概念
Astra Control Center

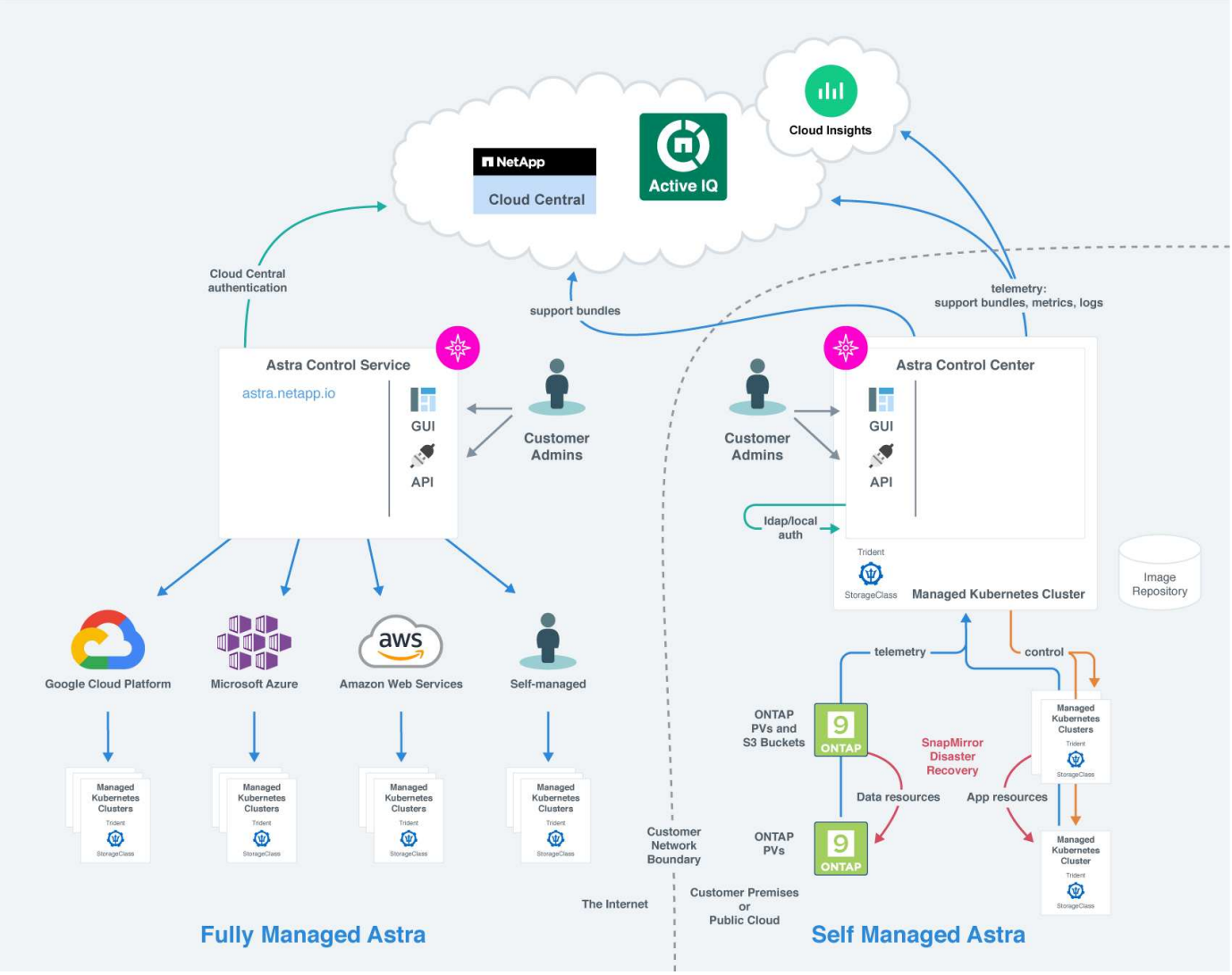
NetApp
November 27, 2023

目錄

概念

架構與元件

以下概述Astra Control環境的各個元件。



Astra控制元件

- * Kubernetes叢集*：Kubernetes是可攜式、可擴充的開放原始碼平台、可用於管理容器化工作負載與服務、同時促進宣告式組態與自動化。Astra為Kubernetes叢集中託管的應用程式提供管理服務。
- * Astra Trident *：Astra Trident *是完全受支援的開放原始碼儲存資源配置程式、由NetApp維護、可讓您為Docker和Kubernetes所管理的容器化應用程式建立儲存磁碟區。Astra Trident部署於Astra Control Center時、包含已設定ONTAP 的整套儲存後端。
- 儲存後端：
  - Astra Control Service使用下列儲存後端：
    - "適用於Cloud Volumes Service Google Cloud的NetApp解決方案" 或Google持續磁碟做為GKE叢集

的儲存後端

- "Azure NetApp Files" 或Azure託管磁碟做為高效能叢集的儲存後端。
- "Amazon彈性區塊儲存區（EBS）" 或 "Amazon FSX for NetApp ONTAP 產品" 作為EKS叢集的後端儲存選項。

◦ Astra Control Center使用下列儲存後端：

- 不只是部分、不只是部分、更是部分ASA FAS ONTAP AFF 。作為儲存軟體與硬體平台ONTAP 、支援核心儲存服務、支援多種儲存存取傳輸協定、以及快照與鏡射等儲存管理功能。
- Cloud Volumes ONTAP

- * Cloud Insights * ： Cloud Insights 是 NetApp 雲端基礎架構監控工具、可讓您監控 Astra 控制中心所管理的 Kubernetes 叢集的效能與使用率。可將儲存使用量與工作負載建立關聯。Cloud Insights當您在Cloud Insights Astra控制中心啟用「支援不中斷連線」時、遙測資訊會顯示在Astra控制中心UI頁面中。

Astra控制介面

您可以使用不同的介面來完成工作：

- 網路使用者介面（**UI**）：Astra Control Service和Astra Control Center都使用相同的網路型UI來管理、移轉及保護應用程式。也可以使用UI來管理使用者帳戶和組態設定。
- * API*：Astra Control Service和Astra Control Center都使用相同的Astra Control API。使用API、您可以執行與使用UI相同的工作。

Astra Control Center也能讓您管理、移轉及保護在VM環境中執行的Kubernetes叢集。

以取得更多資訊

- "Astra Control Service文件"
- "Astra Control Center文件"
- "Astra Trident文件"
- "使用Astra Control API"
- "本文檔 Cloud Insights"
- "本文檔 ONTAP"

資料保護

瞭解Astra Control Center中可用的資料保護類型、以及如何以最佳方式使用這些類型來保護應用程式。

快照、備份及保護原則

快照和備份都能保護下列類型的資料：

- 應用程式本身
- 與應用程式相關的任何持續資料磁碟區

- 屬於應用程式的任何資源成品

_snapshot是應用程式的時間點複本、儲存在與應用程式相同的已配置磁碟區上。通常速度很快。您可以使用本機快照、將應用程式還原至較早的時間點。快照對快速複製非常實用；快照包括應用程式的所有Kubernetes物件、包括組態檔案。快照可用於複製或還原同一個叢集內的應用程式。

備份_是以快照為基礎。它儲存在外部物件存放區中、因此相較於本機快照、拍攝速度可能較慢。您可以將應用程式備份還原至同一個叢集、也可以將應用程式備份還原至不同的叢集、藉此移轉應用程式。您也可以選擇較長的備份保留期間。由於備份儲存在外部物件存放區中、因此在伺服器故障或資料遺失的情況下、備份通常比快照提供更好的保護。

_protection policy_is是一種保護應用程式的方法、可根據您為該應用程式定義的排程、自動建立快照、備份或兩者。保護原則也可讓您選擇要在排程中保留多少個快照和備份、並設定不同的排程精細度層級。使用保護原則將備份與快照自動化、是確保每個應用程式都能根據組織和服務層級協議（SLA）需求來保護的最佳方式。

> 您必須等到最近進行備份之後、才能獲得完整保護。這很重要、因為備份儲存在遠離持續磁碟區的物件存放區中。如果發生故障或意外、會清除叢集及其相關的持續儲存設備、則需要備份才能恢復。快照無法讓您恢復。

複製

_clon__是應用程式、其組態及其持續資料磁碟區的完全複製。您可以在相同的Kubernetes叢集或其他叢集上手動建立複本。如果您需要將應用程式和儲存設備從一個Kubernetes叢集移至另一個叢集、複製應用程式就很有用。

儲存後端之間的複寫

使用Astra Control、您可以利用NetApp SnapMirror技術的非同步複寫功能、利用低RPO（恢復點目標）和低RTO（恢復時間目標）、為應用程式建立營運不中斷。設定完成後、您的應用程式就能將資料和應用程式變更從一個儲存後端複寫到另一個儲存後端、在同一個叢集或不同叢集之間複寫。

您可以在同一個 ONTAP 叢集或不同 ONTAP 叢集上的兩個 ONTAP VM 之間進行複寫。

Astra Control 會以非同步方式將應用程式快照複本複寫到目的地叢集。複寫程序包括SnapMirror複寫之持續磁碟區中的資料、以及由Astra Control保護的應用程式中繼資料。

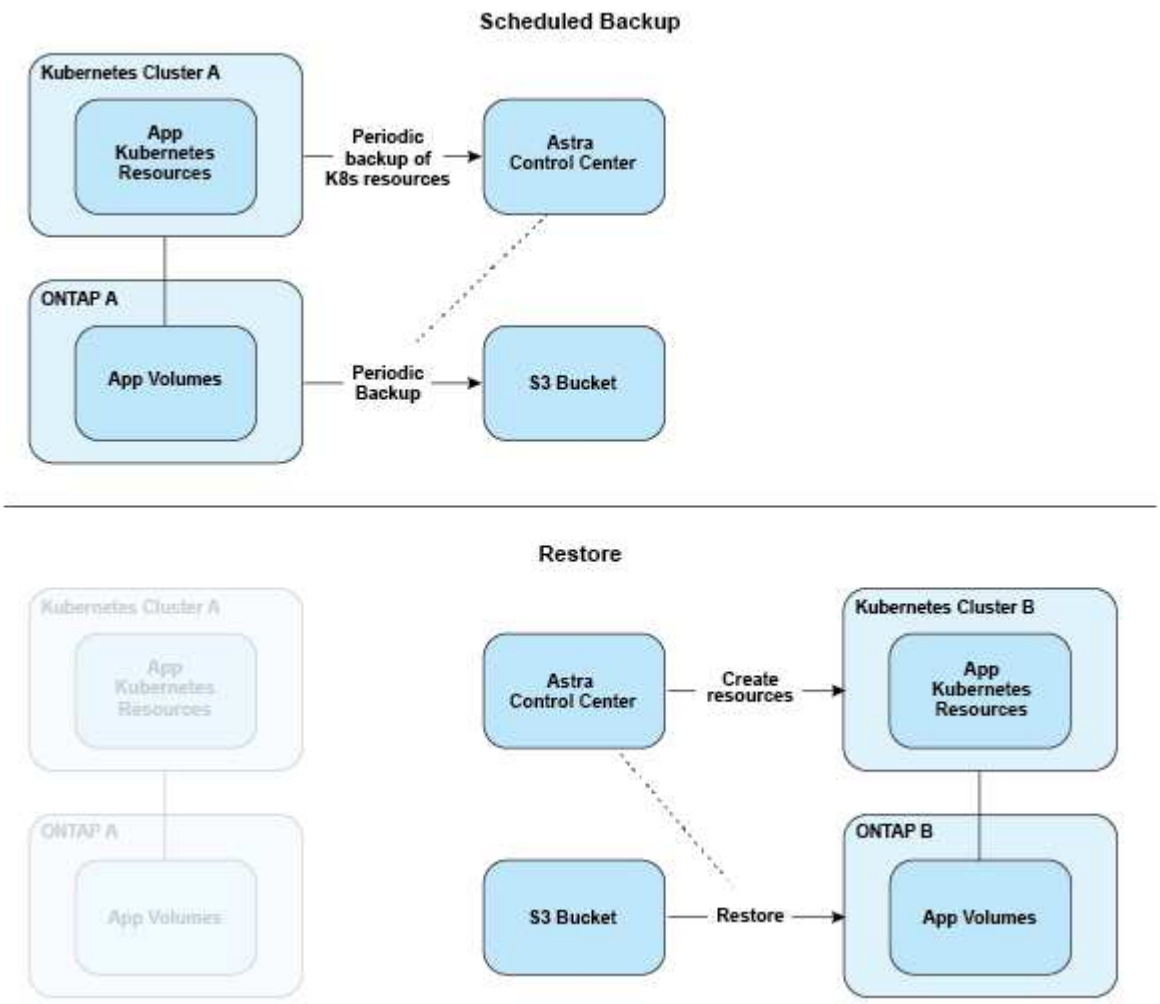
應用程式複寫不同於應用程式備份與還原、方法如下：

- * 應用程式複寫 * ： Astra Control 需要來源和目的地 Kubernetes 叢集（可以是同一個叢集）、才能使用和管理各自的 ONTAP 儲存後端、並將其設定為啟用 NetApp SnapMirror 。Astra Control 會擷取原則導向的應用程式快照、並將其複寫到目的地儲存後端。NetApp SnapMirror 技術用於複寫持續性 Volume 資料。若要容錯移轉、Astra Control可以在目的地Kubernetes叢集上重新建立應用程式物件、並在目的地ONTAP 叢集上重新建立複寫的磁碟區、使複寫的應用程式上線。由於目的地 ONTAP 叢集上已存在持續磁碟區資料、因此 Astra Control 可提供快速的容錯移轉恢復時間。
- * 應用程式備份與還原 * ：當備份應用程式時、 Astra Control 會建立應用程式資料的快照、並將其儲存在物件儲存貯體中。需要還原時、必須將儲存庫中的資料複製到ONTAP 位在該叢集上的持續磁碟區。備份/還原作業不需要次要Kubernetes/ONTAP叢集可供使用和管理、但額外的資料複本可能會導致較長的還原時間。

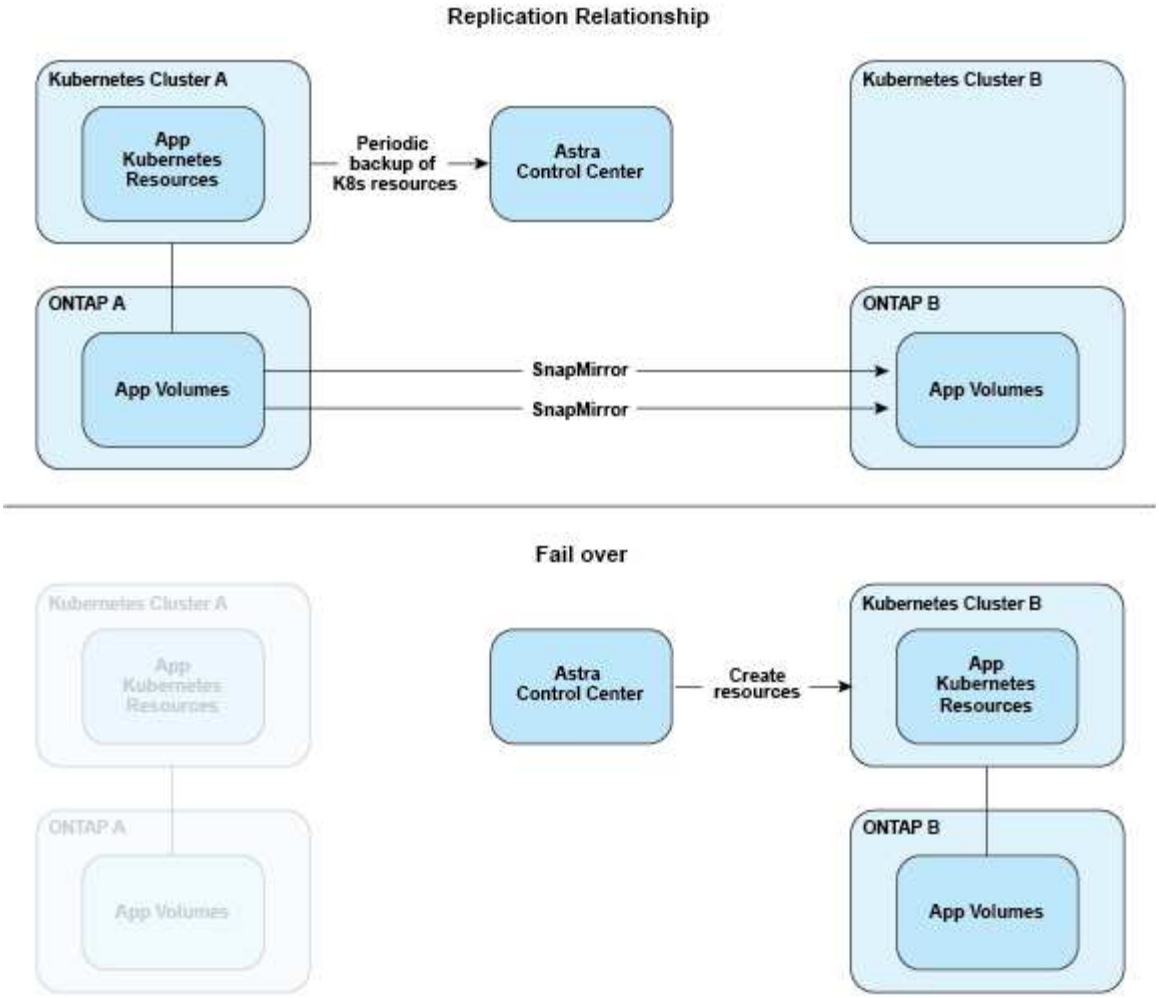
若要瞭解如何複寫應用程式、請參閱 "使用SnapMirror技術將應用程式複寫到遠端系統"。

下列影像顯示排程的備份與還原程序、與複寫程序比較。

備份程序會將資料複製到S3儲存區、並從S3儲存區還原：



另一方面、複寫是透過複寫到 ONTAP 、然後容錯移轉會建立 Kubernetes 資源：



具有過期授權的備份、快照和複本

如果授權過期、您只能在新增或保護的應用程式是另一個 Astra Control Center 執行個體時、新增應用程式或執行應用程式保護作業（例如快照、備份、複本和還原作業）。

授權

當您部署 Astra Control Center 時、系統會安裝內嵌式 90 天試用版授權、適用於 4 、 800 個 CPU 單元。如果您需要更多容量或更長的評估期、或想要升級至完整授權、您可以向 NetApp 取得不同的評估授權或完整授權。

您可以使用下列其中一種方式取得授權：

- 如果您正在評估 Astra Control Center 、並需要不同於內嵌評估授權所含的評估條款、請聯絡 NetApp 以申請不同的評估授權檔案。
- "如果您已購買Astra Control Center、請產生您的NetApp授權檔案（NLF）" 登入 NetApp 支援網站 並瀏覽至系統功能表下的軟體授權。

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"。

請確定您的授權至少能啟用所需的 CPU 單位。如果 Astra Control Center 目前所管理的 CPU 單位數量超過所套用新授權中的可用 CPU 單位、您將無法套用新授權。

評估授權與完整授權

內嵌評估授權隨附全新的 Astra Control Center 安裝。評估授權可在有限（ 90 天）期間內、提供與完整授權相同的功能與功能。評估期結束後、必須取得完整授權才能繼續使用完整功能。

授權過期

如果作用中的 Astra Control Center 授權過期、下列功能的 UI 和 API 功能將無法使用：

- 手動本機快照與備份
- 排程的本機快照與備份
- 從快照或備份還原
- 從快照或目前狀態複製
- 管理新應用程式
- 設定複寫原則

如何計算授權使用量

當您將新叢集新增至Astra Control Center時、除非至少有一個執行於叢集上的應用程式由Astra Control Center管理、否則它不會將使用的授權列入計算。

當您開始管理叢集上的應用程式時、 Astra Control Center 的所有 CPU 單元都會包含在 Astra Control Center 授權使用量中、但 Red Hat OpenShift 叢集節點 CPU 單元則會使用標籤回報 `node-role.kubernetes.io/infra: ""`。

Red Hat OpenShift 基礎架構節點不會使用 Astra Control Center 中的授權。若要將節點標記為基礎架構節點、請套用標籤 `node-role.kubernetes.io/infra: ""` 至節點。

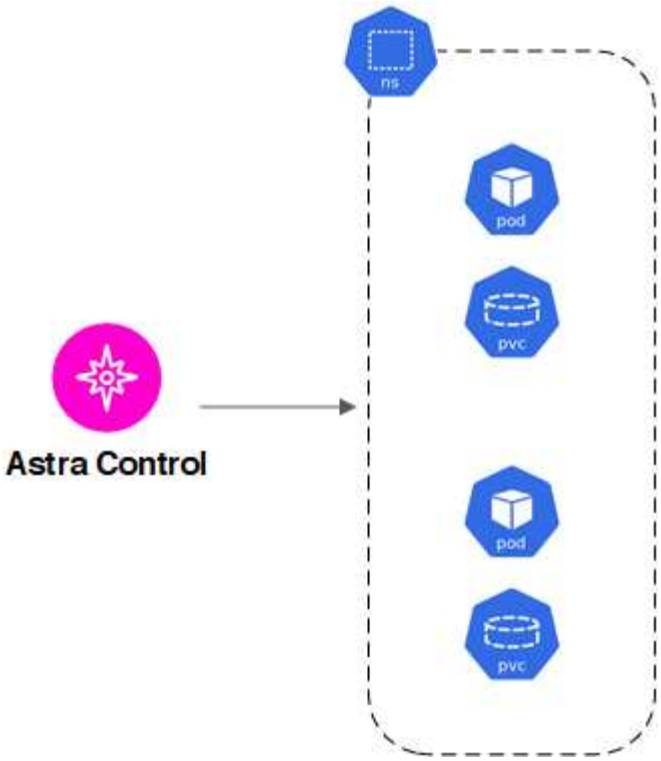
如需詳細資訊、請參閱

- "第一次設定Astra Control Center時、請新增授權"
- "更新現有授權"

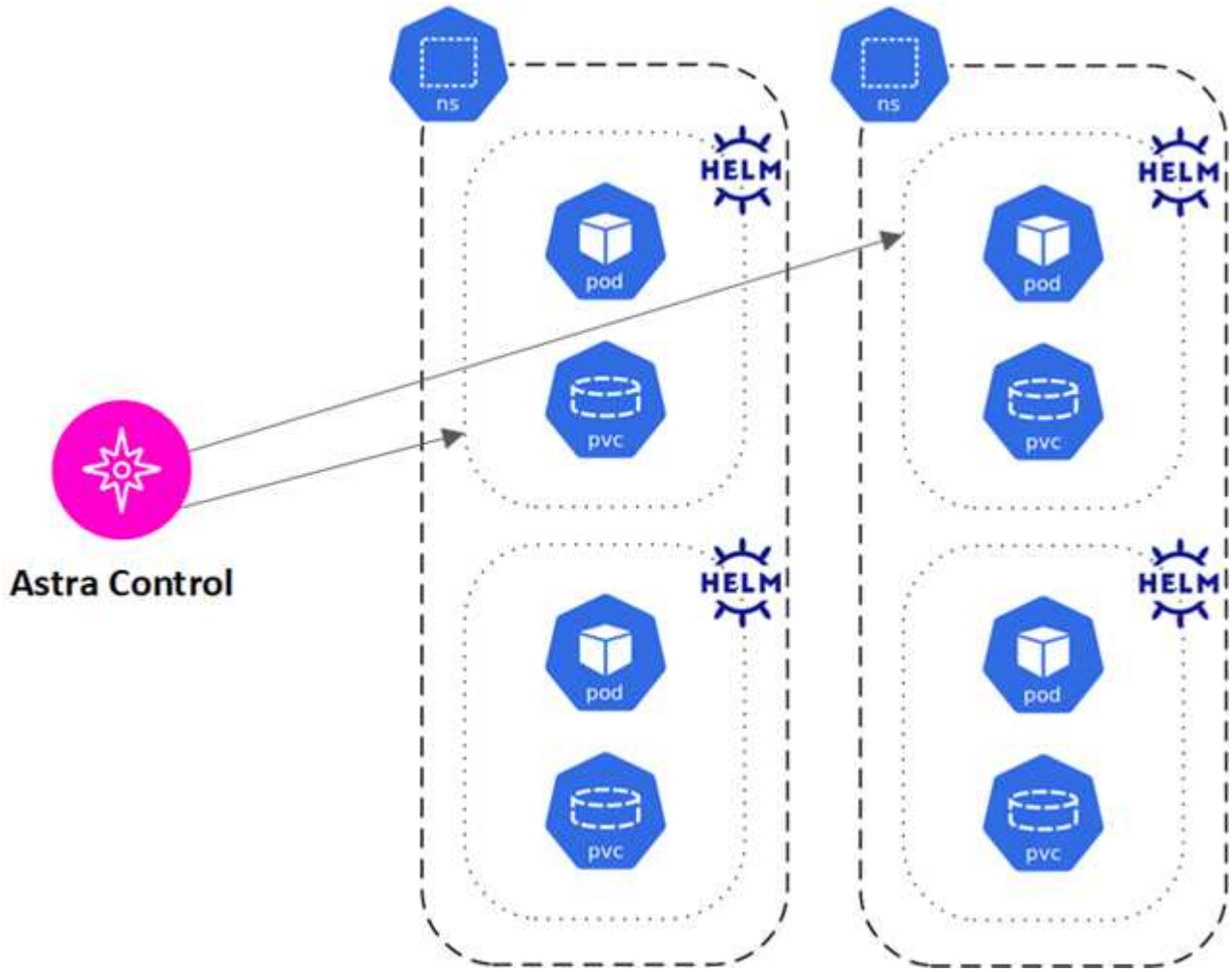
應用程式管理

當Astra Control探索叢集時、這些叢集上的應用程式將無法管理、直到您選擇要管理的方式為止。Astra Control中的託管應用程式可以是下列任一項：

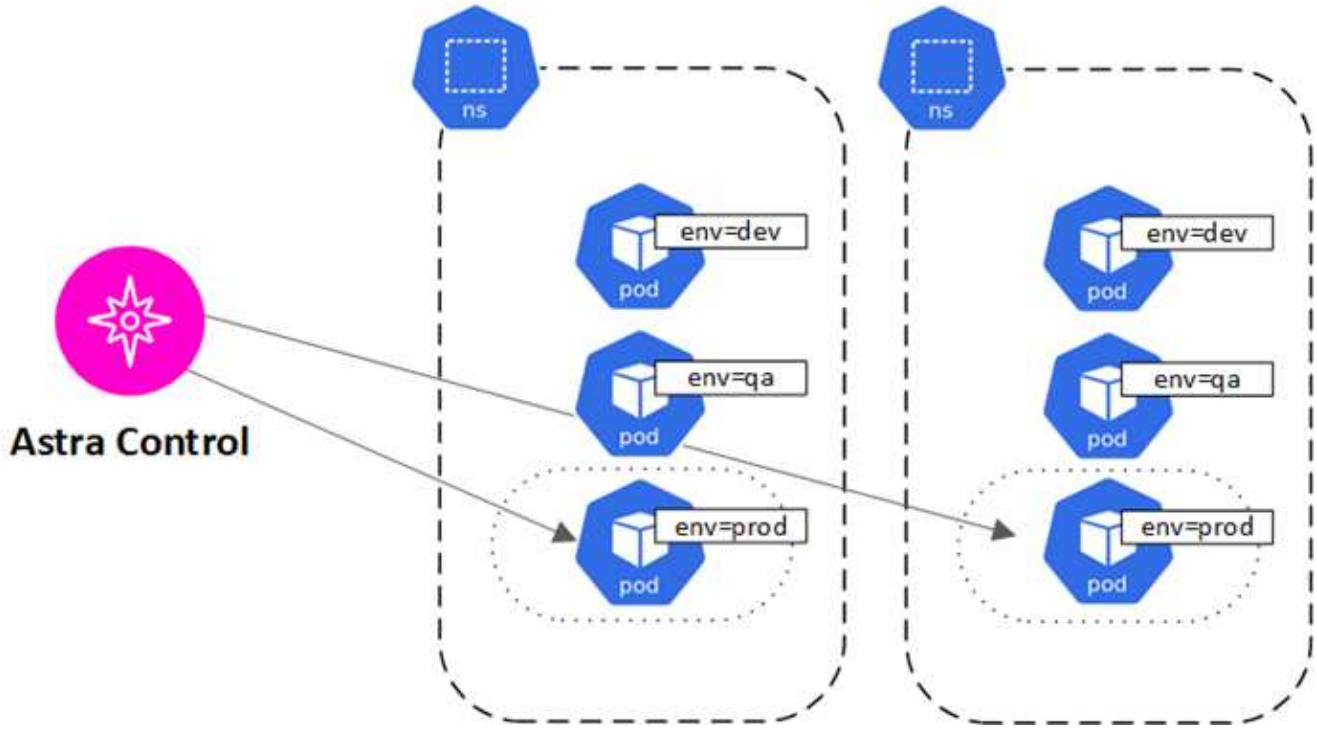
- 命名空間、包括該命名空間中的所有資源



- 部署在一個或多個命名空間內的個別應用程式（本範例使用helm3）



- 一組資源、由一個或多個命名空間內的Kubernetes標籤識別



儲存類別和持續Volume大小

Astra Control Center 支援 NetApp ONTAP 和 Longhorn 作為儲存後端。

總覽

Astra Control Center支援下列項目：

- * Astra Trident 儲存類別以 ONTAP 儲存 * 為後盾：如果您使用的是 ONTAP 後端、 Astra 控制中心可以匯入 ONTAP 後端、以報告各種監控資訊。
- * 以 Longhorn* 為後盾的 CSI 型儲存類別：您可以搭配 Longhorn Container Storage Interface （ CSI ）驅動程式使用 Longhorn 。

Astra Trident 儲存類別應在 Astra Control Center 之外預先設定。

儲存類別

當您將叢集新增至Astra Control Center時、系統會提示您在該叢集上選取先前設定的儲存類別作為預設儲存類別。當持續磁碟區宣告（PVc）中未指定任何儲存類別時、就會使用此儲存類別。預設儲存類別可隨時在Astra Control Center內變更、而任何儲存類別都可隨時在PVc或Helm圖表中指定儲存類別名稱、以供使用。請確定您只為Kubernetes叢集定義單一預設儲存類別。

以取得更多資訊

- "Astra Trident文件"

使用者角色和命名空間

瞭解Astra Control中的使用者角色和命名空間、以及如何使用這些角色和命名空間來控制組織中的資源存取。

使用者角色

您可以使用角色來控制使用者對Astra Control資源或功能的存取。以下是Astra Control的使用者角色：

- *檢視器*可以檢視資源。
- *成員*具有檢視者角色權限、可管理應用程式與叢集、取消管理應用程式、以及刪除快照與備份。
- 「管理」具有「成員角色」權限、可新增及移除擁有者以外的任何其他使用者。
- *擁有者*具有管理員角色權限、可新增及移除任何使用者帳戶。

您可以新增限制給成員或檢視者使用者、將使用者限制為一或多個 [命名空間]。

命名空間

命名空間是可指派給由Astra Control管理之叢集內特定資源的範圍。當您將叢集新增至Astra Control時、Astra Control會探索叢集的命名空間。一旦發現命名空間、就能將其指派為限制給使用者。只有具有該命名空間存取權的成員才能使用該資源。您可以使用命名空間來控制對資源的存取、這種模式對您的組織而言很合理、例如依實體區域或公司內部的部門而定。當您新增限制給使用者時、可以將該使用者設定為只能存取所有命名空間或特定的命名空間集合。您也可以使用命名空間標籤指派命名空間限制。

如需詳細資訊、請參閱

"管理本機使用者和角色"

Pod安全性

Astra Control Center透過pod安全性原則（ASP）和pod安全性許可（Ps）來支援權限限制。這些架構可讓您限制哪些使用者或群組能夠執行容器、以及這些容器可以擁有哪些權限。

部分Kubernetes發佈版本的預設Pod安全性組態可能過於嚴加限制、因此在安裝Astra Control Center時會發生問題。

您可以使用此處提供的資訊和範例來瞭解Astra Control Center所做的Pod安全性變更、並使用pod安全方法來提供所需的保護、而不會干擾Astra Control Center功能。

由Astra Control Center執行的SSA

Astra Control Center 可將下列標籤新增至安裝 Astra 的命名空間（ NetApp-acc 或自訂命名空間）、以及為備份建立的命名空間、藉此強制執行 Pod 安全許可。

```
pod-security.kubernetes.io/enforce: privileged
```

由Astra Control Center安裝的PSPS

當您在Kubernetes 1.23或1.24上安裝Astra Control Center時、會在安裝期間建立數個Pod安全性原則。其中有些是永久性的、有些是在特定作業期間建立、一旦作業完成、就會移除。當主機叢集執行Kubernetes 1.25或更新版本時、Astra Control Center不會嘗試安裝ASP、因為這些版本不支援這些應用程式。

在安裝期間建立PSPS

在Astra Control Center安裝期間、Astra Control Center營運者會安裝自訂的Pod安全性原則A `Role` 物件和 `RoleBinding` 用於支援Astra Control Center命名空間中Astra Control Center服務部署的物件。

新原則和物件具有下列屬性：

```
kubectl get psp

NAME                              PRIV    CAPS          SELINUX    RUNASUSER
FSGROUP     SUPGROUP    READONLYROOTFS   VOLUMES
netapp-astra-deployment-psp    false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *

kubectl get role -n <namespace_name>

NAME                                        CREATED AT
netapp-astra-deployment-role                2022-06-27T19:34:58Z

kubectl get rolebinding -n <namespace_name>

NAME                                        ROLE
AGE
netapp-astra-deployment-rb                  Role/netapp-astra-deployment-role
32m
```

在備份作業期間建立PSPS

在備份作業期間、Astra Control Center會建立動態Pod安全性原則 `ClusterRole` 物件和 `RoleBinding` 物件：這些支援在個別命名空間中執行的備份程序。

新原則和物件具有下列屬性：

```
kubectl get psp

NAME                             PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-astra-backup             false   DAC_READ_SEARCH
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role -n <namespace_name>

NAME                   CREATED AT
netapp-astra-backup   2022-07-21T00:00:00Z

kubectl get rolebinding -n <namespace_name>

NAME                   ROLE                         AGE
netapp-astra-backup   Role/netapp-astra-backup   62s
```

叢集管理期間建立的**PSPS**

當您管理叢集時、Astra Control Center會在託管叢集中安裝NetApp監控操作員。這位營運者會建立一個Pod安全性原則、a `ClusterRole` 物件和 `RoleBinding` 在Astra Control Center命名空間中部署遙測服務的物件。

新原則和物件具有下列屬性：

```
kubectl get psp

NAME                             PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-monitoring-psp-nkmo      true    AUDIT_WRITE,NET_ADMIN,NET_RAW
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role -n <namespace_name>

NAME                                          CREATED AT
netapp-monitoring-role-privileged             2022-07-21T00:00:00Z

kubectl get rolebinding -n <namespace_name>

NAME                                                ROLE
AGE
netapp-monitoring-role-binding-privileged           Role/netapp-
monitoring-role-privileged             2m5s
```

版權資訊

商標資訊