該會看到這個檔案和目錄：

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

2. 登入您的登錄：

```
podman login <YOUR_REGISTRY>
```

3. 針對您使用的Podman版本、準備並執行下列其中一個自訂指令碼。以包含任何子目錄的儲存庫URL取代<MY_FULL_REGISTRY_PATH>。

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

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
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=22.11.0-82
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
```



指令碼所建立的映像路徑應如下所示、視登錄組態而定：

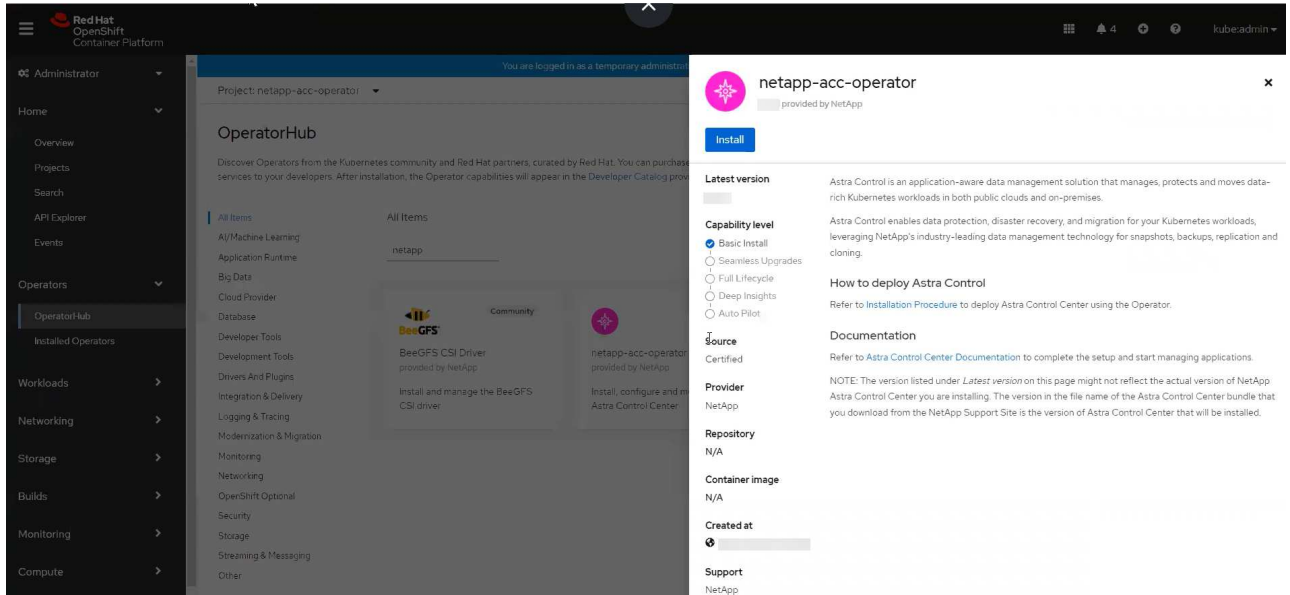
<https://netappdownloads.jfrog.io/docker-astra-control-prod/netapp/astra/acc/22.11.0-82/image:version>

尋找操作員安裝頁面

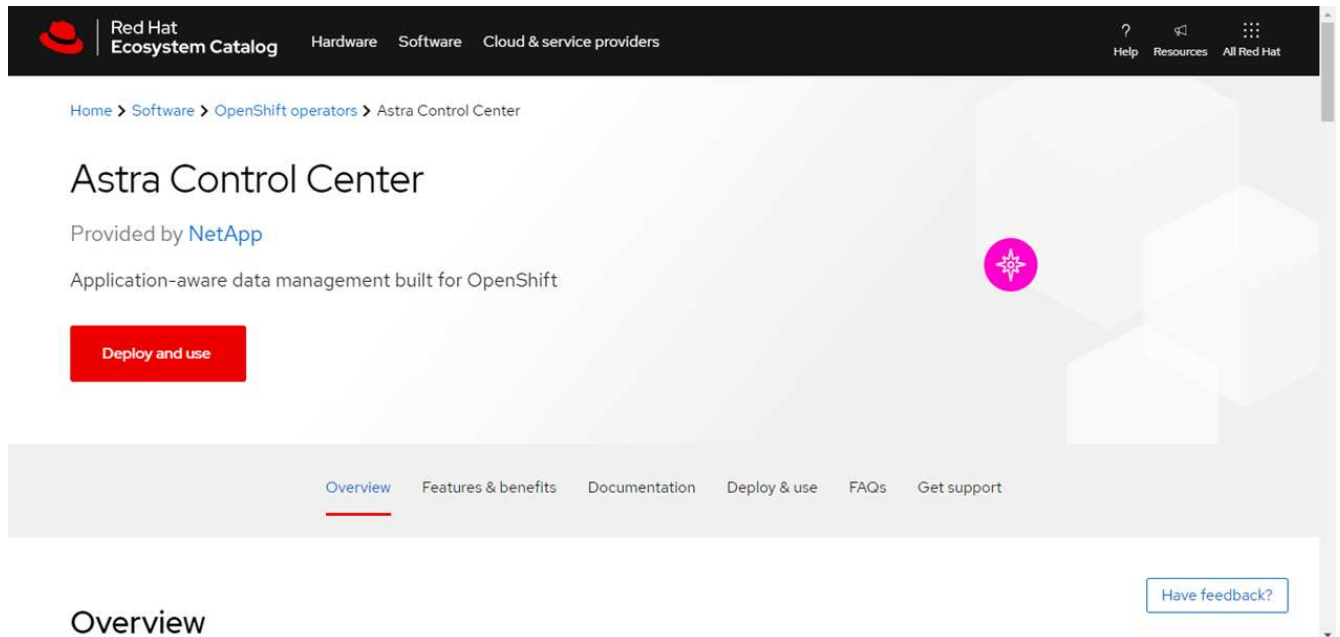
1. 請完成下列其中一個程序、以存取操作員安裝頁面：

- 從Red Hat OpenShift Web主控台：
 - i. 登入OpenShift Container Platform UI ◦

- ii. 從側功能表中、選取*運算子>運算子中樞*。
- iii. 搜尋並選擇NetApp Astra Control Center營運者。




- 從Red Hat生態系統目錄：
 - i. 選擇NetApp Astra Control Center "營運者"。
 - ii. 選擇*部署和使用*。



安裝操作員

1. 完成*安裝操作員*頁面並安裝操作員：

 此運算子可用於所有叢集命名空間。

- a. 選取運算子命名空間或 netapp-acc-operator 命名空間將會自動建立、做為操作員安裝的一部分。

b. 選取手動或自動核准策略。



建議手動核准。每個叢集只能執行單一運算子執行個體。

c. 選擇*安裝*。

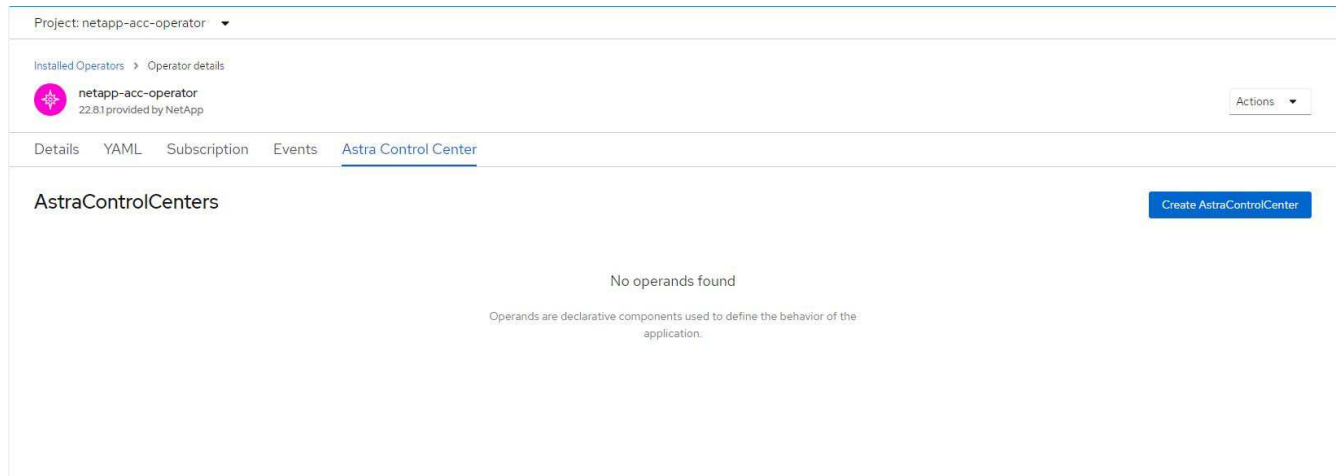


如果您選擇手動核准策略、系統會提示您核准此操作員的手動安裝計畫。

2. 從主控台移至「作業系統集線器」功能表、確認操作員已成功安裝。

安裝Astra Control Center

1. 從Astra控制中心操作員* Astra控制中心*索引標籤內的主控台、選取*建立適用的*



2. 完成 Create AstraControlCenter 表單欄位：

- 保留或調整Astra Control Center名稱。
- 新增Astra Control Center的標籤。
- 啟用或停用自動支援。建議保留「自動支援」功能。
- 輸入Astra Control Center FQDN或IP位址。請勿進入 `http://` 或 `https://` 在「地址」欄位中。
- 輸入Astra Control Center版本、例如22.04.1。
- 輸入帳戶名稱、電子郵件地址和管理員姓氏。
- 選擇的Volume回收原則 Retain、Recycle、或 Delete。預設值為 Retain。
- 選取入口類型：

▪ **Generic** (ingressType: "Generic") (預設)

如果您使用另一個入口控制器、或偏好使用自己的入口控制器、請使用此選項。部署Astra Control Center之後、您需要設定 "入口控制器" 使用URL公開Astra Control Center。

▪ **AccTraefik** (ingressType: "AccTraefik")

如果您不想設定入口控制器、請使用此選項。這會部署Astra控制中心 traefik 閘道即

Kubernetes 「負載平衡器」 類型服務。

Astra Control Center使用「負載平衡器」類型的服務 (svc/traefik (在Astra Control Center命名空間中)、並要求指派可存取的外部IP位址。如果您的環境允許負載平衡器、但您尚未設定負載平衡器、則可以使用MetalLB或其他外部服務負載平衡器、將外部IP位址指派給服務。在內部DNS伺服器組態中、您應該將Astra Control Center所選的DNS名稱指向負載平衡的IP位址。



如需有關「負載平衡器」和入口服務類型的詳細資訊、請參閱 ["需求"](#)。

- a. 在*映像登錄*中、輸入您的本機容器映像登錄路徑。請勿進入 http:// 或 https:// 在「地址」欄位中。
- b. 如果您使用需要驗證的映像登錄、請輸入映像秘密。



如果您使用需要驗證的登錄、[在叢集上建立秘密](#)。

- c. 輸入管理員名字。
- d. 設定資源擴充。
- e. 提供預設的儲存類別。



如果已設定預設儲存類別、請確定它是唯一具有預設註釋的儲存類別。

- f. 定義客戶需求日處理偏好設定。
3. 選取「Yaml」檢視以檢閱您所選的設定。
 4. 選取 Create。

建立登錄機密

如果您使用需要驗證的登錄、請在Openshift叢集上建立密碼、然後在中輸入密碼名稱 Create AstraControlCenter 表單欄位。

1. 為Astra Control Center運算子建立命名空間：

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

2. 在此命名空間中建立秘密：

```
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僅支援Docker登錄機密。

3. 填寫中的其餘欄位 [「Create」](#) ([建立](#)) [「吧！Control Center」](#) 表單欄位。

下一步

完成 "剩餘步驟" 若要驗證Astra Control Center是否安裝成功、請設定入口控制器（選用）、然後登入UI。此外、您還需要執行 "設定工作" 安裝完成後。

安裝Astra Control Center搭配Cloud Volumes ONTAP 一套功能性儲存後端

有了Astra Control Center、您就能在混合雲環境中使用自我管理的Kubernetes叢集和Cloud Volumes ONTAP 實例來管理應用程式。您可以在內部部署的Kubernetes叢集或雲端環境中的其中一個自我管理Kubernetes叢集上部署Astra Control Center。

有了其中一項部署、您就能使用Cloud Volumes ONTAP 下列其中一項部署、以下列方式執行應用程式資料管理作業：將NetApp當成儲存後端。您也可以將S3儲存區設定為備份目標。

若要在Amazon Web Services (AWS)、Google Cloud Platform (GCP) 和Microsoft Azure中安裝Astra Control Center、並搭配Cloud Volumes ONTAP 使用整套儲存後端、請視您的雲端環境而定、執行下列步驟。

- [在Amazon Web Services中部署Astra Control Center](#)
- [在Google Cloud Platform中部署Astra Control Center](#)
- [在Microsoft Azure中部署Astra Control Center](#)

您可以使用自我管理的Kubernetes叢集、例如OpenShift Container Platform (OCP)、在發佈版本中管理應用程式。只有自我管理的OCP叢集已通過驗證、可用於部署Astra Control Center。

在Amazon Web Services中部署Astra Control Center

您可以在Amazon Web Services (AWS) 公有雲上的自我管理Kubernetes叢集上部署Astra Control Center。

AWS所需的功能

在AWS中部署Astra Control Center之前、您需要下列項目：

- Astra Control Center授權。請參閱 "[Astra Control Center授權要求](#)"。
- "[符合Astra Control Center的要求](#)"。
- NetApp Cloud Central帳戶
- 如果使用OCP、則Red Hat OpenShift Container Platform (OCP) 權限（位於命名空間層級以建立Pod）
- AWS認證資料、存取ID和秘密金鑰、具備可讓您建立儲存區和連接器的權限
- AWS帳戶彈性容器登錄（ECR）存取與登入
- 存取Astra Control UI所需的AWS託管區域和Route 53項目

AWS的作業環境需求

Astra Control Center需要下列AWS作業環境：

- Red Hat OpenShift Container Platform 4.8.



確保您選擇裝載Astra Control Center的作業環境符合環境正式文件中所述的基本資源需求。

除了環境的資源需求之外、Astra Control Center還需要下列資源：

元件	需求
後端NetApp Cloud Volumes ONTAP 功能儲存容量	至少提供300 GB
工作者節點 (AWS EC2需求)	總共至少3個工作節點、每個節點有4個vCPU核心和12GB RAM
負載平衡器	服務類型「負載平衡器」可用於將入口流量傳送至作業環境叢集中的服務
FQDN	將Astra Control Center的FQDN指向負載平衡IP位址的方法
Astra Trident (安裝於NetApp BlueXP (前身為Cloud Manager) 的Kubernetes叢集探索中)	Astra Trident 21.004或更新版本已安裝並設定、且NetApp ONTAP 的版本9.5或更新為儲存後端
映像登錄	<p>您必須擁有現有的私有登錄、例如AWS Elastic Container登錄、才能將Astra Control Center建置映像推入其中。您需要提供映像登錄的URL、以便上傳映像。</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Astra Control Center託管叢集和託管叢集必須能夠存取相同的映像登錄、才能使用還原型映像來備份和還原應用程式。</p> </div>
Astra Trident / ONTAP Estra組態	<p>Astra Control Center需要建立儲存類別、並將其設為預設儲存類別。Astra Control Center支援下列ONTAP 將Kubernetes叢集匯入NetApp BlueXP (前身為Cloud Manager) 時所建立的支援功能。這些資料由Astra Trident提供：</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san csi.trident.netapp.io</code>



這些需求假設Astra Control Center是營運環境中唯一執行的應用程式。如果環境正在執行其他應用程式、請相應調整這些最低需求。



AWS登錄權杖會在12小時內過期、之後您必須更新Docker映像登錄機密。

AWS部署總覽

以下是安裝Astra Control Center for AWS的程序總覽、Cloud Volumes ONTAP 其中包含以作為儲存後端的功能。

以下將詳細說明每個步驟。

1. [確保您擁有足夠的IAM權限](#)。
2. [在AWS上安裝RedHat OpenShift叢集](#)。
3. [設定AWS](#)。
4. [設定適用於AWS的NetApp BlueXP](#)。
5. [安裝AWS的Astra Control Center](#)。

確保您擁有足夠的IAM權限

確保您擁有足夠的IAM角色和權限、可讓您安裝RedHat OpenShift叢集和NetApp BlueXP（前身為Cloud Manager）Connector。

請參閱 ["初始 AWS 認證資料"](#)。

在AWS上安裝RedHat OpenShift叢集

在AWS上安裝RedHat OpenShift Container Platform叢集。

如需安裝指示、請參閱 ["在OpenShift Container Platform的AWS上安裝叢集"](#)。

設定AWS

接下來、設定AWS以建立虛擬網路、設定EC2運算執行個體、建立AWS S3儲存區、建立彈性容器登錄（ECR）以裝載Astra Control Center映像、然後將映像推送至此登錄。

請遵循AWS文件完成下列步驟。請參閱 ["AWS安裝文件"](#)。

1. 建立AWS虛擬網路。
2. 檢閱EC2運算執行個體。這可以是AWS中的裸機伺服器或VM。
3. 如果執行個體類型尚未符合主節點和工作節點的Astra最低資源需求、請在AWS中變更執行個體類型以符合Astra需求。請參閱 ["Astra Control Center需求"](#)。
4. 建立至少一個AWS S3儲存區來儲存備份。
5. 建立AWS彈性Container登錄（ECR）、以裝載所有的主動定速控制系統映像。



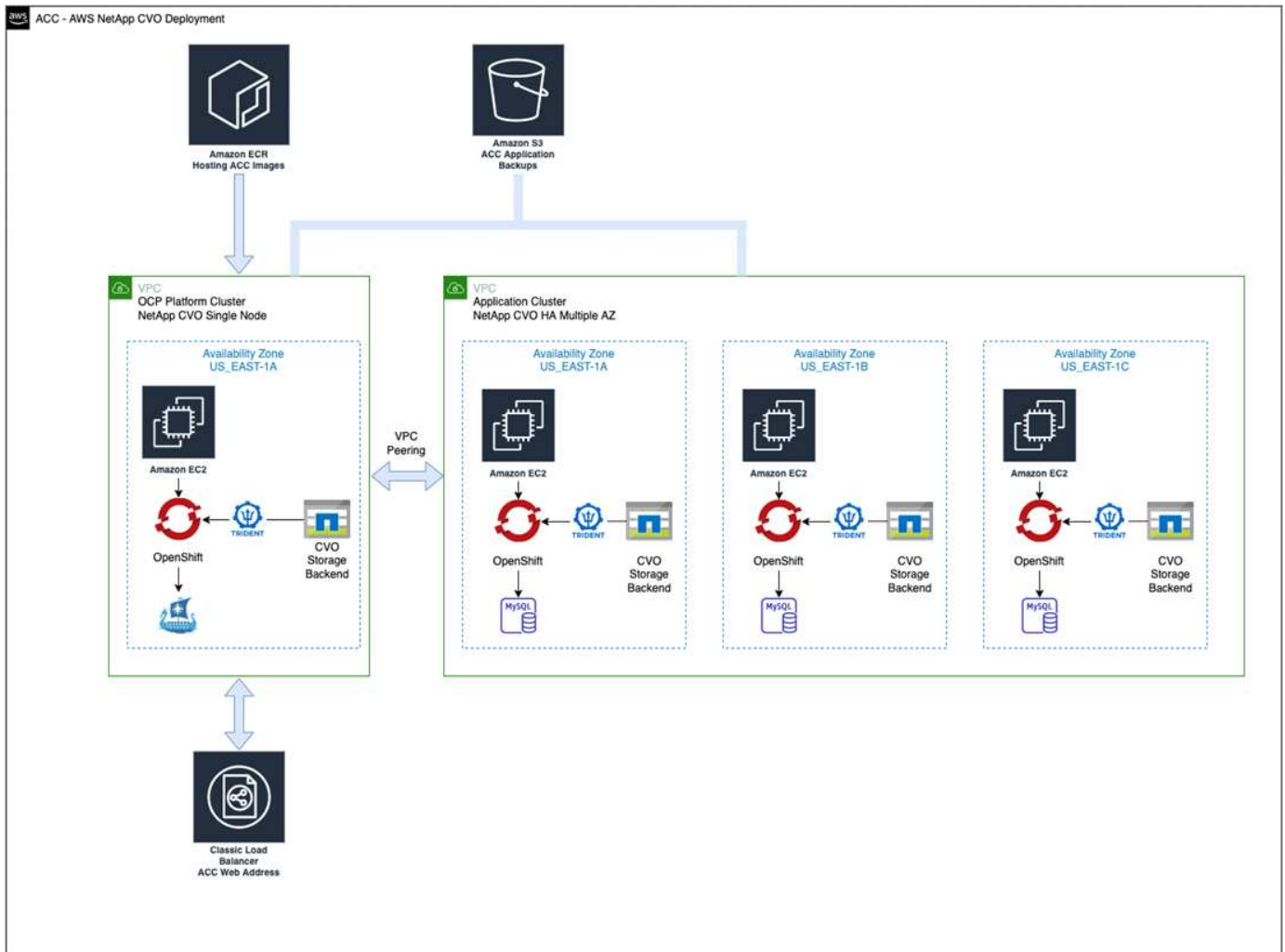
如果您未建立ECR、Astra Control Center將無法從含有Cloud Volumes ONTAP AWS後端的支援的叢集存取監控資料。此問題是因為您嘗試使用Astra Control Center探索及管理的叢集無法存取AWS ECR。

6. 將Acc映像推送到您定義的登錄。



AWS Elastic Container登錄（ECR）權杖會在12小時後過期、導致跨叢集複製作業失敗。從Cloud Volumes ONTAP 針對AWS設定的功能進行的功能區管理儲存後端時、就會發生此問題。若要修正此問題、請再次向ECR驗證、並產生新的秘密、讓複製作業順利恢復。

以下是AWS部署範例：



設定適用於AWS的NetApp BlueXP

使用NetApp BlueXP（前身為Cloud Manager）建立工作區、新增AWS連接器、建立工作環境、以及匯入叢集。

請遵循BlueXP文件完成下列步驟。請參閱下列內容：

- "開始使用Cloud Volumes ONTAP AWS的功能"。
- "使用BlueXP在AWS中建立連接器"

步驟

1. 將您的認證資料新增至BlueXP。
2. 建立工作區。
3. 新增AWS的連接器。選擇AWS做為供應商。
4. 為您的雲端環境建立工作環境。
 - a. 位置：「Amazon Web Services (AWS)」
 - b. 類型：Cloud Volumes ONTAP 「EHA」
5. 匯入OpenShift叢集。叢集將連線至您剛建立的工作環境。
 - a. 選擇* K8s*>*叢集清單*>*叢集詳細資料*、即可檢視NetApp叢集詳細資料。

- b. 請注意右上角的Trident版本。
- c. 請注意Cloud Volumes ONTAP、顯示NetApp為資源配置程式的叢集儲存類別。

這會匯入您的Red Hat OpenShift叢集、並將其指派為預設儲存類別。您可以選取儲存類別。Trident會在匯入和探索程序中自動安裝。

6. 請注意此Cloud Volumes ONTAP 功能部署中的所有持續磁碟區和磁碟區。



可作為單一節點或高可用度運作。Cloud Volumes ONTAP如果已啟用HA、請記下在AWS中執行的HA狀態和節點部署狀態。

安裝AWS的Astra Control Center

遵循標準 ["Astra Control Center安裝說明"](#)。



AWS使用一般S3儲存區類型。

在Google Cloud Platform中部署Astra Control Center

您可以在Google Cloud Platform (GCP) 公有雲上的自我管理Kubernetes叢集上部署Astra Control Center。

GCP的必備功能

在GCP中部署Astra Control Center之前、您需要下列項目：

- Astra Control Center授權。請參閱 ["Astra Control Center授權要求"](#)。
- ["符合Astra Control Center的要求"](#)。
- NetApp Cloud Central帳戶
- 如果使用OCP、Red Hat OpenShift Container Platform (OCP) 4.10
- 如果使用OCP、則Red Hat OpenShift Container Platform (OCP) 權限 (位於命名空間層級以建立Pod)
- GCP服務帳戶具備權限、可讓您建立貯體和連接器


GCP的作業環境需求



確保您選擇裝載Astra Control Center的作業環境符合環境正式文件中所述的基本資源需求。

除了環境的資源需求之外、Astra Control Center還需要下列資源：

元件	需求
後端NetApp Cloud Volumes ONTAP 功能儲存容量	至少提供300 GB
工作者節點 (GCP運算需求)	總共至少3個工作節點、每個節點有4個vCPU核心和12GB RAM
負載平衡器	服務類型「負載平衡器」可用於將入口流量傳送至作業環境叢集中的服務

元件	需求
FQDN (GCP DNS區域)	將Astra Control Center的FQDN指向負載平衡IP位址的方法
Astra Trident (安裝於NetApp BlueXP (前身為Cloud Manager) 的Kubernetes叢集探索中)	Astra Trident 21.004或更新版本已安裝並設定、且NetApp ONTAP 的版本9.5或更新為儲存後端
映像登錄	<p>您必須擁有現有的私有登錄、例如Google Container登錄、才能將Astra Control Center建置映像推送至該登錄。您需要提供映像登錄的URL、以便上傳映像。</p> <p> 您必須啟用匿名存取、才能拉出還原映像進行備份。</p>
Astra Trident / ONTAP Estra組態	<p>Astra Control Center需要建立儲存類別、並將其設為預設儲存類別。Astra Control Center支援下列ONTAP 將Kubernetes叢集匯入NetApp BlueXP時所建立的物件庫伯內特儲存類別。這些資料由Astra Trident提供：</p> <ul style="list-style-type: none"> • vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io • vsaworkingenvironment-<>-ha-san csi.trident.netapp.io • vsaworkingenvironment-<>-single-nas csi.trident.netapp.io • vsaworkingenvironment-<>-single-san csi.trident.netapp.io



這些需求假設Astra Control Center是營運環境中唯一執行的應用程式。如果環境正在執行其他應用程式、請相應調整這些最低需求。

GCP部署總覽

以下是將Astra Control Center安裝在GCP的自我管理OCP叢集上的程序總覽、Cloud Volumes ONTAP 其中包含以作儲存後端的功能。

以下將詳細說明每個步驟。

1. [在GCP上安裝RedHat OpenShift叢集](#)。
2. [建立GCP專案和虛擬私有雲端](#)。
3. [確保您擁有足夠的IAM權限](#)。
4. [設定GCP](#)。
5. [設定適用於GCP的NetApp BlueXP](#)。
6. [安裝Astra Control Center for GCP](#)。

在GCP上安裝RedHat OpenShift叢集

第一步是在GCP上安裝RedHat OpenShift叢集。

如需安裝指示、請參閱下列內容：

- ["在GCP中安裝OpenShift叢集"](#)
- ["建立GCP服務帳戶"](#)

建立GCP專案和虛擬私有雲端

建立至少一個GCP專案和虛擬私有雲端（VPC）。



OpenShift可能會建立自己的資源群組。此外、您也應該定義GCP VPC。請參閱OpenShift文件。

您可能想要建立平台叢集資源群組和目標應用程式OpenShift叢集資源群組。

確保您擁有足夠的IAM權限

確保您擁有足夠的IAM角色和權限、可讓您安裝RedHat OpenShift叢集和NetApp BlueXP（前身為Cloud Manager）Connector。

請參閱 ["初始GCP認證與權限"](#)。

設定GCP

接下來、設定GCP以建立VPC、設定運算執行個體、建立Google Cloud Object Storage、建立Google Container Register以裝載Astra Control Center映像、然後將映像推送至此登錄。

請遵循GCP文件完成下列步驟。請參閱在GCP中安裝OpenShift叢集。

1. 在您計畫用於具有CVO後端的OCP叢集的GCP中建立GCP專案和VPC。
2. 檢閱運算執行個體。這可以是GCP中的裸機伺服器或VM。
3. 如果執行個體類型尚未符合主節點和工作節點的Astra最低資源需求、請在GCP中變更執行個體類型以符合Astra需求。請參閱 ["Astra Control Center需求"](#)。
4. 建立至少一個GCP雲端儲存庫來儲存備份。
5. 建立儲存貯體存取所需的機密。
6. 建立Google Container登錄、以裝載所有Astra Control Center映像。
7. 設定所有Astra Control Center映像的Google Container登錄存取權、以供Docker推/拉。

範例：輸入下列指令碼、即可將Acc映像推送至此登錄：

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

此指令碼需要Astra Control Center資訊清單檔案和Google Image登錄位置。

範例：

```
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. 設定DNS區域。

設定適用於GCP的NetApp BlueXP

使用NetApp BlueXP（前身為Cloud Manager）建立工作區、將連接器新增至GCP、建立工作環境、以及匯入叢集。

請遵循BlueXP文件完成下列步驟。請參閱 ["從GCP開始使用Cloud Volumes ONTAP"](#)。

您需要的產品

- 以所需的IAM權限和角色存取GCP服務帳戶

步驟

1. 將您的認證資料新增至BlueXP。請參閱 ["新增GCP帳戶"](#)。
2. 新增GCP的連接器。
 - a. 選擇「GCP」作為供應商。
 - b. 輸入GCP認證。請參閱 ["從BlueXP在GCP中建立連接器"](#)。
 - c. 確認連接器正在執行、並切換至該連接器。
3. 為您的雲端環境建立工作環境。
 - a. 地點：「GCP」
 - b. 類型：Cloud Volumes ONTAP 「EHA」
4. 匯入OpenShift叢集。叢集將連線至您剛建立的工作環境。
 - a. 選擇* K8s*>*叢集清單*>*叢集詳細資料*、即可檢視NetApp叢集詳細資料。
 - b. 請注意右上角的Trident版本。
 - c. 請注意Cloud Volumes ONTAP、顯示「NetApp」為資源配置程式的叢集儲存類別。

這會匯入您的Red Hat OpenShift叢集、並將其指派為預設儲存類別。您可以選取儲存類別。Trident會在匯入和探索程序中自動安裝。

5. 請注意此Cloud Volumes ONTAP 功能部署中的所有持續磁碟區和磁碟區。



可作為單一節點或高可用度（HA）運作。Cloud Volumes ONTAP如果已啟用HA、請記下在GCP中執行的HA狀態和節點部署狀態。

安裝Astra Control Center for GCP

遵循標準 "[Astra Control Center安裝說明](#)"。



GCP使用通用S3儲存區類型。

1. 產生Docker祕密以擷取Astra Control Center安裝的映像：

```
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 Control Center

您可以將Astra Control Center部署在Microsoft Azure公有雲上的自我管理Kubernetes叢集上。

Azure的必備功能

在Azure中部署Astra Control Center之前、您需要下列項目：

- Astra Control Center授權。請參閱 "[Astra Control Center授權要求](#)"。
- "[符合Astra Control Center的要求](#)"。
- NetApp Cloud Central帳戶
- 如果使用OCP、Red Hat OpenShift Container Platform（OCP）4.8
- 如果使用OCP、則Red Hat OpenShift Container Platform（OCP）權限（位於命名空間層級以建立Pod）
- Azure認證、具備可讓您建立儲存區和連接器的權限

Azure的營運環境需求

確保您選擇裝載Astra Control Center的作業環境符合環境正式文件中所述的基本資源需求。

除了環境的資源需求之外、Astra Control Center還需要下列資源：

請參閱 "[Astra Control Center營運環境需求](#)"。

元件	需求
後端NetApp Cloud Volumes ONTAP 功能儲存容量	至少提供300 GB
工作者節點（Azure運算需求）	總共至少3個工作節點、每個節點有4個vCPU核心和12GB RAM

元件	需求
負載平衡器	服務類型「負載平衡器」可用於將入口流量傳送至作業環境叢集中的服務
FQDN (Azure DNS區域)	將Astra Control Center的FQDN指向負載平衡IP位址的方法
Astra Trident (安裝於NetApp BlueXP的Kubernetes叢集探索中)	Astra Trident 21.004或更新版本已安裝並設定、NetApp ONTAP 版本9.5或更新版本將作為儲存後端使用
映像登錄	<p>您必須擁有現有的私有登錄、例如Azure Container登錄 (ACR)、才能將Astra Control Center建置映像推送至該登錄。您需要提供映像登錄的URL、以便上傳映像。</p> <p> 您必須啟用匿名存取、才能拉出還原映像進行備份。</p>
Astra Trident / ONTAP Estra 組態	<p>Astra Control Center需要建立儲存類別、並將其設為預設儲存類別。Astra Control Center支援下列ONTAP 將Kubernetes叢集匯入NetApp BlueXP時所建立的物件庫伯內特儲存類別。這些資料由Astra Trident提供：</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san csi.trident.netapp.io</code>



這些需求假設Astra Control Center是營運環境中唯一執行的應用程式。如果環境正在執行其他應用程式、請相應調整這些最低需求。

Azure部署總覽

以下是安裝Astra Control Center for Azure的程序總覽。

以下將詳細說明每個步驟。

1. [在Azure上安裝RedHat OpenShift叢集](#)。
2. [建立Azure資源群組](#)。
3. [確保您擁有足夠的IAM權限](#)。
4. [設定Azure](#)。
5. [設定適用於Azure的NetApp BlueXP \(前身為Cloud Manager\)](#)。
6. [安裝及設定Azure的Astra Control Center](#)。

在Azure上安裝RedHat OpenShift叢集

第一步是在Azure上安裝RedHat OpenShift叢集。

如需安裝指示、請參閱下列內容：

- ["在Azure上安裝OpenShift叢集"](#)。
- ["安裝Azure帳戶"](#)。

建立Azure資源群組

建立至少一個Azure資源群組。



OpenShift可能會建立自己的資源群組。此外、您也應該定義Azure資源群組。請參閱OpenShift文件。

您可能想要建立平台叢集資源群組和目標應用程式OpenShift叢集資源群組。

確保您擁有足夠的IAM權限

確保您擁有足夠的IAM角色和權限、可讓您安裝RedHat OpenShift叢集和NetApp BlueXP Connector。

請參閱 ["Azure 認證與權限"](#)。

設定Azure

接下來、設定Azure以建立虛擬網路、設定運算執行個體、建立Azure Blob容器、建立Azure Container Register (ACR) 來裝載Astra Control Center映像、然後將映像推送至此登錄。

請依照Azure文件完成下列步驟。請參閱 ["在Azure上安裝OpenShift叢集"](#)。

1. 建立Azure虛擬網路。
2. 檢閱運算執行個體。這可以是Azure中的裸機伺服器或VM。
3. 如果執行個體類型尚未符合主節點和工作節點的Astra最低資源需求、請變更Azure中的執行個體類型以符合Astra要求。請參閱 ["Astra Control Center需求"](#)。
4. 建立至少一個Azure Blob容器來儲存備份。
5. 建立儲存帳戶。您需要儲存帳戶來建立容器、以便在Astra Control Center中作為儲存庫。
6. 建立儲存貯體存取所需的機密。
7. 建立Azure Container登錄 (ACR) 、以裝載所有Astra Control Center映像。
8. 設定Docker推/拉所有Astra Control Center影像的ACR存取。
9. 輸入下列指令碼、將Acc映像推入此登錄：

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

範例：

```
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. 設定DNS區域。

設定適用於**Azure**的**NetApp BlueXP**（前身為**Cloud Manager**）

使用BlueXP（前身為Cloud Manager）建立工作區、將連接器新增至Azure、建立工作環境、以及匯入叢集。

請遵循BlueXP文件完成下列步驟。請參閱 ["Azure中的BlueXP入門指南"](#)。

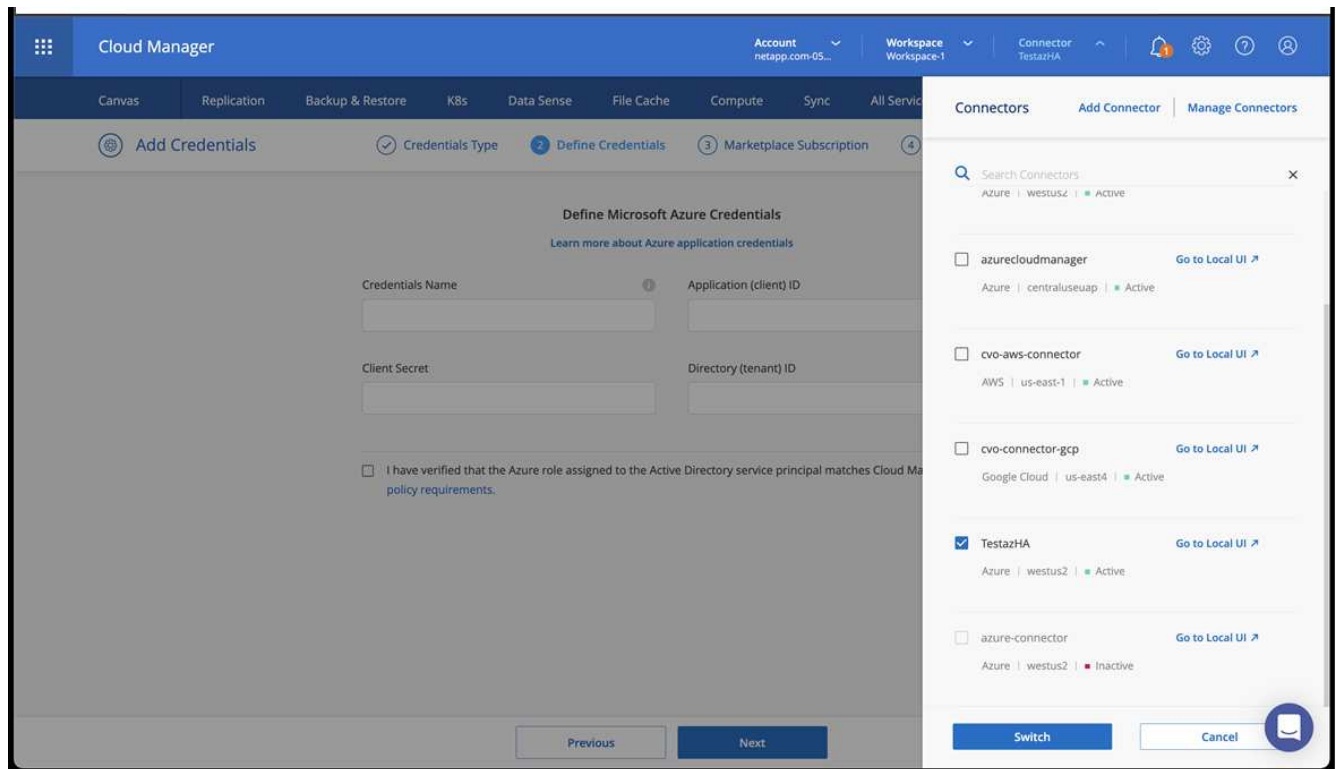
您需要的產品

以所需的IAM權限和角色存取Azure帳戶

步驟

1. 將您的認證資料新增至BlueXP。
2. 新增Azure連接器。請參閱 ["BlueXP原則"](#)。
 - a. 選擇* Azure *作為供應商。
 - b. 輸入Azure認證資料、包括應用程式ID、用戶端機密和目錄（租戶）ID。

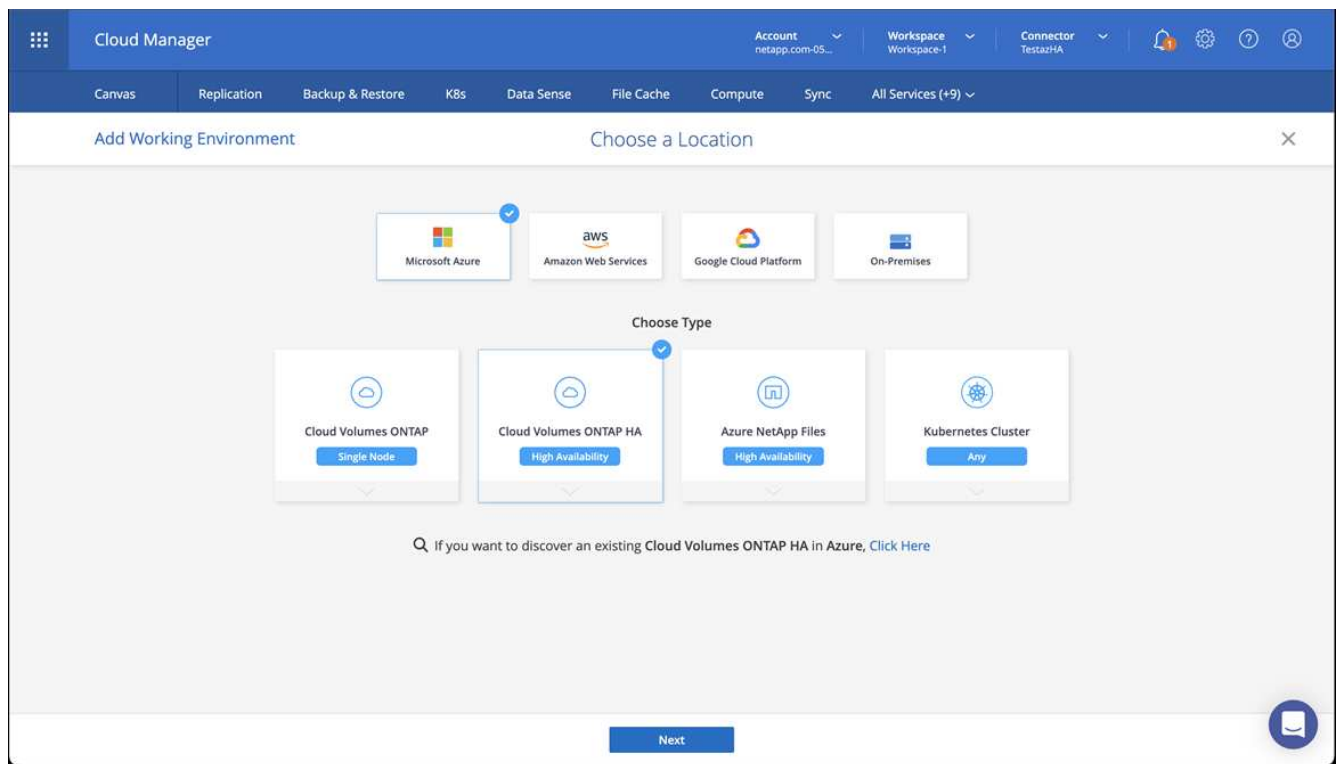
請參閱 ["從BlueXP在Azure中建立連接器"](#)。
3. 確認連接器正在執行、並切換至該連接器。



4. 為您的雲端環境建立工作環境。

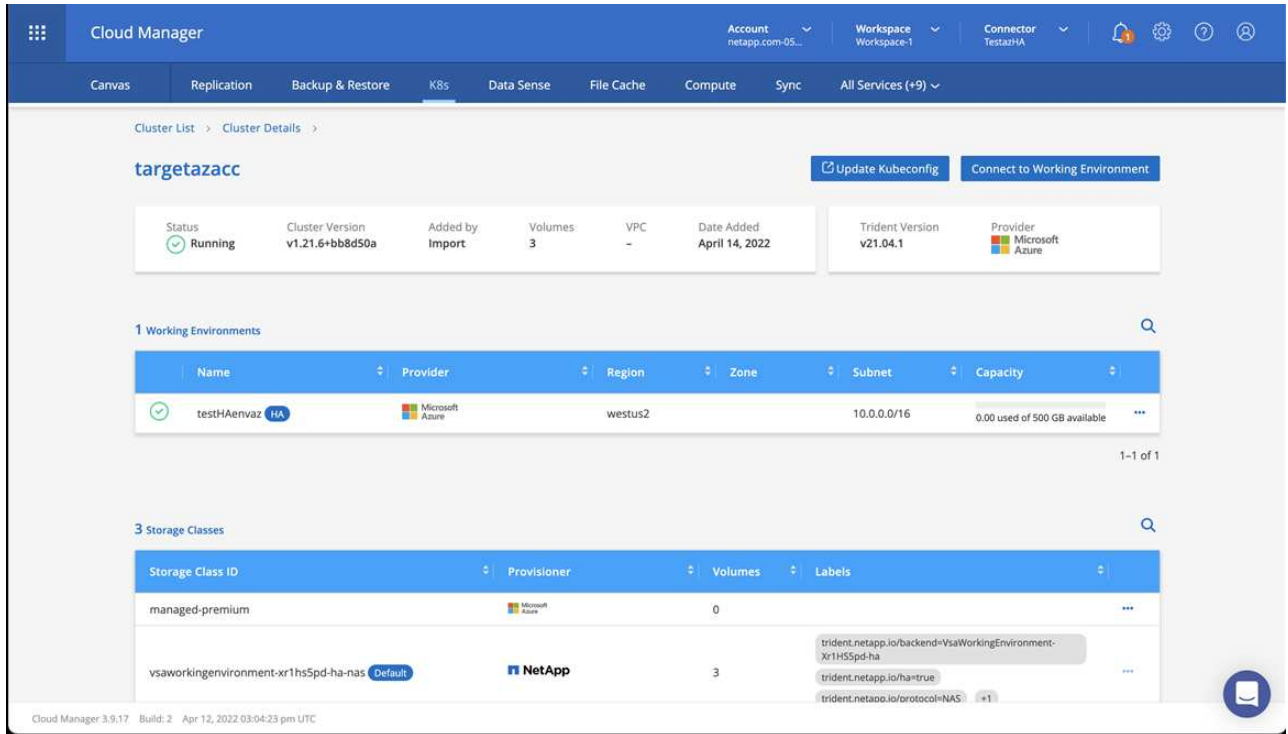
a. 位置：「Microsoft Azure」。

b. 輸入：Cloud Volumes ONTAP 「EHA」。



5. 匯入OpenShift叢集。叢集將連線至您剛建立的工作環境。

a. 選擇 * K8s*>*叢集清單*>*叢集詳細資料*、即可檢視NetApp叢集詳細資料。



b. 請注意右上角的Trident版本。

c. 請注意Cloud Volumes ONTAP、顯示NetApp為資源配置程式的叢集儲存類別。

這會匯入您的Red Hat OpenShift叢集、並指派預設的儲存類別。您可以選取儲存類別。Trident會在匯入和探索程序中自動安裝。

6. 請注意此Cloud Volumes ONTAP 功能部署中的所有持續磁碟區和磁碟區。

7. 可作為單一節點或高可用性運作。Cloud Volumes ONTAP如果已啟用HA、請記下Azure中執行的HA狀態和節點部署狀態。

安裝及設定Azure的Astra Control Center

使用標準安裝Astra Control Center "[安裝說明](#)"。

使用Astra Control Center新增Azure儲存庫。請參閱 "[設定Astra Control Center並新增鏟斗](#)"。

=
:allow-uri-read:

設定Astra控制中心

安裝Astra Control Center、登入UI並變更密碼之後、您將需要設定授權、新增叢集、管理儲存設備及新增儲存區。

工作

- [新增Astra Control Center授權](#)

- [使用Astra Control為環境做好叢集管理準備](#)
- [\[新增叢集\]](#)
- [\[新增儲存後端\]](#)
- [\[新增儲存庫\]](#)

新增Astra Control Center授權

您可以使用Astra Control UI或新增授權 ["API"](#) 以獲得完整的Astra控制中心功能。若無授權、您使用Astra Control Center的使用僅限於管理使用者及新增叢集。

Astra Control Center授權會使用Kubernetes CPU單元來測量CPU資源、並計算指派給所有受管理Kubernetes叢集之工作節點的CPU資源。授權是根據vCPU使用率而定。如需如何計算授權的詳細資訊、請參閱 ["授權"](#)。



如果您的安裝量成長到超過授權的CPU單元數量、Astra Control Center會防止您管理新的應用程式。超過容量時會顯示警示。



若要更新現有的評估或完整授權、請參閱 ["更新現有授權"](#)。

您需要的產品

- 存取新安裝的Astra Control Center執行個體。
- 系統管理員角色權限。
- 答 ["NetApp授權檔案"](#) (If)。

步驟

1. 登入Astra Control Center UI。
2. 選擇*帳戶*>*授權*。
3. 選擇*新增授權*。
4. 瀏覽至您下載的授權檔案 (NLF)。
5. 選擇*新增授權*。

「帳戶>*授權*」頁面會顯示授權資訊、到期日、授權序號、帳戶ID及使用的CPU單位。



如果您擁有評估授權、但並未將資料傳送AutoSupport 至效益分析系統、請務必儲存您的帳戶ID、以免發生Astra Control Center故障時發生資料遺失。

使用Astra Control為環境做好叢集管理準備

在新增叢集之前、您應確保符合下列先決條件。您也應該執行資格檢查、以確保叢集已準備好新增至Astra Control Center、並建立叢集管理的角色。

您需要的產品

- 確保叢集中的工作節點已設定適當的儲存驅動程式、以便Pod與後端儲存設備互動。
- 您的環境符合 ["營運環境需求"](#) 適用於Astra Trident與Astra Control Center。

- 這是Astra Trident的版本 "由Astra Control Center支援" 已安裝：



您可以 "部署Astra Trident" 使用Trident運算子（手動或使用Helm圖表）或 `tridentctl`。在安裝或升級Astra Trident之前、請先檢閱 "支援的前端、後端及主機組態"。

- 已設定Trident儲存後端：至少必須有一個Astra Trident儲存後端 "已設定" 在叢集上。
 - 已設定Trident儲存類別：至少必須有一個Astra Trident儲存類別 "已設定" 在叢集上。如果已設定預設儲存類別、請確定它是唯一具有預設註釋的儲存類別。
 - 已安裝並設定的Astra Trident Volume Snapshot控制器與Volume Snapshot類別：Volume Snapshot控制器必須是 "已安裝" 以便在Astra Control中建立快照。至少有一個Astra Trident `VolumeSnapshotClass` 過去了 "設定" 由系統管理員執行。
- *可存取的Kubeconfig*：您可以存取 "叢集管理圖" 這只包含一個內容元素。
 - 《支援》認證：您需要使用支援版的支援版支援系統上設定的支援認證和超級使用者與使用者ID、才能使用Astra Control Center來備份及還原應用程式ONTAP ONTAP ONTAP。

在flexf2命令列中執行下列命令ONTAP：

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

- *僅限Rancher*：在Rancher環境中管理應用程式叢集時、請在Rancher提供的Kubeconfig檔案中修改應用程式叢集的預設內容、以使用控制面內容而非Rancher API伺服器內容。如此可減少Rancher API伺服器的負載、並改善效能。

執行資格檢查

執行下列資格檢查、確保您的叢集已準備好新增至Astra控制中心。

步驟

1. 檢查Trident版本。

```
kubectl get tridentversions -n trident
```

如果存在Trident、您會看到類似下列的輸出：

NAME	VERSION
trident	22.10.0

如果Trident不存在、您會看到類似下列的輸出：

```
error: the server doesn't have a resource type "tridentversions"
```



如果未安裝Trident或安裝的版本不是最新版本、您必須先安裝最新版本的Trident、才能繼續進行。請參閱 "[Trident文件](#)" 以取得相關指示。

2. 確保Pod正在執行：

```
kubectl get pods -n trident
```

3. 判斷儲存類別是否使用支援的Trident驅動程式。置備程式名稱應為 `csi.trident.netapp.io`。請參閱下列範例：

```
kubectl get sc
```

回應範例：

NAME	PROVISIONER	RECLAIMPOLICY
VOLUMEBINDINGMODE	ALLOWVOLUMEEXPANSION	AGE
ontap-gold (default)	csi.trident.netapp.io	Delete
true	5d23h	Immediate

建立有限的叢集角色KECBEConfig

您可以選擇性地為Astra Control Center建立有限的系統管理員角色。這不是Astra Control Center設定所需的程序。此程序有助於建立獨立的Kbeconfig、以限制Astra Control在其管理的叢集上的權限。

您需要的產品

在完成程序步驟之前、請確定您要管理的叢集具備下列項目：

- 已安裝KECV1.23或更新版本
- 利用Astra Control Center來存取您要新增及管理的叢集



在此程序中、您不需要透過KECBEVL存取執行Astra Control Center的叢集。

- 使用叢集管理權限來管理作用中內容的叢集的作用中KECBEConfig

步驟

1. 建立服務帳戶：

- a. 建立名為的服務帳戶檔案 `astracontrol-service-account.yaml`。

視需要調整名稱和命名空間。如果在此處進行變更、您應該在下列步驟中套用相同的變更。

```
<strong>astracontrol-service-account.yaml</strong>
```

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astracontrol-service-account
  namespace: default
```

- a. 套用服務帳戶：

```
kubectl apply -f astracontrol-service-account.yaml
```

2. 建立具有由Astra Control管理叢集所需最低權限的有限叢集角色：

- a. 建立 ClusterRole 檔案已呼叫 `astra-admin-account.yaml`。

視需要調整名稱和命名空間。如果在此處進行變更、您應該在下列步驟中套用相同的變更。

```
<strong>astra-admin-account.yaml</strong>
```

+

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
  - '*'
  resources:
```

```
- '*'
verbs:
- get
- list
- create
- patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
- ""
- apps
- autoscaling
- batch
- crd.projectcalico.org
- extensions
- networking.k8s.io
- policy
- rbac.authorization.k8s.io
- snapshot.storage.k8s.io
- trident.netapp.io
resources:
- configmaps
- cronjobs
- daemonsets
- deployments
- horizontalpodautoscalers
- ingresses
- jobs
- namespaces
- networkpolicies
- persistentvolumeclaims
- poddisruptionbudgets
- pods
- podtemplates
- podsecuritypolicies
- replicaset
- replicationcontrollers
- replicationcontrollers/scale
- rolebindings
- roles
- secrets
- serviceaccounts
- services
- statefulsets
- tridentmirrorrelationships
```

```
- tridentnapshotinfos
- volumesnapshots
- volumesnapshotcontents
verbs:
- delete

# Watch resources
# Necessary to monitor progress
- apiGroups:
  - ""
  resources:
  - pods
  - replicationcontrollers
  - replicationcontrollers/scale
  verbs:
  - watch

# Update resources
- apiGroups:
  - ""
  - build.openshift.io
  - image.openshift.io
  resources:
  - builds/details
  - replicationcontrollers
  - replicationcontrollers/scale
  - imagestreams/layers
  - imagestreamtags
  - imagetags
  verbs:
  - update

# Use PodSecurityPolicies
- apiGroups:
  - extensions
  - policy
  resources:
  - podsecuritypolicies
  verbs:
  - use
```

a. 套用叢集角色：

```
kubectl apply -f astra-admin-account.yaml
```

3. 建立叢集角色與服務帳戶的叢集角色繫結：

- a. 建立 ClusterRoleBinding 檔案已呼叫 `astracontrol-clusterrolebinding.yaml`。
視需要在建立服務帳戶時調整任何已修改的名稱和命名空間。

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

+

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: astra-admin-account
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

- a. 套用叢集角色繫結：

```
kubectl apply -f astracontrol-clusterrolebinding.yaml
```

4. 列出取代的服務帳戶機密 <context> 正確的安裝環境：

```
kubectl get serviceaccount astracontrol-service-account --context
<context> --namespace default -o json
```

輸出的結尾應類似於下列內容：

```
"secrets": [
  { "name": "astracontrol-service-account-dockercfg-vhz87"},
  { "name": "astracontrol-service-account-token-r59kr" }
]
```

中每個元素的索引 `secrets` 陣列開頭為0。在上述範例中、索引為 `astracontrol-service-account-dockercfg-vhz87` 將為0、索引則為 `astracontrol-service-account-token-r59kr` 應該是1。在輸出中、記下含有「權杖」一詞的服務帳戶名稱索引。

5. 產生以下的Kbeconfig：

- a. 建立 create-kubeconfig.sh 檔案：更換 TOKEN_INDEX 在下列指令碼開頭、使用正確的值。

```
<strong>create-kubeconfig.sh</strong>
```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=astraccontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astraccontrol
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
\
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-
context ${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
```

```

rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp

```

b. 請輸入命令以將其套用至Kubernetes叢集。

```
source create-kubeconfig.sh
```

6. (選用) 將Kbeconfig重新命名為有意義的叢集名稱。

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

接下來呢？

現在您已確認已符合先決條件、您已經準備好了 [新增叢集](#)。

新增叢集

若要開始管理應用程式、請新增Kubernetes叢集、並將其當作運算資源來管理。您必須為Astra Control Center新增叢集、才能探索Kubernetes應用程式。



我們建議Astra Control Center先管理部署於上的叢集、再將其他叢集新增至Astra Control Center進行管理。需要管理初始叢集、才能傳送Kubmetrics資料和叢集相關資料、以供進行度量和疑難排解。

您需要的產品

- 新增叢集之前、請先檢閱並執行必要的 [必要工作](#)。

步驟

1. 從儀表板或叢集功能表瀏覽：

- 從「資源摘要」的*「儀表板」中、從「叢集」窗格中選取「新增*」。
- 在左側導覽區域中、選取*叢集*、然後從「叢集」頁面選取*新增叢集*。

2. 在打開的* Add Cluster-* (添加叢集) 窗口中、上傳 kubeconfig.yaml 檔案或貼上的內容 kubeconfig.yaml 檔案：



- kubeconfig.yaml 檔案應*僅包含一個叢集*的叢集認證資料。



如果您自行建立 kubeconfig 檔案中、您應該只定義*一個*內容元素。請參閱 "[Kubernetes 文件](#)" 以取得有關建立的資訊 kubeconfig 檔案；如果您使用為有限的叢集角色建立了Kbeconfig [上述程序](#)請務必在本步驟中上傳或貼上該KECBEConnfig。

3. 提供認證名稱。根據預設、認證名稱會自動填入為叢集名稱。

4. 選擇*下一步*。

5. 選取要用於此Kubernetes叢集的預設儲存類別、然後選取* Next*。



您應該選擇以ONTAP 不受資料儲存設備支援的Trident儲存類別。

6. 檢閱資訊、如果一切看起來都很好、請選取*新增*。

結果

叢集進入*探索*狀態、然後變更為*健全*。您現在正使用Astra Control Center來管理叢集。



在Astra Control Center中新增要管理的叢集之後、可能需要幾分鐘的時間來部署監控操作員。在此之前、通知圖示會變成紅色、並記錄*監控代理程式狀態檢查失敗*事件。您可以忽略這一點、因為當Astra Control Center取得正確狀態時、問題就能解決。如果幾分鐘內仍無法解決問題、請前往叢集並執行 `oc get pods -n netapp-monitoring` 做為起點。您需要查看監控操作員記錄、以偵錯問題。

新增儲存後端

您可以將現有ONTAP 的不支援儲存後端新增至Astra Control Center、以管理其資源。

將Astra Control中的儲存叢集管理為儲存後端、可讓您在持續磁碟區 (PV) 與儲存後端之間建立連結、以及取得額外的儲存指標。

步驟

1. 從左側導覽區域的儀表板中、選取*後端*。
2. 執行下列其中一項：
 - 新後端：選擇*「Add*」（新增*）以管理現有後端、選擇* ONTAP 「Send*」、然後選擇*「Next*」（下一步*）。
 - 探索到的後端：從「動作」功能表中、從受管理的叢集選取探索到的後端上的*管理*。
3. 輸入ONTAP 「叢集管理IP位址」和「管理認證」。認證資料必須是整個叢集的認證資料。



您在此處輸入認證的使用者必須擁有 `ontapi` 使用者登入存取方法已在ONTAP 支援的叢集上的「支援系統管理程式」中啟用ONTAP。如果您打算使用SnapMirror複寫、請套用具有「admin」角色的使用者認證、該角色具有存取方法 `ontapi` 和 `http`、在來源ONTAP 和目的地等叢集上。請參閱 ["管理ONTAP 使用者帳戶、請參閱本文檔"](#) 以取得更多資訊。

4. 選擇*下一步*。
5. 確認後端詳細資料、然後選取*管理*。

結果

後端隨即出現在中 Healthy 列出摘要資訊。



您可能需要重新整理頁面、以便顯示後端。

新增儲存庫

您可以使用Astra Control UI或來新增儲存區 **"API"**。如果您想要備份應用程式和持續儲存設備、或是想要跨叢集複製應用程式、則必須新增物件存放區資源庫供應商。Astra Control會將這些備份或複製儲存在您定義的物件存放區中。

如果您要將應用程式組態和持續儲存設備複製到同一個叢集、則無需使用Astra Control中的儲存庫。應用程式快照功能不需要儲存庫。

您需要的產品

- 可從由Astra Control Center管理的叢集存取的儲存庫。
- 庫位認證資料。
- 下列類型的儲存桶：
 - NetApp ONTAP 產品S3
 - NetApp StorageGRID 產品S3
 - Microsoft Azure
 - 一般S3



Amazon Web Services (AWS) 和Google Cloud Platform (GCP) 使用通用S3儲存區類型。



雖然Astra Control Center支援Amazon S3做為通用S3儲存區供應商、但Astra Control Center可能不支援所有聲稱Amazon S3支援的物件儲存區廠商。

步驟

1. 在左側導覽區域中、選取*鏟斗*。
2. 選取*「Add*」。
3. 選取貯體類型。



新增儲存庫時、請選擇正確的儲存庫供應商、並提供該供應商的適當認證資料。例如、UI接受NetApp ONTAP S3作為類型並接受StorageGRID 驗證、但這將導致所有未來使用此儲存庫的應用程式備份與還原失敗。

4. 輸入現有的庫位名稱和選用說明。



庫位名稱和說明會顯示為備份位置、您可以在建立備份時稍後選擇。此名稱也會在保護原則組態期間顯示。

5. 輸入S3端點的名稱或IP位址。
6. 在「選取認證」下、選擇「新增」或「使用現有」索引標籤。
 - 如果您選擇*新增*：
 - i. 在Astra Control中輸入認證與其他認證不同的名稱。
 - ii. 從剪貼簿貼上內容、輸入存取ID和秘密金鑰。
 - 如果您選擇*使用現有*：
 - i. 選取您要搭配儲存區使用的現有認證資料。
7. 選取 Add。



當您新增貯體時、Astra Control會使用預設的貯體指標來標記一個貯體。您建立的第一個儲存區會成為預設儲存區。當您新增儲存庫時、可以稍後決定 ["設定另一個預設儲存區"](#)。

接下來呢？

現在您已經登入Astra Control Center並新增叢集、就能開始使用Astra Control Center的應用程式資料管理功能。

- ["管理本機使用者和角色"](#)
- ["開始管理應用程式"](#)
- ["保護應用程式"](#)
- ["管理通知"](#)
- ["連線Cloud Insights 至"](#)
- ["新增自訂TLS憑證"](#)
- ["變更預設儲存類別"](#)

如需詳細資訊、請參閱

- ["使用Astra Control API"](#)

- "已知問題"

Astra Control Center的常見問題集

如果您只是想要快速回答問題、這個常見問題集就能幫上忙。

總覽

以下各節提供使用Astra Control Center時可能會遇到的其他問題解答。如需進一步的說明、請聯絡astra.feedback@netapp.com

存取Astra Control Center

什麼是Astra Control URL？

Astra Control Center使用本機驗證和每個環境的專屬URL。

對於URL、請在瀏覽器中輸入您在安裝Astra Control Center時、於Astra_control_center.yaml自訂資源 (CR) 檔案的SPEC.astraAddress欄位中所設定的完整網域名稱 (FQDN) 。電子郵件是您
在Astra_control_center.yaml CR的spec.email*欄位中設定的值。

授權

我正在使用評估授權。如何變更為完整授權？

您可以取得NetApp授權檔案 (NLF) 、輕鬆變更為完整授權。

步驟

1. 從左側導覽中、選取*帳戶*>*授權*。
2. 選擇*新增授權*。
3. 瀏覽至您下載的授權檔案、然後選取*「Add* (新增*)」。

我正在使用評估授權。我還能管理應用程式嗎？

是的、您可以使用評估授權測試管理應用程式功能。

正在登錄Kubernetes叢集

新增Astra Control之後、我需要將工作節點新增至Kubernetes叢集。我該怎麼辦？

新的工作者節點可新增至現有的資源池。Astra Control會自動探索這些功能。如果在Astra Control中看不到新節點、請檢查新的工作節點是否執行支援的映像類型。您也可以使用驗證新工作節點的健全狀況 `kubectl get nodes` 命令。

如何正確地取消管理叢集？

1. "從Astra Control取消應用程式管理"。

2. "從Astra Control取消管理叢集"。

從Astra Control移除Kubernetes叢集之後、應用程式和資料會發生什麼變化？

從Astra Control移除叢集不會對叢集的組態（應用程式和持續儲存）進行任何變更。在該叢集上執行的任何Astra Control快照或應用程式備份都無法還原。由Astra Control所建立的持續儲存備份仍在Astra Control之內、但無法還原。



透過任何其他方法刪除叢集之前、請務必先從Astra Control移除叢集。使用另一個工具刪除叢集時、如果叢集仍由Astra Control進行管理、可能會對Astra Control帳戶造成問題。

*當我取消管理叢集時、NetApp Trident是否會自動從叢集解除安裝？*當您從Astra Control Center取消管理叢集時、Trident不會自動從叢集解除安裝。若要解除安裝Trident、您需要 ["請遵循Trident文件中的下列步驟"](#)。

管理應用程式

- Astra Control是否能部署應用程式？*

Astra Control不會部署應用程式。應用程式必須部署在Astra Control之外。

停止從Astra Control管理應用程式之後、應用程式會發生什麼事？

將刪除任何現有的備份或快照。應用程式與資料仍可繼續使用。資料管理作業無法用於未受管理的應用程式、或屬於它的任何備份或快照。

- Astra Control能否管理非NetApp儲存設備上的應用程式？*

不可以雖然Astra Control可以探索使用非NetApp儲存設備的應用程式、但它無法管理使用非NetApp儲存設備的應用程式。

*我應該自行管理Astra Control嗎？*不、您不應該自行管理Astra Control、因為它是「系統應用程式」。

*不良的Pod是否會影響應用程式管理？*如果託管應用程式的Pod處於不良狀態、Astra Control將無法建立新的備份與複製。

資料管理作業

我的應用程式使用數個PV。Astra Control是否會擷取這些PV的快照與備份？

是的。Astra Control在應用程式上執行的快照作業包括繫結至應用程式PVCS的所有PV快照。

我可以直接透過不同的介面或物件儲存設備來管理Astra Control所拍攝的快照嗎？

不可以Astra Control所拍攝的快照與備份、只能透過Astra Control進行管理。

版權資訊

Copyright © 2023 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。