



# **Astra Trident 23.01.1文件**

## **Astra Trident**

NetApp  
April 16, 2024

# 目錄

Astra Trident 23.01.1文件	1
版本資訊	2
23.01.1的新功能	2
23.01年的變更	2
22.10的變更	3
22.07年的變動	4
22.04年的變化	5
22.01.1中的變更	5
22.01.0版的變更	6
210.1的變更	6
21.0	6
已知問題	7
如需詳細資訊、請參閱	8
概念	9
瞭解Astra Trident	9
驅動程式ONTAP	10
資源配置	11
Volume快照	11
虛擬資源池	12
Volume存取群組	14
開始使用	15
歡迎試用	15
需求	15
安裝Astra Trident	20
接下來呢？	49
管理Astra Trident	55
升級Astra Trident	55
解除安裝Astra Trident	68
降級Astra Trident	70
使用Astra Trident	74
準備工作節點	74
設定後端	78
使用kubectl建立後端	163
以KECBECVL執行後端管理	169
使用tridentctl執行後端管理	170
在後端管理選項之間切換	171
管理儲存類別	178
執行Volume作業	180
跨命名空間共用NFS磁碟區	204

監控Astra Trident .....	207
適合Docker的Astra Trident .....	211
部署的先決條件 .....	211
部署Astra Trident .....	214
升級或解除安裝Astra Trident .....	218
使用Volume .....	220
收集記錄 .....	227
管理多個Astra Trident執行個體 .....	228
儲存組態選項 .....	229
已知問題與限制 .....	237
常見問題集 .....	239
一般問題 .....	239
在Kubernetes叢集上安裝及使用Astra Trident .....	239
疑難排解與支援 .....	240
升級Astra Trident .....	242
管理後端和磁碟區 .....	242
支援 .....	247
疑難排解 .....	248
一般疑難排解 .....	248
使用操作員疑難排解不成功的Trident部署 .....	249
使用疑難排解不成功的Trident部署 <code>tridentctl</code> .....	251
最佳實務做法與建議 .....	252
部署 .....	252
儲存組態 .....	252
整合Astra Trident .....	258
資料保護 .....	266
安全性 .....	271
參考資料 .....	277
Astra Trident連接埠 .....	277
Astra Trident REST API .....	277
命令列選項 .....	278
與Kubernetes整合的NetApp產品 .....	279
Kubernetes和Trident物件 .....	280
<code>tridentctl</code> 命令和選項 .....	291
Pod安全標準（PSS）與安全內容限制（SCC） .....	296
較早版本的文件 .....	300
法律聲明 .....	301
版權 .....	301
商標 .....	301
專利 .....	301
隱私權政策 .....	301



# Astra Trident 23.01.1文件

# 版本資訊

版本資訊提供最新版Astra Trident的新功能、增強功能及錯誤修正資訊。



◦ `tridentctl` 安裝程式壓縮檔中提供的Linux二進位檔是經過測試且受支援的版本。請注意 `macos` 中提供的二進位元 `/extras` 未測試或支援部分的Zip檔案。

## 23.01.1的新功能

### 修正

- 固定Trident運算子在SPEC中指定安裝時使用IPv6 localhost。
- 固定的Trident運算子叢集角色權限、可與套件組合權限同步 "[問題#799](#)"。
- 新增修正程式、允許外部程序執行至完成。
- 已解決在rwx模式下、在多個節點上附加原始區塊Volume的問題。
- 針對FlexGroup SMB Volume提供固定的實體複製支援和Volume匯入。

## 23.01年的變更



Kubernetes 1.26現在已在Trident中受到支援。升級Kubernetes之前、請先升級Astra Trident。

### 修正

- Kubernetes：新增選項以排除建立Pod安全性原則、以修正透過Helm ("[問題#783](#)、[#794](#)")。

### 增強功能

#### Kubernetes

- 新增對Kubernetes 1.26的支援。
- 改善整體Trident RBAC資源使用率 ("[問題#757](#)")。
- 新增自動化功能、可偵測並修正主機節點上的中斷或過時iSCSI工作階段。
- 新增對擴充LUKS加密磁碟區的支援。
- Kubernetes：新增了對LUKS加密磁碟區的認證旋轉支援。

#### Astra Trident

- 新增支援SMB Volume搭配Amazon FSX ONTAP for Sfor Sfor ONTAP - NAS儲存驅動程式。
- 新增使用SMB磁碟區時對NTFS權限的支援。
- 新增對採用CVS服務層級之GCP磁碟區的儲存資源池支援。
- 新增對使用ONTAP-NAS-Flexgroup儲存驅動程式建立FlexGroups時、FlexGroupAggregateList的選用使用支援。

- 在管理多個FlexVols時、為ONTAP-NAS經濟型儲存驅動程式提升效能。
- 已啟用所有ONTAP 的支援不支援NAS儲存驅動程式的資料LIF更新。
- 更新Trident部署和示範設定命名慣例、以反映主機節點作業系統。

## 棄用

- Kubernetes：將支援的Kubernetes最低更新為1.21。
- 在設定時、不應再指定資料生命期 `ontap-san` 或 `ontap-san-economy` 驅動程式：

## 22.10的變更

\*在升級至Astra Trident 22.10\*之前、您必須先閱讀下列重要資訊

### **<strong>關於Astra Trident 22.10</strong>的重要資訊**



- Kubernetes 1.25現在已在Trident中受到支援。在升級至Kubernetes 1.25之前、您必須先將Astra Trident升級至22.10。
- Astra Trident現在嚴格強制執行SAN環境中的多重路徑組態使用、建議使用的值為 `find_multipaths: no` 在多重路徑.conf檔案中。

使用非多重路徑組態或使用 `find_multipaths: yes` 或 `find_multipaths: smart` 多重路徑.conf檔案中的值會導致掛載失敗。Trident建議使用 `find_multipaths: no` 自21.07版本以來。

## 修正

- 已修正ONTAP 特定於使用建立的靜止後端的問題 `credentials` 在22.07.0升級期間、現場無法上線（.."問題#759"）。
- 修正導致Docker Volume外掛程式無法在某些環境中啟動的問題（"問題#548" 和 "問題#760"）。
- 修正ONTAP 了特定於SAN後端的SLE問題、以確保僅發佈屬於報告節點的資料生命期子集。
- 修正連接磁碟區時發生不必要的iSCSI LUN掃描的效能問題。
- 移除Astra Trident iSCSI工作流程中的精細重試次數、以快速失敗並縮短外部重試時間間隔。
- 修正當對應的多重路徑裝置已排清時、在排清iSCSI裝置時傳回錯誤的問題。

## 增強功能

- Kubernetes：
  - 新增對Kubernetes 1.25的支援。在升級至Kubernetes 1.25之前、您必須先將Astra Trident升級至22.10。
  - 針對Trident部署和示範集新增了另一個ServiceAccount、ClusterRO容 和ClusterROlexBinding功能、以允許未來的權限增強功能。
  - 新增支援 "跨命名空間磁碟區共用"。
- 所有Trident `ontap-*` 儲存驅動程式現在可搭配ONTAP 使用靜態API。

- 新增運算子yaml (bundle\_post\_1\_25.yaml) 沒有 PodSecurityPolicy 支援Kubernetes 1.25。
- 新增 "支援LUKS加密磁碟區" 適用於 ontap-san 和 ontap-san-economy 儲存驅動程式：
- 新增對Windows Server 2019節點的支援。
- 新增 "支援Windows節點上的SMB Volume" 透過 azure-netapp-files 儲存驅動程式：
- 目前市面上已普遍提供適用於整個過程的自動功能、例如針對不適用的驅動程式進行交換偵測。MetroCluster ONTAP

## 棄用

- \*\* Kubernetes：\*將支援的Kubernetes最低更新為1.20。
- 移除Astra Data Store（廣告）驅動程式。
- 已移除的支援 yes 和 smart 選項 find\_multipaths 在設定iSCSI的工作節點多重路徑時。

## 22.07年的變動

### 修正

- Kubernetes\*
  - 修正使用Helm或Trident運算子設定Trident時、處理節點選取器的布林值和數字值的問題。（"[GitHub問題#700](#)"）
  - 修正非CHAP路徑處理錯誤的問題、以便Kubelet在失敗時重試。（"[GitHub問題#736](#)"）

### 增強功能

- 將k8s.gcr.IO轉換為登錄.k8s.IO、做為SCSI映像的預設登錄
- ONTAP-SAN磁碟區現在會使用每節點igroup、只將LUN對應至igroup、同時主動發佈至這些節點、以改善我們的安全狀態。當Trident判斷在不影響作用中工作負載的情況下、現有的磁碟區將會在適當時機切換至新的igroup方案。
- 隨附資源配額與Trident安裝、可確保在優先級類別使用量預設受限時、排定Trident示範集。
- 新增對Anf驅動程式的網路功能支援。（"[GitHub問題#717](#)"）
- 新增技術預覽功能可自動MetroCluster 切換偵測ONTAP 到不完整的驅動程式。（"[GitHub問題#228](#)"）

## 棄用

- \*\* Kubernetes：\*將支援的Kubernetes最低更新為1.19。
- 後端組態不再允許在單一組態中使用多種驗證類型。

## 移除

- AWS CVS驅動程式（自22.04年起已過時）已移除。
- Kubernetes
  - 已從節點Pod移除不必要的SYS\_ADMIN功能。



- 將節點準備工作減至簡單的主機資訊和主動服務探索、以盡力確認工作節點上是否有NFS/iSCSI服務可用。

## 文件

全新 "Pod安全標準" (PSS) 部分已新增、詳述由Astra Trident在安裝時啟用的權限。

## 22.04年的變化

NetApp持續改善及強化其產品與服務。以下是Astra Trident的一些最新功能。如需舊版的資訊、請參閱 ["較早版本的文件"](#)。



如果您要從任何先前的Trident版本升級並使用Azure NetApp Files 更新版本、請使用 `location` 組態參數現在是必填的單一欄位。

## 修正

- 改善iSCSI啟動器名稱的剖析。 (["GitHub問題#681"](#))
- 修正不允許使用csi儲存類別參數的問題。 (["GitHub問題#598"](#))
- 修復Trident CRD中的重複金鑰宣告。 (["GitHub問題#671"](#))
- 修正不正確的「csi Snapshot記錄」。 (["GitHub問題#629"](#))
- 已修正在刪除節點上解除發佈磁碟區的問題。 (["GitHub問題#691"](#))
- 新增區塊裝置上檔案系統不一致的處理方式。 (["GitHub問題#656"](#))
- 修正設定時拉出自動支援影像的問題 `imageRegistry` 安裝期間標示。 (["GitHub問題#715"](#))
- 修正ANF驅動程式無法複製具有多個匯出規則的磁碟區的問題。

## 增強功能

- 若要連入Trident的安全端點、現在至少需要TLS 1.3。 (["GitHub問題#698"](#))
- Trident現在將HSTC標頭新增至其安全端點的回應。
- Trident現在會自動嘗試啟用Azure NetApp Files 「UNIX權限」功能。
- \* Kubernetes\*：Trident取消程式集現在以系統節點關鍵優先順序類別執行。 (["GitHub問題#694"](#))

## 移除

E系列驅動程式（自20.07起停用）已移除。

## 22.01.1中的變更

## 修正

- 已修正在刪除節點上解除發佈磁碟區的問題。 (["GitHub問題#691"](#))
- 存取零欄位以取得ONTAP 靜止API回應中的集合空間時、會出現固定的恐慌。

## 22.01.0版的變更

### 修正

- \* Kubernetes：\*增加大型叢集的節點登錄回退重試時間。
- 已解決以下問題：azure-NetApp-Files驅動程式可能會被同名的多個資源混淆。
- 如果使用方括弧指定SAN IPv6資料生命量、現在就能正常運作。ONTAP
- 修正嘗試匯入已匯入磁碟區傳回EOF、使PVC處於擱置狀態的問題。（["GitHub問題#489"](#)）
- 修正當在SolidFire 一個穩定區上建立超過32個快照時、Astra Trident效能變慢的問題。
- 在建立SSL憑證時、以SHA-256取代SHA-1。
- 固定ANF驅動程式、允許重複的資源名稱、並將作業限制在單一位置。
- 固定ANF驅動程式、允許重複的資源名稱、並將作業限制在單一位置。

### 增強功能

- Kubernetes增強功能：
  - 新增對Kubernetes 1.23的支援。
  - 透過Trident運算子或Helm安裝Trident Pod時、請新增排程選項。（["GitHub問題#65"](#)）
- 允許GCP驅動程式中的跨區域磁碟區。（["GitHub問題#633"](#)）
- 新增對anf磁碟區「unix權限」選項的支援。（["GitHub問題#6666"](#)）

### 棄用

Trident REST介面只能以127.0.0.1或[:1]位址接聽和使用

## 210.1的變更



v21.10.0版本發生問題、可在移除節點後將Trident控制器重新新增回Kubernetes叢集時、將其置於CrashLoopBackOff狀態。此問題已在版本210.1中修正（[GitHub問題669](#)）。

### 修正

- 修正在GCP CVS後端匯入磁碟區時可能發生的競爭狀況、導致無法匯入。
- 修正刪除節點後、將Trident控制器重新加入Kubernetes叢集（[GitHub問題669](#)）時、使Trident控制器進入CrashLoopBackOff狀態的問題。
- 修正未指定SVM名稱時不再探索SVM的問題（[GitHub問題612](#)）。

## 21.0

## 修正

- 修正XFS磁碟區的複本無法與來源磁碟區掛載在同一個節點上的問題（GitHub問題514）。
- 修正Astra Trident在關機時記錄嚴重錯誤的問題（GitHub問題597）。
- Kubernetes相關修正：
  - 使用建立快照時、會傳回磁碟區已用空間做為最小重述大小 `ontap-nas` 和 `ontap-nas-flexgroup` 驅動程式（GitHub問題645）。
  - 修正何處發生的問題 `Failed to expand filesystem` 在磁碟區重新調整大小後記錄錯誤（GitHub問題560）。
  - 已解決Pod可能卡住的問題 `Terminating` 狀態（GitHub問題572）。
  - 解決了其中的問題 `ontap-san-economy` 可能已滿快照LUN（GitHub問題533）FlexVol。
  - 修正不同映像的自訂Yaml安裝程式問題（GitHub問題613）。
  - 修正快照大小計算（GitHub問題611）。
  - 修正所有Astra Trident安裝程式可將純Kubernetes識別為OpenShift的問題（GitHub問題639）。
  - 修正Trident運算子、在Kubernetes API伺服器無法連線時停止協調（GitHub問題599）。

## 增強功能

- 新增支援 `unixPermissions` GCP-CVS效能磁碟區的選項。
- 在GCP中新增對大規模最佳化的CVS磁碟區的支援、範圍介於600 GiB到1 TiB之間。
- Kubernetes相關增強功能：
  - 新增對Kubernetes 1.22的支援。
  - 讓Trident運算子和Helm圖表能與Kubernetes 1.22搭配使用（GitHub問題628）。
  - 新增操作員映像至 `tridentctl` 映像命令（GitHub問題570）。

## 實驗性增強功能

- 新增了對中磁碟區複寫的支援 `ontap-san` 驅動程式：
- 新增\*技術預覽\* REST支援 `ontap-nas-flexgroup`、`ontap-san``和 ``ontap-nas-economy` 驅動程式：

## 已知問題

已知問題可識別可能導致您無法成功使用產品的問題。

- 將Kubernetes叢集從1.24升級至1.25或更新版本、且已安裝Astra Trident時、您必須更新`vales.yaml`才能設定 `excludePodSecurityPolicy` 至 `true` 或新增 `--set excludePodSecurityPolicy=true` 至 `helm upgrade` 命令、然後才能升級叢集。
- Astra Trident現在強制執行空白 `fsType` (`fsType=""`) `fsType` 在其StorageClass中指定。使用Kubernetes 1.17或更新版本時、Trident支援提供空白 `fsType` 適用於NFS磁碟區。對於iSCSI磁碟區、您必須設定 `fsType` 在StorageClass上執行 `fsGroup` 使用安全性內容。

- 在多個Astra Trident執行個體之間使用後端時、每個後端組態檔都應有不同的組態檔 `storagePrefix` 價值用於不一樣的後端或使用不同的ONTAP `TenantName` 用於SolidFire 後端。Astra Trident無法偵測其他Astra Trident執行個體所建立的磁碟區。嘗試在ONTAP 不穩定或SolidFire 不穩定的後端上建立現有的Volume是成功的、因為Astra Trident將建立Volume視為強大的作業。如果 `storagePrefix` 或 `TenantName` 別有不同、在相同後端上建立的磁碟區可能會發生名稱衝突。
- 安裝Astra Trident時（使用 `tridentctl` 或Trident運算子）和使用 `tridentctl` 若要管理Astra Trident、您應確保 `KUBECONFIG` 環境變數已設定。這是表示Kubernetes叢集的必要資訊 `tridentctl` 應該與之合作。在使用多個Kubernetes環境時、您應確保 `KUBECONFIG` 檔案來源正確。
- 若要執行iSCSI PV的線上空間回收、工作節點上的基礎作業系統可能需要將掛載選項傳遞至磁碟區。這適用於需要的RHEL/RedHat CoreOS執行個體 discard "掛載選項"；請確定您的隨附了捨棄掛載選項[StorageClass]支援線上區塊捨棄。
- 如果每個Kubernetes叢集有一個以上的Astra Trident執行個體、Astra Trident就無法與其他執行個體通訊、也無法探索他們所建立的其他磁碟區、如果叢集內有多個執行個體執行、就會導致非預期和不正確的行為。每個Kubernetes叢集只應有一個Astra Trident執行個體。
- 如果是Astra Trident型 StorageClass 當Astra Trident離線時、會從Kubernetes刪除物件、當Astra Trident重新上線時、不會從資料庫中移除對應的儲存類別。您應該使用刪除這些儲存類別 `tridentctl` 或REST API。
- 如果使用者刪除由Astra Trident提供的PV、然後再刪除對應的PVC、則Astra Trident不會自動刪除備份Volume。您應該透過移除Volume `tridentctl` 或REST API。
- 除非集合體是每個資源配置要求的唯一集合體、否則無法同時配置多個支援區。ONTAP FlexGroup
- 使用Astra Trident over IPv6時、您應該指定 `managementLIF` 和 `dataLIF` 在後端定義的方括弧內。例如、`[fd20:8b1e:b258:2000:f816:3eff:feec:0]`。



您無法指定 `dataLIF` 在SAN後端ONTAP。Astra Trident會探索所有可用的iSCSI LIF、並使用它們來建立多重路徑工作階段。

- 如果使用 `solidfire-san` 使用OpenShift 4.5的驅動程式、請確保基礎工作者節點使用MD5做為CHAP驗證演算法。元素12.7提供安全的FIPS相容CHAP演算法SHA1、SHA-256和SHA3-256。

## 如需詳細資訊、請參閱

- ["Astra Trident GitHub"](#)
- ["Astra Trident部落格"](#)

# 概念

## 瞭解Astra Trident

Astra Trident是由NetApp維護的完整支援開放原始碼專案、也是其中的一部分 "[Astra產品系列](#)"。其設計旨在協助您使用業界標準介面（例如Container Storage介面（SCSI））來滿足容器化應用程式的持續需求。

### 總覽

Astra Trident將Kubernetes叢集部署為Pod、為Kubernetes工作負載提供動態儲存協調服務。它可讓您的容器化應用程式快速輕鬆地使用NetApp廣泛產品組合中的持續儲存設備、包括ONTAP：VMware的各種產品組合（AFF/FAS/Select/Cloud / Amazon FSX for NetApp ONTAP）、Element軟體（NetApp HCI / SolidFire）、Azure NetApp Files 以及Google Cloud Volumes Service Cloud上的整套服務和功能。

Astra Trident也是NetApp Astra的一項基礎技術、運用NetApp領先業界的資料管理技術、提供快照、備份、複製及複製等快照、備份、複製及複製功能、為Kubernetes工作負載提供資料保護、災難恢復、可攜性及移轉使用案例。

### 支援的Kubernetes叢集架構

下列Kubernetes架構支援Astra Trident：

Kubernetes叢集架構	支援	預設安裝
單一主機、運算	是的	是的
多重主機、運算	是的	是的
主要、`etcd`運算	是的	是的
主要、基礎架構、運算	是的	是的

### 什麼是Astra？

Astra可讓企業更輕鬆地管理、保護及搬移在公有雲內部及內部部署的Kubernetes上執行的資料豐富的容器化工作負載。Astra透過NetApp在公有雲和內部部署環境中備受肯定且廣泛的儲存產品組合、運用Astra Trident來提供持續的容器儲存設備。此外、它還提供一組豐富的進階應用程式感知資料管理功能、例如Snapshot、備份與還原、活動記錄、以及資料保護、災難/資料恢復、資料稽核、以及Kubernetes工作負載的移轉使用案例等主動複製功能。

您可以在Astra頁面註冊免費試用。

### 以取得更多資訊

- "[NetApp Astra產品系列](#)"

- ["Astra Control Service文件"](#)
- ["Astra Control Center文件"](#)
- ["Astra API文件"](#)

## 驅動程式ONTAP

Astra Trident提供五ONTAP 種獨特的Intel儲存驅動程式、可與ONTAP 各種叢集進行通訊。深入瞭解每個驅動程式如何處理磁碟區的建立、存取控制及其功能。

### 深入瞭ONTAP 解NetApp儲存驅動程式



Astra Control可為使用建立的磁碟區提供無縫保護、災難恢復和移動性（在Kubernetes叢集之間移動磁碟區） `ontap-nas`、`ontap-nas-flexgroup`和 `ontap-san` 驅動程式：請參閱 ["Astra Control複寫先決條件"](#) 以取得詳細資料。

- 您必須使用 `ontap-nas` 適用於需要資料保護、災難恢復和行動力的正式作業工作負載。
- 使用 `ontap-san-economy` 當預期的Volume使用量將遠高於ONTAP 支援的容量時。
- 使用 `ontap-nas-economy` 只有在預期的Volume使用量會比ONTAP 支援的高出許多、以及 `ontap-san-economy` 無法使用驅動程式。
- 請勿使用 `ontap-nas-economy` 如果您預期需要資料保護、災難恢復或行動性、

驅動程式	傳輸協定	Volume模式	支援的存取模式	支援的檔案系統
<code>ontap-nas</code>	NFS	檔案系統	<code>rwo</code> 、 <code>ROX</code> 、 <code>rwX</code>	<code>J</code> 、NFS
<code>ontap-nas-economy</code>	NFS	檔案系統	<code>rwo</code> 、 <code>ROX</code> 、 <code>rwX</code>	<code>J</code> 、NFS
<code>ontap-nas-flexgroup</code>	NFS	檔案系統	<code>rwo</code> 、 <code>ROX</code> 、 <code>rwX</code>	<code>J</code> 、NFS
<code>ontap-san</code>	iSCSI	區塊	<code>rwo</code> 、 <code>ROX</code> 、 <code>rwX</code>	無檔案系統；原始區塊裝置
<code>ontap-san</code>	iSCSI	檔案系統	<code>Rwo</code> 、 <code>ROX</code>  <code>RwX</code> 無法在Filesystem Volume模式中使用。	<code>xfS</code> 、 <code>ext3</code> 、 <code>ext4</code>
<code>ontap-san-economy</code>	iSCSI	區塊	<code>rwo</code> 、 <code>ROX</code> 、 <code>rwX</code>	無檔案系統；原始區塊裝置

驅動程式	傳輸協定	Volume模式	支援的存取模式	支援的檔案系統
ontap-san-economy	iSCSI	檔案系統	Rwo、ROX  Rwx無法在Filesystem Volume模式中使用。	xfs、ext3、ext4



利用安全角色（使用者名稱/密碼）的登入認證、或是使用安裝在該叢集上的私密金鑰和憑證、來驗證後端。ONTAP ONTAP您可以使用更新現有的後端、以便從一個驗證模式移至另一個驗證模式 `tridentctl update backend`。

## 資源配置

Astra Trident的資源配置有兩個主要階段。第一階段會將儲存類別與一組適當的後端儲存資源池建立關聯、並在進行資源配置之前做好必要準備。第二階段包括磁碟區建立本身、並要求從與擱置磁碟區儲存類別相關的儲存資源池中選擇儲存資源池。

### 儲存類別關聯

將後端儲存資源池與儲存類別建立關聯、取決於儲存類別的要求屬性及其屬性 `storagePools`、`additionalStoragePools` 和 `excludeStoragePools` 清單。當您建立儲存類別時、Trident會比較每個後端所提供的屬性和集區、以及儲存類別所要求的屬性和集區。如果儲存資源池的屬性和名稱符合所有要求的屬性和資源池名稱、Astra Trident會將該儲存資源池新增至該儲存類別適用的儲存資源池集合。此外、Astra Trident也會新增中列出的所有儲存集區 `additionalStoragePools` 列出該集合、即使其屬性無法滿足所有或任何儲存類別的要求屬性。您應該使用 `excludeStoragePools` 用於置換及移除儲存資源池以供儲存類別使用的清單。每次新增後端時、Astra Trident都會執行類似的程序、檢查其儲存集區是否符合現有儲存類別的儲存集區、以及是否移除任何已標記為「已排除」的儲存資源池。

### Volume建立

Astra Trident接著會使用儲存類別與儲存資源池之間的關聯、來決定要在何處配置磁碟區。當您建立Volume時、Astra Trident會先取得該磁碟區儲存類別的儲存集區集區集區、此外、如果您指定磁碟區的傳輸協定、Astra Trident會移除無法提供所需傳輸協定的儲存資源池（例如、NetApp HCI / SolidFire後端無法提供檔案型磁碟區、ONTAP 而非由NAS後端提供區塊型磁碟區）。Astra Trident會隨機排列此結果集的順序、以利均勻散佈磁碟區、然後透過磁碟區重複資料、進而嘗試在每個儲存集區上配置磁碟區。如果某個項目成功、則會成功傳回、並記錄程序中發生的任何故障。Astra Trident返回故障\*僅當\*無法在\* all \*上配置所需儲存類別和傳輸協定可用的儲存資源池時。

## Volume快照

深入瞭解Astra Trident如何為其驅動程式建立磁碟區快照。

### 深入瞭解Volume Snapshot建立

- 適用於 `ontap-nas`、`ontap-san`、`gcp-cvs` 和 `azure-netapp-files` 驅動程式、每個持續Volume (PV) 都會對應FlexVol 至一個功能區。因此、磁碟區快照會建立為NetApp快照。NetApp的Snapshot技術



提供比競爭快照技術更高的穩定性、擴充性、可恢復性和效能。這些Snapshot複本無論在建立所需的時間、還是在儲存空間中、都能發揮極高的效率。

- 適用於 `ontap-nas-flexgroup` 驅動程式、每個持續Volume (PV) 都會對應FlexGroup 至一個功能區。因此、磁碟區快照會建立為NetApp FlexGroup 的「資訊快照」。NetApp的Snapshot技術提供比競爭快照技術更高的穩定性、擴充性、可恢復性和效能。這些Snapshot複本無論在建立所需的時間、還是在儲存空間中、都能發揮極高的效率。
- 適用於 `ontap-san-economy` 驅動程式、PV對應至在共享FlexVols上建立的LUN。PV的Volume Snapshot 是透過執行相關LUN的FlexClones來達成的。ONTAP的FlexClone技術幾乎可以即時建立最大資料集的複本。複本會與其父實體共用資料區塊、除了中繼資料所需的儲存空間外、不需要使用任何儲存設備。
- 適用於 `solidfire-san` 驅動程式、每個PV對應至NetApp Element 在Escale軟體/NetApp HCI叢集上建立的LUN。Volume Snapshot以基礎LUN的元素快照來表示。這些快照是時間點複本、只佔用少量系統資源和空間。
- 使用時 `ontap-nas` 和 `ontap-san` 驅動程式ONTAP、不含快照、是FlexVol 指將資料複本的時間點複本、會佔用FlexVol 整個過程中的空間。這可能會產生磁碟區中的可寫入空間量、以便在建立/排程快照時縮短時間。解決此問題的一種簡單方法、就是透過Kubernetes調整大小來擴充磁碟區。另一個選項是刪除不再需要的快照。當透過Kubernetes建立的Volume Snapshot被刪除時、Astra Trident會刪除相關的ONTAP 功能快照。不透過Kubernetes建立的支援快照也可以刪除。ONTAP

有了Astra Trident、您可以使用Volume Snapshot來建立新的PV。使用FlexClone技術建立這些快照的PV、以支援ONTAP 支援的支援的支援功能和CVS後端。從快照建立PV時、備份磁碟區是Snapshot父磁碟區的FlexClone。。`solidfire-san` 驅動程式使用Element軟體磁碟區複製、從快照建立PV。在此、它會從元素快照建立複本。

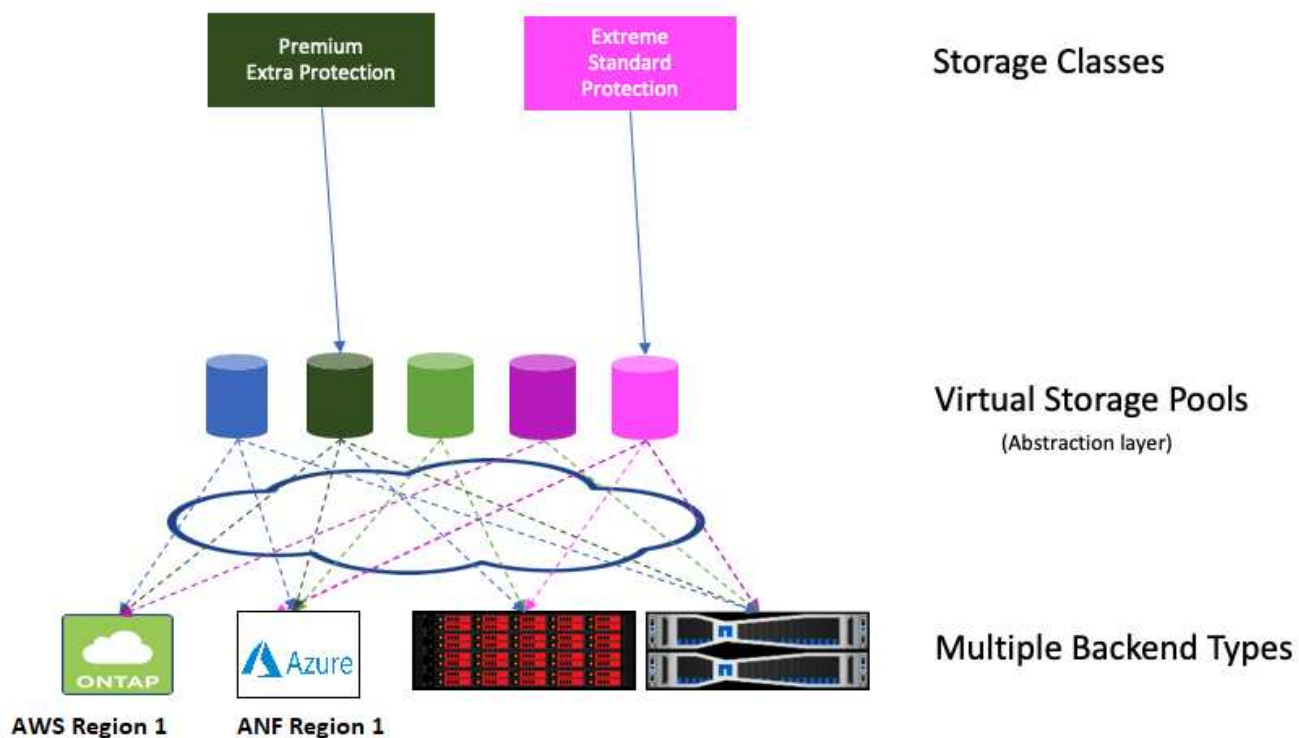
## 虛擬資源池

虛擬資源池可在Astra Trident儲存後端與Kubernetes之間提供抽象層 `StorageClasses`。管理員可以透過通用的後端不受限制的方式、定義各個方面、例如位置、效能及每個後端的保護、而無需進行任何操作 `StorageClass` 指定要用於符合所需條件的實體後端、後端集區或後端類型。

### 瞭解虛擬資源池

儲存管理員可在Json或Yaml定義檔案的任何Astra Trident後端上定義虛擬資源池。





在虛擬資源池清單之外指定的任何層面、都會對後端進行全域設定、並套用至所有虛擬資源池、而每個虛擬資源池則可個別指定一個或多個層面（覆寫任何後端全域層面）。



- 定義虛擬資源池時、請勿嘗試重新排列後端定義中現有虛擬資源池的順序。
- 我們建議您不要修改現有虛擬資源池的屬性。您應該定義新的虛擬資源池以進行變更。

大部分方面都是以後端特定的詞彙來指定。最重要的是、在後端驅動程式之外、不會顯示高寬比值、也無法在中進行比對 **StorageClasses**。而是由系統管理員為每個虛擬資源池定義一或多個標籤。每個標籤都是「金鑰：值配對」、而且標籤可能在獨特的後端之間通用。如同個別層面、標籤可依資源池指定、也可全域指定至後端。不同於具有預先定義名稱和值的各個層面、系統管理員有充分的判斷權、可視需要定義標籤金鑰和值。為了方便起見、儲存管理員可以針對每個虛擬資源池定義標籤、並依標籤將磁碟區分組。

答 **StorageClass** 透過參照選取元參數中的標籤來識別要使用的虛擬資源池。虛擬資源池選取器支援下列運算子：

營運者	範例	集區的標籤值必須：
=	效能=優異	相符
!=	效能 != 極致	不相符
in	位置（東部、西部）	加入一組值
notin	效能附註（銀、銅）	不在一組值中
<key>	保護	存在於任何值
!<key>	!保護	不存在

# Volume存取群組

深入瞭解Astra Trident的使用方式 "[Volume存取群組](#)"。



如果您使用的是CHAP、建議您略過本節、以簡化管理並避免以下所述的擴充限制。此外、如果您在「csi」模式中使用Astra Trident、則可以忽略本節。Astra Trident在安裝為增強的SCSI資源配置程式時、會使用CHAP。

## 深入瞭解Volume存取群組

Astra Trident可使用Volume存取群組來控制其所配置之磁碟區的存取。如果停用CHAP、則會尋找稱為的存取群組 `trident` 除非您在組態中指定一或多個存取群組ID。

雖然Astra Trident會將新磁碟區與已設定的存取群組建立關聯、但它不會自行建立或管理存取群組。存取群組必須先存在、儲存後端才會新增至Astra Trident、而且必須包含Kubernetes叢集中每個節點的iSCSI IQN、這些節點可能會掛載該後端所配置的磁碟區。在大多數安裝中、這包括叢集中的每個工作節點。

對於具有超過64個節點的Kubernetes叢集、您應該使用多個存取群組。每個存取群組最多可包含64個IQN、每個磁碟區可屬於四個存取群組。在設定最多四個存取群組的情況下、叢集中最多256個節點的任何節點都能存取任何磁碟區。如需Volume存取群組的最新限制、請參閱 "[請按這裡](#)"。

如果您要從使用預設值的組態中修改組態 `trident` 存取群組也會使用其他群組、包括的ID `trident` 清單中的存取群組。

# 開始使用

## 歡迎試用

NetApp提供立即可用的實驗室映像、您可以透過申請 ["NetApp試用"](#)。

### 深入瞭解測試磁碟機

測試磁碟機提供您一個沙箱環境、其中安裝並設定了三節點Kubernetes叢集和Astra Trident。這是熟悉Astra Trident並探索其特色的絕佳方式。

另一個選項是查看 ["Kubeadm安裝指南"](#) 由Kubernetes提供。



您不應該在正式作業中使用這些指令所建置的Kubernetes叢集。請使用經銷商提供的正式作業部署指南、建立正式作業就緒的叢集。

如果這是您第一次使用Kubernetes、請熟悉這些概念和工具 ["請按這裡"](#)。

## 需求

在安裝Astra Trident之前、您應該先檢閱這些一般系統需求。特定後端可能有其他需求。

### Astra Trident的重要資訊23.01

您必須閱讀下列有關**Astra Trident**的重要資訊。

關於**Astra Trid-功能** 的資訊

- Kubernetes 1.26現在已在Trident中受到支援。升級Kubernetes之前先升級Trident。
- Astra Trident在SAN環境中嚴格執行多重路徑組態的使用、建議的值為 `find_multipaths: no` 在多重路徑.conf檔案中。

使用非多重路徑組態或使用 `find_multipaths: yes` 或 `find_multipaths: smart` 多重路徑.conf檔案中的值會導致掛載失敗。Trident建議使用 `find_multipaths: no` 自21.07版本以來。

### 支援的前端（協調器）

Astra Trident支援多個容器引擎和協調器、包括：

- Anthos on -Prem (VMware) 和Anthos on裸機1.9、1.10、1.11
- Kubernetes 1.21 - 1.26
- Mirantis Kubernetes Engine 3.5
- OpenShift 4.9 - 4.12

這些版本支援Trident運算子：

- Anthos on -Prem (VMware) 和Anthos on裸機1.9、1.10、1.11
- Kubernetes 1.21 - 1.26
- OpenShift 4.9 - 4.12

Astra Trident也能與其他全管理且自我管理的Kubernetes產品搭配使用、包括Google Kubernetes Engine (GKE) 、Amazon Elastic Kubernetes Services (EKS) 、Azure Kubernetes Service (KS) 、Rancher及VMware Tanzu Portfolio 。



在將Kubernetes叢集從1.24升級至1.25或更新版本、且已安裝Astra Trident之前、請參閱 "[升級Helm型的營運者安裝](#)" 。

## 支援的後端（儲存）

若要使用Astra Trident、您需要下列一或多個支援的後端：

- Amazon FSX for NetApp ONTAP 產品
- Azure NetApp Files
- Cloud Volumes ONTAP
- 適用於 GCP Cloud Volumes Service
- FAS/AFF/選取9.5或更新版本
- NetApp All SAN Array ASA (ESAN)
- NetApp HCI / Element軟體11或更新版本

## 功能需求

下表摘要說明此Astra Trident版本的可用功能及其支援的Kubernetes版本。

功能	Kubernetes版本	需要功能閘道？
csi Trident	1.21 - 1.26	否
Volume Snapshot	1.21 - 1.26	否
來自Volume Snapshot的PVC	1.21 - 1.26	否
iSCSI PV調整大小	1.21 - 1.26	否
資訊雙向CHAP ONTAP	1.21 - 1.26	否
動態匯出原則	1.21 - 1.26	否
Trident運算子	1.21 - 1.26	否
csi拓撲	1.21 - 1.26	否

## 已測試的主機作業系統

儘管Astra Trident並未正式支援特定作業系統、但已知下列項目仍能正常運作：

- 受OpenShift Container Platform支援的RedHat CoreOS (RMCOS) 版本
- RHEL 8以上
- Ubuntu 22.04或更新版本
- Windows Server 2019

依預設、Astra Trident會在容器中執行、因此會在任何Linux工作者上執行。不過、這些員工必須能夠使用標準NFS用戶端或iSCSI啟動器來掛載Astra Trident提供的磁碟區、視您使用的後端而定。

◦ `tridentctl` 公用程式也可在這些Linux版本中的任何一種上執行。

## 主機組態

Kubernetes叢集中的所有工作節點都必須能夠掛載您已為Pod配置的磁碟區。若要準備工作節點、您必須根據所選的驅動程式來安裝NFS或iSCSI工具。

["準備工作節點"](#)

## 儲存系統組態

Astra Trident可能需要變更儲存系統、才能使用後端組態。

["設定後端"](#)

## Astra Trident連接埠

Astra Trident需要存取特定連接埠才能進行通訊。

["Astra Trident連接埠"](#)

## Container映像和對應的Kubernetes版本

對於空拍安裝、下列清單是安裝Astra Trident所需的容器映像參考資料。使用 `tridentctl images` 用於驗證所需容器映像清單的命令。

Kubernetes版本	Container映像
1.21.0版	<ul style="list-style-type: none"> <li>• Docker ◦ IO/NetApp/Trident : 23.01.1</li> <li>• Docker ◦ IO/NetApp/trident 自動支援 : 23.01</li> <li>• registry ◦ k8s.io/SIG-storage / csi 置備程序 : v3.4.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 附加程式 : v4.1.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 大小調整 : v1.7.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 快照機 : v6.2.1</li> <li>• 登錄 .k8s.io/SIG-storage / csi 節點驅動程式登錄器 : v2.2.0</li> <li>• Docker ◦ IO/NetApp/Trident 營運商 : 23.01.1 (選用)</li> </ul>
1.22.0版	<ul style="list-style-type: none"> <li>• Docker ◦ IO/NetApp/Trident : 23.01.1</li> <li>• Docker ◦ IO/NetApp/trident 自動支援 : 23.01</li> <li>• registry ◦ k8s.io/SIG-storage / csi 置備程序 : v3.4.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 附加程式 : v4.1.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 大小調整 : v1.7.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 快照機 : v6.2.1</li> <li>• 登錄 .k8s.io/SIG-storage / csi 節點驅動程式登錄器 : v2.2.0</li> <li>• Docker ◦ IO/NetApp/Trident 營運商 : 23.01.1 (選用)</li> </ul>
1.23.0版	<ul style="list-style-type: none"> <li>• Docker ◦ IO/NetApp/Trident : 23.01.1</li> <li>• Docker ◦ IO/NetApp/trident 自動支援 : 23.01</li> <li>• registry ◦ k8s.io/SIG-storage / csi 置備程序 : v3.4.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 附加程式 : v4.1.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 大小調整 : v1.7.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 快照機 : v6.2.1</li> <li>• 登錄 .k8s.io/SIG-storage / csi 節點驅動程式登錄器 : v2.2.0</li> <li>• Docker ◦ IO/NetApp/Trident 營運商 : 23.01.1 (選用)</li> </ul>

Kubernetes版本	Container映像
1.24.0版	<ul style="list-style-type: none"> <li>• Docker ◦ IO/NetApp/Trident : 23.01.1</li> <li>• Docker ◦ IO/NetApp/trident 自動支援 : 23.01</li> <li>• registry ◦ k8s.io/SIG-storage / csi 置備程序 : v3.4.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 附加程式 : v4.1.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 大小調整 : v1.7.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 快照機 : v6.2.1</li> <li>• 登錄 .k8s.io/SIG-storage / csi 節點驅動程式登錄器 : v2.2.0</li> <li>• Docker ◦ IO/NetApp/Trident 營運商 : 23.01.1 (選用)</li> </ul>
v1.25.0	<ul style="list-style-type: none"> <li>• Docker ◦ IO/NetApp/Trident : 23.01.1</li> <li>• Docker ◦ IO/NetApp/trident 自動支援 : 23.01</li> <li>• registry ◦ k8s.io/SIG-storage / csi 置備程序 : v3.4.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 附加程式 : v4.1.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 大小調整 : v1.7.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 快照機 : v6.2.1</li> <li>• 登錄 .k8s.io/SIG-storage / csi 節點驅動程式登錄器 : v2.2.0</li> <li>• Docker ◦ IO/NetApp/Trident 營運商 : 23.01.1 (選用)</li> </ul>
1.26.0版	<ul style="list-style-type: none"> <li>• Docker ◦ IO/NetApp/Trident : 23.01.1</li> <li>• Docker ◦ IO/NetApp/trident 自動支援 : 23.01</li> <li>• registry ◦ k8s.io/SIG-storage / csi 置備程序 : v3.4.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 附加程式 : v4.1.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 大小調整 : v1.7.0</li> <li>• 登錄 .k8s.io/SIG-storage / csi 快照機 : v6.2.1</li> <li>• 登錄 .k8s.io/SIG-storage / csi 節點驅動程式登錄器 : v2.2.0</li> <li>• Docker ◦ IO/NetApp/Trident 營運商 : 23.01.1 (選用)</li> </ul>



在Kubernetes 1.21版及更新版本上、請使用已驗證的 `registry.k8s.gcr.io/sig-storage/csi-snapshotter:v6.x` 僅在以下情況下顯示映像 v1 版本正在提供 `volumesnapshots.snapshot.storage.k8s.gcr.io` 客戶需求日如果是 v1beta1 版本為CRD提供/不提供 v1 版本、請使用已驗證的 `registry.k8s.gcr.io/sig-storage/csi-snapshotter:v3.x` 映像。

## 安裝Astra Trident

### 瞭解Astra Trident安裝

為了確保Astra Trident可安裝在各種環境和組織中、NetApp提供多種安裝選項。您可以使用Trident運算子（手動或使用Helm）或搭配安裝Astra Trident `tridentctl`。本主題提供重要資訊、協助您選擇正確的安裝程序。

#### Astra Trident的重要資訊23.01

您必須閱讀下列有關Astra Trident的重要資訊。

關於Astra Trident-功能 的資訊

- Kubernetes 1.26現在已在Trident中受到支援。升級Kubernetes之前先升級Trident。
- Astra Trident在SAN環境中嚴格執行多重路徑組態的使用、建議的值為 `find_multipaths: no` 在多重路徑.conf檔案中。

使用非多重路徑組態或使用 `find_multipaths: yes` 或 `find_multipaths: smart` 多重路徑.conf檔案中的值會導致掛載失敗。Trident建議使用 `find_multipaths: no` 自21.07版本以來。

### 開始之前

無論安裝路徑為何、您都必須具備：

- 對執行支援版本Kubernetes及啟用功能需求的Kubernetes叢集擁有完整權限。檢閱 ["需求"](#) 以取得詳細資料。
- 存取支援的NetApp儲存系統。
- 能夠從所有Kubernetes工作節點掛載磁碟區。
- Linux主機 `kubectl` （或 `oc`（如果您使用OpenShift）已安裝並設定為管理您要使用的Kubernetes叢集。
- `KUBECONFIG` 環境變數設定為指向Kubernetes叢集組態。
- 如果您使用Kubernetes搭配Docker Enterprise、["請依照他們的步驟啟用CLI存取"](#)。



如果您尚未熟悉 ["基本概念"](#)現在正是這麼做的好時機。

### 選擇您的安裝方法

選取最適合您的安裝方法。您也應該檢閱的考量事項 ["在方法之間移動"](#) 做出決定之前。



## 使用Trident運算子

無論是手動部署或使用Helm、Trident營運者都是簡化安裝及動態管理Astra Trident資源的絕佳方式。您甚至可以["自訂您的Trident營運者部署"](#) 使用中的屬性 `TridentOrchestrator` 自訂資源（CR）。

使用Trident營運者的好處包括：

不只是個Trident物件、更是個可說是個可說是個地方

Trident運算子會自動為Kubernetes版本建立下列物件。

- 營運者服務帳戶
- 叢集角色和叢集角色繫結至服務帳戶
- 專屬的PodSecurity原則（適用於Kubernetes 1.25及更早版本）
- 營運者本身

## 還原功能的功能

營運者會監控Astra Trident安裝、並主動採取措施來處理問題、例如刪除部署或意外修改部署。答 `trident-operator-<generated-id>` 建立Pod以建立關聯 `TridentOrchestrator` 含Astra Trident安裝的CR。如此可確保叢集中只有一個Astra Trident執行個體、並控制其設定、確保安裝功能強大。當對安裝進行變更（例如刪除部署或節點取消設定）時、操作員會分別識別並修正這些變更。

## 更新至現有安裝的更新功能

您可以輕鬆地與營運者一起更新現有的部署。您只需要編輯 `TridentOrchestrator` 以更新安裝。

例如、假設您需要啟用Astra Trident來產生偵錯記錄的案例。若要這麼做、請修補您的 `TridentOrchestrator` 以設定 `spec.debug` 至 `true`：

```
kubectl patch torc <trident-orchestrator-name> -n trident --type=merge  
-p '{"spec":{"debug":true}}'
```

之後 `TridentOrchestrator` 更新後、營運者會處理更新並修補現有安裝。這可能會觸發建立新的Pod、以據此修改安裝。

## 支援升級功能的不一樣之處

當叢集的Kubernetes版本升級至支援的版本時、營運者會自動更新現有的Astra Trident安裝、並加以變更、以確保其符合Kubernetes版本的要求。



如果叢集升級至不受支援的版本、則操作員將無法安裝Astra Trident。如果操作員已安裝Astra Trident、則會顯示警告、指出Astra Trident安裝在不受支援的Kubernetes版本上。

## 使用BlueXP（前身為Cloud Manager）進行叢集管理

與 "使用BlueXP的Astra Trident"、您可以升級至最新版的Astra Trident、新增及管理儲存類別、並將其連線至工作環境、以及使用Cloud Backup Service NetApp備份持續的Volume。BlueXP支援使用Trident操作者手動或使用Helm進行Astra Trident部署。

使用 `tridentctl`

如果您現有的部署必須升級、或是想要高度自訂部署、您應該考慮。這是部署Astra Trident的傳統方法。

您可以以產生Trident資源的資訊清單。這包括部署、取消程式集、服務帳戶、以及Astra Trident在安裝過程中所建立的叢集角色。



從22.04版開始、每次安裝Astra Trident時、AES金鑰就不會再重新產生。在這個版本中、Astra Trident會安裝一個新的秘密物件、並在安裝過程中持續存在。這表示、`tridentctl` 在22.04中可以解除安裝舊版Trident、但舊版無法解除安裝22.04安裝。選取適當的安裝方法。

### 選擇安裝模式

根據組織所需的安裝模式（標準、離線或遠端）來判斷您的部署程序。

#### 標準安裝

這是安裝Astra Trident最簡單的方法、適用於大多數不受網路限制的環境。標準安裝模式使用預設登錄來儲存所需的Trident (`docker.io`) 和csi (`registry.k8s.io`) 映像。

使用標準模式時、Astra Trident安裝程式會：

- 透過網際網路擷取容器映像
- 在Kubernetes叢集中的所有合格節點上建立部署或節點取消設定、以執行Astra Trident Pod

#### 離線安裝

在無線或安全的位置可能需要離線安裝模式。在此案例中、您可以建立單一私有、鏡射的登錄或兩個鏡射登錄、以儲存所需的Trident和csi映像。



無論您的登錄組態為何、都必須將csi映像存放在單一登錄中。

#### 遠端安裝

以下是遠端安裝程序的高階概觀：

- 部署適當版本的 `kubectl` 在您要部署Astra Trident的遠端機器上。
- 從Kubernetes叢集複製組態檔案、然後設定 `KUBECONFIG` 遠端機器上的環境變數。
- 啟動 `kubectl get nodes` 命令來驗證您是否可以連線至所需的Kubernetes叢集。
- 使用標準安裝步驟、從遠端機器完成部署。

根據您的方法和模式選取程序

做出決策後、請選擇適當的程序。

方法	安裝模式
Trident運算子（手動）	"標準安裝"  "離線安裝"
Trident運算子（Helm）	"標準安裝"  "離線安裝"
tridentctl	"標準或離線安裝"

### 在安裝方法之間移動

您可以決定變更安裝方法。在執行此操作之前、請先考慮下列事項：

- 安裝及解除安裝Astra Trident時、請務必使用相同的方法。如果您已部署 `tridentctl`、您應該使用適當版本的 `tridentctl` 二進位以解除安裝Astra Trident。同樣地、如果您是與操作員一起部署、則應該編輯 `TridentOrchestrator` 並設定 `spec.uninstall=true` 解除安裝Astra Trident。
- 如果您想要移除並改用以營運者為基礎的部署 `tridentctl` 若要部署Astra Trident、您應該先編輯 `TridentOrchestrator` 並設定 `spec.uninstall=true` 解除安裝Astra Trident。然後刪除 `TridentOrchestrator` 以及營運者部署。然後您可以使用安裝 `tridentctl`。
- 如果您有手動的操作員型部署、而且想要使用以Helm為基礎的Trident操作員部署、您應該先手動解除安裝操作員、然後再執行Helm安裝。如此一來、Helm就能部署具有所需標籤和註釋的Trident運算子。如果您不這麼做、則Helm型Trident營運者部署將會失敗、並顯示標籤驗證錯誤和註釋驗證錯誤。如果您有 `tridentctl` 根據部署、您可以使用以Helm為基礎的部署、而不會發生問題。

### 其他已知組態選項

在VMware Tanzu產品組合產品上安裝Astra Trident時：

- 叢集必須支援特殊權限的工作負載。
- `--kubelet-dir` 旗標應設定為kubelet目錄的位置。依預設、這是 `/var/vcap/data/kubelet`。

使用指定kubelet位置 `--kubelet-dir` 已知適用於Trident運算子、Helm和 `tridentctl` 部署：

## 使用Trident操作員安裝

### 手動部署Trident運算子（標準模式）

您可以手動部署Trident運算子來安裝Astra Trident。此程序適用於未將Astra Trident所需的容器映像儲存在私有登錄中的安裝。如果您有私有映像登錄、請使用 ["離線部署程序"](#)。

## Astra Trident的重要資訊23.01

您必須閱讀下列有關**Astra Trident**的重要資訊。

關於**Astra Trident**-功能 的資訊

- Kubernetes 1.26現在已在Trident中受到支援。升級Kubernetes之前先升級Trident。
- Astra Trident在SAN環境中嚴格執行多重路徑組態的使用、建議的值為 `find_multipaths: no` 在多重路徑.conf檔案中。

使用非多重路徑組態或使用 `find_multipaths: yes` 或 `find_multipaths: smart` 多重路徑.conf檔案中的值會導致掛載失敗。Trident建議使用 `find_multipaths: no` 自21.07版本以來。

### 手動部署Trident運算子並安裝Trident

檢閱 ["安裝總覽"](#) 為了確保您符合安裝先決條件、並為您的環境選擇正確的安裝選項。

#### 開始之前

在開始安裝之前、請先登入Linux主機、然後確認它正在管理正常運作的 ["支援的Kubernetes叢集"](#) 而且您擁有必要的權限。



使用OpenShift、使用 `oc` 而非 `kubectl` 在以下所有範例中、請先執行\*系統：admin\*登入 `oc login -u system:admin` 或 `oc login -u kube-admin`。

#### 1. 驗證Kubernetes版本：

```
kubectl version
```

#### 2. 驗證叢集管理員權限：

```
kubectl auth can-i '*' '*' --all-namespaces
```

#### 3. 確認您可以啟動使用Docker Hub映像的Pod、並透過Pod網路連線至儲存系統：

```
kubectl run -i --tty ping --image=busybox --restart=Never --rm -- \
ping <management IP>
```

### 步驟1：下載Trident安裝程式套件

Astra Trident安裝程式套件包含部署Trident操作員及安裝Astra Trident所需的一切。從下載並擷取Trident安裝程式的最新版本 ["GitHub的\\_Assets區段"](#)。

```
wget https://github.com/NetApp/trident/releases/download/v23.01.1/trident-
installer-23.01.1.tar.gz
tar -xf trident-installer-23.01.1.tar.gz
cd trident-installer
```

## 步驟2：建立 TridentOrchestrator 客戶需求日

建立 TridentOrchestrator 自訂資源定義 (CRD)。您將建立 TridentOrchestrator 稍後再自訂資源。請使用中適當的CRD Y反 洗錢版本 deploy/crds 以建立 TridentOrchestrator 客戶需求日

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
```

## 步驟3：部署Trident運算子

Astra Trident安裝程式提供一個套件檔案、可用來安裝運算子及建立相關的物件。套裝組合檔案是使用預設組態部署操作員及安裝Astra Trident的簡易方法。

- 對於執行Kubernetes 1.24或更低層級的叢集、請使用 bundle\_pre\_1\_25.yaml。
- 對於執行Kubernetes 1.25或更新版本的叢集、請使用 bundle\_post\_1\_25.yaml。

Trident安裝程式會在中部署操作員 trident 命名空間。如果是 trident 命名空間不存在、請使用 kubectl apply -f deploy/namespace.yaml 以建立。

### 步驟

#### 1. 建立資源並部署營運者：

```
kubectl create -f deploy/<bundle>.yaml
```



可在非的命名空間中部署運算子 trident 命名空間、更新 serviceaccount.yaml、clusterrolebinding.yaml 和 operator.yaml 並使用產生套裝組合檔案 kustomization.yaml：

```
kubectl kustomize deploy/ > deploy/<bundle>.yaml
```

#### 2. 驗證是否已部署操作員。

```
kubectl get deployment -n <operator-namespace>
```

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
trident-operator	1/1	1	1	3m



Kubernetes叢集中只應有\*一個運算子執行個體\*。請勿建立Trident營運者的多個部署。

#### 步驟4：建立 TridentOrchestrator 並安裝Trident

您現在可以建立 TridentOrchestrator 並安裝Astra Trident。您也可以選擇 "自訂您的Trident安裝" 使用中的屬性 TridentOrchestrator 規格

```
kubectl create -f deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created

kubectl describe torc trident

Name:          trident
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:   trident.netapp.io/v1
Kind:          TridentOrchestrator
...
Spec:
  Debug:      true
  Namespace:  trident
Status:
  Current Installation Params:
    IPv6:          false
    Autosupport Hostname:
    Autosupport Image:      netapp/trident-autosupport:23.01
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:          true
    Image Pull Secrets:
    Image Registry:
    k8sTimeout:      30
    Kubelet Dir:      /var/lib/kubelet
    Log Format:        text
    Silence Autosupport:  false
    Trident Image:     netapp/trident:23.01.1
  Message:          Trident installed  Namespace:
trident
  Status:          Installed
  Version:         v23.01.1
Events:
  Type Reason Age From Message ---- -
Installing 74s trident-operator.netapp.io Installing Trident Normal
Installed 67s trident-operator.netapp.io Trident installed
```

## 驗證安裝

驗證安裝的方法有多種。

### 使用 TridentOrchestrator 狀態

狀態 TridentOrchestrator 指出安裝是否成功、並顯示安裝的Trident版本。安裝期間的狀態 TridentOrchestrator 變更來源 Installing 至 Installed。如果您觀察到 Failed 狀態、而且營運者無法自行恢復、["檢查記錄"](#)。

狀態	說明
安裝	操作員正在使用此工具安裝Astra Trident TridentOrchestrator CR.
已安裝	Astra Trident已成功安裝。
正在解除安裝	因為、操作者正在解除安裝Astra Trident spec.uninstall=true。
已解除安裝	Astra Trident已解除安裝。
失敗	營運者無法安裝、修補、更新或解除安裝Astra Trident；營運者將自動嘗試從此狀態恢復。如果此狀態持續存在、您將需要疑難排解。
正在更新	營運者正在更新現有的安裝。
錯誤	◦ TridentOrchestrator 未使用。另一個已經存在。

### 使用Pod建立狀態

您可以檢閱建立的Pod狀態、確認是否已完成Astra Trident安裝：

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

NAME	READY	STATUS	RESTARTS
trident-controller-7d466bf5c7-v4cpw 1m	6/6	Running	0
trident-node-linux-mr6zc 1m	2/2	Running	0
trident-node-linux-xrp7w 1m	2/2	Running	0
trident-node-linux-zh2jt 1m	2/2	Running	0
trident-operator-766f7b8658-ldzsv 3m	1/1	Running	0

使用 `tridentctl`

您可以使用 `tridentctl` 檢查安裝的Astra Trident版本。

```
./tridentctl -n trident version
```

```
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 23.01.1        | 23.01.1        |
+-----+-----+
```

下一步

現在您可以了 "[建立後端和儲存類別、配置磁碟區、並將磁碟區掛載到Pod中](#)"。

手動部署Trident運算子（離線模式）

您可以手動部署Trident運算子來安裝Astra Trident。此程序適用於將Astra Trident所需的容器映像儲存在私有登錄中的安裝。如果您沒有私有映像登錄、請使用 "[標準部署程序](#)"。

#### Astra Trident的重要資訊23.01

您必須閱讀下列有關Astra Trident的重要資訊。

關於Astra Trid-功能 的資訊

- Kubernetes 1.26現在已在Trident中受到支援。升級Kubernetes之前先升級Trident。
- Astra Trident在SAN環境中嚴格執行多重路徑組態的使用、建議的值為 `find_multipaths: no` 在多重路徑.conf檔案中。

使用非多重路徑組態或使用 `find_multipaths: yes` 或 `find_multipaths: smart` 多重路徑.conf檔案中的值會導致掛載失敗。Trident建議使用 `find_multipaths: no` 自21.07版本以來。

手動部署Trident運算子並安裝Trident

檢閱 "[安裝總覽](#)" 為了確保您符合安裝先決條件、並為您的環境選擇正確的安裝選項。

開始之前

登入Linux主機、驗證其是否正在管理正常運作的和 "[支援的Kubernetes叢集](#)" 而且您擁有必要的權限。



使用OpenShift、使用 `oc` 而非 `kubectl` 在以下所有範例中、請先執行\*系統：admin\*登入 `oc login -u system:admin` 或 `oc login -u kube-admin`。



1. 驗證Kubernetes版本：

```
kubectl version
```

2. 驗證叢集管理員權限：

```
kubectl auth can-i '*' '*' --all-namespaces
```

3. 確認您可以啟動使用Docker Hub映像的Pod、並透過Pod網路連線至儲存系統：

```
kubectl run -i --tty ping --image=busybox --restart=Never --rm -- \
ping <management IP>
```

### 步驟1：下載Trident安裝程式套件

Astra Trident安裝程式套件包含部署Trident操作員及安裝Astra Trident所需的一切。從下載並擷取Trident安裝程式的最新版本 "[GitHub的\\_Assets區段](#)"。

```
wget https://github.com/NetApp/trident/releases/download/v23.01.1/trident-
installer-23.01.1.tar.gz
tar -xf trident-installer-23.01.1.tar.gz
cd trident-installer
```

### 步驟2：建立 TridentOrchestrator 客戶需求日

建立 TridentOrchestrator 自訂資源定義（CRD）。您將建立 TridentOrchestrator 稍後再自訂資源。請使用中適當的CRD Y反 洗錢版本 deploy/crds 以建立 TridentOrchestrator 客戶需求日：

```
kubectl create -f deploy/crds/<VERSION>.yaml
```

### 步驟3：更新操作員中的登錄位置

在中 /deploy/operator.yaml、更新 image: docker.io/netapp/trident-operator:23.01.1 以反映映像登錄的位置。您的 "[Trident和csi影像](#)" 可以位於一個登錄或不同的登錄中、但所有的SCSI映像都必須位於同一個登錄中。例如：

- image: <your-registry>/trident-operator:23.01.1 如果您的映像都位於單一登錄中。
- image: <your-registry>/netapp/trident-operator:23.01.1 如果Trident映像與您的csi映像位於不同的登錄中。

## 步驟4：部署Trident運算子

Trident安裝程式會在中部署操作員 trident 命名空間。如果是 trident 命名空間不存在、請使用 `kubectl apply -f deploy/namespace.yaml` 以建立。

可在非的命名空間中部署運算子 trident 命名空間、更新 `serviceaccount.yaml`、`clusterrolebinding.yaml` 和 `operator.yaml` 部署營運者之前。

### 1. 建立資源並部署營運者：

```
kubectl kustomize deploy/ > deploy/<BUNDLE>.yaml
```



Astra Trident安裝程式提供一個套件檔案、可用來安裝運算子及建立相關的物件。套裝組合檔案是使用預設組態部署操作員及安裝Astra Trident的簡易方法。

- 對於執行Kubernetes 1.24或更低層級的叢集、請使用 `bundle_pre_1_25.yaml`。
- 對於執行Kubernetes 1.25或更新版本的叢集、請使用 `bundle_post_1_25.yaml`。

### 2. 驗證是否已部署操作員。

```
kubectl get deployment -n <operator-namespace>
```

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
trident-operator	1/1	1	1	3m



Kubernetes叢集中只應有\*一個運算子執行個體\*。請勿建立Trident營運者的多個部署。

## 步驟5：更新中的映像登錄位置 TridentOrchestrator

您的 "[Trident和csi影像](#)" 可以位於一個登錄或不同的登錄中、但所有的SCSI映像都必須位於同一個登錄中。更新 `deploy/crds/tridentorchestrator_cr.yaml` 根據登錄組態新增額外的位置規格。

#### 一個登錄中的映像

```
imageRegistry: "<your-registry>"
autosupportImage: "<your-registry>/trident-autosupport:23.01"
tridentImage: "<your-registry>/trident:23.01.1"
```

#### 不同登錄中的映像

您必須附加 sig-storage 至 imageRegistry 使用不同的登錄位置。

```
imageRegistry: "<your-registry>/sig-storage"
autosupportImage: "<your-registry>/netapp/trident-autosupport:23.01"
tridentImage: "<your-registry>/netapp/trident:23.01.1"
```

### 步驟6：建立 TridentOrchestrator 並安裝Trident

您現在可以建立 TridentOrchestrator 並安裝Astra Trident。您也可以選擇進一步 ["自訂您的Trident安裝"](#) 使用中的屬性 TridentOrchestrator 規格下列範例顯示Trident與csi映像位於不同登錄中的安裝。

```

kubectl create -f deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created

kubectl describe torc trident

Name:          trident
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:   trident.netapp.io/v1
Kind:          TridentOrchestrator
...
Spec:
  Autosupport Image: <your-registry>/netapp/trident-autosupport:23.01
  Debug:             true
  Image Registry:    <your-registry>/sig-storage
  Namespace:         trident
  Trident Image:     <your-registry>/netapp/trident:23.01.1
Status:
  Current Installation Params:
    IPv6:             false
    Autosupport Hostname:
    Autosupport Image: <your-registry>/netapp/trident-
autosupport:23.01
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:            true
    Http Request Timeout: 90s
    Image Pull Secrets:
    Image Registry:    <your-registry>/sig-storage
    k8sTimeout:        30
    Kubelet Dir:       /var/lib/kubelet
    Log Format:        text
    Probe Port:        17546
    Silence Autosupport: false
    Trident Image:     <your-registry>/netapp/trident:23.01.1
  Message:            Trident installed
  Namespace:          trident
  Status:             Installed
  Version:            v23.01.1
Events:
  Type Reason Age From Message ----
  Installing 74s trident-operator.netapp.io Installing Trident Normal
  Installed 67s trident-operator.netapp.io Trident installed

```

## 驗證安裝

驗證安裝的方法有多種。

### 使用 TridentOrchestrator 狀態

狀態 TridentOrchestrator 指出安裝是否成功、並顯示安裝的Trident版本。安裝期間的狀態 TridentOrchestrator 變更來源 Installing 至 Installed。如果您觀察到 Failed 狀態、而且營運者無法自行恢復、["檢查記錄"](#)。

狀態	說明
安裝	操作員正在使用此工具安裝Astra Trident TridentOrchestrator CR.
已安裝	Astra Trident已成功安裝。
正在解除安裝	因為、操作者正在解除安裝Astra Trident spec.uninstall=true。
已解除安裝	Astra Trident已解除安裝。
失敗	營運者無法安裝、修補、更新或解除安裝Astra Trident；營運者將自動嘗試從此狀態恢復。如果此狀態持續存在、您將需要疑難排解。
正在更新	營運者正在更新現有的安裝。
錯誤	◦ TridentOrchestrator 未使用。另一個已經存在。

### 使用Pod建立狀態

您可以檢閱建立的Pod狀態、確認是否已完成Astra Trident安裝：

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

NAME	READY	STATUS	RESTARTS
AGE			
trident-controller-7d466bf5c7-v4cpw	6/6	Running	0
1m			
trident-node-linux-mr6zc	2/2	Running	0
1m			
trident-node-linux-xrp7w	2/2	Running	0
1m			
trident-node-linux-zh2jt	2/2	Running	0
1m			
trident-operator-766f7b8658-ldzsv	1/1	Running	0
3m			

使用 `tridentctl`

您可以使用 `tridentctl` 檢查安裝的Astra Trident版本。

```
./tridentctl -n trident version
```

```
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 23.01.1        | 23.01.1        |
+-----+-----+
```

下一步

現在您可以了 "[建立後端和儲存類別、配置磁碟區、並將磁碟區掛載到Pod中](#)"。

使用Helm部署Trident運算子（標準模式）

您可以部署Trident運算子、並使用Helm安裝Astra Trident。此程序適用於未將Astra Trident所需的容器映像儲存在私有登錄中的安裝。如果您有私有映像登錄、請使用 "[離線部署程序](#)"。

#### Astra Trident的重要資訊23.01

您必須閱讀下列有關Astra Trident的重要資訊。

關於Astra Trid-功能 的資訊

- Kubernetes 1.26現在已在Trident中受到支援。升級Kubernetes之前先升級Trident。
- Astra Trident在SAN環境中嚴格執行多重路徑組態的使用、建議的值為 `find_multipaths: no` 在多重路徑.conf檔案中。

使用非多重路徑組態或使用 `find_multipaths: yes` 或 `find_multipaths: smart` 多重路徑.conf檔案中的值會導致掛載失敗。Trident建議使用 `find_multipaths: no` 自21.07版本以來。

部署Trident操作員、並使用Helm安裝Astra Trident

使用Trident "[掌舵表](#)" 您可以部署Trident運算子、並在單一步驟中安裝Trident。

檢閱 "[安裝總覽](#)" 為了確保您符合安裝先決條件、並為您的環境選擇正確的安裝選項。

開始之前

此外 "[部署先決條件](#)" 您的需求 "[Helm版本3](#)"。

步驟

1. 新增Astra Trident Helm儲存庫：

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. 使用 `helm install` 並指定部署名稱、如下例所示 23.01.1 是您要安裝的Astra Trident版本。

```
helm install <name> netapp-trident/trident-operator --version 23.01.1  
--create-namespace --namespace <trident-namespace>
```



如果您已經為Trident建立命名空間 `--create-namespace` 參數不會建立額外的命名空間。

您可以使用 `helm list` 若要檢閱安裝詳細資料、例如名稱、命名空間、圖表、狀態、應用程式版本、和修訂編號。

在安裝期間傳遞組態資料

安裝期間有兩種傳遞組態資料的方法：

選項	說明
<code>--values</code> (或 <code>-f</code> )	指定具有覆寫的Yaml檔案。這可以多次指定、最右邊的檔案會優先。
<code>--set</code>	在命令列上指定置換。

例如、變更的預設值 `debug`、請執行下列步驟 `--set` 命令位置 23.01.1 您要安裝的Astra Trident版本：

```
helm install <name> netapp-trident/trident-operator --version 23.01.1  
--create-namespace --namespace --set tridentDebug=true
```

組態選項

此表格和 `values.yaml` 檔案是 Helm 圖表的一部分、提供按鍵清單及其預設值。

選項	說明	預設
<code>nodeSelector</code>	Pod 指派的節點標籤	
<code>podAnnotations</code>	Pod 註釋	
<code>deploymentAnnotations</code>	部署註釋	
<code>tolerations</code>	Pod 指派的容錯功能	
<code>affinity</code>	Pod 指派的關聯性	
<code>tridentControllerPluginNodeSelector</code>	用於 Pod 的其他節點選取器。請參閱 <a href="#">瞭解控制器 Pod 和節點 Pod</a> 以取得詳細資料。	

選項	說明	預設
tridentControllerPluginTolerations	覆寫 Pod 的 Kubernetes 公差。請參閱 <a href="#">瞭解控制器 Pod 和節點 Pod</a> 以取得詳細資料。	
tridentNodePluginNodeSelector	用於 Pod 的其他節點選取器。請參閱 <a href="#">瞭解控制器 Pod 和節點 Pod</a> 以取得詳細資料。	
tridentNodePluginTolerations	覆寫 Pod 的 Kubernetes 公差。請參閱 <a href="#">瞭解控制器 Pod 和節點 Pod</a> 以取得詳細資料。	
imageRegistry	識別的登錄 trident-operator、`trident` 和其他影像。保留空白以接受預設值。	"
imagePullPolicy	設定的映像拉出原則 trident-operator。	IfNotPresent
imagePullSecrets	設定的影像拉出秘密 trident-operator、`trident` 和其他影像。	
kubeletDir	允許覆寫 kubelet 內部狀態的主機位置。	'/var/lib/kubelet'
operatorLogLevel	允許 Trident 運算子的記錄層級設定為：trace、debug、info、warn、error 或 fatal。	"info"
operatorDebug	允許將 Trident 運算子的記錄層級設為偵錯。	true
operatorImage	允許完全置換的映像 trident-operator。	"
operatorImageTag	允許覆寫的標記 trident-operator 映像。	"
tridentIPv6	允許 Astra Trident 在 IPv6 叢集中運作。	false
tridentK8sTimeout	覆寫大部分 Kubernetes API 作業的預設 30 秒逾時（如果非零、則以秒為單位）。	0
tridentHttpRequestTimeout	以取代 HTTP 要求的預設 90 秒逾時 0s 是超時的無限持續時間。不允許使用負值。	"90s"
tridentSilenceAutosupport	可停用 Astra Trident 定期 AutoSupport 報告。	false
tridentAutosupportImageTag	可覆寫 Astra Trident AutoSupport 容器的映像標記。	<version>
tridentAutosupportProxy	允許 Astra Trident AutoSupport 容器透過 HTTP Proxy 撥打電話回家。	"



選項	說明	預設
tridentLogFormat	設定 Astra Trident 記錄格式 (text 或 json) 。	"text"
tridentDisableAuditLog	停用 Astra Trident 稽核記錄程式。	true
tridentLogLevel	允許將 Astra Trident 的記錄層級設定為：trace、debug、info、warn、error、或 fatal。	"info"
tridentDebug	允許將 Astra Trident 的記錄層級設定為 debug。	false
tridentLogWorkflows	允許啟用特定的 Astra Trident 工作流程、以進行追蹤記錄或記錄抑制。	"
tridentLogLayers	允許啟用特定的 Astra Trident 圖層、以進行追蹤記錄或記錄抑制。	"
tridentImage	允許完整置換 Astra Trident 的影像。	"
tridentImageTag	可覆寫 Astra Trident 的影像標記。	"
tridentProbePort	允許覆寫 Kubernetes 活性 / 整備性探查所使用的預設連接埠。	"
windows	允許在 Windows 工作節點上安裝 Astra Trident 。	false
enableForceDetach	允許啟用強制分離功能。	false
excludePodSecurityPolicy	不建立營運商 Pod 安全性原則。	false

## 瞭解控制器 Pod 和節點 Pod

Astra Trident 會以單一控制器 Pod 的形式執行、並在叢集中的每個工作節點上提供節點 Pod。節點 Pod 必須在任何想要裝載 Astra Trident Volume 的主機上執行。

Kubernetes ["節點選取器"](#) 和 ["容忍和污染"](#) 用於限制 Pod 在特定或偏好的節點上執行。使用「ControllerPlugin」和 NodePlugin，您可以指定限制和置換。

- 控制器外掛程式可處理磁碟區資源配置與管理、例如快照和調整大小。
- 節點外掛程式會處理將儲存設備附加至節點的問題。

下一步

現在您可以了 ["建立後端和儲存類別、配置磁碟區、並將磁碟區掛載到Pod中"](#)。

## 使用Helm部署Trident運算子（離線模式）

您可以部署Trident運算子、並使用Helm安裝Astra Trident。此程序適用於將Astra Trident所需的容器映像儲存在私有登錄中的安裝。如果您沒有私有映像登錄、請使用 ["標準部署程序"](#)。

## Astra Trident的重要資訊23.01

您必須閱讀下列有關**Astra Trident**的重要資訊。

關於**Astra Trident**功能的資訊

- Kubernetes 1.26現在已在Trident中受到支援。升級Kubernetes之前先升級Trident。
- Astra Trident在SAN環境中嚴格執行多重路徑組態的使用、建議的值為 `find_multipaths: no` 在多重路徑.conf檔案中。

使用非多重路徑組態或使用 `find_multipaths: yes` 或 `find_multipaths: smart` 多重路徑.conf檔案中的值會導致掛載失敗。Trident建議使用 `find_multipaths: no` 自21.07版本以來。

部署Trident操作員、並使用Helm安裝Astra Trident

使用Trident ["掌舵表"](#) 您可以部署Trident運算子、並在單一步驟中安裝Trident。

檢閱 ["安裝總覽"](#) 為了確保您符合安裝先決條件、並為您的環境選擇正確的安裝選項。

開始之前

此外 ["部署先決條件"](#) 您的需求 ["Helm版本3"](#)。

步驟

1. 新增Astra Trident Helm儲存庫：

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. 使用 `helm install` 並指定部署和映像登錄位置的名稱。您的 ["Trident和csi影像"](#) 可以位於一個登錄或不同的登錄中、但所有的SCSI映像都必須位於同一個登錄中。在範例中、23.01.1 是您要安裝的Astra Trident版本。

### 一個登錄中的映像

```
helm install <name> netapp-trident/trident-operator --version
23.01.1 --set imageRegistry=<your-registry> --create-namespace
--namespace <trident-namespace>
```

### 不同登錄中的映像

您必須附加 sig-storage 至 imageRegistry 使用不同的登錄位置。

```
helm install <name> netapp-trident/trident-operator --version
23.01.1 --set imageRegistry=<your-registry>/sig-storage --set
operatorImage=<your-registry>/netapp/trident-operator:23.01.1 --set
tridentAutosupportImage=<your-registry>/netapp/trident-
autosupport:23.01 --set tridentImage=<your-
registry>/netapp/trident:23.01.1 --create-namespace --namespace
<trident-namespace>
```



如果您已經為Trident建立命名空間 --create-namespace 參數不會建立額外的命名空間。

您可以使用 `helm list` 若要檢閱安裝詳細資料、例如名稱、命名空間、圖表、狀態、應用程式版本、和修訂編號。

### 在安裝期間傳遞組態資料

安裝期間有兩種傳遞組態資料的方法：

選項	說明
--values (或 -f)	指定具有覆寫的Yaml檔案。這可以多次指定、最右邊的檔案會優先。
--set	在命令列上指定置換。

例如、變更的預設值 debug，請執行下列步驟 --set 命令位置 23.01.1 您要安裝的Astra Trident版本：

```
helm install <name> netapp-trident/trident-operator --version 23.01.1
--create-namespace --namespace --set tridentDebug=true
```

### 組態選項

此表格和 values.yaml 檔案是 Helm 圖表的一部分、提供按鍵清單及其預設值。

選項	說明	預設
nodeSelector	Pod 指派的節點標籤	
podAnnotations	Pod 註釋	
deploymentAnnotations	部署註釋	
tolerations	Pod 指派的容錯功能	
affinity	Pod 指派的關聯性	
tridentControllerPluginNodeSelector	用於 Pod 的其他節點選取器。請參閱 <a href="#">瞭解控制器 Pod 和節點 Pod</a> 以取得詳細資料。	
tridentControllerPluginTolerations	覆寫 Pod 的 Kubernetes 公差。請參閱 <a href="#">瞭解控制器 Pod 和節點 Pod</a> 以取得詳細資料。	
tridentNodePluginNodeSelector	用於 Pod 的其他節點選取器。請參閱 <a href="#">瞭解控制器 Pod 和節點 Pod</a> 以取得詳細資料。	
tridentNodePluginTolerations	覆寫 Pod 的 Kubernetes 公差。請參閱 <a href="#">瞭解控制器 Pod 和節點 Pod</a> 以取得詳細資料。	
imageRegistry	識別的登錄 trident-operator、`trident` 和其他影像。保留空白以接受預設值。	"
imagePullPolicy	設定的映像拉出原則 trident-operator。	IfNotPresent
imagePullSecrets	設定的影像拉出秘密 trident-operator、`trident` 和其他影像。	
kubeletDir	允許覆寫 kubelet 內部狀態的主機位置。	'/var/lib/kubelet'
operatorLogLevel	允許 Trident 運算子的記錄層級設定為：trace、debug、info、warn、error 或 fatal。	"info"
operatorDebug	允許將 Trident 運算子的記錄層級設為偵錯。	true
operatorImage	允許完全置換的映像 trident-operator。	"
operatorImageTag	允許覆寫的標記 trident-operator 映像。	"
tridentIPv6	允許 Astra Trident 在 IPv6 叢集中運作。	false
tridentK8sTimeout	覆寫大部分 Kubernetes API 作業的預設 30 秒逾時（如果非零、則以秒為單位）。	0

選項	說明	預設
tridentHttpRequestTimeout	以取代 HTTP 要求的預設 90 秒逾時 0s 是超時的無限持續時間。不允許使用負值。	"90s"
tridentSilenceAutosupport	可停用 Astra Trident 定期 AutoSupport 報告。	false
tridentAutosupportImageTag	可覆寫 Astra Trident AutoSupport 容器的映像標記。	<version>
tridentAutosupportProxy	允許 Astra Trident AutoSupport 容器透過 HTTP Proxy 撥打電話回家。	"
tridentLogFormat	設定 Astra Trident 記錄格式 (text 或 json)。	"text"
tridentDisableAuditLog	停用 Astra Trident 稽核記錄程式。	true
tridentLogLevel	允許將 Astra Trident 的記錄層級設定為：trace、debug、info、warn、error 或 fatal。	"info"
tridentDebug	允許將 Astra Trident 的記錄層級設定為 debug。	false
tridentLogWorkflows	允許啟用特定的 Astra Trident 工作流程、以進行追蹤記錄或記錄抑制。	"
tridentLogLayers	允許啟用特定的 Astra Trident 圖層、以進行追蹤記錄或記錄抑制。	"
tridentImage	允許完整置換 Astra Trident 的影像。	"
tridentImageTag	可覆寫 Astra Trident 的影像標記。	"
tridentProbePort	允許覆寫 Kubernetes 活性 / 整備性探查所使用的預設連接埠。	"
windows	允許在 Windows 工作節點上安裝 Astra Trident。	false
enableForceDetach	允許啟用強制分離功能。	false
excludePodSecurityPolicy	不建立營運商 Pod 安全性原則。	false

## 瞭解控制器 Pod 和節點 Pod

Astra Trident 會以單一控制器 Pod 的形式執行、並在叢集中的每個工作節點上提供節點 Pod。節點 Pod 必須在任何想要裝載 Astra Trident Volume 的主機上執行。

Kubernetes ["節點選取器"](#) 和 ["容忍和污染"](#) 用於限制 Pod 在特定或偏好的節點上執行。使用「ControllerPlugin」和 NodePlugin，您可以指定限制和置換。

- 控制器外掛程式可處理磁碟區資源配置與管理、例如快照和調整大小。

- 節點外掛程式會處理將儲存設備附加至節點的問題。

下一步

現在您可以了 ["建立後端和儲存類別、配置磁碟區、並將磁碟區掛載到Pod中"](#)。

## 自訂Trident操作員安裝

Trident運算子可讓您使用中的屬性來自訂Astra Trident安裝 `TridentOrchestrator` 規格如果您想要自訂安裝內容以外的內容 `TridentOrchestrator` 引數允許、請考慮使用 `tridentctl` 產生自訂的 YAML 資訊清單、以視需要進行修改。

## 瞭解控制器 Pod 和節點 Pod

Astra Trident 會以單一控制器 Pod 的形式執行、並在叢集中的每個工作節點上提供節點 Pod。節點 Pod 必須在任何想要裝載 Astra Trident Volume 的主機上執行。

Kubernetes ["節點選取器"](#) 和 ["容忍和污染"](#) 用於限制 Pod 在特定或偏好的節點上執行。使用「ControllerPlugin」和 NodePlugin，您可以指定限制和置換。

- 控制器外掛程式可處理磁碟區資源配置與管理、例如快照和調整大小。
- 節點外掛程式會處理將儲存設備附加至節點的問題。

## 組態選項



`spec.namespace` 在中指定 `TridentOrchestrator` 表示 Astra Trident 安裝的命名空間。此參數\*無法在安裝Astra Trident之後更新\*。嘗試這麼做會導致 `TridentOrchestrator` 要變更為的狀態 `Failed`。Astra Trident不打算跨命名空間移轉。

本表詳細說明 `TridentOrchestrator` 屬性。

參數	說明	預設
<code>namespace</code>	用於安裝Astra Trident的命名空間	"預設"
<code>debug</code>	啟用Astra Trident的偵錯功能	錯
<code>windows</code>	設定為 <code>true</code> 可在Windows工作節點上安裝。	錯
<code>IPv6</code>	透過IPv6安裝Astra Trident	錯
<code>k8sTimeout</code>	Kubernetes作業逾時	30秒
<code>silenceAutosupport</code>	請勿AutoSupport 自動將此套裝組合傳送至NetApp	錯
<code>enableNodePrep</code>	自動管理工作節點相依性 (* BETA *)	錯
<code>autosupportImage</code>	遙測的容器影像AutoSupport	「NetApp/Trident自動支援：23.01」

參數	說明	預設
autosupportProxy	代理伺服器的位址/連接埠、用於傳送AutoSupport「遙測」功能	"<a href="http://proxy.example.com:8888" class="bare">http://proxy.example.com:8888"</a>
uninstall	用來解除安裝Astra Trident的旗標	錯
logFormat	要使用的Astra Trident記錄格式 [text、json]	"文字"
tridentImage	要安裝的Astra Trident映像	「NetApp/Trident：21.04」
imageRegistry	內部登錄的路徑、格式 <registry FQDN>[:port] [/subpath]	"k8s.gcr.io/sig-storage (k8s 1.19+) 或kay.io/k8scsi"
kubeletDir	主機上的kubelet目錄路徑	"/var/lib/kubelet"
wipeout	要刪除以執行完整移除Astra Trident的資源清單	
imagePullSecrets	從內部登錄擷取映像的機密	
imagePullPolicy	設定Trident運算子的影像提取原則。有效值包括： Always 永遠拉出映像。 IfNotPresent 僅當節點上尚未存在映像時才提取映像。 Never 永遠不要拉動映像。	IfNotPresent
controllerPluginNodeSelector	用於 Pod 的其他節點選取器。格式與pod.spec.nodeSelector相同。	無預設值；選用
controllerPluginTolerations	覆寫 Pod 的 Kubernetes 公差。格式與po.spec.TBolerations相同。	無預設值；選用
nodePluginNodeSelector	用於 Pod 的其他節點選取器。格式與pod.spec.nodeSelector相同。	無預設值；選用
nodePluginTolerations	覆寫 Pod 的 Kubernetes 公差。格式與po.spec.TBolerations相同。	無預設值；選用



如需格式化Pod參數的詳細資訊、請參閱 ["將Pod指派給節點"](#)。

#### 組態範例

您可以在定義時使用上述屬性 TridentOrchestrator 以自訂安裝。

### 範例1：基本自訂組態

這是基本自訂組態的範例。

```
cat deploy/crds/tridentorchestrator_cr_imagepullsecrets.yaml
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullSecrets:
    - thisisasecret
```

### 範例2：使用節點選取器進行部署

此範例說明如何使用節點選取器來部署Trident：

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  controllerPluginNodeSelector:
    nodetype: master
  nodePluginNodeSelector:
    storage: netapp
```



### 範例3：部署在Windows工作節點上

此範例說明如何在Windows工作節點上進行部署。

```
cat deploy/crds/tridentorchestrator_cr.yaml
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  windows: true
```

## 使用tridentctl安裝

### 使用tridentctl安裝

您可以使用安裝Astra Trident `tridentctl`。此程序適用於將Astra Trident所需的容器映像儲存在私有登錄中或不儲存在私有登錄中的安裝。以自訂您的 `tridentctl` 部署、請參閱["自訂試用部署"](#)。

### Astra Trident的重要資訊23.01

您必須閱讀下列有關Astra Trident的重要資訊。

關於Astra Trident-功能 的資訊

- Kubernetes 1.26現在已在Trident中受到支援。升級Kubernetes之前先升級Trident。
- Astra Trident在SAN環境中嚴格執行多重路徑組態的使用、建議的值為 `find_multipaths: no` 在多重路徑.conf檔案中。

使用非多重路徑組態或使用 `find_multipaths: yes` 或 `find_multipaths: smart` 多重路徑.conf檔案中的值會導致掛載失敗。Trident建議使用 `find_multipaths: no` 自21.07版本以來。

使用安裝Astra Trident `tridentctl`

檢閱 ["安裝總覽"](#) 為了確保您符合安裝先決條件、並為您的環境選擇正確的安裝選項。

### 開始之前

在開始安裝之前、請先登入Linux主機、然後確認它正在管理正常運作的 ["支援的Kubernetes叢集"](#) 而且您擁有必要的權限。



使用OpenShift、使用 `oc` 而非 `kubectl` 在以下所有範例中、請先執行\*系統：`admin`\*登入 `oc login -u system:admin` 或 `oc login -u kube-admin`。

1. 驗證Kubernetes版本：

```
kubectl version
```

2. 驗證叢集管理員權限：

```
kubectl auth can-i '*' '*' --all-namespaces
```

3. 確認您可以啟動使用Docker Hub映像的Pod、並透過Pod網路連線至儲存系統：

```
kubectl run -i --tty ping --image=busybox --restart=Never --rm -- \
ping <management IP>
```

步驟1：下載Trident安裝程式套件

Astra Trident安裝程式套件會建立Trident pod、設定用來維持其狀態的CRD物件、並初始化csi sidecar以執行資源配置和將磁碟區附加至叢集主機等動作。從下載並擷取Trident安裝程式的最新版本 "[GitHub的\\_Assets區段](#)"。請使用<trident-installer-XX.XX.X.tar.gz> 您所選的Astra Trident版本來更新範例中的\_SUR\_\_。

```
wget https://github.com/NetApp/trident/releases/download/v23.01.1/trident-
installer-23.01.1.tar.gz
tar -xf trident-installer-23.01.1.tar.gz
cd trident-installer
```

步驟2：安裝Astra Trident

執行、在所需的命名空間中安裝Astra Trident `tridentctl install` 命令。您可以新增其他引數來指定映像登錄位置。



若要在Windows節點上執行Astra Trident、請新增 `--windows` 安裝命令的旗標：`$ ./tridentctl install --windows -n trident`。

## 標準模式

```
./tridentctl install -n trident
```

## 一個登錄中的映像

```
./tridentctl install -n trident --image-registry <your-registry>  
--autosupport-image <your-registry>/trident-autosupport:23.01 --trident  
-image <your-registry>/trident:23.01.1
```

## 不同登錄中的映像

您必須附加 sig-storage 至 imageRegistry 使用不同的登錄位置。

```
./tridentctl install -n trident --image-registry <your-registry>/sig-  
storage --autosupport-image <your-registry>/netapp/trident-  
autosupport:23.01 --trident-image <your-  
registry>/netapp/trident:23.01.1
```

您的安裝狀態應該類似這樣。

```
....  
INFO Starting Trident installation.                namespace=trident  
INFO Created service account.  
INFO Created cluster role.  
INFO Created cluster role binding.  
INFO Added finalizers to custom resource definitions.  
INFO Created Trident service.  
INFO Created Trident secret.  
INFO Created Trident deployment.  
INFO Created Trident daemonset.  
INFO Waiting for Trident pod to start.  
INFO Trident pod started.                          namespace=trident  
pod=trident-controller-679648bd45-cv2mx  
INFO Waiting for Trident REST interface.  
INFO Trident REST interface is up.                 version=23.01.1  
INFO Trident installation succeeded.  
....
```

## 驗證安裝

您可以使用Pod建立狀態或來驗證安裝 tridentctl。

## 使用Pod建立狀態

您可以檢閱建立的Pod狀態、確認是否已完成Astra Trident安裝：

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

NAME	READY	STATUS	RESTARTS	AGE
trident-controller-679648bd45-cv2mx	6/6	Running	0	5m29s
trident-node-linux-vgc8n	2/2	Running	0	5m29s



如果安裝程式未成功完成或 trident-controller-<generated id> (trident-csi-<generated id> 在23.01之前的版本中) 沒有\*執行中\*的狀態、表示平台尚未安裝。使用 -d 至 ["開啟偵錯模式"](#) 並疑難排解問題。

## 使用 tridentctl

您可以使用 tridentctl 檢查安裝的Astra Trident版本。

```
./tridentctl -n trident version
```

```
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 23.01.1       | 23.01.1       |
+-----+-----+
```

## 下一步

現在您可以了 ["建立後端和儲存類別、配置磁碟區、並將磁碟區掛載到Pod中"](#)。

## 自訂tridentctl安裝

您可以使用Astra Trident安裝程式來自訂安裝。

### 深入瞭解安裝程式

Astra Trident安裝程式可讓您自訂屬性。例如、如果您已將Trident映像複製到私有儲存庫、則可以使用來指定映像名稱 --trident-image。如果您已將Trident映像及所需的csi sidecar映像複製到私有儲存庫、最好使用指定該儲存庫的位置 --image-registry 交換器、採用格式 <registry FQDN>[:port]。

如果您使用Kubernetes的發佈版本、其中 kubelet 將資料保留在一般路徑以外的路徑上 /var/lib/kubelet、您可以使用來指定替代路徑 --kubelet-dir。

如果您需要自訂安裝、而不需要安裝程式的引數允許、也可以自訂部署檔案。使用 --generate-custom-yaml 參數會在安裝程式中建立下列Yaml檔案 setup 目錄：

- trident-clusterrolebinding.yaml
- trident-deployment.yaml
- trident-crds.yaml
- trident-clusterrole.yaml
- trident-daemonset.yaml
- trident-service.yaml
- trident-namespace.yaml
- trident-serviceaccount.yaml
- trident-resourcequota.yaml

產生這些檔案之後、您可以根據自己的需求加以修改、然後使用 `--use-custom-yaml` 以安裝自訂部署。

```
./tridentctl install -n trident --use-custom-yaml
```

## 接下來呢？

安裝Astra Trident之後、您可以繼續建立後端、建立儲存類別、配置磁碟區、以及將磁碟區掛載至Pod。

### 步驟1：建立後端

您現在可以繼續建立後端、由Astra Trident用來配置磁碟區。若要這麼做、請建立 `backend.json` 包含必要參數的檔案。不同後端類型的組態檔範例可在中找到 `sample-input` 目錄。

請參閱 ["請按這裡"](#) 如需如何為後端類型設定檔案的詳細資訊、請參閱。

```
cp sample-input/<backend template>.json backend.json  
vi backend.json
```

```
./tridentctl -n trident create backend -f backend.json
```

NAME	STORAGE DRIVER	UUID
nas-backend	ontap-nas	98e19b74-aec7-4a3d-8dcf-128e5033b214

如果建立失敗、表示後端組態有問題。您可以執行下列命令來檢視記錄、以判斷原因：

```
./tridentctl -n trident logs
```

解決問題之後、只要返回此步驟的開頭、然後再試一次即可。如需更多疑難排解秘訣、請參閱 ["疑難排解"](#) 區段。

## 步驟2：建立儲存類別

Kubernetes使用者使用指定的持續磁碟區宣告（PVCS）來配置磁碟區 ["儲存類別"](#) 依名稱。使用者會隱藏詳細資料、但儲存類別會識別該類別所使用的資源配置程式（本例中為Trident）、以及該類別對資源配置程式的意義。

建立儲存類別Kubernetes使用者要指定何時需要磁碟區。類別的組態需要建構您在上一個步驟中建立的後端、以便Astra Trident使用它來配置新的磁碟區。

最簡單的儲存類別是以為基礎的 `sample-input/storage-class-csi.yaml.template` 安裝程式隨附的檔案、取代 `BACKEND_TYPE` 儲存驅動程式名稱。

```

./tridentctl -n trident get backend
+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |          UUID          |
STATE | VOLUMES |
+-----+-----+-----+
+-----+-----+
| nas-backend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |         0 |
+-----+-----+-----+
+-----+-----+

cp sample-input/storage-class-csi.yaml.templ sample-input/storage-class-
basic-csi.yaml

# Modify __BACKEND_TYPE__ with the storage driver field above (e.g.,
ontap-nas)
vi sample-input/storage-class-basic-csi.yaml

```

這是Kubernetes物件、所以您可以使用 `kubectl` 在Kubernetes中建立。

```
kubectl create -f sample-input/storage-class-basic-csi.yaml
```

現在您應該會看到Kubernetes和Astra Trident中的\* basic、csi \*儲存類別、而Astra Trident應該已經在後端探索集區。

```
kubectl get sc basic-csi
NAME          PROVISIONER          AGE
basic-csi     csi.trident.netapp.io 15h

./tridentctl -n trident get storageclass basic-csi -o json
{
  "items": [
    {
      "Config": {
        "version": "1",
        "name": "basic-csi",
        "attributes": {
          "backendType": "ontap-nas"
        },
        "storagePools": null,
        "additionalStoragePools": null
      },
      "storage": {
        "ontapnas_10.0.0.1": [
          "aggr1",
          "aggr2",
          "aggr3",
          "aggr4"
        ]
      }
    }
  ]
}
```

### 步驟3：配置第一個Volume

現在您可以動態配置第一個Volume了。這是透過建立Kubernetes來完成 ["持續磁碟區宣告"](#)（PVC）物件。

為使用您剛建立之儲存類別的磁碟區建立一個永久虛擬磁碟。

請參閱 `sample-input/pvc-basic-csi.yaml` 例如：請確定儲存類別名稱符合您所建立的名稱。



```
kubectl create -f sample-input/pvc-basic-csi.yaml
```

```
kubectl get pvc --watch
```

NAME	STATUS	VOLUME	CAPACITY
ACCESS MODES	STORAGECLASS	AGE	
basic	Pending		
basic	1s		
basic	Pending	pvc-3acb0d1c-b1ae-11e9-8d9f-5254004dfdb7	0
basic	5s		
basic	Bound	pvc-3acb0d1c-b1ae-11e9-8d9f-5254004dfdb7	1Gi
RWO	basic	7s	

## 步驟4：在Pod中掛載磁碟區

現在讓我們掛載磁碟區。我們將推出可安裝PV的Ngin像Pod /usr/share/nginx/html。

```
cat << EOF > task-pv-pod.yaml
kind: Pod
apiVersion: v1
metadata:
  name: task-pv-pod
spec:
  volumes:
    - name: task-pv-storage
      persistentVolumeClaim:
        claimName: basic
  containers:
    - name: task-pv-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/usr/share/nginx/html"
          name: task-pv-storage
EOF
kubectl create -f task-pv-pod.yaml
```

```
# Wait for the pod to start
kubectl get pod --watch

# Verify that the volume is mounted on /usr/share/nginx/html
kubectl exec -it task-pv-pod -- df -h /usr/share/nginx/html

# Delete the pod
kubectl delete pod task-pv-pod
```

此時、Pod（應用程式）不再存在、但磁碟區仍然存在。如果需要、您可以從其他Pod使用。

若要刪除磁碟區、請刪除請款：

```
kubectl delete pvc basic
```

您現在可以執行其他工作、例如：

- ["設定其他後端。"](#)
- ["建立其他儲存類別。"](#)

# 管理Astra Trident

## 升級Astra Trident

### 升級Astra Trident

Astra Trident依照每季發行時段進行、每一日曆年發行四個主要版本。每個新版本均以舊版為基礎、提供新功能與效能增強功能、以及錯誤修正與改善功能。我們鼓勵您每年至少升級一次、以善用Astra Trident的新功能。

#### 選取版本

Astra Trident版本遵循日期型 YY.MM 命名慣例、其中「是」是一年的最後兩位數、「公釐」是月份。DOT版本遵循A YY.MM.X 慣例、其中「X」是修補程式層級。您將根據要升級的版本、選擇要升級的版本。

- 您可以直接升級至安裝版本的四個版本範圍內的任何目標版本。例如、您可以直接從22.01升級至23.01（包括任何點版本、例如22.01.1）。
- 如果您有較早的版本、則應使用個別版本的文件來執行多步驟升級、以取得特定指示。這需要您先升級至最新版本、以符合您的四個版本。例如、如果您執行的是18.07、想要升級至20.07版本、請依照下列多步驟升級程序進行：
  - a. 第一次從18.07升級至19.07。
  - b. 然後從19.07升級至20.07。



- 19.04版及更早版本的所有升級都需要從本身移轉Astra Trident中繼資料 etcd 至CRD物件。請務必查看版本文件、瞭解升級的運作方式。
- 升級時、請務必提供 `parameter.fsType` 在中 `StorageClasses` 由Astra Trident使用。您可以刪除並重新建立 `StorageClasses` 無需中斷既有的磁碟區。這是對 SAN 磁碟區強制執行 `security` 內容範圍 ^ 的需求。 <https://github.com/NetApp/trident/tree/master/trident-installer/sample-input> 目錄包含例如 <https://github.com/NetApp/trident/blob/master/trident-installer/sample-input/storage-class-samples/storage-class-basic.yaml.template> 等範例[`storage-class-basic.yaml.template`] 和連結：`storage-class-bronze-default.yaml`。如需詳細資訊、請參閱 "已知問題"。

#### 選取升級選項

有兩種方法可以升級Astra Trident。一般而言、您可以使用與初始安裝相同的選項 "在安裝方法之間移動"。

- "使用Trident營運者進行升級"

\*



現在、自Kubernetes 1.20開始、「csi Volume Snapshot」就是GA的一項功能。升級Astra Trident時、必須先移除所有先前的Alpha Snapshot CRS和CRD（Volume Snapshot類別、Volume Snapshot和Volume Snapshot內容）、才能執行升級。請參閱 "這篇部落格" 瞭解將Alpha快照移轉至測試版/GA規格所需的步驟。

## 操作員變更

Astra Trident的21.01版為營運者帶來了一些重要的架構變更、如下所示：

- 運算子現在\*叢集範圍\*。Trident運算子先前的執行個體（20.04到20.10版）為\*命名空間範圍\*。叢集範圍內的運算子具有下列優點：
  - 資源責任：營運者現在可在叢集層級管理與Astra Trident安裝相關的資源。在安裝Astra Trident的過程中、營運者會使用來建立及維護多項資源 `ownerReferences`。維護 `ownerReferences` 在叢集範圍內的資源上、某些Kubernetes經銷商（例如OpenShift）可能會發生錯誤。叢集範圍的運算子可減輕此問題。對於自動修復和修補Trident資源、這是必要的需求。
  - 卸載期間清理：完整移除Astra Trident將需要刪除所有相關資源。命名空間範圍的運算子可能會在移除叢集範圍的資源（例如叢集角色、叢集角色繫結和Podcast安全性原則）時遇到問題、並導致不完整的清理。叢集範圍的運算子可消除此問題。使用者可以完全解除安裝Astra Trident、並視需要重新安裝。
- `TridentProvisioner` 現已取代為 `TridentOrchestrator` 作為用於安裝及管理Astra Trident的自訂資源。此外、也會在中引進新的欄位 `TridentOrchestrator` 規格使用者可以指定命名空間Trident必須使用安裝/升級 `spec.namespace` 欄位。您可以參考範例 ["請按這裡"](#)。

## 與營運者一起升級

您可以使用業者輕鬆升級現有的Astra Trident安裝。

### 開始之前

若要使用營運者進行升級、應符合下列條件：

- 您必須安裝以SCSI為基礎的Astra Trident。從19.07版開始的所有版本均採用基於SCSI的。您可以檢查Trident命名空間中的Pod以進行驗證。
  - 23.01之前版本中的Pod命名如下 `trident-csi-*` 慣例。
  - 23.01及更新版本中的Pod命名使用：`trident-controller-<generated id>`（用於控制器pod）；`trident-node-<operating system>-<generated id>`（用於節點Pod）；`trident-operator-<generated id>` 適用於營運者Pod。
- 如果您已解除安裝了「csi Trident」、而且安裝中的中繼資料持續存在、您可以使用操作者進行升級。
- 在特定Kubernetes叢集中的所有命名空間中、只應有一個Astra Trident安裝。
- 您應該使用執行的Kubernetes叢集 ["支援的Kubernetes版本"](#)。
- 如果存在Alpha Snapshot客戶需求日、您應該使用移除 `tridentctl obliviate alpha-snapshot-crd`。這會刪除Alpha Snapshot規格的客戶需求日。如需應刪除/移轉的現有快照、請參閱 ["這篇部落格"](#)。
  - 使用OpenShift Container Platform上的運算子來升級Trident時、您應該升級至Trident 21.01.1或更新版本。隨21.01.0一起發行的Trident運算子包含已在21.01.1中修正的已知問題。如需詳細資訊、請參閱 ["GitHub問題詳細資料"](#)。
  - 如果您使用的是、請勿使用運算子來升級Trident `etcd` Trident版本（19.04或更早版本）。



### 升級叢集範圍的Trident操作員安裝

請依照下列步驟升級叢集範圍的Trident操作員安裝。所有Astra Trident版本21.01及更新版本均使用叢集範圍的運算子。

## 步驟

### 1. 驗證 Astra Trident 版本：

```
./tridentctl -n trident version
```

### 2. 刪除用來安裝目前Astra Trident執行個體的Trident運算子。例如、如果您要從22.01升級、請執行下列命令：

```
kubectl delete -f 22.01/trident-installer/deploy/bundle.yaml -n trident
```

### 3. 如果您使用自訂初始安裝 TridentOrchestrator 屬性、您可以編輯 TridentOrchestrator 物件以修改安裝參數。這可能包括針對離線模式指定鏡射Trident和csi映像登錄、啟用偵錯記錄或指定映像提取機密所做的變更。

### 4. 使用適用於您環境的正確套裝組合Yaml檔案和Astra Trident版本來安裝Astra Trident。例如、如果您要為Kubernetes 1.26安裝Astra Trident 23.01、請執行下列命令：

```
kubectl create -f 23.01.1/trident-installer/deploy/bundle_post_1_25.yaml  
-n trident
```



Trident提供一個套裝組合檔案、可用來安裝運算子、並為Kubernetes版本建立相關的物件。

- 對於執行Kubernetes 1.24或更低層級的叢集、請使用 "[bunder\\_pre\\_1\\_25.yaml](#)"。
- 對於執行Kubernetes 1.25或更新版本的叢集、請使用 "[bunder\\_POST\\_1\\_25.yaml](#)"。

## 結果

Trident營運者將識別現有的Astra Trident安裝、並將其升級至與營運者相同的版本。

## 升級命名空間範圍內的操作員安裝

請依照下列步驟、從使用命名空間範圍運算子（20.07至20.10版）安裝的Astra Trident執行個體進行升級。

## 步驟

### 1. 確認現有Trident安裝的狀態。若要執行此動作、請查看的\*狀態\* TridentProvisioner。狀態應為 Installed。

```
kubectl describe tprov trident -n trident | grep Message: -A 3  
Message:  Trident installed  
Status:   Installed  
Version:  v20.10.1
```



如果狀態顯示 Updating、請務必先解決此問題、再繼續進行。如需可能狀態值的清單、請參閱 "[請按這裡](#)"。

2. 建立 TridentOrchestrator 請使用Trident安裝程式隨附的資訊清單來進行CRD。

```
# Download the release required [23.01.1]
mkdir 23.01.1
cd 23.01.1
wget
https://github.com/NetApp/trident/releases/download/v23.01.1/trident-
installer-23.01.1.tar.gz
tar -xf trident-installer-23.01.1.tar.gz
cd trident-installer
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
```

3. 使用命名空間範圍的運算子資訊清單來刪除。若要完成此步驟、您需要使用套裝組合Yaml檔案來部署命名空間範圍的運算子 <https://github.com/NetApp/trident/tree/stable/vXX.XX/deploy/BUNDLE.YAML> 其中 *vXX.XX* 為版本編號和 *BUNDLE.YAML* 為套裝組合Yaml檔案名稱。



您應該對Trident安裝參數進行必要的變更（例如、變更的值） *tridentImage*、*autosupportImage*、私有映像儲存庫、以及提供 *imagePullSecrets*）刪除命名空間範圍的運算子之後、安裝叢集範圍的運算子之前。如需可更新的完整參數清單、請參閱 "[組態選項](#)"。

```
#Ensure you are in the right directory
pwd
/root/20.10.1/trident-installer

#Delete the namespace-scoped operator
kubectl delete -f deploy/<BUNDLE.YAML> -n trident
serviceaccount "trident-operator" deleted
clusterrole.rbac.authorization.k8s.io "trident-operator" deleted
clusterrolebinding.rbac.authorization.k8s.io "trident-operator" deleted
deployment.apps "trident-operator" deleted
podsecuritypolicy.policy "tridentoperatorpods" deleted

#Confirm the Trident operator was removed
kubectl get all -n trident
```

NAME	READY	STATUS	RESTARTS	AGE
pod/trident-csi-68d979fb85-dsrmn	6/6	Running	12	99d
pod/trident-csi-8jfhf	2/2	Running	6	105d
pod/trident-csi-jtnjz	2/2	Running	6	105d
pod/trident-csi-lcxvh	2/2	Running	8	105d

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
service/trident-csi	ClusterIP	10.108.174.125	<none>	34571/TCP, 9220/TCP	105d

NAME	DESIRED	CURRENT	READY	UP-TO-DATE	AGE
daemonset.apps/trident-csi	3	3	3	3	3
kubernetes.io/arch=amd64, kubernetes.io/os=linux			105d		

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/trident-csi	1/1	1	1	105d

NAME	DESIRED	CURRENT	READY	AGE
replicaset.apps/trident-csi-68d979fb85	1	1	1	105d

在這個階段 trident-operator-xxxxxxxxxx-xxxxxx Pod已刪除。

- （選用）如果需要修改安裝參數、請更新 TridentProvisioner 規格這些變更可能包括：修改私有映像登錄以從擷取容器映像、啟用偵錯記錄或指定映像提取機密。

```
kubectl patch tprov <trident-provisioner-name> -n <trident-namespace>
--type=merge -p '{"spec":{"debug":true}}'
```

## 5. 安裝Trident運算子。



安裝叢集範圍的運算子會開始移轉 `TridentProvisioner` 物件 `TridentOrchestrator` 物件、刪除 `TridentProvisioner` 物件和 `tridentprovisioner` CRD、並將Astra Trident升級至所使用的叢集範圍運算子版本。在接下來的範例中、Trident已升級至23.01.1。



使用Trident營運者升級Astra Trident會導致移轉 `tridentProvisioner` 至 `tridentOrchestrator` 具有相同名稱的物件。這會由操作員自動處理。升級也會將Astra Trident安裝在與之前相同的命名空間中。



```

#Ensure you are in the correct directory
pwd
/root/23.01.1/trident-installer

#Install the cluster-scoped operator in the **same namespace**
kubectl create -f deploy/<BUNDLE.YAML>
serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created

#All tridentProvisioners will be removed, including the CRD itself
kubectl get tprov -n trident
Error from server (NotFound): Unable to list "trident.netapp.io/v1,
Resource=tridentprovisioners": the server could not find the requested
resource (get tridentprovisioners.trident.netapp.io)

#tridentProvisioners are replaced by tridentOrchestrator
kubectl get torc
NAME          AGE
trident       13s

#Examine Trident pods in the namespace
kubectl get pods -n trident

```

NAME	READY	STATUS	RESTARTS
trident-controller-79df798bdc-m79dc 1m41s	6/6	Running	0
trident-node-linux-xrst8 1m41s	2/2	Running	0
trident-operator-5574dbbc68-nthjv 1m52s	1/1	Running	0

```

#Confirm Trident has been updated to the desired version
kubectl describe torc trident | grep Message -A 3
Message:          Trident installed
Namespace:        trident
Status:           Installed
Version:          v23.01.1

```



◦ trident-controller 和Pod名稱反映了23.01中引入的命名慣例。

## 升級Helm型的營運者安裝

請執行下列步驟、升級Helm型的操作員安裝。



將Kubernetes叢集從1.24升級至1.25或更新版本、且已安裝Astra Trident時、您必須更新`values.yaml`才能設定 `excludePodSecurityPolicy` 至 `true` 或新增 `--set excludePodSecurityPolicy=true` 至 `helm upgrade` 命令、然後才能升級叢集。

### 步驟

1. 下載最新的Astra Trident版本。
2. 使用 `helm upgrade` 命令位置 `trident-operator-23.01.1.tgz` 反映您要升級的版本。

```
helm upgrade <name> trident-operator-23.01.1.tgz
```

如果您在初始安裝期間設定任何非預設選項（例如指定Trident和csi映像的私有、鏡射登錄）、請使用 `--set` 為了確保升級命令中包含這些選項、否則這些值會重設為預設值。



例如、變更的預設值 `tridentDebug`，執行下列命令：

```
helm upgrade <name> trident-operator-23.01.1-custom.tgz --set tridentDebug=true
```

3. 執行 `helm list` 以確認圖表和應用程式版本均已升級。執行 `tridentctl logs` 以檢閱任何偵錯訊息。

### 結果

Trident營運者將識別現有的Astra Trident安裝、並將其升級至與營運者相同的版本。

## 從非營運者安裝升級

您可以從升級至最新版的Trident運算子 `tridentctl` 安裝：

### 步驟

1. 下載最新的Astra Trident版本。

```
# Download the release required [23.01.1]
mkdir 23.01.1
cd 23.01.1
wget
https://github.com/NetApp/trident/releases/download/v22.01.1/trident-
installer-23.01.1.tar.gz
tar -xf trident-installer-23.01.1.tar.gz
cd trident-installer
```

2. 建立 tridentorchestrator 資訊清單中的CRD。

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
```

3. 部署營運者。

```
#Install the cluster-scoped operator in the **same namespace**
kubectl create -f deploy/<BUNDLE.YAML>
serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created

#Examine the pods in the Trident namespace
```

NAME	READY	STATUS	RESTARTS	AGE
trident-controller-79df798bdc-m79dc	6/6	Running	0	150d
trident-node-linux-xrst8	2/2	Running	0	150d
trident-operator-5574dbbc68-nthjv	1/1	Running	0	1m30s

4. 建立 TridentOrchestrator 用於安裝Astra Trident的CR。

```
#Create a tridentOrchestrator to initiate a Trident install
cat deploy/crds/tridentorchestrator_cr.yaml
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident

kubectl create -f deploy/crds/tridentorchestrator_cr.yaml

#Examine the pods in the Trident namespace
NAME                                READY   STATUS    RESTARTS   AGE
trident-csi-79df798bdc-m79dc        6/6     Running   0           1m
trident-csi-xrst8                    2/2     Running   0           1m
trident-operator-5574dbbc68-nthjv    1/1     Running   0           5m41s

#Confirm Trident was upgraded to the desired version
kubectl describe torc trident | grep Message -A 3
Message:                             Trident installed
Namespace:                           trident
Status:                               Installed
Version:                              v23.01.1
```

## 結果

現有的後端和PVCS會自動提供使用。

## 使用tridentctl進行升級

您可以使用輕鬆升級現有的Astra Trident安裝 tridentctl。

### 升級前的考量

升級至最新版Astra Trident時、請考慮下列事項：

- 從Trident 20.01開始、只有的試用版 "[Volume快照](#)" 支援。Kubernetes系統管理員應謹慎地將Alpha快照物件安全備份或轉換成試用版、以保留舊版Alpha快照。
- Volume快照的試用版推出一組經過修改的CRD和快照控制器、這兩個控制器都應該在安裝Astra Trident之前設定。"[這篇部落格](#)" 討論將Alpha Volume快照移轉至試用版格式的相關步驟。
- 解除安裝和重新安裝Astra Trident可做為升級。當您解除安裝Trident時、不會刪除由Astra Trident部署所使用的持續磁碟區宣告（PVC）和持續磁碟區（PV）。當Astra Trident離線時、已配置的PV仍可繼續使用、而Astra Trident會在任何建立於過渡期間的永久虛電路恢復上線後、為其配置磁碟區。



升級Astra Trident時、請勿中斷升級程序。確保安裝程式執行完成。

## 升級後的後續步驟

若要使用較新的Trident版本（例如隨需Volume Snapshots）所提供的豐富功能集、您可以使用升級磁碟區 `tridentctl upgrade` 命令。

如果有舊版磁碟區、您應該將其從NFS/iSCSI類型升級為「csi」類型、以便使用Astra Trident的完整新功能集。Trident提供的舊PV支援傳統功能集。

決定將磁碟區升級為「csi」類型時、請考慮下列事項：

- 您可能不需要升級所有磁碟區。先前建立的磁碟區將繼續可供存取、並正常運作。
- 在升級時、PV可作為部署/狀態集的一部分掛載。不需要關閉部署/狀態集。
- 您\*無法\*在升級時將PV附加至獨立式Pod。在升級磁碟區之前、您應該先關閉Pod。
- 您只能升級綁定到PVC的磁碟區。在升級之前、應先移除和匯入未繫結至PVCS的磁碟區。

### Volume升級範例

以下範例顯示如何執行Volume升級。

1. 執行 `kubectl get pv` 以列出PV。

```
kubectl get pv
```

NAME	CAPACITY	ACCESS MODES	RECLAIM POLICY
STATUS CLAIM	STORAGECLASS	REASON	AGE
default-pvc-1-a8475	1073741824	RWO	Delete
Bound default/pvc-1	standard		19h
default-pvc-2-a8486	1073741824	RWO	Delete
Bound default/pvc-2	standard		19h
default-pvc-3-a849e	1073741824	RWO	Delete
Bound default/pvc-3	standard		19h
default-pvc-4-a84de	1073741824	RWO	Delete
Bound default/pvc-4	standard		19h
trident	2Gi	RWO	Retain
Bound trident/trident			19h

目前有四個PV是由Trident 20.07使用所建立 `netapp.io/trident` 置備程式：

2. 執行 `kubectl describe pv` 以取得PV的詳細資料。

```
kubectl describe pv default-pvc-2-a8486
```

```
Name:                default-pvc-2-a8486
Labels:              <none>
Annotations:         pv.kubernetes.io/provisioned-by: netapp.io/trident
                    volume.beta.kubernetes.io/storage-class: standard
Finalizers:          [kubernetes.io/pv-protection]
StorageClass:        standard
Status:              Bound
Claim:               default/pvc-2
Reclaim Policy:      Delete
Access Modes:        RWO
VolumeMode:          Filesystem
Capacity:             1073741824
Node Affinity:       <none>
Message:
Source:
  Type:              NFS (an NFS mount that lasts the lifetime of a pod)
  Server:             10.xx.xx.xx
  Path:               /trid_1907_alpha_default_pvc_2_a8486
  ReadOnly:          false
```

PV是使用建立的 `netapp.io/trident` 資源配置程式、類型為NFS。為了支援Astra Trident提供的所有新功能、此PV應升級為「csi」類型。

3. 執行 `tridentctl upgrade volume <name-of-trident-volume>` 將舊Astra Trident Volume升級至csi規格的命令。

```

./tridentctl get volumes -n trident
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS | PROTOCOL |
BACKEND UUID            |  STATE  |  MANAGED  |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| default-pvc-2-a8486 | 1.0 GiB | standard      | file      | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true          |          |
| default-pvc-3-a849e | 1.0 GiB | standard      | file      | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true          |          |
| default-pvc-1-a8475 | 1.0 GiB | standard      | file      | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true          |          |
| default-pvc-4-a84de | 1.0 GiB | standard      | file      | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

./tridentctl upgrade volume default-pvc-2-a8486 -n trident
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS | PROTOCOL |
BACKEND UUID            |  STATE  |  MANAGED  |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| default-pvc-2-a8486 | 1.0 GiB | standard      | file      | c5a6f6a4-
b052-423b-80d4-8fb491a14a22 | online | true          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

```

4. 執行 `kubectl describe pv` 以驗證Volume是否為「csi Volume」 (SCSI Volume) 。

```
kubectl describe pv default-pvc-2-a8486
Name:                default-pvc-2-a8486
Labels:              <none>
Annotations:         pv.kubernetes.io/provisioned-by: csi.trident.netapp.io
                    volume.beta.kubernetes.io/storage-class: standard
Finalizers:          [kubernetes.io/pv-protection]
StorageClass:        standard
Status:              Bound
Claim:               default/pvc-2
Reclaim Policy:      Delete
Access Modes:        RWO
VolumeMode:          Filesystem
Capacity:            1073741824
Node Affinity:       <none>
Message:
Source:
  Type:              CSI (a Container Storage Interface (CSI) volume
source)
  Driver:             csi.trident.netapp.io
  VolumeHandle:       default-pvc-2-a8486
  ReadOnly:           false
  VolumeAttributes:   backendUUID=c5a6f6a4-b052-423b-80d4-
8fb491a14a22

internalName=trid_1907_alpha_default_pvc_2_a8486
                    name=default-pvc-2-a8486
                    protocol=file
Events:              <none>
```

如此一來、您就能將由Astra Trident建立的NFS/iSCSI類型磁碟區、以每個磁碟區為基礎、升級為「csi」類型。

## 解除安裝Astra Trident

視Astra Trident的安裝方式而定、有多種選項可供您解除安裝。

### 使用Helm解除安裝

如果您使用Helm安裝了Astra Trident、您可以使用解除安裝 `helm uninstall`。



```
#List the Helm release corresponding to the Astra Trident install.
helm ls -n trident
NAME                NAMESPACE          REVISION              UPDATED
STATUS              CHART                APP VERSION
trident             trident              1                    2021-04-20
00:26:42.417764794 +0000 UTC deployed    trident-operator-21.07.1
21.07.1

#Uninstall Helm release to remove Trident
helm uninstall trident -n trident
release "trident" uninstalled
```

## 使用Trident運算子解除安裝

如果您使用運算子安裝了Astra Trident、您可以執行下列其中一項來解除安裝：

- 編輯 TridentOrchestrator 若要設定解除安裝旗標：\*您可以編輯 TridentOrchestrator 並設定 spec.uninstall=true。編輯 TridentOrchestrator 並設定 uninstall 旗標如下所示：

```
kubectl patch torc <trident-orchestrator-name> --type=merge -p
'{"spec":{"uninstall":true}}'
```

當 uninstall 旗標設定為 true、Trident運算子會卸載Trident、但不會移除TridentOrchestrator本身。如果您想要再次安裝Trident、請清理TridentOrchestrator並建立新的Trident。

- 刪除 TridentOrchestrator：\*移除 TridentOrchestrator 用來部署Astra Trident的CR、您可以指示操作員解除安裝Trident。操作員會處理的移除作業 TridentOrchestrator 然後繼續移除Astra Trident部署和取消安裝、刪除它在安裝過程中建立的Trident Pod。若要完全移除Astra Trident（包括它所建立的CRD）、並有效清除Slate Clean、您可以編輯 TridentOrchestrator 以通過 wipeout 選項。請參閱下列範例：

```
kubectl patch torc <trident-orchestrator-name> --type=merge -p
'{"spec":{"wipeout":["crds"],"uninstall":true}}'
```

這會完全解除安裝Astra Trident、並清除所有與後端及其管理的磁碟區相關的中繼資料。後續安裝會視為全新安裝。



執行完整解除安裝時、您只能考慮抹除客戶需求日。此動作無法復原。除非您想要重新開始並建立全新的**Astra Trident**安裝、否則請勿清除客戶需求日。

## 使用解除安裝 tridentctl

執行 uninstall 命令輸入 tridentctl 如下所示、移除所有與Astra Trident相關的資源（CRD和相關物件除外）、如此一來、就能輕鬆再次執行安裝程式以更新至較新的版本。

```
./tridentctl uninstall -n <namespace>
```

若要完整移除Astra Trident、您應移除由Astra Trident所建立之CRD的微調工具、然後刪除CRD。

## 降級Astra Trident

瞭解降級至舊版Astra Trident的相關步驟。

### 何時降級

您可能會考慮降級的原因有多種、例如：

- 應變規劃
- 立即修正升級後發現的錯誤
- 相依性問題、不成功和不完整的升級

移至使用CRD的Astra Trident版本時、您應該考慮降級。由於Astra Trident使用CRD來維護狀態、因此所建立的所有儲存實體（後端、儲存類別、PV和Volume快照）都會建立關聯的CRD物件、而非寫入的資料 `trident PV`（由舊版Astra Trident使用）。新建立的PV、後端和儲存類別都會維護為CRD物件。

僅嘗試降級使用CRD（19.07及更新版本）執行的Astra Trident版本。如此可確保在降級發生後、可以看到目前Astra Trident版本上執行的作業。

### 何時不降級

您不應降級至使用的Trident版本 `etcd` 以維持狀態（19.04及更早版本）。所有以目前Astra Trident版本執行的作業、都不會在降級後反映出來。移回舊版時、無法使用新建立的PV。當您移回舊版時、Astra Trident不會看到對物件所做的變更、例如後端、PV、儲存類別和Volume快照（已建立/更新/刪除）。返回舊版不會中斷已使用舊版建立之PV的存取、除非已升級。

### 使用業者安裝Astra Trident時的降級程序

對於使用Trident操作員完成的安裝、降級程序會有所不同、不需要使用 `tridentctl`。

對於使用Trident營運者完成的安裝、Astra Trident可降級為下列任一項：

- 使用命名空間範圍運算子安裝的版本（20.07 - 20.10）。
- 使用叢集範圍運算子（21.01及更新版本）安裝的版本。

#### 降級至叢集範圍的運算子

若要將Astra Trident降級為使用叢集範圍運算子的版本、請遵循下列步驟。

##### 步驟

1. **"解除安裝Astra Trident"**。除非您想要完全移除現有的安裝、否則請勿刪除客戶需求日。
2. 您可以使用與Trident版本相關的運算子資訊清單來刪除Trident運算子。例如、

<https://github.com/NetApp/trident/tree/stable/vXX.XX/deploy/bundle.yaml> 其中 *vXX.XX* 為版本編號（例如 v22.10）和 *bundle.yaml* 為套裝組合Yaml檔案名稱。

3. 安裝所需版本的Astra Trident、以繼續降級。請遵循所需版本的說明文件。

## 降級至命名空間範圍的運算子

本節摘要說明降級至Astra Trident版本所需的步驟、範圍介於20.07到20.10之間、此版本將使用命名空間範圍的運算子來安裝。

### 步驟

1. "解除安裝Astra Trident"。\*除非您想要完全移除現有的安裝、否則請勿使用CRD。\*請確定 `tridentorchestrator` 已刪除。

```
#Check to see if there are any tridentorchestrators present
kubectl get torc
NAME          AGE
trident       20h

#Looks like there is a tridentorchestrator that needs deleting
kubectl delete torc trident
tridentorchestrator.trident.netapp.io "trident" deleted
```

2. 您可以使用與Trident版本相關的運算子資訊清單來刪除Trident運算子。例如、  
<https://github.com/NetApp/trident/tree/stable/vXX.XX/deploy/bundle.yaml> 其中 *vXX.XX* 為版本編號（例如 v22.10）和 *bundle.yaml* 為套裝組合Yaml檔案名稱。
3. 刪除 `tridentorchestrator` 客戶需求日

```
#Check to see if ``tridentorchestrators.trident.netapp.io`` CRD is
present and delete it.

kubectl get crd tridentorchestrators.trident.netapp.io

NAME                                CREATED AT
tridentorchestrators.trident.netapp.io  2021-01-21T21:11:37Z

kubectl delete crd tridentorchestrators.trident.netapp.io

customresourcedefinition.apiextensions.k8s.io
"tridentorchestrators.trident.netapp.io" deleted
```

Astra Trident已解除安裝。

4. 安裝所需的版本、繼續降級。請遵循所需版本的說明文件。

## 使用Helm降級

若要降級、請使用 `helm rollback trident` 命令。請參閱下列範例：

```
helm rollback trident [revision #]
```

## 使用安裝Astra Trident時的降級程序 `tridentctl`

如果您使用安裝了Astra Trident `tridentctl` 降級程序包括下列步驟。此順序將引導您完成從Astra Trident 21.007 移至20.07的降級程序。



在開始降級之前、您應該先擷取Kubernetes叢集的快照 `etcd`。這可讓您備份Astra Trident客戶需求日的目前狀態。

### 步驟

1. 請確定使用安裝Trident `tridentctl`。如果您不確定Astra Trident的安裝方式、請執行以下簡單測試：
  - a. 列出Trident命名空間中的Pod。
  - b. 識別叢集中執行的Astra Trident版本。您可以使用 `tridentctl` 或是查看Trident Pod中使用的影像。
  - c. 如果\*看不到\*A `tridentOrchestrator` (或) `tridentprovisioner` (或) 名為的Pod `trident-operator-xxxxxxxx-xxxxx`、Astra Trident 安裝 `tridentctl`。
2. 使用現有的解除安裝Astra Trident `tridentctl` 二進位。在這種情況下、您將會以21.07二進位檔解除安裝。

```
tridentctl version -n trident
+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+
| 21.07.0        | 21.07.0        |
+-----+

tridentctl uninstall -n trident
INFO Deleted Trident deployment.
INFO Deleted Trident daemonset.
INFO Deleted Trident service.
INFO Deleted Trident secret.
INFO Deleted cluster role binding.
INFO Deleted cluster role.
INFO Deleted service account.
INFO Deleted pod security policy.
podSecurityPolicy=tridentpods
INFO The uninstaller did not delete Trident's namespace in case it is
going to be reused.
INFO Trident uninstallation succeeded.
```

3. 完成後、請取得所需版本的Trident二進位檔（本範例為20.07）、並使用它來安裝Astra Trident。您可以為產生自訂YAML "自訂安裝" 如有需要。

```
cd 20.07/trident-installer/
./tridentctl install -n trident-ns
INFO Created installer service account.
serviceaccount=trident-installer
INFO Created installer cluster role.                clusterrole=trident-
installer
INFO Created installer cluster role binding.
clusterrolebinding=trident-installer
INFO Created installer configmap.                  configmap=trident-
installer
...
...
INFO Deleted installer cluster role binding.
INFO Deleted installer cluster role.
INFO Deleted installer service account.
```

降級程序已完成。

# 使用Astra Trident

## 準備工作節點

Kubernetes叢集中的所有工作節點都必須能夠掛載您已為Pod配置的磁碟區。若要準備工作節點、您必須根據所選的驅動程式來安裝NFS或iSCSI工具。

### 選擇適當的工具

如果您使用的是驅動程式組合、則應該安裝NFS和iSCSI工具。

#### NFS工具

如果您使用的是： `ontap-nas`、`ontap-nas-economy`、`ontap-nas-flexgroup`、`azure-netapp-files`、`gcp-cvs`

#### iSCSI工具

如果您使用的是： `ontap-san`、`ontap-san-economy`、`solidfire-san`



最新版本的RedHat CoreOS預設會安裝NFS和iSCSI。

## 節點服務探索

Astra Trident會嘗試自動偵測節點是否能執行iSCSI或NFS服務。



節點服務探索可識別探索到的服務、但無法保證服務已正確設定。相反地、沒有探索到的服務並不保證磁碟區掛載會失敗。

### 檢閱事件

Astra Trident會為節點建立事件、以識別探索到的服務。若要檢閱這些事件、請執行：

```
kubectl get event -A --field-selector involvedObject.name=<Kubernetes node name>
```

### 檢閱探索到的服務

Astra Trident可識別Trident節點CR上每個節點所啟用的服務。若要檢視探索到的服務、請執行：

```
tridentctl get node -o wide -n <Trident namespace>
```

## NFS磁碟區

使用作業系統的命令來安裝NFS工具。確保NFS服務在開機期間啟動。

## RHEL 8以上

```
sudo yum install -y nfs-utils
```

## Ubuntu

```
sudo apt-get install -y nfs-common
```



安裝NFS工具之後、請重新啟動工作節點、以避免將磁碟區附加至容器時發生故障。

## iSCSI磁碟區

Astra Trident可自動建立iSCSI工作階段、掃描LUN、探索多重路徑裝置、將其格式化、並將其掛載至Pod。

### iSCSI自我修復功能

對於支援此技術的系統、Astra Trident每五分鐘執行一次iSCSI自我修復、以便ONTAP：

1. \*識別\*所需的iSCSI工作階段狀態和目前的iSCSI工作階段狀態。
2. \*比較\*所需狀態與目前狀態、以識別所需的維修。Astra Trident決定了維修優先順序、以及何時預先排除維修。
3. 執行必要的修復、以將目前的iSCSI工作階段狀態恢復至所需的iSCSI工作階段狀態。



自我修復活動記錄位於 `trident-main` 容器位於各自的Demmon Pod上。若要檢視記錄、您必須設定好 `debug` 在Astra Trident安裝期間達到「true」。

Astra Trident iSCSI自我修復功能有助於預防：

- 發生網路連線問題後、可能會發生過時或不正常的iSCSI工作階段。在過時的工作階段中、Astra Trident會在登出前等待七分鐘、重新建立與入口網站的連線。



例如、如果在儲存控制器上旋轉CHAP機密、而網路失去連線、則舊的 (`stal_`) CHAP機密可能會持續存在。自我修復可辨識此情況、並自動重新建立工作階段、以套用更新的CHAP機密。

- 遺失iSCSI工作階段
- 遺失LUN

## 安裝iSCSI工具

使用適用於您作業系統的命令來安裝iSCSI工具。

### 開始之前

- Kubernetes叢集中的每個節點都必須具有唯一的IQN。這是必要的先決條件。

- 若搭配使用RMCOS 4.5或更新版本、或其他與RHEL相容的Linux套裝作業系統 solidfire-san 驅動程式和元素OS 12.5或更早版本、請確定CHAP驗證演算法已在中設定為MD5 /etc/iscsi/iscsid.conf。元素12.7提供安全的FIPS相容CHAP演算法SHA1、SHA-256和SHA3-256。

```
sudo sed -i 's/^\(node.session.auth.chap_algs\) .*/\1 = MD5/'  
/etc/iscsi/iscsid.conf
```

- 使用執行RHEL/RedHat CoreOS搭配iSCSI PV的工作節點時、請指定 discard StorageClass中的掛載選項、以執行即時空間回收。請參閱 ["RedHat的文件"](#)。



## RHEL 8以上

1. 安裝下列系統套件：

```
sudo yum install -y lsscsi iscsi-initiator-utils sg3_utils device-  
mapper-multipath
```

2. 檢查iscsi-initier-utils版本是否為6.6.0.874-2.el7或更新版本：

```
rpm -q iscsi-initiator-utils
```

3. 將掃描設為手動：

```
sudo sed -i 's/^\(node.session.scan\).*$/\1 = manual/'  
/etc/iscsi/iscsid.conf
```

4. 啟用多重路徑：

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```



確保 `etc/multipath.conf` 包含 `find_multipaths no` 低於 `defaults`。

5. 請確保如此 `iscsid` 和 `multipathd` 執行中：

```
sudo systemctl enable --now iscsid multipathd
```

6. 啟用並啟動 `iscsi`：

```
sudo systemctl enable --now iscsi
```

## Ubuntu

1. 安裝下列系統套件：

```
sudo apt-get install -y open-iscsi lsscsi sg3-utils multipath-tools  
scsitools
```

2. 檢查開放式iSCSI版本是否為2.0.874-5ubuntu2・10或更新版本（適用於雙聲網路）或2.0.874-7.1ubuntu6.1或更新版本（適用於焦點）：

```
dpkg -l open-iscsi
```

3. 將掃描設為手動：

```
sudo sed -i 's/^\(node.session.scan\).*\/\1 = manual/'  
/etc/iscsi/iscsid.conf
```

4. 啟用多重路徑：

```
sudo tee /etc/multipath.conf <<-'EOF'  
defaults {  
    user_friendly_names yes  
    find_multipaths no  
}  
EOF  
sudo systemctl enable --now multipath-tools.service  
sudo service multipath-tools restart
```



確保 `etc/multipath.conf` 包含 `find_multipaths no` 低於 `defaults`。

5. 請確保如此 `open-iscsi` 和 `multipath-tools` 已啟用並執行：

```
sudo systemctl status multipath-tools  
sudo systemctl enable --now open-iscsi.service  
sudo systemctl status open-iscsi
```



若為Ubuntu 18.04、您必須使用探索目標連接埠 `iscsiadm` 開始之前 `open-iscsi` 以啟動iSCSI精靈。您也可以修改 `iscsi` 服務開始 `iscsid` 自動：



安裝iSCSI工具之後、請重新啟動工作節點、以避免將磁碟區附加至容器時發生故障。

## 設定後端

後端定義了Astra Trident與儲存系統之間的關係。它告訴Astra Trident如何與該儲存系統通訊、以及Astra Trident如何從該儲存系統配置磁碟區。

Astra Trident會自動從後端提供符合儲存類別所定義需求的儲存資源池。瞭解如何設定儲存系統的後端。

- ["設定Azure NetApp Files 一個靜態後端"](#)

- "設定Cloud Volumes Service 適用於Google Cloud Platform後端的功能"
- "設定NetApp HCI 一個不只是功能的SolidFire 後端"
- "使用ONTAP 功能不一的Cloud Volumes ONTAP NAS驅動程式來設定後端"
- "使用ONTAP 不支援的Cloud Volumes ONTAP SAN驅動程式來設定後端"
- "使用Astra Trident搭配Amazon FSX for NetApp ONTAP 解決方案"

## Azure NetApp Files

### 設定Azure NetApp Files 一個靜態後端

您可以將Azure NetApp Files 靜態（ANF）設定為Astra Trident的後端。您可以使用ANF後端連接NFS和SMB磁碟區。

- "準備"
- "組態選項與範例"

### 考量

- 此支援服務不支援小於100 GB的磁碟區。Azure NetApp Files如果要求較小的磁碟區、Astra Trident會自動建立100-GB磁碟區。
- Astra Trident僅支援安裝在Windows節點上執行的Pod上的SMB磁碟區。
- Astra Trident不支援Windows ARM 的架構。

### 準備設定Azure NetApp Files 一個功能完善的後端

在您設定Azure NetApp Files 完後端功能之前、您必須確保符合下列要求。



如果您是第一次使用 Azure NetApp Files 、或是在新位置使用、則必須先進行一些初始設定、才能設定 Azure NetApp Files 並建立 NFS Volume 。請參閱 "[Azure：設定Azure NetApp Files 功能以建立NFS Volume](#)"。

### NFS 和 SMB 磁碟區的必要條件

若要設定及使用 "[Azure NetApp Files](#)" 後端、您需要下列項目：

- 容量集區。請參閱 "[Microsoft：為 Azure NetApp Files 建立容量集區](#)"。
- 委派給 Azure NetApp Files 的子網路。請參閱 "[Microsoft：將子網路委派給 Azure NetApp Files](#)"。
- subscriptionID 透過啟用Azure NetApp Files 了支援功能的Azure訂閱。
- tenantID、clientID、和 clientSecret 從 "[應用程式註冊](#)" 在Azure Active Directory中、具備Azure NetApp Files 充分的權限執行此功能。應用程式登錄應使用下列其中一項：
  - 擁有者或貢獻者角色 "[由Azure預先定義](#)"。
  - 答 "[自訂貢獻者角色](#)" 在訂購層級 (assignableScopes) 具有下列權限、僅限於Astra Trident所需的權限。建立自訂角色之後、"[使用Azure入口網站指派角色](#)"。

```

{
  "id": "/subscriptions/<subscription-id>/providers/Microsoft.Authorization/roleDefinitions/<role-definition-id>",
  "properties": {
    "roleName": "custom-role-with-limited-perms",
    "description": "custom role providing limited permissions",
    "assignableScopes": [
      "/subscriptions/<subscription-id>"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.NetApp/netAppAccounts/capacityPools/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/delete",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/delete",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/GetMetadata/action",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/MountTargets/r

```

```

    "read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/read",

    "Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/write",

    "Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/delete",

        "Microsoft.Features/features/read",
        "Microsoft.Features/operations/read",
        "Microsoft.Features/providers/features/read",

    "Microsoft.Features/providers/features/register/action",

    "Microsoft.Features/providers/features/unregister/action",

    "Microsoft.Features/subscriptionFeatureRegistrations/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
}
}

```

- Azure location 至少包含一個 ["委派的子網路"](#)。從Trident 22.01起 location 參數是後端組態檔最上層的必填欄位。會忽略虛擬資源池中指定的位置值。

#### SMB磁碟區的其他需求

若要建立 SMB Volume 、您必須具備：

- Active Directory 已設定並連線至 Azure NetApp Files 。請參閱 ["Microsoft：建立及管理 Azure NetApp Files 的 Active Directory 連線"](#)。
- Kubernetes叢集具備Linux控制器節點、以及至少一個執行Windows Server 2019的Windows工作節點。Astra Trident僅支援安裝在Windows節點上執行的Pod上的SMB磁碟區。
- 至少有一個 Astra Trident 秘密、內含您的 Active Directory 認證、以便 Azure NetApp Files 能夠驗證至 Active Directory 。以產生機密 smbcreds：

```
kubectl create secret generic smbcreds --from-literal username=user
--from-literal password='password'
```

- 設定為Windows服務的SCSI Proxy。若要設定 csi-proxy、請參閱 ["GitHub：csi Proxy"](#) 或 ["GitHub：適用於Windows的SCSI Proxy"](#) 適用於Windows上執行的Kubernetes節點。

## 列舉後端組態選項與範例Azure NetApp Files

深入瞭解ANF的NFS和SMB後端組態選項、並檢閱組態範例。

Astra Trident使用您的後端組態（子網路、虛擬網路、服務層級和位置）、在所要求位置可用的容量集區上建立ANF磁碟區、並符合所要求的服務層級和子網路。



Astra Trident不支援手動QoS容量集區。

### 後端組態選項

Anf後端提供這些組態選項。

參數	說明	預設
version		永遠為1
storageDriverName	儲存驅動程式名稱	「Azure - NetApp-Files」
backendName	自訂名稱或儲存後端	驅動程式名稱+「_」+隨機字元
subscriptionID	Azure訂閱的訂閱ID	
tenantID	應用程式註冊的租戶ID	
clientID	應用程式註冊的用戶端ID	
clientSecret	應用程式註冊的用戶端機密	
serviceLevel	其中之一 Standard、Premium、或 Ultra	""（隨機）
location	要建立新磁碟區的Azure位置名稱	
resourceGroups	用於篩選已探索資源的資源群組清單	「[]」（無篩選器）
netappAccounts	篩選探索資源的NetApp帳戶清單	「[]」（無篩選器）
capacityPools	用於篩選已探索資源的容量集區清單	「[]」（無篩選器、隨機）
virtualNetwork	具有委派子網路的虛擬網路名稱	"
subnet	委派給的子網路名稱 Microsoft.Netapp/volumes	"

參數	說明	預設
networkFeatures	Volume的vnet功能集可能是 Basic 或 Standard。並非所有地區都提供網路功能、可能必須在訂閱中啟用。指定 networkFeatures 如果未啟用此功能、則會導致磁碟區資源配置失敗。	"
nfsMountOptions	精細控制NFS掛載選項。SMB磁碟區已忽略。若要使用NFS 4.1版掛載磁碟區、請包含 nfsvers=4 在以逗號分隔的掛載選項清單中、選擇NFS v4.1。儲存類別定義中設定的掛載選項會覆寫在後端組態中設定的掛載選項。	"nfsvers=3"
limitVolumeSize	如果要求的磁碟區大小高於此值、則資源配置失敗	""（預設不強制執行）
debugTraceFlags	疑難排解時要使用的偵錯旗標。範例：\{"api": false, "method": true, "discovery": true}。除非您正在進行疑難排解並需要詳細的記錄傾印、否則請勿使用此功能。	null
nasType	設定NFS或SMB磁碟區建立。選項包括 nfs、smb 或null。NFS磁碟區的預設值設為null。	nfs



如需網路功能的詳細資訊、請參閱 ["設定Azure NetApp Files 適用於某個聲音量的網路功能"](#)。

## 必要的權限與資源

如果您在建立永久虛擬基礎架構時收到「找不到容量資源池」錯誤、您的應用程式註冊可能沒有相關的必要權限和資源（子網路、虛擬網路、容量資源池）。如果啟用偵錯、Astra Trident會記錄在建立後端時探索到的Azure資源。確認使用的角色是否適當。

的值 resourceGroups、netappAccounts、capacityPools、virtualNetwork和 subnet 可以使用簡短或完整名稱來指定。在大多數情況下、建議使用完整名稱、因為短名稱可以符合多個名稱相同的資源。

。 resourceGroups、netappAccounts和 capacityPools 值是篩選器、可將探索到的資源集合限制在此儲存後端可用的資源、並可任意組合指定。完整名稱格式如下：

類型	格式
資源群組	<資源群組>
NetApp帳戶	資源群組/<NetApp帳戶>
容量資源池	資源群組/<NetApp帳戶>/<容量資源池>
虛擬網路	資源群組/<虛擬網路>
子網路	資源群組/<虛擬網路>/<子網路>

## Volume資源配置

您可以在組態檔的特殊區段中指定下列選項、以控制預設的Volume資源配置。請參閱 [\[組態範例\]](#) 以取得詳細資料。

參數	說明	預設
exportRule	匯出新磁碟區的規則。 exportRule 必須是以逗號分隔的清單、以CIDR表示法列出所有的IPv4位址或IPv4子網路組合。SMB磁碟區已忽略。	「0.0.0.0/0」
snapshotDir	控制.snapshot目錄的可見度	"假"
size	新磁碟區的預設大小	100公克
unixPermissions	新磁碟區的UNIX權限（4個八進位數字）。SMB磁碟區已忽略。	""（預覽功能、訂閱時需要白名單）

### 組態範例

#### 範例1：最低組態

這是絕對最低的后端組態。使用此組態、Astra Trident會在設定的位置探索所有NetApp帳戶、容量集區和委派給ANF的子網路、並隨機將新磁碟區放在其中一個集區和子網路上。因為 `nasType` 省略 `nfs` 預設會套用、后端會為NFS磁碟區進行資源配置。

當您剛開始使用ANF並嘗試各種功能時、這種組態是理想的選擇、但實際上您想要為您所配置的磁碟區提供額外的範圍。

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
```



## 範例2：使用容量集區篩選器的特定服務層級組態

此後端組態可將Volume置於Azure中 `eastus` 位置 `Ultra` 容量資源池：Astra Trident會自動探索該位置委派給ANF的所有子網路、並隨機在其中一個磁碟區上放置新磁碟區。

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
- application-group-1/account-1/ultra-1
- application-group-1/account-1/ultra-2
```

### 範例3：進階組態

此後端組態可進一步將磁碟區放置範圍縮小至單一子網路、並修改部分Volume資源配置預設值。

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
- application-group-1/account-1/ultra-1
- application-group-1/account-1/ultra-2
virtualNetwork: my-virtual-network
subnet: my-subnet
networkFeatures: Standard
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 500Gi
defaults:
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  snapshotDir: 'true'
  size: 200Gi
  unixPermissions: '0777'
```

#### 範例4：虛擬資源池組態

此後端組態可在單一檔案中定義多個儲存集區。當您有多個容量集區支援不同的服務層級、而且想要在Kubernetes中建立代表這些層級的儲存類別時、這很有用。虛擬資源池標籤是用來區分資源池的依據 performance。

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
resourceGroups:
- application-group-1
networkFeatures: Basic
nfsMountOptions: vers=3,proto=tcp,timeo=600
labels:
  cloud: azure
storage:
- labels:
    performance: gold
    serviceLevel: Ultra
    capacityPools:
    - ultra-1
    - ultra-2
    networkFeatures: Standard
- labels:
    performance: silver
    serviceLevel: Premium
    capacityPools:
    - premium-1
- labels:
    performance: bronze
    serviceLevel: Standard
    capacityPools:
    - standard-1
    - standard-2
```

#### 儲存類別定義

以下內容 StorageClass 定義請參閱上述儲存資源池。

使用的範例定義 `parameter.selector` 欄位

使用 `parameter.selector` 您可以為每個項目指定 `StorageClass` 用於裝載磁碟區的虛擬集區。該磁碟區會在所選的資源池中定義各個層面。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: bronze
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze"
allowVolumeExpansion: true
```

### **SMB**磁碟區的定義範例

使用 `nasType`、`node-stage-secret-name` 和 `node-stage-secret-namespace`、您可以指定SMB磁碟區、並提供所需的Active Directory認證資料。

### 範例1：預設命名空間的基本組態

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
```

### 範例2：每個命名空間使用不同的機密

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

### 範例3：每個磁碟區使用不同的機密

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: ${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```



nasType: `smb` 支援SMB磁碟區的集區篩選器。nasType: `nfs` 或 nasType: `null` NFS 集區的篩選器。

## 建立後端

建立後端組態檔之後、請執行下列命令：

```
tridentctl create backend -f <backend-file>
```

如果後端建立失敗、表示後端組態有問題。您可以執行下列命令來檢視記錄、以判斷原因：

```
tridentctl logs
```

識別並修正組態檔的問題之後、您可以再次執行create命令。

## 設定Cloud Volumes Service 適用於Google Cloud後端的功能

瞭解Cloud Volumes Service 解如何使用提供的範例組態、將NetApp for Google Cloud設定為Astra Trident安裝的後端。

深入瞭解Astra Trident對Cloud Volumes Service Google Cloud的支援

Astra Trident可在Cloud Volumes Service 兩個地方建立一個不二的資料區 "服務類型"：

- \* CVS效能\*：預設的Astra Trident服務類型。這種效能最佳化的服務類型最適合重視效能的正式作業工作負載。CVS效能服務類型是一種硬體選項、可支援最小100 GiB大小的磁碟區。您可以選擇其中一項 "三種服務層級"：
  - standard
  - premium
  - extreme
- \* CVS：CVS服務類型提供高分區可用度、但效能等級僅限於中度。CVS服務類型是一種軟體選項、使用儲存資源池來支援小至1 GiB的磁碟區。儲存資源池最多可包含50個磁碟區、其中所有磁碟區都會共用資源池的容量和效能。您可以選擇其中一項 "兩種服務層級"：
  - standardsw
  - zoneredundantstandardsw

## 您需要的產品

以設定及使用 "適用於 Google Cloud Cloud Volumes Service" 後端、您需要下列項目：

- Google Cloud帳戶已設定NetApp Cloud Volumes Service 功能
- Google Cloud帳戶的專案編號
- Google Cloud服務帳戶 netappcloudvolumes.admin 角色

- API金鑰檔案、供Cloud Volumes Service 您的I方面 帳戶使用

## 後端組態選項

每個後端都會在單一Google Cloud區域中配置磁碟區。若要在其他區域建立磁碟區、您可以定義其他後端。

參數	說明	預設
version		永遠為1
storageDriverName	儲存驅動程式名稱	「GCP-CVS」
backendName	自訂名稱或儲存後端	驅動程式名稱+ 「_」 + API金鑰的一部分
storageClass	用於指定CVS服務類型的選用參數。使用 software 可選擇CVS服務類型。否則、Astra Trident會採用CVS效能服務類型 (hardware) 。	
storagePools	僅限CVS服務類型。選用參數、用於指定用於建立磁碟區的儲存資源池。	
projectNumber	Google Cloud帳戶專案編號。此值可在Google Cloud入口網站首頁找到。	
hostProjectNumber	如果使用共享VPC網路、則為必要項目。在此案例中、projectNumber 是服務專案、以及 hostProjectNumber 是主機專案。	
apiRegion	Astra Trident在Google Cloud區域建立Cloud Volumes Service 了各種不全的功能。建立跨區域Kubernetes叢集時、會在中建立磁碟區apiRegion 可用於在多個Google Cloud區域的節點上排程的工作負載。跨區域流量會產生額外成本。	
apiKey	的Google Cloud服務帳戶API金鑰netappcloudvolumes.admin 角色：其中包含Google Cloud服務帳戶私密金鑰檔案（逐字複製到後端組態檔）的JSON-格式內容。	
proxyURL	Proxy URL（如果需要Proxy伺服器才能連線至CVS帳戶）。Proxy伺服器可以是HTTP Proxy或HTTPS Proxy。對於HTTPS Proxy、會跳過憑證驗證、以允許在Proxy伺服器中使用自我簽署的憑證。不支援已啟用驗證的Proxy伺服器。	
nfsMountOptions	精細控制NFS掛載選項。	"nfsves=3"

參數	說明	預設
limitVolumeSize	如果要求的磁碟區大小高於此值、則資源配置失敗。	""（預設不強制執行）
serviceLevel	適用於新磁碟區的CVS效能或CVS服務層級。CVS的效能值為standard、premium、或extreme。CVS值包括standardsw 或zoneredundantstandardsw。	CVS效能預設為「標準」。CVS預設為「標準」。
network	Google Cloud網路用於Cloud Volumes Service 解決資料不整的問題。	「預設」
debugTraceFlags	疑難排解時要使用的偵錯旗標。範例：\{"api":false, "method":true}。除非您正在進行疑難排解並需要詳細的記錄傾印、否則請勿使用此功能。	null
allowedTopologies	若要啟用跨區域存取、您的StorageClass定義適用於allowedTopologies 必須包含所有區域。例如： - key: topology.kubernetes.io/region values: - us-east1 - europe-west1	

## Volume資源配置選項

您可以在中控制預設的Volume資源配置 defaults 組態檔的一節。

參數	說明	預設
exportRule	新磁碟區的匯出規則。必須是以逗號分隔的清單、以CIDR表示法列出所有的IPv4位址或IPv4子網路組合。	「0.0.0.0/0」
snapshotDir	存取 .snapshot 目錄	"假"
snapshotReserve	保留給快照的磁碟區百分比	""（接受CVS預設值為0）
size	新磁碟區的大小。CVS效能最低為100 GiB。CVS最低為1 GiB。	CVS效能服務類型預設為「100GiB」。CVS服務類型並未設定預設值、但至少需要1 GiB。

## CVS效能服務類型範例

下列範例提供CVS效能服務類型的範例組態。



[illegible]

```
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
```

### 範例2：服務層級組態

本範例說明後端組態選項、包括服務層級和Volume預設值。

```
--
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
apiRegion: us-west2
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    znHczZsr rtHisIsAbOguSaPIKeyAZNchRAGz lzZE4jK3bl /qp8B4Kws8zX5ojY9m
    XsYg6gyxy4zq70lwWgLwGa==
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
  client_id: '123456789012345678901'
  auth uri: https://accounts.google.com/o/oauth2/auth
```

```
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
proxyURL: http://proxy-server-hostname/
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 10Ti
serviceLevel: premium
defaults:
  snapshotDir: 'true'
  snapshotReserve: '5'
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  size: 5Ti
```

### 範例3：虛擬資源池組態

此範例使用 `storage` 來設定虛擬集區和 `StorageClasses` 請回頭參考。請參閱 [\[儲存類別定義\]](#) 以瞭解如何定義儲存類別。

此處會針對所有設定的虛擬資源池設定特定的預設值 `snapshotReserve 5%`和 `exportRule 至 0.00.0/0`。虛擬資源池是在中定義的 `storage` 區段。每個個別虛擬集區都會定義自己的虛擬集區 `serviceLevel``和某些資源池會覆寫預設值。虛擬資源池標籤是用來區分資源池的依據 ``performance`和 `protection`。

[illegible]

```

XsYg6gyxy4zq7OlwWgLwGa==
-----END PRIVATE KEY-----
client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
client_id: '123456789012345678901'
auth_uri: https://accounts.google.com/o/oauth2/auth
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
nfsMountOptions: vers=3,proto=tcp,timeo=600
defaults:
  snapshotReserve: '5'
  exportRule: 0.0.0.0/0
labels:
  cloud: gcp
region: us-west2
storage:
- labels:
  performance: extreme
  protection: extra
  serviceLevel: extreme
  defaults:
    snapshotDir: 'true'
    snapshotReserve: '10'
    exportRule: 10.0.0.0/24
- labels:
  performance: extreme
  protection: standard
  serviceLevel: extreme
- labels:
  performance: premium
  protection: extra
  serviceLevel: premium
  defaults:
    snapshotDir: 'true'
    snapshotReserve: '10'
- labels:
  performance: premium
  protection: standard
  serviceLevel: premium
- labels:
  performance: standard
  serviceLevel: standard

```

下列StorageClass定義適用於虛擬集區組態範例。使用 `parameters.selector`、您可以為每個StorageClass指定用於裝載磁碟區的虛擬集區。該磁碟區會在所選的資源池中定義各個層面。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-extra-protection
provisioner: netapp.io/trident
parameters:
  selector: "performance=extreme; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-standard-protection
provisioner: netapp.io/trident
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium-extra-protection
provisioner: netapp.io/trident
parameters:
  selector: "performance=premium; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium
provisioner: netapp.io/trident
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-standard
provisioner: netapp.io/trident
parameters:
  selector: "performance=standard"
```



```
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extra-protection
provisioner: netapp.io/trident
parameters:
  selector: "protection=extra"
allowVolumeExpansion: true
```

- 第一個StorageClass (cvs-extreme-extra-protection) 對應至第一個虛擬資源池。這是唯一提供極致效能、快照保留率為10%的資源池。
- 最後一個StorageClass (cvs-extra-protection) 撥出提供快照保留10%的任何儲存資源池。Astra Trident決定選取哪個虛擬集區、並確保符合快照保留需求。

### CVS服務類型範例

下列範例提供CVS服務類型的範例組態。

[illegible]

```
auth_uri: https://accounts.google.com/o/oauth2/auth
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
serviceLevel: standardsw
```

## 範例2：儲存資源池組態

此範例後端組態使用 `storagePools` 以設定儲存資源池。

```
---
version: 1
storageDriverName: gcp-cvs
backendName: gcp-std-so-with-pool
projectNumber: '531265380079'
apiRegion: europe-west1
apiKey:
  type: service_account
  project_id: cloud-native-data
  private_key_id: "<id_value>"
  private_key: |-
    -----BEGIN PRIVATE KEY-----
    MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQDaT+Oui9FBAw19
    L1AGEkrYU5xd9K5NlO5jMkIFND5wCD+Nv+jd1GvtFRLaLK5RvXyF5wzvztmODNS+
    qtScpQ+5cFpQkuGtv9U9+N6qtuVYYO3b504Kp5CtqVPJCgMJaK2j8pZTIqUiMum/
    5/Y9oTbZrjAHSMgJm2nHzFq2X0rqVMaHghI6ATm4DOuWx8XGWKTGIPlc0qPqJlqS
    LLaWOH4VIZQZCAyW5IU9p9CAmwqHgdG0uhFNfCgMmED6PBUvVLsLvcq86X+QSWR9k
    ETqElj/sGCenPF7ti1DhGBFafd9hPnxg9PZY29ArEZwY9G/ZjZQX7WPgs0VvxiNR
    DxZRC3GXAgMBAAECggEACn5c59bG/qnVEVI1CwMAalM5M2z09JFhlL1ljKwntNPj
    Vilw2eTW2+UE7HbJru/S7KQgA5Dnn9kvCraEahPRuddUMrD0vG4kTl/IODV6uFuk
    Y0sZfbqd4jMUQ21smvGsqFzwloYWS5qzO1W83ivXH/HW/iqkmY2eW+EPRS/hwSSu
    SscR+SojI7PB0BWSJhlV4yqYf3vcD/D95e12CVHfRCkL85DKumeZ+yHENpiXGZAE
    t8xSs4a50OPm6NHhevCw2a/UQ95/foXNUR450HtbjieJo5o+FF6EYZQGfU2ZHZO8
    37FBKuaJkdGW5xqaI9TL7aqkGkFMF4F2qvOZM+vy8QKBgQD4oVuOkJD1hkTHP86W
    esFlw1kpWyJR9ZA7LI0g/rVpslnX+XdDq0WQf4umDLNau5hYEH9LU6ZSGs1Xk3/B
    NHwR6OXFuqEKNiu83d0zSlHhTy7PZpOZdj5a/vVvQfPDMz7OvsqLRd7YCAbdzuQ0
    +Ahq0Ztwvg0HQ64hdW0ukpYRRwKBgQDgyHj98oqswoYuIa+pPlyS0pPwLmjwKyNm
    /HayzCp+Qjiyy7Tzg8AUqlH1Ou83XbV428jvg7kDhO7PCCKFq+mMmfqHmTpb0Maq
    KpKnZg4ipsqPlyHNNEoRmcailXbwIhCLewMqMrggUiLOmCw4PscL5nK+4GKu2XE1
    jLqjWAZFMQKBgFhkQ9XXRAJ1kR3XpGHOgn890pZOkCVSrqu6aUef/5KY1Fct8ew
    F/+aIxM2iQSVmWQYOvVCnhuY/F2GfAQ7d0om3decuwIOCX/xy7PjHMkLXa2uaZs4
    WR17sLduj62RqXRLX0c0QkwBiNFyHbRcpdkZJQujbYMhBa+7j7SxT4BtAoGAWMWT
    UucocRXZm/pdvz9wteNH3YDwnJLMxm1KC06qMXbBoYrliY4sm3ywJWMC+iCd/H8A
    Gecxd/xVu5mA2L2N3KMq18Zhz8Th0G5DwKyDRJgOQ0Q46yuNXOoYEjlo4Wjyk8Me
    +t1Q8iK98E0UmZnhTgfSpSNElbz2AqnzQ3MN9uECgYAqdvdpVnKGfvdT2ZDjyMoJ
    E89UIC41WjjJGmHsd8W65+3X0RwMzKMT6aZc5tK9J5dHvmWIETnbM+lTImdBbFga
    NWOC6f3r2xbGXHhaWSl+nobpTuvlo56ZRJVvVk7lFMsiddzMuHH8pxfgNJemwA4P
    ThDHCEjv035NNV6KyoO0tA==
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@cloud-native-
  data.iam.gserviceaccount.com
  client_id: '107071413297115343396'
```

```
auth_uri: https://accounts.google.com/o/oauth2/auth
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40cloud-native-data.iam.gserviceaccount.com
storageClass: software
zone: europe-west1-b
network: default
storagePools:
- 1bc7f380-3314-6005-45e9-c7dc8c2d7509
serviceLevel: Standardsw
```

接下來呢？

建立後端組態檔之後、請執行下列命令：

```
tridentctl create backend -f <backend-file>
```

如果後端建立失敗、表示後端組態有問題。您可以執行下列命令來檢視記錄、以判斷原因：

```
tridentctl logs
```

識別並修正組態檔的問題之後、您可以再次執行create命令。

## 設定NetApp HCI 一個不只是功能的SolidFire 後端

瞭解如何在安裝Astra Trident時建立及使用元素後端。

您需要的產品

- 支援的儲存系統、可執行Element軟體。
- 提供給NetApp HCI / SolidFire叢集管理員或租戶使用者的認證、以管理磁碟區。
- 您所有的Kubernetes工作節點都應該安裝適當的iSCSI工具。請參閱 ["工作節點準備資訊"](#)。

您需要知道的資訊

◦ solidfire-san 儲存驅動程式支援兩種Volume模式：檔案和區塊。適用於 Filesystem 磁碟區代碼、Astra Trident會建立磁碟區並建立檔案系統。檔案系統類型由StorageClass指定。

驅動程式	傳輸協定	Volume模式	支援的存取模式	支援的檔案系統
solidfire-san	iSCSI	區塊	rwo、ROX、rwx	無檔案系統。原始區塊裝置。

驅動程式	傳輸協定	Volume模式	支援的存取模式	支援的檔案系統
solidfire-san	iSCSI	區塊	rwo、ROX、rwx	無檔案系統。原始區塊裝置。
solidfire-san	iSCSI	檔案系統	Rwo、ROX	xfs、ext3、ext4
solidfire-san	iSCSI	檔案系統	Rwo、ROX	xfs、ext3、ext4



Astra Trident在做為增強型的csi資源配置程式時使用CHAP。如果您使用的是CHAP（這是「csi」的預設值）、則不需要進一步準備。建議明確設定 UseCHAP 可選擇搭配非csi Trident使用CHAP。否則請參閱 ["請按這裡"](#)。



Volume存取群組僅受Astra Trident的傳統非csi架構支援。當Astra Trident設定為以「csi」模式運作時、會使用CHAP。

否則 AccessGroups 或 UseCHAP 已設定、適用下列其中一項規則：

- 如果是預設值 trident 偵測到存取群組、使用存取群組。
- 如果未偵測到存取群組、且Kubernetes版本為1.7或更新版本、則會使用CHAP。

## 後端組態選項

如需後端組態選項、請參閱下表：

參數	說明	預設
version		永遠為1
storageDriverName	儲存驅動程式名稱	永遠是「solidfire-san」
backendName	自訂名稱或儲存後端	「S指_」+儲存設備（iSCSI）IP位址SolidFire
Endpoint	MVIP、適用於SolidFire 採用租戶認證的不含用戶身分證明的叢集	
SVIP	儲存設備（iSCSI）IP位址和連接埠	
labels	套用到磁碟區的任意JSON-格式化標籤集。	「」
TenantName	要使用的租戶名稱（如果找不到、請建立）	
InitiatorIFace	將iSCSI流量限制在特定的主機介面	「預設」
UseCHAP	使用CHAP驗證iSCSI	是的
AccessGroups	要使用的存取群組ID清單	尋找名為「Trident」的存取群組ID
Types	QoS規格	

參數	說明	預設
limitVolumeSize	如果要求的磁碟區大小高於此值、則資源配置失敗	「」（預設不強制執行）
debugTraceFlags	疑難排解時要使用的偵錯旗標。範例：{"API":假、「方法」:true}	null



請勿使用 debugTraceFlags 除非您正在疑難排解並需要詳細的記錄傾印。

#### 範例1：的後端組態 solidfire-san 三種磁碟區類型的驅動程式

此範例顯示使用CHAP驗證的後端檔案、並建立具有特定QoS保證的三種Volume類型模型。您很可能會定義儲存類別、以便使用來使用這些類別 IOPS 儲存類別參數。

```
---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
SVIP: "<svip>:3260"
TenantName: "<tenant>"
labels:
  k8scluster: dev1
  backend: dev1-element-cluster
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000
```

#### 範例2：的後端與儲存類別組態 solidfire-san 驅動程式與虛擬資源池

此範例顯示使用虛擬資源池設定的後端定義檔、以及參照這些資源池的StorageClass。

Astra Trident會在資源配置時、將儲存資源池上的標籤複製到後端儲存LUN。為了方便起見、儲存管理員可以針對每個虛擬資源池定義標籤、並依標籤將磁碟區分組。

在下圖所示的範例後端定義檔中、會針對所有設定的儲存資源池設定特定的預設值 `type` 銀級。虛擬資源池是在中定義的 `storage` 區段。在此範例中、有些儲存資源池會設定自己的類型、有些資源池則會覆寫上述設定的預設值。

```
---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
SVIP: "<svip>:3260"
TenantName: "<tenant>"
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000
type: Silver
labels:
  store: solidfire
  k8scluster: dev-1-cluster
region: us-east-1
storage:
- labels:
    performance: gold
    cost: '4'
  zone: us-east-1a
  type: Gold
- labels:
    performance: silver
    cost: '3'
  zone: us-east-1b
  type: Silver
```



```
- labels:
  performance: bronze
  cost: '2'
  zone: us-east-1c
  type: Bronze
- labels:
  performance: silver
  cost: '1'
  zone: us-east-1d
```

下列StorageClass定義是指上述虛擬資源池。使用 `parameters.selector` 欄位中、每個StorageClass會呼叫哪些虛擬資源池可用於裝載Volume。磁碟區將會在所選的虛擬資源池中定義各個層面。

第一個StorageClass (`solidfire-gold-four`) 將對應至第一個虛擬資源池。這是唯一提供黃金級效能的資源池 Volume Type QoS 金級。最後一個StorageClass (`solidfire-silver`) 撥出任何提供銀級效能的儲存資源池。Astra Trident將決定選取哪個虛擬集區、並確保符合儲存需求。

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-gold-four
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold; cost=4"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-three
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=3"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-bronze-two
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze; cost=2"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-one
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=1"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
  fsType: "ext4"

```

如需詳細資訊、請參閱

- ["Volume存取群組"](#)

## 使用ONTAP SAN驅動程式設定後端

深入瞭解如何使用ONTAP 支援功能的功能和功能性SAN驅動程式來設定功能性的後端。ONTAP Cloud Volumes ONTAP

- ["準備"](#)
- ["組態與範例"](#)

Astra Control可為使用建立的磁碟區提供無縫保護、災難恢復和移動性（在Kubernetes叢集之間移動磁碟區） `ontap-nas`、`ontap-nas-flexgroup`和 `ontap-san` 驅動程式：請參閱 ["Astra Control複寫先決條件"](#) 以取得詳細資料。



- 您必須使用 `ontap-nas` 適用於需要資料保護、災難恢復和行動力的正式作業工作負載。
- 使用 `ontap-san-economy` 當預期的Volume使用量將遠高於ONTAP 支援的容量時。
- 使用 `ontap-nas-economy` 只有在預期的Volume使用量會比ONTAP 支援的高出許多、以及 `ontap-san-economy` 無法使用驅動程式。
- 請勿使用 `ontap-nas-economy` 如果您預期需要資料保護、災難恢復或行動性、

### 使用者權限

Astra Trident希望以ONTAP 支援的形式執行、通常是以支援的方式執行 `admin` 叢集使用者或 `vsadmin` SVM使用者、或具有相同角色之不同名稱的使用者。對於Amazon FSX for NetApp ONTAP 支援的NetApp功能、Astra Trident預期會以ONTAP 使用叢集的形式執行、以執行支援或SVM管理員的身分 `fsxadmin` 使用者或 `vsadmin` SVM使用者、或具有相同角色之不同名稱的使用者。。 `fsxadmin` 使用者是叢集管理使用者的有限替代。



如果您使用 `limitAggregateUsage` 參數：需要叢集管理權限。當使用Amazon FSX for NetApp ONTAP 時、搭配Astra Trident `limitAggregateUsage` 參數無法搭配使用 `vsadmin` 和 `fsxadmin` 使用者帳戶：如果您指定此參數、組態作業將會失敗。

雖然可以在ONTAP 功能區內建立更嚴格的角色、讓Trident驅動程式能夠使用、但我們不建議您這麼做。Trident的大多數新版本都會呼叫額外的API、而這些API必須納入考量、使升級變得困難且容易出錯。

### 準備使用ONTAP 支援的SAN驅動程式來設定後端

瞭解如何準備使用ONTAP 支援不支援的SAN驅動程式來設定支援功能的後端。ONTAP對於所有ONTAP 的不支援端點、Astra Trident至少需要指派一個集合體給SVM。

請記住、您也可以執行多個驅動程式、並建立指向一個或多個驅動程式的儲存類別。例如、您可以設定 `san-dev` 使用的類別 `ontap-san` 驅動程式與 `san-default` 使用的類別 `ontap-san-economy` 一、

您所有的Kubernetes工作節點都必須安裝適當的iSCSI工具。請參閱 ["請按這裡"](#) 以取得更多詳細資料。

## 驗證

Astra Trident提供兩種驗證ONTAP 證功能來驗證支援的後端。

- 認證型：ONTAP 對具備所需權限的使用者名稱和密碼。建議使用預先定義的安全登入角色、例如 admin 或 vsadmin 以確保與ONTAP 更新版本的最大相容性。
- 憑證型：Astra Trident也能ONTAP 使用安裝在後端的憑證與某個叢集進行通訊。在此處、後端定義必須包含用戶端憑證、金鑰及信任的CA憑證（建議使用）的Base64編碼值。

您可以更新現有的後端、以便在認證型和憑證型方法之間移動。不過、一次只支援一種驗證方法。若要切換至不同的驗證方法、您必須從後端組態中移除現有方法。



如果您嘗試同時提供\*認證與認證\*、後端建立將會失敗、並在組態檔中提供多種驗證方法。

### 啟用認證型驗證

Astra Trident需要SVM範圍/叢集範圍管理員的認證資料、才能與ONTAP 該後端進行通訊。建議使用預先定義的標準角色、例如 admin 或 vsadmin。這可確保與未來ONTAP 的支援版本保持前瞻相容、因為未來的Astra Trident版本可能會使用功能API。您可以建立自訂的安全登入角色、並與Astra Trident搭配使用、但不建議使用。

後端定義範例如下所示：

#### YAML

```
版本： 1 個後端名稱： ExampleBackend storageDriverName : ONTAP-SAN 管理 LIF : 10.0.0.1 SVM : SVM_NFS 使用者名稱： vsadmin 密碼：密碼
```

#### JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password"
}
```

請記住、後端定義是唯一以純文字儲存認證的位置。建立後端之後、使用者名稱/密碼會以Base64編碼、並儲存為Kubernetes機密。建立或更新後端是唯一需要具備認證知識的步驟。因此、這是一項純管理員操作、由Kubernetes /儲存管理員執行。

### 啟用憑證型驗證

新的和現有的後端可以使用憑證、並與ONTAP 該後端通訊。後端定義需要三個參數。

- 用戶端憑證：用戶端憑證的Base64編碼值。
- 用戶端私密金鑰：關聯私密金鑰的Base64編碼值。
- 信任的CACertificate：受信任CA憑證的Base64編碼值。如果使用信任的CA、則必須提供此參數。如果未使用信任的CA、則可忽略此問題。

典型的工作流程包括下列步驟。

#### 步驟

1. 產生用戶端憑證和金鑰。產生時、請將Common Name (CN) (一般名稱 (CN)) 設定為ONTAP 驗證身分。

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=admin"
```

2. 將信任的CA憑證新增ONTAP 至整個叢集。這可能已由儲存管理員處理。如果未使用信任的CA、請忽略。

```
security certificate install -type server -cert-name <trusted-ca-cert-
name> -vserver <vserver-name>
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled
true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca
<cert-authority>
```

3. 在ONTAP 支援叢集上安裝用戶端憑證和金鑰 (步驟1)。

```
security certificate install -type client-ca -cert-name <certificate-
name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

4. 確認ONTAP 支援的不安全登入角色 cert 驗證方法。

```
security login create -user-or-group-name admin -application ontapi
-authentication-method cert
security login create -user-or-group-name admin -application http
-authentication-method cert
```

5. 使用產生的憑證測試驗證。以ONTAP Management LIF IP和SVM名稱取代<SfManagement LIF>和<vserver name>。

```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns="http://www.netapp.com/filer/admin" version="1.21"
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

## 6. 使用Base64編碼憑證、金鑰和信任的CA憑證。

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

## 7. 使用從上一步取得的值建立後端。

```
cat cert-backend.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuueeeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "trustedCACertificate": "QNFinfO...SiqOyN",
  "storagePrefix": "myPrefix_"
}

tridentctl create backend -f cert-backend.json -n trident
+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                      UUID                      |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |         0 |
+-----+-----+-----+-----+
+-----+-----+
```

## 更新驗證方法或旋轉認證資料

您可以更新現有的後端、以使用不同的驗證方法或旋轉其認證資料。這兩種方法都可行：使用使用者名稱/密碼的後端可更新以使用憑證；使用憑證的後端可更新為使用者名稱/密碼。若要這麼做、您必須移除現有的驗證方

法、然後新增驗證方法。然後使用更新的backend.json檔案、其中包含要執行的必要參數 tridentctl backend update。

```
cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "password",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend SanBackend -f cert-backend-updated.json -n
trident

+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                      UUID                      |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |          9 |
+-----+-----+-----+-----+
+-----+-----+
```



當您旋轉密碼時、儲存管理員必須先更新ONTAP 使用者的密碼（位於BIOS）。接著是後端更新。在循環憑證時、可將多個憑證新增至使用者。然後更新後端以使用新的憑證、之後可從ONTAP 該叢集刪除舊的憑證。

更新後端不會中斷對已建立之磁碟區的存取、也不會影響之後建立的磁碟區連線。成功的後端更新顯示Astra Trident可以與ONTAP 該後端通訊、並處理未來的Volume作業。

#### 指定igroup

Astra Trident使用igroup來控制其所配置的磁碟區（LUN）存取。系統管理員在指定後端的igroup時有兩種選擇：

- Astra Trident可自動建立及管理每個後端的igroup。如果 igroupName 未包含在後端定義中、Astra Trident 會建立名為的igroup trident-<backend-UUID> 在SVM上。如此可確保每個後端都有專屬的igroup、並處理Kubernetes節點IQN的自動新增/刪除作業。
- 或者、也可以在後端定義中提供預先建立的igroup。您可以使用來完成此作業 igroupName 組態參數。Astra Trident會將Kubernetes節點IQN新增/刪除至預先存在的igroup。

適用於具有後端 `igroupName` 定義 `igroupName` 可以使用刪除 `tridentctl backend update` 使用 Astra Trident 自動處理 `igroup`。這不會中斷對已附加至工作負載之磁碟區的存取。未來的連線將使用建立的 `igroup` Astra Trident 來處理。



針對每個獨特的 Astra Trident 執行個體指定 `igroup` 是最適合 Kubernetes 管理員和儲存管理員的最佳實務做法。「csi Trident」可自動新增及移除 `igroup` 的叢集節點 IQN、大幅簡化其管理。在 Kubernetes 環境中使用相同的 SVM（以及 Astra Trident 安裝）時、使用專屬的 `igroup` 可確保對 Kubernetes 叢集所做的變更不會影響與其他叢集相關的 `igroup`。此外、也必須確保 Kubernetes 叢集中的每個節點都有唯一的 IQN。如上所述、Astra Trident 會自動處理 IQN 的新增與移除。重複使用主機間的 IQN 可能會導致主機彼此誤用、並拒絕存取 LUN 的不良情況。

如果將 Astra Trident 設定為使用「csi 資源配置程式」、則 Kubernetes 節點 IQN 會自動新增至 `igroup` 或從其中移除。當節點新增至 Kubernetes 叢集時、`trident-csi` 示範集部署 Pod (`trident-csi-xxxxxx` 在 23.01 或之前的版本中 `trident-node<operating system>-xxxx` 在 23.01 及更新版本中)、登錄新增的節點、然後登錄可附加磁碟區的新節點。節點 IQN 也會新增至後端的 `igroup`。當節點封鎖、排放及從 Kubernetes 刪除時、類似的一組步驟可處理刪除 IQN。

如果 Astra Trident 並未以 csi 資源配置程式的形式執行、則必須手動更新 `igroup`、以包含 Kubernetes 叢集中每個工作節點的 iSCSI IQN。加入 Kubernetes 叢集的節點 IQN 必須新增至 `igroup`。同樣地、從 Kubernetes 叢集移除的節點 IQN 也必須從 `igroup` 移除。

#### 使用雙向 CHAP 驗證連線

Astra Trident 可以使用雙向 CHAP 驗證 iSCSI 工作階段 `ontap-san` 和 `ontap-san-economy` 驅動程式：這需要啟用 `useCHAP` 選項。設定為時 `true` Astra Trident 將 SVM 的預設啟動器安全性設定為雙向 CHAP、並從後端檔案設定使用者名稱和機密。NetApp 建議使用雙向 CHAP 來驗證連線。請參閱下列組態範例：

```
---
version: 1
storageDriverName: ontap-san
backendName: ontap_san_chap
managementLIF: 192.168.0.135
svm: ontap_iscsi_svm
useCHAP: true
username: vsadmin
password: password
igroupName: trident
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
```



。 `useCHAP` 參數是布林選項、只能設定一次。預設值設為假。將其設為 `true` 之後、您就無法將其設為假。

此外 `useCHAP=true`、`chapInitiatorSecret`、`chapTargetInitiatorSecret`、`chapTargetUsername` 和 `chapUsername` 欄位必須包含在後端定義中。執行建立後端後端之後、即可變更機密資訊 `tridentctl update`。



## 運作方式

透過設定 `useCHAP` 為真、儲存管理員指示Astra Trident在儲存後端上設定CHAP。這包括下列項目：

- 在SVM上設定CHAP：
  - 如果SVM的預設啟動器安全性類型為無（預設設定）和、則磁碟區中沒有已存在的預先存在LUN、Astra Trident會將預設安全性類型設為 `CHAP` 並繼續設定CHAP啟動器和目標使用者名稱和機密。
  - 如果SVM包含LUN、Astra Trident將不會在SVM上啟用CHAP。如此可確保不限制存取SVM上已存在的LUN。
- 設定CHAP啟動器和目標使用者名稱和機密；這些選項必須在後端組態中指定（如上所示）。
- 管理新增的啟動器至 `igroupName` 在後端中提供。如果未指定、則預設為 `trident`。

建立後端之後、Astra Trident會建立對應的 `tridentbackend` 將CHAP機密與使用者名稱儲存為Kubernetes機密。由Astra Trident在此後端上建立的所有PV、都會掛載並附加於CHAP上。

## 旋轉認證資料並更新後端

您可以更新中的CHAP參數來更新CHAP認證 `backend.json` 檔案：這需要更新CHAP機密並使用 `tridentctl update` 命令以反映這些變更。



更新後端的CHAP機密時、您必須使用 `tridentctl` 以更新後端。請勿透過CLI/ONTAP UI更新儲存叢集上的認證資料、因為Astra Trident無法接受這些變更。

```

cat backend-san.json
{
    "version": 1,
    "storageDriverName": "ontap-san",
    "backendName": "ontap_san_chap",
    "managementLIF": "192.168.0.135",
    "svm": "ontap_iscsi_svm",
    "useCHAP": true,
    "username": "vsadmin",
    "password": "password",
    "igroupName": "trident",
    "chapInitiatorSecret": "cl9qxUpDaTeD",
    "chapTargetInitiatorSecret": "rqxigXgkeUpDaTeD",
    "chapTargetUsername": "iJF4heBRT0TCwxyz",
    "chapUsername": "uh2aNCLSD6cNwxyz",
}

./tridentctl update backend ontap_san_chap -f backend-san.json -n trident
+-----+-----+-----+-----+
+-----+-----+
|  NAME          | STORAGE DRIVER |                               UUID                               |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| ontap_san_chap | ontap-san      | aa458f3b-ad2d-4378-8a33-1a472ffbeb5c |
online |      7 |
+-----+-----+-----+-----+
+-----+-----+

```

現有的連線不會受到影響；如果SVM上的Astra Trident更新認證、它們將繼續保持作用中狀態。新連線將使用更新的認證資料、而現有連線仍保持作用中狀態。中斷舊PV的連線並重新連線、將會使用更新的認證資料。

## SAN組態選項與範例ONTAP

瞭解如何透過ONTAP Astra Trident安裝來建立及使用支援NetApp的SAN驅動程式。本節提供後端組態範例、以及如何將後端對應至StorageClass的詳細資料。

後端組態選項

如需後端組態選項、請參閱下表：

參數	說明	預設
version		永遠為1

參數	說明	預設
storageDriverName	儲存驅動程式名稱	「ONTAP-NAS」、「ONTAP-NAS-節約 型」、「ONTAP-NAS-flexgroup」、「ONTAP-SAN」、「ONTAP-san經濟型」
backendName	自訂名稱或儲存後端	驅動程式名稱+「_」+ dataLIF
managementLIF	叢集的IP位址或SVM管理LIF若要順暢MetroCluster 切換、您必須指定SVM管理LIF。您可以指定完整網域名稱（FQDN）。如果使用安裝Astra Trident、則可設定使用IPv6位址 --use-ipv6 旗標。IPv6位址必須以方括弧來定義、例如[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。	「10.0.0.1」、「[2001:1234:abcd:::fefo]」
dataLIF	傳輸協定LIF的IP位址。請勿指定iSCSI。Astra Trident的用途 " <a href="#">可選擇的LUN對應ONTAP</a> " 探索建立多重路徑工作階段所需的iSCSI LIF。如果發生此情況、將會產生警告 dataLIF 已明確定義。	源自SVM
useCHAP	使用CHAP驗證iSCSI以供ONTAP支援不支援的SAN驅動程式使用[布林值]。設定為 true 用於Astra Trident設定及使用雙向CHAP做為後端SVM的預設驗證。請參閱 " <a href="#">準備使用ONTAP 支援的SAN驅動程式來設定後端</a> " 以取得詳細資料。	錯
chapInitiatorSecret	CHAP啟動器密碼。必要條件 useCHAP=true	「」
labels	套用到磁碟區的任意JSON-格式化標籤集	「」
chapTargetInitiatorSecret	CHAP目標啟動器機密。必要條件 useCHAP=true	「」
chapUsername	傳入使用者名稱。必要條件 useCHAP=true	「」
chapTargetUsername	目標使用者名稱。必要條件 useCHAP=true	「」
clientCertificate	用戶端憑證的Base64編碼值。用於憑證型驗證	「」
clientPrivateKey	用戶端私密金鑰的Base64編碼值。用於憑證型驗證	「」
trustedCACertificate	受信任CA憑證的Base64編碼值。選用。用於憑證型驗證。	「」

參數	說明	預設
username	與ONTAP 該叢集通訊所需的使用者名稱。用於認證型驗證。	「」
password	與ONTAP 該叢集通訊所需的密碼。用於認證型驗證。	「」
svm	要使用的儲存虛擬機器	如果是SVM則衍生 managementLIF 已指定
igroupName	要使用之SAN磁碟區的igroup名稱。請參閱 以取得更多資訊。	「Trident -<後端-UUID>」
storagePrefix	在SVM中配置新磁碟區時所使用的前置碼。稍後無法修改。若要更新此參數、您需要建立新的後端。	「Trident」
limitAggregateUsage	如果使用率高於此百分比、則無法進行資源配置。如果您使用Amazon FSX for NetApp ONTAP Sendbackend、請勿指定 limitAggregateUsage。提供的 fsxadmin 和 vsadmin 請勿包含擷取Aggregate使用量所需的權限、並使用Astra Trident加以限制。	「」（預設不強制執行）
limitVolumeSize	如果要求的磁碟區大小高於此值、則資源配置失敗。也會限制其管理的qtree和LUN磁碟區大小上限。	「」（預設不強制執行）
lunsPerFlexvol	每FlexVol 個LUN的最大LUN數量、範圍必須在[50、200]	「100」
debugTraceFlags	疑難排解時要使用的偵錯旗標。例如、除非您正在疑難排解並需要詳細的記錄傾印、否則請勿使用 { "API": 假、 "method": true } 。	null
useREST	使用ONTAP Isrest API的布林參數。技術預覽 useREST 以*技術預覽*的形式提供、建議用於測試環境、而非用於正式作業工作負載。設定為時 true、Astra Trident將使用ONTAP 靜止API與後端進行通訊。此功能需要ONTAP 使用更新版本的版本。此外ONTAP 、所使用的登入角色必須能夠存取 ontap 應用程式：這是預先定義的 vsadmin 和 cluster-admin 角色： useREST 不支援MetroCluster 使用支援。	錯

## 詳細資料 igroupName

igroupName 可設定為ONTAP 已在叢集上建立的igroup。如果未指定、Astra Trident會自動建立名為的igroup trident-`<backend-UUID>`。

如果提供預先定義的igroupName、我們建議每個Kubernetes叢集使用一個igroup、如果要在不同環境之間共用SVM。這是Astra Trident自動維護IQN新增與刪除作業所必需的。

- igroupName 可更新以指向在Astra Trident以外的SVM上建立及管理的新igroup。
- igroupName 可省略。在此案例中、Astra Trident將建立並管理名為的igroup trident-`<backend-UUID>` 自動：

在這兩種情況下、仍可繼續存取Volume附件。未來的Volume附件將使用更新的igroup。此更新不會中斷對後端磁碟區的存取。

## 用於資源配置磁碟區的後端組態選項

您可以使用中的這些選項來控制預設資源配置 defaults 組態區段。如需範例、請參閱下列組態範例。

參數	說明	預設
spaceAllocation	LUN的空間分配	「真的」
spaceReserve	空間保留模式；「無」（精簡）或「Volume」（完整）	「無」
snapshotPolicy	要使用的Snapshot原則	「無」
qosPolicy	要指派給所建立磁碟區的QoS原則群組。選擇每個儲存集區/後端的其中一個qosPolicy或adaptiveQosPolicy。搭配Astra Trident使用QoS原則群組需要ONTAP 使用更新版本的版本。我們建議使用非共用的QoS原則群組、並確保原則群組會個別套用至每個組成群組。共享的QoS原則群組將強制所有工作負載的總處理量上限。	「」
adaptiveQosPolicy	要指派給所建立磁碟區的調適性QoS原則群組。選擇每個儲存集區/後端的其中一個qosPolicy或adaptiveQosPolicy	「」
snapshotReserve	保留給快照「0」的磁碟區百分比	如果 snapshotPolicy 為「無」、否則為「」
splitOnClone	建立複本時、從其父複本分割複本	「假」

參數	說明	預設
encryption	在新磁碟區上啟用NetApp Volume Encryption (NVE) ；預設為 false。必須在叢集上授權並啟用NVE、才能使用此選項。如果在後端啟用NAE、則Astra Trident中配置的任何磁碟區都會啟用NAE。如需詳細資訊、請參閱： <a href="#">"Astra Trident如何與NVE和NAE搭配運作"</a> 。	「假」
luksEncryption	啟用LUKS加密。請參閱 <a href="#">"使用Linux 統一金鑰設定 (LUKS)"</a> 。	"
securityStyle	新磁碟區的安全樣式	unix
tieringPolicy	分層原則以使用「無」	ONTAP 9.5之前的SVM-DR組態為「純快照」

## Volume資源配置範例

以下是已定義預設值的範例：

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: trident_svm
username: admin
password: password
labels:
  k8scluster: dev2
  backend: dev2-sanbackend
storagePrefix: alternate-trident
igroupName: custom
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: standard
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```



針對使用建立的所有Volume `ontap-san` 驅動程式Astra Trident在FlexVol 支援LUN中繼資料的過程中、額外增加10%的容量。LUN的配置大小與使用者在PVC中要求的大小完全相同。Astra Trident在FlexVol 整個過程中增加10%的速度（顯示ONTAP 在畫面上可用的尺寸）。使用者現在可以取得所要求的可用容量。此變更也可防止LUN成為唯讀、除非可用空間已充分利用。這不適用於ONTAP-san經濟型。

用於定義的後端 `snapshotReserve`、Astra Trident會依照下列方式計算Volume大小：

```
Total volume size = [(PVC requested size) / (1 - (snapshotReserve
percentage) / 100)] * 1.1
```

1.1是額外10%的Astra Trident加入FlexVol 到the支援LUN中繼資料的功能。適用於 `snapshotReserve = 5%`、而PVC要求= 5GiB、磁碟區總大小為5.79GiB、可用大小為5.5GiB。。 `volume show` 命令應顯示類似以下範例的結果：

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
		_pvc_89f1c156_3801_4de4_9f9d_034d54c395f4	online	RW	10GB	5.00GB	0%
		_pvc_e42ec6fe_3baa_4af6_996d_134adbbb8e6d	online	RW	5.79GB	5.50GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

3 entries were displayed.

目前、只有調整大小、才能將新計算用於現有的Volume。

最低組態範例

下列範例顯示基本組態、讓大部分參數保留預設值。這是定義後端最簡單的方法。



如果您在NetApp ONTAP 支援Astra Trident的NetApp上使用Amazon FSX、建議您指定lifs的DNS名稱、而非IP位址。

`ontap-san` 具有憑證型驗證的驅動程式

這是最小的後端組態範例。 `clientCertificate`、`clientPrivateKey`和 `trustedCACertificate`（選用、如果使用信任的CA）會填入 `backend.json` 並分別取得用戶端憑證、私密金鑰及信任CA憑證的基礎64編碼值。

```

---
version: 1
storageDriverName: ontap-san
backendName: DefaultSANBackend
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
igroupName: trident
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz

```

ontap-san 使用雙向**CHAP**的驅動程式

這是最小的後端組態範例。此基本組態會建立 ontap-san 後端 useCHAP 設定為 true。

```

---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
igroupName: trident
username: vsadmin
password: password

```

ontap-san-economy 驅動程式



```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
igroupName: trident
username: vsadmin
password: password
```

#### 虛擬集區的後端範例

在下圖所示的範例後端定義檔案中、會針對所有儲存資源池設定特定的預設值、例如 `spaceReserve` 無、`spaceAllocation` 假、和 `encryption` 錯。虛擬資源池是在儲存區段中定義的。

Astra Trident會在「Comments」欄位中設定資源配置標籤。請在FlexVol The過程中提出意見。Astra Trident會在資源配置時、將虛擬資源池上的所有標籤複製到儲存磁碟區。為了方便起見、儲存管理員可以針對每個虛擬資源池定義標籤、並依標籤將磁碟區分組。

在此範例中、有些儲存資源池會自行設定 `spaceReserve`、`spaceAllocation` 和 `encryption` 值、部分集區會覆寫上述設定的預設值。

```

---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
igroupName: trident
username: vsadmin
password: password
defaults:
  spaceAllocation: 'false'
  encryption: 'false'
  qosPolicy: standard
labels:
  store: san_store
  kubernetes-cluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  protection: gold
  creditpoints: '40000'
  zone: us_east_1a
  defaults:
    spaceAllocation: 'true'
    encryption: 'true'
    adaptiveQosPolicy: adaptive-extreme
- labels:
  protection: silver
  creditpoints: '20000'
  zone: us_east_1b
  defaults:
    spaceAllocation: 'false'
    encryption: 'true'
    qosPolicy: premium
- labels:
  protection: bronze
  creditpoints: '5000'
  zone: us_east_1c
  defaults:
    spaceAllocation: 'true'
    encryption: 'false'

```

以下是的iSCSI範例 ontap-san-economy 驅動程式：

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
igroupName: trident
username: vsadmin
password: password
defaults:
  spaceAllocation: 'false'
  encryption: 'false'
labels:
  store: san_economy_store
  region: us_east_1
storage:
- labels:
  app: oracledb
  cost: '30'
  zone: us_east_1a
  defaults:
    spaceAllocation: 'true'
    encryption: 'true'
- labels:
  app: postgresdb
  cost: '20'
  zone: us_east_1b
  defaults:
    spaceAllocation: 'false'
    encryption: 'true'
- labels:
  app: mysqldb
  cost: '10'
  zone: us_east_1c
  defaults:
    spaceAllocation: 'true'
    encryption: 'false'
```

## 將後端對應至StorageClass

下列StorageClass定義是指上述虛擬資源池。使用 `parameters.selector` 欄位中、每個StorageClass會呼叫哪些虛擬資源池可用於裝載Volume。磁碟區將會在所選的虛擬資源池中定義各個層面。

- 第一個StorageClass (`protection-gold`) 將對應至中的第一個、第二個虛擬集區 `ontap-nas-flexgroup` 後端和中的第一個虛擬集區 `ontap-san` 後端：這是唯一提供金級保護的資源池。
- 第二個StorageClass (`protection-not-gold`) 將對應至中的第三、第四個虛擬集區 `ontap-nas-flexgroup` 中的後端和第二個、第三個虛擬集區 `ontap-san` 後端：這是唯一提供金級以外保護層級的資源池。
- 第三個StorageClass (`app-mysqldb`) 將對應至中的第四個虛擬資源池 `ontap-nas` 中的後端和第三個虛擬集區 `ontap-san-economy` 後端：這些是唯一提供mysqldb類型應用程式儲存池組態的集區。
- 第四個StorageClass (`protection-silver-creditpoints-20k`) 將對應至中的第三個虛擬集區 `ontap-nas-flexgroup` 中的後端和第二個虛擬集區 `ontap-san` 後端：這些資源池是唯一能以20000個信用點數提供金級保護的資源池。
- 第五個StorageClass (`creditpoints-5k`) 將對應至中的第二個虛擬資源池 `ontap-nas-economy` 中的後端和第三個虛擬集區 `ontap-san` 後端：這些是唯一提供5000個信用點數的資源池產品。

Astra Trident將決定選取哪個虛擬集區、並確保符合儲存需求。

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: netapp.io/trident
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: netapp.io/trident
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: netapp.io/trident
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

## 設定ONTAP 一個靜態NAS後端

深入瞭解如何使用ONTAP 功能性和功能性NAS驅動程式來設定功能性的後端。ONTAP Cloud Volumes ONTAP

- ["準備"](#)
- ["組態與範例"](#)

Astra Control可為使用建立的磁碟區提供無縫保護、災難恢復和移動性（在Kubernetes叢集之間移動磁碟區） `ontap-nas`、`ontap-nas-flexgroup`和 `ontap-san` 驅動程式：請參閱 ["Astra Control複寫先決條件"](#) 以取得詳細資料。



- 您必須使用 `ontap-nas` 適用於需要資料保護、災難恢復和行動力的正式作業工作負載。
- 使用 `ontap-san-economy` 當預期的Volume使用量將遠高於ONTAP 支援的容量時。
- 使用 `ontap-nas-economy` 只有在預期的Volume使用量會比ONTAP 支援的高出許多、以及 `ontap-san-economy` 無法使用驅動程式。
- 請勿使用 `ontap-nas-economy` 如果您預期需要資料保護、災難恢復或行動性、

### 使用者權限

Astra Trident希望以ONTAP 支援的形式執行、通常是以支援的方式執行 `admin` 叢集使用者或 `vsadmin` SVM使用者、或具有相同角色之不同名稱的使用者。對於Amazon FSX for NetApp ONTAP 支援的NetApp功能、Astra Trident預期會以ONTAP 使用叢集的形式執行、以執行支援或SVM管理員的身分 `fsxadmin` 使用者或 `vsadmin` SVM使用者、或具有相同角色之不同名稱的使用者。 `fsxadmin` 使用者是叢集管理使用者的有限替代。



如果您使用 `limitAggregateUsage` 參數：需要叢集管理權限。當使用Amazon FSX for NetApp ONTAP 時、搭配Astra Trident `limitAggregateUsage` 參數無法搭配使用 `vsadmin` 和 `fsxadmin` 使用者帳戶：如果您指定此參數、組態作業將會失敗。

雖然可以在ONTAP 功能區內建立更嚴格的角色、讓Trident驅動程式能夠使用、但我們不建議您這麼做。Trident 的大多數新版本都會呼叫額外的API、而這些API必須納入考量、使升級變得困難且容易出錯。

### 準備使用ONTAP 不含NAS的驅動程式來設定後端

瞭解如何準備使用ONTAP 不含NetApp功能的NAS驅動程式來設定功能完善的後端。ONTAP對於所有ONTAP 的不支援端點、Astra Trident至少需要指派一個集合體給SVM。

對於所有ONTAP 的不支援端點、Astra Trident至少需要指派一個集合體給SVM。

請記住、您也可以執行多個驅動程式、並建立指向一個或多個驅動程式的儲存類別。例如、您可以設定使用的Gold類別 `ontap-nas` 驅動程式和銅級、使用 `ontap-nas-economy` 一、

您所有的Kubernetes工作節點都必須安裝適當的NFS工具。請參閱 ["請按這裡"](#) 以取得更多詳細資料。

### 驗證

Astra Trident提供兩種驗證ONTAP 證功能來驗證支援的後端。

- 認證型：ONTAP 對具備所需權限的使用者名稱和密碼。建議使用預先定義的安全登入角色、例如 `admin` 或 `vsadmin` 以確保與ONTAP 更新版本的最大相容性。

- 憑證型：Astra Trident也能ONTAP 使用安裝在後端的憑證與某個叢集進行通訊。在此處、後端定義必須包含用戶端憑證、金鑰及信任的CA憑證（建議使用）的Base64編碼值。

您可以更新現有的後端、以便在認證型和憑證型方法之間移動。不過、一次只支援一種驗證方法。若要切換至不同的驗證方法、您必須從後端組態中移除現有方法。



如果您嘗試同時提供\*認證與憑證\*、後端建立將會失敗、並在組態檔中提供多種驗證方法。

### 啟用認證型驗證

Astra Trident需要SVM範圍/叢集範圍管理員的認證資料、才能與ONTAP 該後端進行通訊。建議使用預先定義的標準角色、例如 `admin` 或 `vsadmin`。這可確保與未來ONTAP 的支援版本保持前瞻相容、因為未來的Astra Trident版本可能會使用功能API。您可以建立自訂的安全登入角色、並與Astra Trident搭配使用、但不建議使用。

後端定義範例如下所示：

#### YAML

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

#### JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password"
}
```

請記住、後端定義是唯一以純文字儲存認證的位置。建立後端之後、使用者名稱/密碼會以Base64編碼、並儲存為Kubernetes機密。建立/更新後端是唯一需要知道認證資料的步驟。因此、這是一項純管理員操作、由Kubernetes /儲存管理員執行。

## 啟用憑證型驗證

新的和現有的後端可以使用憑證、並與ONTAP 該後端通訊。後端定義需要三個參數。

- 用戶端憑證：用戶端憑證的Base64編碼值。
- 用戶端私密金鑰：關聯私密金鑰的Base64編碼值。
- 信任的CACertificate：受信任CA憑證的Base64編碼值。如果使用信任的CA、則必須提供此參數。如果未使用信任的CA、則可忽略此問題。

典型的工作流程包括下列步驟。

### 步驟

1. 產生用戶端憑證和金鑰。產生時、請將Common Name (CN) (一般名稱 (CN)) 設定為ONTAP 驗證身分。

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key  
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=vsadmin"
```

2. 將信任的CA憑證新增ONTAP 至整個叢集。這可能已由儲存管理員處理。如果未使用信任的CA、請忽略。

```
security certificate install -type server -cert-name <trusted-ca-cert-name> -vserver <vserver-name>  
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled  
true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca  
<cert-authority>
```

3. 在ONTAP 支援叢集上安裝用戶端憑證和金鑰 (步驟1) 。

```
security certificate install -type client-ca -cert-name <certificate-name> -vserver <vserver-name>  
security ssl modify -vserver <vserver-name> -client-enabled true
```

4. 確認ONTAP 支援的不安全登入角色 cert 驗證方法。

```
security login create -user-or-group-name vsadmin -application ontapi  
-authentication-method cert -vserver <vserver-name>  
security login create -user-or-group-name vsadmin -application http  
-authentication-method cert -vserver <vserver-name>
```

5. 使用產生的憑證測試驗證。以ONTAP Management LIF IP和SVM名稱取代<SfManagement LIF>和<vserver name>。您必須確保LIF的服務原則設定為 default-data-management。



```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns="http://www.netapp.com/filer/admin" version="1.21"
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

## 6. 使用Base64編碼憑證、金鑰和信任的CA憑證。

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

## 7. 使用從上一步取得的值建立後端。

```
cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident

+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                      UUID                      |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |          9 |
+-----+-----+-----+-----+
+-----+-----+
```

## 更新驗證方法或旋轉認證資料

您可以更新現有的後端、以使用不同的驗證方法或旋轉其認證資料。這兩種方法都可行：使用使用者名稱/密碼的後端可更新以使用憑證；使用憑證的後端可更新為使用者名稱/密碼。若要這麼做、您必須移除現有的驗證方法、然後新增驗證方法。然後使用更新的backend.json檔案、其中包含要執行的必要參數 `tridentctl update backend`。

```
cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "password",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                      UUID                      |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |      9 |
+-----+-----+-----+-----+
+-----+-----+
```



當您旋轉密碼時、儲存管理員必須先更新ONTAP 使用者的密碼（位於BIOS）。接著是後端更新。在循環憑證時、可將多個憑證新增至使用者。然後更新後端以使用新的憑證、之後可從ONTAP 該叢集刪除舊的憑證。

更新後端不會中斷對已建立之磁碟區的存取、也不會影響之後建立的磁碟區連線。成功的後端更新顯示Astra Trident可以與ONTAP 該後端通訊、並處理未來的Volume作業。

## 管理NFS匯出原則

Astra Trident使用NFS匯出原則來控制其所配置之磁碟區的存取。

使用匯出原則時、Astra Trident提供兩種選項：

- Astra Trident可動態管理匯出原則本身；在此作業模式中、儲存管理員會指定代表可接受IP位址的CIDR區塊清單。Astra Trident會自動將這些範圍內的節點IP新增至匯出原則。或者、如果未指定CIDR、則會將節點上找到的任何全域範圍單點傳送IP新增至匯出原則。
- 儲存管理員可以建立匯出原則、並手動新增規則。除非在組態中指定不同的匯出原則名稱、否則Astra Trident會使用預設的匯出原則。

## 動態管理匯出原則

「csi Trident」的20.04版提供動態管理輸出原則的能力ONTAP、以利實現幕後。這可讓儲存管理員為工作節點IP指定允許的位址空間、而非手動定義明確的規則。它可大幅簡化匯出原則管理；修改匯出原則不再需要在儲存叢集上進行手動介入。此外、這有助於限制只有在指定範圍內有IP的工作者節點才能存取儲存叢集、以支援精細且自動化的管理。



只有「csi Trident」才能動態管理匯出原則。請務必確保工作節點未被NATed。

## 範例

必須使用兩種組態選項。以下是後端定義範例：

```
---
version: 1
storageDriverName: ontap-nas
backendName: ontap_nas_auto_export
managementLIF: 192.168.0.135
svm: svm1
username: vsadmin
password: password
autoExportCIDRs:
- 192.168.0.0/24
autoExportPolicy: true
```



使用此功能時、您必須確保SVM中的根連接點具有先前建立的匯出原則、並具有允許節點CIDR區塊（例如預設匯出原則）的匯出規則。請務必遵循NetApp建議的最佳實務做法、為Astra Trident指定SVM。

以下是使用上述範例說明此功能的運作方式：

- autoExportPolicy 設為 true。這表示Astra Trident將為建立匯出原則 svm1 並使用來處理新增和刪除規則的作業 autoExportCIDRs 位址區塊。例如、UUID為403b5326-8482-40dB/96d0-d83fb3f4daec和的後端 autoExportPolicy 設定為 true 建立名為的匯出原則 trident-403b5326-8482-40db-96d0-d83fb3f4daec 在SVM上。
- autoExportCIDRs 包含位址區塊清單。此欄位為選用欄位、預設為「0.00.0.0/0」、「：/0」。如果未定義、Astra Trident會新增在工作者節點上找到的所有全域範圍單點傳送位址。

在此範例中 192.168.0.0/24 提供位址空間。這表示、屬於此位址範圍的Kubernetes節點IP將新增至Astra Trident所建立的匯出原則。當Astra Trident登錄其執行的節點時、會擷取節點的IP位址、並對照中提供的位址區塊來檢查這些位址 autoExportCIDRs。篩選IP之後、Astra Trident會針對所探索的用戶端IP建立匯出原則規

則、並針對所識別的每個節點建立一個規則。

您可以更新 `autoExportPolicy` 和 `autoExportCIDRs` 建立後端後端。您可以為自動管理或刪除現有CIDR的後端附加新的CIDR。刪除CIDR時請務必謹慎、以確保不會中斷現有的連線。您也可以選擇停用 `autoExportPolicy` 用於後端、然後回到手動建立的匯出原則。這需要設定 `exportPolicy` 參數。

在Astra Trident建立或更新後端之後、您可以使用檢查後端 `tridentctl` 或對應的 `tridentbackend` 客戶需求日：

```
./tridentctl get backends ontap_nas_auto_export -n trident -o yaml
items:
- backendUUID: 403b5326-8482-40db-96d0-d83fb3f4daec
  config:
    aggregate: ""
    autoExportCIDRs:
    - 192.168.0.0/24
    autoExportPolicy: true
    backendName: ontap_nas_auto_export
    chapInitiatorSecret: ""
    chapTargetInitiatorSecret: ""
    chapTargetUsername: ""
    chapUsername: ""
    dataLIF: 192.168.0.135
    debug: false
    debugTraceFlags: null
    defaults:
      encryption: "false"
      exportPolicy: <automatic>
      fileType: ext4
```

當節點新增至Kubernetes叢集並向Astra Trident控制器登錄時、會更新現有後端的匯出原則（前提是它們位於中指定的位址範圍內） `autoExportCIDRs` （後端）。

移除節點時、Astra Trident會檢查所有線上的後端、以移除節點的存取規則。Astra Trident將此節點IP從託管後端的匯出原則中移除、可防止惡意掛載、除非叢集中的新節點重複使用此IP。

對於先前現有的後端、請使用更新後端 `tridentctl update backend` 將確保Astra Trident自動管理匯出原則。這會建立以後端UUID命名的新匯出原則、而後端上的磁碟區會在重新掛載時使用新建立的匯出原則。



刪除具有自動管理匯出原則的後端、將會刪除動態建立的匯出原則。如果重新建立後端、則會將其視為新的後端、並導致建立新的匯出原則。

如果即時節點的IP位址已更新、您必須重新啟動節點上的Astra Trident Pod。Astra Trident接著會更新其管理的後端匯出原則、以反映此IP變更。

## 列舉NAS組態選項與範例ONTAP

瞭解如何透過ONTAP Astra Trident安裝來建立及使用NetApp NAS驅動程式。本節提供後端組態範例、以及如何將後端對應至StorageClass的詳細資料。

### 後端組態選項

如需後端組態選項、請參閱下表：

參數	說明	預設
version		永遠為1
storageDriverName	儲存驅動程式名稱	「ONTAP-NAS」、「ONTAP-NAS-節約型」、「ONTAP-NAS-flexgroup」、「ONTAP-SAN」、「ONTAP-san經濟型」
backendName	自訂名稱或儲存後端	驅動程式名稱+「_」+ dataLIF
managementLIF	叢集的IP位址或SVM管理LIF若要順暢MetroCluster 切換、您必須指定SVM管理LIF。您可以指定完整網域名稱（FQDN）。如果使用安裝Astra Trident、則可設定使用IPv6位址 --use-ipv6 旗標。IPv6位址必須以方括弧來定義、例如[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。	「10.0.0.1」、「[2001:1234:abcd:::fefo]」
dataLIF	傳輸協定LIF的IP位址。我們建議具體說明 dataLIF。如果未提供、Astra Trident會從SVM擷取資料lifs。您可以指定要用於NFS掛載作業的完整網域名稱（FQDN）、讓您建立循環配置資源DNS、以便在多個資料生命期之間達到負載平衡。可在初始設定之後變更。請參閱。如果使用安裝Astra Trident、則可設定使用IPv6位址 --use-ipv6 旗標。IPv6位址必須以方括弧來定義、例如[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。	指定位址或從SVM衍生（若未指定）（不建議使用）
autoExportPolicy	啟用自動匯出原則建立及更新[布林值]。使用 autoExportPolicy 和 autoExportCIDRs 選項：Astra Trident可自動管理匯出原則。	錯
autoExportCIDRs	根據時間篩選Kubernetes節點IP的CIDR清單 autoExportPolicy 已啟用。使用 autoExportPolicy 和 autoExportCIDRs 選項：Astra Trident可自動管理匯出原則。	[「0.00.0/0」、「:/0」]

參數	說明	預設
labels	套用到磁碟區的任意JSON-格式化標籤集	「」
clientCertificate	用戶端憑證的Base64編碼值。用於憑證型驗證	「」
clientPrivateKey	用戶端私密金鑰的Base64編碼值。用於憑證型驗證	「」
trustedCACertificate	受信任CA憑證的Base64編碼值。選用。用於憑證型驗證	「」
username	連線至叢集/ SVM的使用者名稱。用於認證型驗證	
password	連線至叢集/ SVM的密碼。用於認證型驗證	
svm	要使用的儲存虛擬機器	如果是SVM則衍生managementLIF 已指定
storagePrefix	在SVM中配置新磁碟區時所使用的前置碼。設定後無法更新	「Trident」
limitAggregateUsage	如果使用率高於此百分比、則無法進行資源配置。*不適用於Amazon FSX for ONTAP Sfor Sfor *	「」（預設不強制執行）
limitVolumeSize	如果要求的磁碟區大小高於此值、則資源配置失敗。	「」（預設不強制執行）
limitVolumeSize	如果要求的磁碟區大小高於此值、則資源配置失敗。也會限制其管理的qtree和LUN、以及的磁碟區大小上限 qtreesPerFlexvol 選項可自訂每FlexVol 個支援區的配額樹數上限。	「」（預設不強制執行）
lunsPerFlexvol	每FlexVol 個LUN的最大LUN數量、範圍必須在[50、200]	「100」
debugTraceFlags	疑難排解時要使用的偵錯旗標。範例： {"API":假、「method」:true} 不使用 debugTraceFlags 除非您正在疑難排解並需要詳細的記錄傾印。	null
nfsMountOptions	以逗號分隔的NFS掛載選項清單。Kubernetes持續磁碟區的掛載選項通常會在儲存類別中指定、但如果儲存類別中未指定掛載選項、則Astra Trident會改回使用儲存後端組態檔中指定的掛載選項。如果儲存類別或組態檔中未指定掛載選項、Astra Trident將不會在相關的持續磁碟區上設定任何掛載選項。	「」

參數	說明	預設
qtreesPerFlexvol	每FlexVol 個邊的最大qtree數、必須在範圍內[50、300]	「200」
useREST	使用ONTAP Isrest API的布林參數。技術預覽 useREST 以*技術預覽*的形式提供、建議用於測試環境、而非用於正式作業工作負載。設定為時 true、Astra Trident將使用ONTAP 靜止API與後端進行通訊。此功能需要ONTAP 使用更新版本的版本。此外ONTAP 、所使用的登入角色必須能夠存取 ontap 應用程式：這是預先定義的 vsadmin 和 cluster-admin 角色： useREST 不支援MetroCluster 使用支援。	錯

#### 用於資源配置磁碟區的后端組態選項

您可以使用中的這些選項來控制預設資源配置 defaults 組態區段。如需範例、請參閱下列組態範例。

參數	說明	預設
spaceAllocation	LUN的空間分配	「真的」
spaceReserve	空間保留模式；「無」（精簡）或「Volume」（完整）	「無」
snapshotPolicy	要使用的Snapshot原則	「無」
qosPolicy	要指派給所建立磁碟區的QoS原則群組。選擇每個儲存集區/後端的其中一個qosPolicy 或adaptiveQosPolicy	「」
adaptiveQosPolicy	要指派給所建立磁碟區的調適性QoS原則群組。選擇每個儲存集區/後端的其中一個qosPolicy 或adaptiveQosPolicy。不受ONTAP-NAS-經濟支援。	「」
snapshotReserve	保留給快照「0」的磁碟區百分比	如果 snapshotPolicy 為「無」、否則為「」
splitOnClone	建立複本時、從其父複本分割複本	「假」

參數	說明	預設
encryption	在新磁碟區上啟用NetApp Volume Encryption (NVE)；預設為 false。必須在叢集上授權並啟用NVE、才能使用此選項。如果在後端啟用NAE、則Astra Trident中配置的任何磁碟區都會啟用NAE。如需詳細資訊、請參閱： <a href="#">"Astra Trident如何與NVE和NAE搭配運作"</a> 。	「假」
tieringPolicy	分層原則以使用「無」	ONTAP 9.5之前的SVM-DR組態為「純快照」
unixPermissions	新磁碟區的模式	NFS磁碟區為「777」；SMB磁碟區為空白（不適用）
snapshotDir	控制的可見度 .snapshot 目錄	「假」
exportPolicy	要使用的匯出原則	「預設」
securityStyle	新磁碟區的安全樣式。NFS支援 mixed 和 unix 安全樣式；SMB支援 mixed 和 ntfs 安全樣式：	NFS預設為 unix。SMB預設為 ntfs。



搭配Astra Trident使用QoS原則群組需要ONTAP 使用更新版本的版本。建議使用非共用的QoS原則群組、並確保原則群組會個別套用至每個組成群組。共享的QoS原則群組將強制所有工作負載的總處理量上限。

## Volume資源配置範例

以下是定義預設值的範例：



```

---
version: 1
storageDriverName: ontap-nas
backendName: customBackendName
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
labels:
  k8scluster: dev1
  backend: dev1-nasbackend
svm: trident_svm
username: cluster-admin
password: password
limitAggregateUsage: 80%
limitVolumeSize: 50Gi
nfsMountOptions: nfsvers=4
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: premium
  exportPolicy: myk8scluster
  snapshotPolicy: default
  snapshotReserve: '10'

```

適用於 ontap-nas 和 ontap-nas-flexgroups`Astra Trident現在使用新的計算方法、確保FlexVol 利用snapshotReserve百分比和PVC正確調整尺寸。當使用者要求使用PVCs時、Astra Trident 會FlexVol 使用新的計算方式、建立原始的包含更多空間的候選區。此計算可確保使用者在永久虛擬磁碟中獲得所要求的可寫入空間、且空間不得小於所要求的空間。在v21.07之前、當使用者要求使用PVC（例如5GiB）、快照保留區達到50%時、他們只能獲得2.5GiB的可寫入空間。這是因為使用者要求的是整個Volume和`snapshotReserve 佔此比例。使用Trident 21.07時、使用者要求的是可寫入空間、而Astra Trident定義了snapshotReserve 數字表示整個Volume的百分比。這不適用於 ontap-nas-economy。請參閱下列範例以瞭解此功能的運作方式：

計算方式如下：

```

Total volume size = (PVC requested size) / (1 - (snapshotReserve
percentage) / 100)

```

對於snapshotReserve = 50%、而PVC要求= 5GiB、磁碟區總大小為 $2/0.5 = 10\text{GiB}$ 、可用大小為5GiB、這是使用者在PVC要求中要求的大小。。 volume show 命令應顯示類似以下範例的結果：

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
		_pvc_89f1c156_3801_4de4_9f9d_034d54c395f4	online	RW	10GB	5.00GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

2 entries were displayed.

在升級Astra Trident時、先前安裝的現有後端會按照上述說明來配置磁碟區。對於在升級之前建立的磁碟區、您應該調整其磁碟區大小、以便觀察變更。例如、採用的2GiB PVC `snapshotReserve=50` 先前產生的磁碟區提供1GiB的可寫入空間。例如、將磁碟區大小調整為3GiB、可讓應用程式在6 GiB磁碟區上擁有3GiB的可寫入空間。

範例

最低組態範例

下列範例顯示基本組態、讓大部分參數保留預設值。這是定義後端最簡單的方法。



如果您在NetApp ONTAP 支援Trident的NetApp支援上使用Amazon FSX、建議您指定lif的DNS名稱、而非IP位址。

預設選項開啟 `ontap-nas-economy`

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

這是最小的後端組態範例。clientCertificate、clientPrivateKey`和`trustedCACertificate（選用、如果使用信任的CA）會填入 backend.json 並分別取得用戶端憑證、私密金鑰及信任CA憑證的基礎64編碼值。

```
---
version: 1
backendName: DefaultNASBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.15
svm: nfs_svm
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

這些範例說明如何指示Astra Trident使用動態匯出原則來自動建立及管理匯出原則。這對的運作方式相同 `ontap-nas-economy` 和 `ontap-nas-flexgroup` 驅動程式：

### ONTAP-NAS驅動程式

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-nasbackend
autoExportPolicy: true
autoExportCIDRs:
- 10.0.0.0/24
username: admin
password: password
nfsMountOptions: nfsvers=4
```

### `ontap-nas-flexgroup` 驅動程式

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
labels:
  k8scluster: test-cluster-east-1b
  backend: test1-ontap-cluster
svm: svm_nfs
username: vsadmin
password: password
```

## 使用IPv6位址

此範例顯示 managementLIF 使用IPv6位址。

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas_ipv6_backend
managementLIF: "[5c5d:5edf:8f:7657:bef8:109b:1b41:d491]"
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-ontap-ipv6
svm: nas_ipv6_svm
username: vsadmin
password: password
```

## ontap-nas-economy 驅動程式

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

## ontap-nas 適用於ONTAP Amazon FSX的驅動程式、適用於使用SMB Volume的功能

```
---
version: 1
backendName: SMBBackend
storageDriverName: ontap-nas
managementLIF: example.mgmt.fqdn.aws.com
nasType: smb
dataLIF: 10.0.0.15
svm: nfs_svm
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

## 虛擬集區的後端範例

在下圖所示的範例後端定義檔案中、會針對所有儲存資源池設定特定的預設值、例如 `spaceReserve` 無、`spaceAllocation` 假、和 `encryption` 錯。虛擬資源池是在儲存區段中定義的。

Astra Trident會在「Comments」欄位中設定資源配置標籤。註解設定FlexVol 於支援對象 `ontap-nas` 或FlexGroup 支援 `ontap-nas-flexgroup`。Astra Trident會在資源配置時、將虛擬資源池上的所有標籤複製到儲存磁碟區。為了方便起見、儲存管理員可以針對每個虛擬資源池定義標籤、並依標籤將磁碟區分組。

在此範例中、有些儲存資源池會自行設定 `spaceReserve`、`spaceAllocation` 和 `encryption` 值、部分集區會覆寫上述設定的預設值。

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: admin
password: password
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: 'false'
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  app: msoffice
  cost: '100'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
    adaptiveQosPolicy: adaptive-premium
- labels:
  app: slack
  cost: '75'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  app: wordpress
  cost: '50'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
```

```
- labels:  
  app: mysqldb  
  cost: '25'  
  zone: us_east_1d  
  defaults:  
    spaceReserve: volume  
    encryption: 'false'  
    unixPermissions: '0775'
```



```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
defaults:
  spaceReserve: none
  encryption: 'false'
labels:
  store: flexgroup_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  protection: gold
  creditpoints: '50000'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  protection: gold
  creditpoints: '30000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  protection: silver
  creditpoints: '20000'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
- labels:
  protection: bronze
  creditpoints: '10000'
```

```
zone: us_east_1d
defaults:
  spaceReserve: volume
  encryption: 'false'
  unixPermissions: '0775'
```

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
defaults:
  spaceReserve: none
  encryption: 'false'
labels:
  store: nas_economy_store
region: us_east_1
storage:
- labels:
  department: finance
  creditpoints: '6000'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  department: legal
  creditpoints: '5000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  department: engineering
  creditpoints: '3000'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
- labels:
  department: humanresource
  creditpoints: '2000'
  zone: us_east_1d
```

```
defaults:
  spaceReserve: volume
  encryption: 'false'
  unixPermissions: '0775'
```

更新 dataLIF 初始組態之後

您可以在初始組態後變更資料LIF、方法是執行下列命令、以更新資料LIF提供新的後端Json檔案。

```
tridentctl update backend <backend-name> -f <path-to-backend-json-file-
with-updated-dataLIF>
```



如果將PVCS附加至一或多個Pod、您必須關閉所有對應的Pod、然後將其重新啟動、新的資料LIF才會生效。

將後端對應至StorageClass

下列StorageClass定義是指上述虛擬資源池。使用 `parameters.selector` 欄位中、每個StorageClass會呼叫哪些虛擬資源池可用於裝載Volume。磁碟區將會在所選的虛擬資源池中定義各個層面。

- 第一個StorageClass (protection-gold) 將對應至中的第一個、第二個虛擬集區 `ontap-nas-flexgroup` 後端和中的第一個虛擬集區 `ontap-san` 後端：這是唯一提供金級保護的資源池。
- 第二個StorageClass (protection-not-gold) 將對應至中的第三、第四個虛擬集區 `ontap-nas-flexgroup` 中的後端和第二個、第三個虛擬集區 `ontap-san` 後端：這是唯一提供金級以外保護層級的資源池。
- 第三個StorageClass (app-mysqldb) 將對應至中的第四個虛擬資源池 `ontap-nas` 中的後端和第三個虛擬集區 `ontap-san-economy` 後端：這些是唯一提供mysqldb類型應用程式儲存池組態的集區。
- 第四個StorageClass (protection-silver-creditpoints-20k) 將對應至中的第三個虛擬集區 `ontap-nas-flexgroup` 中的後端和第二個虛擬集區 `ontap-san` 後端：這些資源池是唯一能以20000個信用點數提供金級保護的資源池。
- 第五個StorageClass (creditpoints-5k) 將對應至中的第二個虛擬資源池 `ontap-nas-economy` 中的後端和第三個虛擬集區 `ontap-san` 後端：這些是唯一提供5000個信用點數的資源池產品。

Astra Trident將決定選取哪個虛擬集區、並確保符合儲存需求。

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: netapp.io/trident
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: netapp.io/trident
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: netapp.io/trident
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

## Amazon FSX for NetApp ONTAP 產品

使用Astra Trident搭配Amazon FSX for NetApp ONTAP 解決方案

"Amazon FSX for NetApp ONTAP 產品" 是完全託管的AWS服務、可讓客戶啟動及執行採用NetApp ONTAP 資訊儲存作業系統的檔案系統。FSX for ONTAP VMware可讓您運用熟悉的NetApp功能、效能和管理功能、同時充分發揮儲存AWS資料的簡易性、敏捷度、安全性和擴充性。FSX for ONTAP Sfor支援ONTAP Isf供 檔案系統功能和管理API。

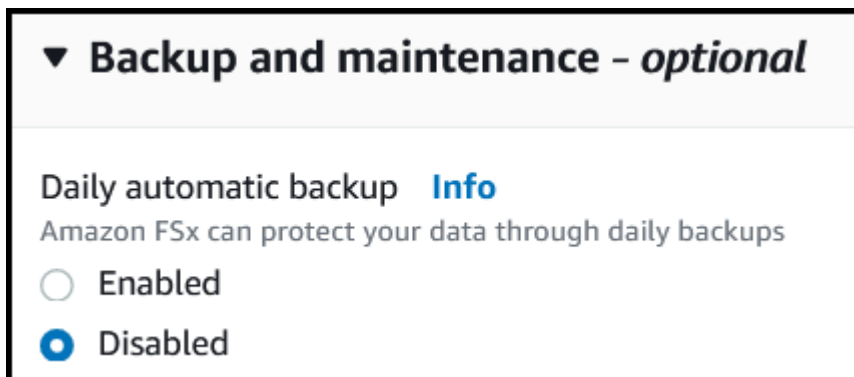
檔案系統是Amazon FSX的主要資源、類似ONTAP 於內部部署的一個叢集。在每個SVM中、您可以建立一個或多個磁碟區、這些磁碟區是儲存檔案系統中檔案和資料夾的資料容器。有了Amazon FSX for NetApp ONTAP 的功能、Data ONTAP 即可在雲端以託管檔案系統的形式提供支援。新的檔案系統類型稱為\* NetApp ONTAP Sing\*。

使用Astra Trident搭配Amazon FSX for NetApp ONTAP 供應NetApp時、您可以確保在Amazon Elastic Kubernetes Service (EKS) 中執行的Kubernetes叢集、能夠配置區塊和檔案以ONTAP 支援的持續磁碟區。

適用於NetApp ONTAP 的Amazon FSX "FabricPool" 管理儲存層。它可讓您根據資料是否經常存取、將資料儲存在一個層級中。

### 考量

- SMB Volume :
  - 使用支援SMB磁碟區 `ontap-nas` 僅限驅動程式。
  - Astra Trident僅支援安裝在Windows節點上執行的Pod上的SMB磁碟區。
  - Astra Trident不支援Windows ARM 的架構。
- 在啟用自動備份的Amazon FSX檔案系統上建立的磁碟區、無法由Trident刪除。若要刪除PVCs、您需要手動刪除PV和FSXfor ONTAP the Sesfvolume。若要避免此問題：
  - 請勿使用「快速建立」來建立FSX for ONTAP the Suse檔案系統。快速建立工作流程可自動備份、但不提供退出選項。
  - 使用「標準建立」時、請停用自動備份。停用自動備份可讓Trident成功刪除磁碟區、而無需進一步手動介入。



### 驅動程式

您可以ONTAP 使用下列驅動程式、將Astra Trident與Amazon FSX for NetApp整合：

- `ontap-san`：配置的每個PV都是自己Amazon FSX for NetApp ONTAP 的LUN。
- `ontap-san-economy`：配置的每個PV都是LUN、每個Amazon FSX for NetApp ONTAP 的LUN數量可設定。
- `ontap-nas`：配置的每個PV都是完整的Amazon FSX for NetApp ONTAP Sf2 Volume。
- `ontap-nas-economy`：每個配置的PV都是qtree、每個Amazon FSX for NetApp ONTAP 供應的qtree有可設定的配額樹數。
- `ontap-nas-flexgroup`：配置的每個PV都是完整的Amazon FSX for NetApp ONTAP FlexGroup Sf2 Volume。

如需驅動程式詳細資料、請參閱 ["驅動程式ONTAP"](#)。

## 驗證

Astra Trident提供兩種驗證模式。

- 憑證型：Astra Trident會使用SVM上安裝的憑證、與FSX檔案系統上的SVM進行通訊。
- 認證型：您可以使用 `fsxadmin` 檔案系統或的使用者 `vsadmin` 為SVM設定的使用者。



Astra Trident希望以 `vsadmin` SVM使用者或具有相同角色之不同名稱的使用者。適用於NetApp ONTAP 的Amazon FSX具備以下功能 `fsxadmin` 使用者只能有限地取代ONTAP 此功能 `admin` 叢集使用者：強烈建議使用 `vsadmin` 使用Astra Trident。

您可以更新後端以在認證型和憑證型方法之間移動。不過、如果您嘗試提供\*認證資料和認證\*、後端建立將會失敗。若要切換至不同的驗證方法、您必須從後端組態中移除現有方法。

如需啟用驗證的詳細資訊、請參閱您的驅動程式類型驗證：

- ["ASNAS驗證ONTAP"](#)
- ["支援SAN驗證ONTAP"](#)

如需詳細資訊、請參閱

- ["Amazon FSX for NetApp ONTAP 的支援文件"](#)
- ["Amazon FSX for NetApp ONTAP 的部落格文章"](#)

## 整合Amazon FSX for NetApp ONTAP 功能

您可以將Amazon FSX for NetApp ONTAP 的支援文件系統與Astra Trident整合、以確保在Amazon Elastic Kubernetes Service (EKS) 中執行的Kubernetes叢集能夠配置區塊並以ONTAP 支援的方式歸檔持續Volume。

## 開始之前

此外 ["Astra Trident的需求"](#)、若要將FSXfor ONTAP 支援與Astra Trident整合、您需要：

- 現有的Amazon EKS叢集或自我管理的Kubernetes叢集 `kubect1` 已安裝。
- 現有的Amazon FSX-適用於NetApp ONTAP 的支援資料系統和儲存虛擬機器 (SVM)、可從叢集的工作節

點存取。

- 已準備好的工作節點 **"NFS或iSCSI"**。



請務必遵循Amazon Linux和Ubuntu所需的節點準備步驟 **"Amazon機器映像"** (AMIs)、視您的EKS AMI類型而定。

### SMB磁碟區的其他需求

- Kubernetes叢集具備Linux控制器節點、以及至少一個執行Windows Server 2019的Windows工作節點。Astra Trident僅支援安裝在Windows節點上執行的Pod上的SMB磁碟區。
- 至少有一個Astra Trident機密、其中包含您的Active Directory認證資料。以產生機密 `smbcreds`：

```
kubectl create secret generic smbcreds --from-literal username=user  
--from-literal password='password'
```

- 設定為Windows服務的SCSI Proxy。若要設定 `csi-proxy`、請參閱 **"GitHub：csi Proxy"** 或 **"GitHub：適用於Windows的SCSI Proxy"** 適用於Windows上執行的Kubernetes節點。

### 整合SAN和NAS驅動程式ONTAP



如果您要設定SMB磁碟區、則必須閱讀 **準備配置SMB磁碟區** 在建立後端之前。

### 步驟

1. 使用其中一項部署Astra Trident **"部署方法"**。
2. 收集SVM管理LIF DNS名稱。例如、使用AWS CLI尋找 `DNSName` 輸入 `Endpoints → Management` 執行下列命令之後：

```
aws fsx describe-storage-virtual-machines --region <file system region>
```

3. 建立及安裝的憑證 **"NAS後端驗證"** 或 **"SAN後端驗證"**。



您可以使用SSH從任何位置登入檔案系統（例如安裝憑證）、而該SSH可連至檔案系統。使用 `fsxadmin` 使用者、您在建立檔案系統時設定的密碼、以及管理DNS名稱 `aws fsx describe-file-systems`。

4. 使用您的憑證和管理LIF的DNS名稱建立後端檔案、如下例所示：



## YAML

```
---
version: 1
storageDriverName: ontap-san
backendName: customBackendName
managementLIF: svm-XXXXXXXXXXXXXXXXXX.fs-XXXXXXXXXXXXXXXXXX.fsx.us-
east-2.aws.internal
svm: svm01
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

## JSON

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "customBackendName",
  "managementLIF": "svm-XXXXXXXXXXXXXXXXXX.fs-
XXXXXXXXXXXXXXXXXX.fsx.us-east-2.aws.internal",
  "svm": "svm01",
  "clientCertificate": "ZXR0ZXJwYXB...ICMgJ3BhcGVyc2",
  "clientPrivateKey": "vciwKIyAgZG...0cnksIGRlc2NyaX",
  "trustedCACertificate": "zcyBbaG...b3Igb3duIGNsYXNz"
}
```

如需建立後端的相關資訊、請參閱下列連結：

- ["使用ONTAP NetApp NAS驅動程式設定後端"](#)
- ["使用ONTAP SAN驅動程式設定後端"](#)

## 結果

部署之後、您可以建立 ["儲存類別、配置磁碟區、然後將磁碟區掛載到Pod中"](#)。

## 準備配置SMB磁碟區

您可以使用來配置SMB磁碟區 `ontap-nas` 驅動程式：完成之前 [整合SAN和NAS驅動程式ONTAP](#) 完成下列步驟。

## 步驟

1. 建立SMB共用區。您可以使用兩種方式之一來建立SMB管理共用區 ["Microsoft管理主控台"](#) 共享資料夾嵌入式管理單元或使用ONTAP CLI。若要使用ONTAP CLI建立SMB共用：
  - a. 如有必要、請建立共用的目錄路徑結構。

。 `vserver cifs share create` 命令會在共用建立期間檢查 `-path` 選項中指定的路徑。如果指定的路徑不存在、則命令會失敗。

b. 建立與指定SVM相關的SMB共用區：

```
vserver cifs share create -vserver vserver_name -share-name  
share_name -path path [-share-properties share_properties,...]  
[other_attributes] [-comment text]
```

c. 確認共用區已建立：

```
vserver cifs share show -share-name share_name
```



請參閱 ["建立SMB共用區"](#) 以取得完整詳細資料。

2. 建立後端時、您必須設定下列項目以指定SMB Volume。如需ONTAP 所有的FSXfor Sendbackend組態選項、請參閱 ["FSX提供ONTAP 各種組態選項和範例"](#)。

參數	說明	範例
smbShare	使用共享資料夾Microsoft管理主控台建立的SMB共用名稱。例如「SMB共用區」。* SMB磁碟區需要。*	smb-share
nasType	*必須設定為 smb.*如果為null、則預設為 nfs。	smb
securityStyle	新磁碟區的安全樣式。必須設定為 <b>ntfs</b> 或 <b>mixed</b> 適用於 <b>SMB</b> 磁碟區。	ntfs 或 mixed 適用於SMB磁碟區
unixPermissions	新磁碟區的模式。SMB磁碟區*必須保留為空白。*	"

## FSX提供ONTAP 各種組態選項和範例

深入瞭解Amazon FSX for ONTAP Sfor Sf。本節提供後端組態範例。

### 後端組態選項

如需後端組態選項、請參閱下表：

參數	說明	範例
version		永遠為1

參數	說明	範例
storageDriverName	儲存驅動程式名稱	「ONTAP-NAS」、「ONTAP-NAS-節約 型」、「ONTAP-NAS-flexgroup」、「ONTAP-SAN」、「ONTAP-san經濟型」
backendName	自訂名稱或儲存後端	驅動程式名稱+「_」+ dataLIF
managementLIF	叢集的IP位址或SVM管理LIF若要順暢MetroCluster 切換、您必須指定SVM管理LIF。您可以指定完整網域名稱（FQDN）。如果使用安裝Astra Trident、則可設定使用IPv6位址 --use-ipv6 旗標。IPv6位址必須以方括弧來定義、例如[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。	「10.0.0.1」、「[2001:1234:abcd:::fefo]」
dataLIF	傳輸協定LIF的IP位址。不適用 <b>NAS</b> 驅動程式：建議您指定dataLIF ONTAP。如果未提供、Astra Trident會從SVM擷取資料lifs。您可以指定要用於NFS掛載作業的完整網域名稱（FQDN）、讓您建立循環配置資源DNS、以便在多個資料生命期之間達到負載平衡。可在初始設定之後變更。請參閱。《 <b>SAN</b> 驅動程式：請勿指定用於iSCSI》ONTAP。Astra Trident使用ONTAP「選擇性LUN地圖」來探索建立多重路徑工作階段所需的iSCSI lifs。如果明確定義dataLIF、就會產生警告。如果使用安裝Astra Trident、則可設定使用IPv6位址 --use-ipv6 旗標。IPv6位址必須以方括弧來定義、例如[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。	
autoExportPolicy	啟用自動匯出原則建立及更新[布林值]。使用 autoExportPolicy 和 autoExportCIDRs 選項：Astra Trident可自動管理匯出原則。	"假"
autoExportCIDRs	根據時間篩選Kubernetes節點IP的CIDR清單 autoExportPolicy已啟用。使用 autoExportPolicy 和 autoExportCIDRs 選項：Astra Trident可自動管理匯出原則。	「[「0.00.0.0/0」、「:/0」]」
labels	套用到磁碟區的任意JSON-格式化標籤集	"
clientCertificate	用戶端憑證的Base64編碼值。用於憑證型驗證	"

參數	說明	範例
clientPrivateKey	用戶端私密金鑰的Base64編碼值。用於憑證型驗證	"
trustedCACertificate	受信任CA憑證的Base64編碼值。選用。用於憑證型驗證。	"
username	連線至叢集或SVM的使用者名稱。用於認證型驗證。例如、vsadmin。	
password	連線至叢集或SVM的密碼。用於認證型驗證。	
svm	要使用的儲存虛擬機器	指定SVM管理LIF時衍生。
igroupName	要使用之SAN磁碟區的igroup名稱。請參閱。	「Trident -<後端-UUID>」
storagePrefix	在SVM中配置新磁碟區時所使用的前置碼。無法在建立後修改。若要更新此參數、您需要建立新的後端。	「Trident」
limitAggregateUsage	*請勿指定Amazon FSX for NetApp ONTAP 的功能。*所提供的 fsxadmin 和 vsadmin 請勿包含擷取Aggregate使用量所需的權限、並使用Astra Trident加以限制。	請勿使用。
limitVolumeSize	如果要求的磁碟區大小高於此值、則資源配置失敗。也會限制其管理的qtree和LUN、以及的磁碟區大小上限 qtreesPerFlexvol 選項可自訂每FlexVol 個支援區的配額樹數上限。	「」（預設不強制執行）
lunsPerFlexvol	每FlexVol 個LUN的最大LUN數量、範圍必須為[50、200]。僅限SAN。	「100」
debugTraceFlags	疑難排解時要使用的偵錯旗標。範例： {"API":假、「method」:true} 不使用 debugTraceFlags 除非您正在疑難排解並需要詳細的記錄傾印。	null
nfsMountOptions	以逗號分隔的NFS掛載選項清單。Kubernetes持續磁碟區的掛載選項通常會在儲存類別中指定、但如果儲存類別中未指定掛載選項、則Astra Trident會改回使用儲存後端組態檔中指定的掛載選項。如果儲存類別或組態檔中未指定掛載選項、Astra Trident將不會在相關的持續磁碟區上設定任何掛載選項。	"

參數	說明	範例
nasType	設定NFS或SMB磁碟區建立。選項包括 <code>nfs</code> 、 <code>smb</code> 或 <code>null</code> 。*必須設定為 <code>smb</code> 對於SMB Volume。*設定為 <code>null</code> 、預設為NFS Volume。	"NFS"
qtreesPerFlexvol	每FlexVol 個邊的最大qtree數、必須在範圍內[50、300]	"200"
smbShare	使用共享資料夾Microsoft管理主控台建立的SMB共用名稱。* SMB磁碟區需要。*	「SMB共用區」
useREST	使用ONTAP Isrest API的布林參數。技術預覽 useREST 以*技術預覽*的形式提供、建議用於測試環境、而非用於正式作業工作負載。設定為 <code>true</code> 、Astra Trident將使用ONTAP靜止API與後端進行通訊。此功能需要ONTAP 使用更新版本的版本。此外ONTAP、所使用的登入角色必須能夠存取 <code>ontap</code> 應用程式：這是預先定義的 <code>vsadmin</code> 和 <code>cluster-admin</code> 角色：	"假"

#### 詳細資料 igroupName

igroupName 可設定為ONTAP 已在叢集上建立的igroup。如果未指定、Astra Trident會自動建立名為igroup trident-`<backend-UUID>`。

如果提供預先定義的igroupName、我們建議每個Kubernetes叢集使用一個igroup、如果要在不同環境之間共用SVM。這是Astra Trident自動維護IQN新增與刪除作業所必需的。

- igroupName 可更新以指向在Astra Trident以外的SVM上建立及管理的新igroup。
- igroupName 可省略。在此案例中、Astra Trident將建立並管理名為igroup trident-`<backend-UUID>` 自動：

在這兩種情況下、仍可繼續存取Volume附件。未來的Volume附件將使用更新的igroup。此更新不會中斷對後端磁碟區的存取。

#### 更新 dataLIF 初始組態之後

您可以在初始組態後變更資料LIF、方法是執行下列命令、以更新資料LIF提供新的後端Json檔案。

```
tridentctl update backend <backend-name> -f <path-to-backend-json-file-with-updated-dataLIF>
```



如果將PVCS附加至一或多個Pod、您必須關閉所有對應的Pod、然後將其重新啟動、新的資料LIF才會生效。

您可以使用中的這些選項來控制預設資源配置 defaults 組態區段。如需範例、請參閱下列組態範例。

參數	說明	預設
spaceAllocation	LUN的空間分配	「真的」
spaceReserve	空間保留模式；「無」（精簡）或「Volume」（完整）	「無」
snapshotPolicy	要使用的Snapshot原則	「無」
qosPolicy	要指派給所建立磁碟區的QoS原則群組。選擇每個儲存集區或後端的其中一個qosPolicy或adaptiveQosPolicy。搭配Astra Trident使用QoS原則群組需要ONTAP 使用更新版本的版本。我們建議使用非共用的QoS原則群組、並確保原則群組會個別套用至每個組成群組。共享的QoS原則群組將強制所有工作負載的總處理量上限。	「」
adaptiveQosPolicy	要指派給所建立磁碟區的調適性QoS原則群組。選擇每個儲存集區或後端的其中一個qosPolicy或adaptiveQosPolicy。不受ONTAP-NAS-經濟支援。	「」
snapshotReserve	保留給快照「0」的磁碟區百分比	如果 snapshotPolicy 為「無」、否則為「」
splitOnClone	建立複本時、從其父複本分割複本	「假」
encryption	在新磁碟區上啟用NetApp Volume Encryption (NVE)；預設為false。必須在叢集上授權並啟用NVE、才能使用此選項。如果在後端啟用NAE、則Astra Trident中配置的任何磁碟區都會啟用NAE。如需詳細資訊、請參閱： <a href="#">"Astra Trident如何與NVE和NAE搭配運作"</a> 。	「假」
luksEncryption	啟用LUKS加密。請參閱 <a href="#">"使用Linux統一金鑰設定 (LUKS)"</a> 。僅限SAN。	"
tieringPolicy	分層原則以使用「無」	ONTAP 9.5之前的SVM-DR組態為「純快照」
unixPermissions	新磁碟區的模式。如果是 <b>SMB</b> 磁碟區、請保留空白。	「」
securityStyle	新磁碟區的安全樣式。NFS支援mixed和unix安全樣式；SMB支援mixed和ntfs安全樣式：	NFS預設為unix。SMB預設為ntfs。

## 範例

使用 `nasType`、`node-stage-secret-name` 和 `node-stage-secret-namespace`、您可以指定SMB磁碟區、並提供所需的Active Directory認證資料。使用支援SMB磁碟區 `ontap-nas` 僅限驅動程式。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: nas-smb-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
```

## 使用kubectl建立後端

後端定義了Astra Trident與儲存系統之間的關係。它告訴Astra Trident如何與該儲存系統通訊、以及Astra Trident如何從該儲存系統配置磁碟區。安裝Astra Trident之後、下一步是建立後端。◦ `TridentBackendConfig` 自訂資源定義 (CRD) 可讓您直接透過Kubernetes介面建立及管理Trident後端。您可以使用執行此作業 `kubectl` 或相當於Kubernetes發佈版本的CLI工具。

### TridentBackendConfig

`TridentBackendConfig` (`tbc`、`tbconfig`、`tbackendconfig`) 是前端、命名式CRD、可讓您使用管理Astra Trident後端 `kubectl`。Kubernetes與儲存管理員現在可以直接透過Kubernetes CLI建立及管理後端、而無需使用專屬的命令列公用程式 (`tridentctl`)。

建立時 `TridentBackendConfig` 物件：

- Astra Trident會根據您提供的組態自動建立後端。這會在內部顯示為 `TridentBackend` (`tbe`、`tridentbackend`) CR。
- `TridentBackendConfig` 唯一綁定到 `TridentBackend` 這是由Astra Trident所建立。

每個 `TridentBackendConfig` 使用維護一對一對應 `TridentBackend`。前者是提供給使用者設計及設定後端的介面、後者是Trident代表實際後端物件的方式。



`TridentBackend` CRS由Astra Trident自動建立。您\*不應該\*修改這些項目。如果您想要對後端進行更新、請修改以執行此動作 `TridentBackendConfig` 物件：

請參閱下列範例以瞭解的格式 `TridentBackendConfig` CR：

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret

```

您也可以查看中的範例 ["Trident安裝程式"](#) 所需儲存平台/服務的範例組態目錄。

- spec 採用後端特定的組態參數。在此範例中、後端使用 ontap-san 儲存驅動程式、並使用此處列出的組態參數。如需所需儲存驅動程式的組態選項清單、請參閱 ["儲存驅動程式的後端組態資訊"](#)。
- spec 部分也包括 credentials 和 deletionPolicy 欄位中新增的 TridentBackendConfig CR：
  - credentials：此參數為必填欄位、包含用於驗證儲存系統/服務的認證資料。此設定為使用者建立的 Kubernetes Secret。認證資料無法以純文字格式傳遞、因此會產生錯誤。
  - deletionPolicy：此欄位可定義在下列情況下應發生的情況 TridentBackendConfig 已刪除。可能需要兩種可能的值之一：
    - delete：這會導致兩者都被刪除 TridentBackendConfig 和相關後端。這是預設值。
    - retain：當 TridentBackendConfig 刪除CR後、後端定義仍會顯示、並可透過進行管理 tridentctl。將刪除原則設定為 retain 可讓使用者降級至較早版本（21.04之前）、並保留建立的後端。此欄位的值可在之後更新 TridentBackendConfig 已建立。



後端名稱是使用設定 spec.backendName。如果未指定、則會將後端名稱設為的名稱 TridentBackendConfig 物件 (metadata.name)。建議使用明確設定後端名稱 spec.backendName。



以建立的後端 tridentctl 沒有關聯的 TridentBackendConfig 物件：您可以選擇使用來管理此類後端 kubectl 建立 TridentBackendConfig CR。必須謹慎指定相同的組態參數（例如 spec.backendName、spec.storagePrefix、spec.storageDriverName 等）。Astra Trident 會自動連結新建立的 TridentBackendConfig 使用預先存在的後端。

## 步驟總覽

若要使用建立新的後端 kubectl、您應該執行下列步驟：

1. 建立 ["Kubernetes機密"](#)。此機密包含Astra Trident與儲存叢集/服務通訊所需的認證資料。
2. 建立 TridentBackendConfig 物件：其中包含有關儲存叢集/服務的詳細資訊、並參考上一步建立的機



密。

建立後端之後、您可以使用觀察其狀態 `kubectl get tbc <tbc-name> -n <trident-namespace>` 並收集其他詳細資料。

## 步驟1：建立Kubernetes機密

建立包含後端存取認證的秘密。這是每個儲存服務/平台所獨有的功能。以下是範例：

```
kubectl -n trident create -f backend-tbc-ontap-san-secret.yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-san-secret
type: Opaque
stringData:
  username: cluster-admin
  password: t@Ax@7q(>
```

下表摘要說明每個儲存平台的機密必須包含的欄位：

儲存平台機密欄位說明	秘密	欄位說明
Azure NetApp Files	ClientID	應用程式註冊的用戶端ID
適用於 GCP Cloud Volumes Service	Private金鑰ID	私密金鑰的ID。GCP服務帳戶API金鑰的一部分、具有CVS管理員角色
適用於 GCP Cloud Volumes Service	Private金鑰	私密金鑰：GCP服務帳戶API金鑰的一部分、具有CVS管理員角色
元素（NetApp HCI / SolidFire）	端點	MVIP、適用於SolidFire 採用租戶認證的不含用戶身分證明的叢集
ONTAP	使用者名稱	連線至叢集/ SVM的使用者名稱。用於認證型驗證
ONTAP	密碼	連線至叢集/ SVM的密碼。用於認證型驗證
ONTAP	用戶端權限金鑰	用戶端私密金鑰的Base64編碼值。用於憑證型驗證

儲存平台機密欄位說明	秘密	欄位說明
ONTAP	chap使用 者名稱	傳入使用者名稱。如果useCHAP=true則需要。適用於ontap-san 和 ontap-san-economy
ONTAP	chapInitiator機密	CHAP啟動器密碼。如果useCHAP=true則需要。適用於ontap-san 和 ontap-san-economy
ONTAP	chapTargetUsername	目標使用者名稱。如果useCHAP=true則需要。適用於ontap-san 和 ontap-san-economy
ONTAP	chapTargetInitiator機密	CHAP目標啟動器機密。如果useCHAP=true則需要。適用於ontap-san 和 ontap-san-economy

在此步驟中建立的機密將會在中參考 `spec.credentials` 的欄位 `TridentBackendConfig` 下一步建立的物件。

## 步驟2：建立 `TridentBackendConfig` CR

您現在已準備好建立 `TridentBackendConfig` CR.在此範例中、使用的後端 `ontap-san` 驅動程式是使用建立的 `TridentBackendConfig` 物件如下所示：

```
kubectl -n trident create -f backend-tbc-ontap-san.yaml
```

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

### 步驟3：確認的狀態 TridentBackendConfig CR

現在您已經建立了 TridentBackendConfig 您可以驗證狀態。請參閱下列範例：

```
kubectl -n trident get tbc backend-tbc-ontap-san
NAME                                BACKEND NAME                                BACKEND UUID
PHASE    STATUS
backend-tbc-ontap-san    ontap-san-backend    8d24fce7-6f60-4d4a-8ef6-
bab2699e6ab8    Bound    Success
```

已成功建立後端並連結至 TridentBackendConfig CR.

階段可以採用下列其中一個值：

- Bound：TridentBackendConfig CR與後端相關聯、且後端包含 configRef 設定為 TridentBackendConfig CR的uid。
- Unbound：表示使用 ""。TridentBackendConfig 物件未繫結至後端。所有新建立的 TridentBackendConfig CRS預設處於此階段。階段變更之後、就無法再恢復為Unbound（未綁定）。
- Deleting：TridentBackendConfig 請參閱 deletionPolicy 已設定為刪除。當 TridentBackendConfig 系統會刪除CR、並轉換為「刪除」狀態。
  - 如果後端上不存在持續磁碟區宣告（PVCS）、請刪除 TridentBackendConfig 將導致Astra Trident 刪除後端及 TridentBackendConfig CR.
  - 如果後端上有一個或多個PVCS、則會進入刪除狀態。TridentBackendConfig 接著、CR也會進入刪除階段。後端和 TridentBackendConfig 僅在刪除所有PVCS之後才會刪除。
- Lost：與關聯的後端 TridentBackendConfig 意外或蓄意刪除及 TridentBackendConfig CR仍有已刪除後端的參考資料。TridentBackendConfig 無論使用何種方法、仍可刪除CR deletionPolicy 價值。
- Unknown：Astra Trident無法判斷與相關聯的後端狀態或存在 TridentBackendConfig CR.例如、如果API伺服器沒有回應或是 tridentbackends.trident.netapp.io CRD遺失。這可能需要使用者介入。

在此階段、成功建立後端！還有多種作業可以額外處理、例如 ["後端更新和後端刪除"](#)。

### （選用）步驟4：取得更多詳細資料

您可以執行下列命令來取得有關後端的詳細資訊：

```
kubectl -n trident get tbc backend-tbc-ontap-san -o wide
```

NAME	BACKEND NAME		BACKEND UUID
PHASE	STATUS	STORAGE DRIVER	DELETION POLICY
backend-tbc-ontap-san	ontap-san-backend	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8	Bound
Success	ontap-san	delete	

此外、您也可以取得的YAML/Json傾印 TridentBackendConfig。

```
kubectl -n trident get tbc backend-tbc-ontap-san -o yaml
```

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  creationTimestamp: "2021-04-21T20:45:11Z"
  finalizers:
  - trident.netapp.io
  generation: 1
  name: backend-tbc-ontap-san
  namespace: trident
  resourceVersion: "947143"
  uid: 35b9d777-109f-43d5-8077-c74a4559d09c
spec:
  backendName: ontap-san-backend
  credentials:
    name: backend-tbc-ontap-san-secret
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  storageDriverName: ontap-san
  svm: trident_svm
  version: 1
status:
  backendInfo:
    backendName: ontap-san-backend
    backendUUID: 8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
  deletionPolicy: delete
  lastOperationStatus: Success
  message: Backend 'ontap-san-backend' created
  phase: Bound
```

backendInfo 包含 backendName 和 backendUUID 為回應所建立的後端 TridentBackendConfig CR。lastOperationStatus 欄位代表的上次作業狀態 TridentBackendConfig 可由使用者觸發的CR（例如、使用者在中變更了內容 spec）或由Astra Trident觸發（例如、在Astra Trident重新啟動期間）。可能是「成功」或「失敗」。phase 表示之間關係的狀態 TridentBackendConfig 和後端。在上述範例中、phase 具有綁定的值、這表示 TridentBackendConfig CR與後端相關聯。

您可以執行 `kubectl -n trident describe tbc <tbc-cr-name>` 命令以取得事件記錄的詳細資料。



您無法更新或刪除包含相關聯的後端 `TridentBackendConfig` 物件使用 `tridentctl`。瞭解切換的步驟 `tridentctl` 和 `TridentBackendConfig`、["請參閱此處"](#)。

## 以KECBECVL執行後端管理

瞭解如何使用執行後端管理作業 `kubectl`。

### 刪除後端

刪除 `TridentBackendConfig`、您可以指示Astra Trident刪除/保留後端（根據 `deletionPolicy`）。若要刪除後端、請確定 `deletionPolicy` 設定為刪除。僅刪除 `TridentBackendConfig`、請務必確認 `deletionPolicy` 設定為保留。如此可確保後端仍存在、並可使用進行管理 `tridentctl`。

執行下列命令：

```
kubectl delete tbc <tbc-name> -n trident
```

Astra Trident並不會刪除使用中的Kubernetes Secrets `TridentBackendConfig`。Kubernetes使用者負責清除機密。刪除機密時必須小心。只有在後端未使用機密時、才應刪除這些機密。

### 檢視現有的後端

執行下列命令：

```
kubectl get tbc -n trident
```

您也可以執行 `tridentctl get backend -n trident` 或 `tridentctl get backend -o yaml -n trident` 以取得所有後端的清單。此清單也會包含使用建立的後端 `tridentctl`。

### 更新後端

更新後端可能有多種原因：

- 儲存系統的認證資料已變更。若要更新認證資料、請使用中的Kubernetes Secret `TridentBackendConfig` 物件必須更新。Astra Trident會自動以提供的最新認證資料更新後端。執行下列命令以更新Kubernetes Secret：

```
kubectl apply -f <updated-secret-file.yaml> -n trident
```

- 需要ONTAP 更新參數（例如使用的SVM名稱）。在此案例中、`TridentBackendConfig` 物件可直接透過Kubernetes更新。

```
kubectl apply -f <updated-backend-file.yaml>
```

或者、也可以變更現有的 TridentBackendConfig 請執行下列命令以執行CR..

```
kubectl edit tbc <tbc-name> -n trident
```

如果後端更新失敗、後端仍會繼續維持其最後已知的組態。您可以檢視記錄、藉由執行來判斷原因 `kubectl get tbc <tbc-name> -o yaml -n trident` 或 `kubectl describe tbc <tbc-name> -n trident`。

識別並修正組態檔的問題之後、即可重新執行update命令。

## 使用tridentctl執行後端管理

瞭解如何使用執行後端管理作業 tridentctl。

### 建立後端

建立之後 "後端組態檔"，執行下列命令：

```
tridentctl create backend -f <backend-file> -n trident
```

如果後端建立失敗、表示後端組態有問題。您可以執行下列命令來檢視記錄、以判斷原因：

```
tridentctl logs -n trident
```

識別並修正組態檔案的問題之後、您只需執行即可 create 命令。

### 刪除後端

若要從Astra Trident刪除後端、請執行下列步驟：

1. 擷取後端名稱：

```
tridentctl get backend -n trident
```

2. 刪除後端：

```
tridentctl delete backend <backend-name> -n trident
```



如果Astra Trident已從這個後端配置磁碟區和快照、但該後端仍存在、則刪除後端會使新的磁碟區無法由其進行資源配置。後端將繼續處於「刪除」狀態、而Trident將繼續管理這些磁碟區和快照、直到它們被刪除為止。

## 檢視現有的後端

若要檢視Trident知道的後端、請執行下列步驟：

- 若要取得摘要、請執行下列命令：

```
tridentctl get backend -n trident
```

- 若要取得所有詳細資料、請執行下列命令：

```
tridentctl get backend -o json -n trident
```

## 更新後端

建立新的後端組態檔之後、請執行下列命令：

```
tridentctl update backend <backend-name> -f <backend-file> -n trident
```

如果後端更新失敗、表示後端組態有問題、或是您嘗試了無效的更新。您可以執行下列命令來檢視記錄、以判斷原因：

```
tridentctl logs -n trident
```

識別並修正組態檔案的問題之後、您只需執行即可 `update` 命令。

## 識別使用後端的儲存類別

這是您可以用Json回答的問題類型範例 `tridentctl` 後端物件的輸出。這會使用 `jq` 公用程式、您需要安裝。

```
tridentctl get backend -o json | jq '[.items[] | {backend: .name, storageClasses: [.storage[].storageClasses]|unique}]'
```

這也適用於使用建立的後端 `TridentBackendConfig`。

## 在後端管理選項之間切換

瞭解Astra Trident管理後端的不同方法。隨之推出 `TridentBackendConfig` 管理員現在有兩種獨特的後端管理方

法。這會提出下列問題：

- 可以使用建立後端 `tridentctl` 以進行管理 `TridentBackendConfig`？
- 可以使用建立後端 `TridentBackendConfig` 使用進行管理 `tridentctl`？

## 管理 `tridentctl` 後端使用 `TridentBackendConfig`

本節說明管理使用建立之後端所需的步驟 `tridentctl` 透過建立、直接透過Kubernetes介面 `TridentBackendConfig` 物件：

這將適用於下列案例：

- 預先存在的後端、但沒有 `TridentBackendConfig` 因為它們是使用建立的 `tridentctl`。
- 使用建立的新後端 `tridentctl`、而其他 `TridentBackendConfig` 物件存在。

在這兩種情況下、後端仍會繼續存在、Astra Trident排程磁碟區會繼續運作。系統管理員有兩種選擇之一：

- 繼續使用 `tridentctl` 管理使用它建立的後端。
- 使用建立連結後端 `tridentctl` 新功能 `TridentBackendConfig` 物件：如此一來、後端就會使用進行管理 `kubectl` 而非 `tridentctl`。

若要使用管理預先存在的後端 `kubectl`、您需要建立 `TridentBackendConfig` 連結至現有後端。以下是如何運作的總覽：

1. 建立Kubernetes機密。此機密包含Astra Trident與儲存叢集/服務通訊所需的認證資料。
2. 建立 `TridentBackendConfig` 物件：其中包含有關儲存叢集/服務的詳細資訊、並參考上一步建立的機密。必須謹慎指定相同的組態參數（例如 `spec.backendName`、`spec.storagePrefix`、`spec.storageDriverName`等）。`spec.backendName` 必須設定為現有後端的名稱。

### 步驟0：識別後端

以建立 `TridentBackendConfig` 若要連結至現有的後端、您必須取得後端組態。在此範例中、假設使用下列Json定義建立後端：

```
tridentctl get backend ontap-nas-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |                      UUID                      |
| STATE  | VOLUMES |                      |                      |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-nas-backend      | ontap-nas      | 52f2eb10-e4c6-4160-99fc-96b3be5ab5d7 |
| online |      25 |                      |                      |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

cat ontap-nas-backend.json
```



```

{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.10.10.1",
  "dataLIF": "10.10.10.2",
  "backendName": "ontap-nas-backend",
  "svm": "trident_svm",
  "username": "cluster-admin",
  "password": "admin-password",

  "defaults": {
    "spaceReserve": "none",
    "encryption": "false"
  },
  "labels": {"store": "nas_store"},
  "region": "us_east_1",
  "storage": [
    {
      "labels": {"app": "msoffice", "cost": "100"},
      "zone": "us_east_1a",
      "defaults": {
        "spaceReserve": "volume",
        "encryption": "true",
        "unixPermissions": "0755"
      }
    },
    {
      "labels": {"app": "mysqldb", "cost": "25"},
      "zone": "us_east_1d",
      "defaults": {
        "spaceReserve": "volume",
        "encryption": "false",
        "unixPermissions": "0775"
      }
    }
  ]
}

```

### 步驟1：建立Kubernetes機密

建立包含後端認證的秘密、如以下範例所示：

```
cat tbc-ontap-nas-backend-secret.yaml

apiVersion: v1
kind: Secret
metadata:
  name: ontap-nas-backend-secret
type: Opaque
stringData:
  username: cluster-admin
  password: admin-password

kubectl create -f tbc-ontap-nas-backend-secret.yaml -n trident
secret/backend-tbc-ontap-san-secret created
```

## 步驟2：建立 TridentBackendConfig CR

下一步是建立 TridentBackendConfig 會自動連結至預先存在的CR ontap-nas-backend（如本範例所示）。確保符合下列要求：

- 中定義了相同的後端名稱 spec.backendName。
- 組態參數與原始後端相同。
- 虛擬資源池（若有）必須維持與原始後端相同的順序。
- 認證資料是透過Kubernetes Secret提供、而非以純文字提供。

在此案例中 TridentBackendConfig 如下所示：

```

cat backend-tbc-ontap-nas.yaml
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: tbc-ontap-nas-backend
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.10.10.1
  dataLIF: 10.10.10.2
  backendName: ontap-nas-backend
  svm: trident_svm
  credentials:
    name: mysecret
  defaults:
    spaceReserve: none
    encryption: 'false'
  labels:
    store: nas_store
  region: us_east_1
  storage:
  - labels:
      app: msoffice
      cost: '100'
      zone: us_east_1a
      defaults:
        spaceReserve: volume
        encryption: 'true'
        unixPermissions: '0755'
  - labels:
      app: mysqldb
      cost: '25'
      zone: us_east_1d
      defaults:
        spaceReserve: volume
        encryption: 'false'
        unixPermissions: '0775'

kubectl create -f backend-tbc-ontap-nas.yaml -n trident
tridentbackendconfig.trident.netapp.io/tbc-ontap-nas-backend created

```

### 步驟3：確認的狀態 TridentBackendConfig **CR**

之後 TridentBackendConfig 已經建立、其階段必須是 Bound。它也應反映與現有後端相同的後端名稱和UUID。

```
kubectl -n trident get tbc tbc-ontap-nas-backend -n trident
```

NAME	BACKEND NAME	BACKEND UUID
tbc-ontap-nas-backend	ontap-nas-backend	52f2eb10-e4c6-4160-99fc-96b3be5ab5d7

```

PHASE    STATUS
Bound    Success

#confirm that no new backends were created (i.e., TridentBackendConfig did
not end up creating a new backend)
tridentctl get backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE  | VOLUMES |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-nas-backend      | ontap-nas      | 52f2eb10-e4c6-4160-99fc-96b3be5ab5d7 |
| online |      25 |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

```

後端現在將使用完全管理 tbc-ontap-nas-backend TridentBackendConfig 物件：

## 管理 TridentBackendConfig 後端使用 tridentctl

`tridentctl` 可用來列出使用建立的後端  
 `TridentBackendConfig`。此外、系統管理員也可以選擇透過完全管理此類後端  
 `tridentctl` 刪除 `TridentBackendConfig` 並確保 `spec.deletionPolicy` 設為  
 `retain`。

### 步驟0：識別後端

例如、假設下列後端是使用建立的 TridentBackendConfig：

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME                                BACKEND UUID
PHASE    STATUS    STORAGE DRIVER    DELETION POLICY
backend-tbc-ontap-san    ontap-san-backend    81abcb27-ea63-49bb-b606-
0a5315ac5f82    Bound    Success    ontap-san    delete

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|      NAME      | STORAGE DRIVER |                                UUID
| STATE  | VOLUMES |
+-----+-----+
+-----+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-
0a5315ac5f82 | online |      33 |
+-----+-----+
+-----+-----+-----+-----+
```

從輸出中可以看出這一點 TridentBackendConfig 已成功建立、並繫結至後端（觀察後端的UUID）。

**步驟1：確認 deletionPolicy 設為 retain**

讓我們來看看的價值 deletionPolicy。這需要設定為 retain。這可確保在發生時 TridentBackendConfig 刪除CR後、後端定義仍會顯示、並可透過進行管理 tridentctl。

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME                                BACKEND UUID
PHASE    STATUS    STORAGE DRIVER    DELETION POLICY
backend-tbc-ontap-san    ontap-san-backend    81abcb27-ea63-49bb-b606-
0a5315ac5f82    Bound    Success    ontap-san    delete

# Patch value of deletionPolicy to retain
kubectl patch tbc backend-tbc-ontap-san --type=merge -p
'{"spec":{"deletionPolicy":"retain"}}' -n trident
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-san patched

#Confirm the value of deletionPolicy
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME                                BACKEND UUID
PHASE    STATUS    STORAGE DRIVER    DELETION POLICY
backend-tbc-ontap-san    ontap-san-backend    81abcb27-ea63-49bb-b606-
0a5315ac5f82    Bound    Success    ontap-san    retain
```



除非如此、否則請勿繼續下一步 deletionPolicy 設為 retain。

## 步驟2：刪除 TridentBackendConfig CR

最後一個步驟是刪除 TridentBackendConfig CR。確認之後 deletionPolicy 設為 retain、您可以繼續刪除：

```
kubectl delete tbc backend-tbc-ontap-san -n trident
tridentbackendconfig.trident.netapp.io "backend-tbc-ontap-san" deleted

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |                      UUID                      |
| STATE  | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-0a5315ac5f82 |
| online |      33 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

刪除時 TridentBackendConfig 物件：Astra Trident只會移除它、而不會實際刪除後端本身。

## 管理儲存類別

尋找建立儲存類別、刪除儲存類別及檢視現有儲存類別的相關資訊。

### 設計儲存類別

請參閱 ["請按這裡"](#) 以取得有關儲存類別及其設定方式的詳細資訊。

### 建立儲存類別

取得儲存類別檔案之後、請執行下列命令：

```
kubectl create -f <storage-class-file>
```

<storage-class-file> 應以您的儲存類別檔案名稱取代。

### 刪除儲存類別

若要從Kubernetes刪除儲存類別、請執行下列命令：

```
kubectl delete storageclass <storage-class>
```

<storage-class> 應更換為您的儲存類別。

透過此儲存類別所建立的任何持續磁碟區都將維持不變、Astra Trident將繼續管理這些磁碟區。



Astra Trident強制執行空白 `fsType` 針對所建立的磁碟區。對於iSCSI後端、建議強制執行 `parameters.fsType` 在StorageClass中。您應該刪除現有的StorageClass並重新建立 `parameters.fsType` 已指定。

## 檢視現有的儲存類別

- 若要檢視現有的Kubernetes儲存類別、請執行下列命令：

```
kubectl get storageclass
```

- 若要檢視Kubernetes儲存類別詳細資料、請執行下列命令：

```
kubectl get storageclass <storage-class> -o json
```

- 若要檢視Astra Trident的同步儲存類別、請執行下列命令：

```
tridentctl get storageclass
```

- 若要檢視Astra Trident的同步儲存類別詳細資料、請執行下列命令：

```
tridentctl get storageclass <storage-class> -o json
```

## 設定預設儲存類別

Kubernetes 1.6新增了設定預設儲存類別的功能。如果使用者未在「持續磁碟區宣告」(PVC) 中指定一個、則此儲存類別將用於配置「持續磁碟區」。

- 設定註釋以定義預設儲存類別 `storageclass.kubernetes.io/is-default-class` 儲存類別定義中的「真」。根據規格、任何其他值或不存在附註都會解譯為假。
- 您可以使用下列命令、將現有的儲存類別設定為預設的儲存類別：

```
kubectl patch storageclass <storage-class-name> -p '{"metadata":  
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

- 同樣地、您也可以使用下列命令移除預設儲存類別註釋：

```
kubectl patch storageclass <storage-class-name> -p '{"metadata":  
{"annotations":{"storageclass.kubernetes.io/is-default-class":"false"}}}'
```

Trident安裝程式套件中也有包含此附註的範例。



在任何指定時間、您的叢集中都只應有一個預設儲存類別。Kubernetes在技術上並不妨礙您擁有多個儲存類別、但它的行為方式就如同完全沒有預設的儲存類別一樣。

## 識別儲存類別的後端

這是您可以用Json回答的問題類型範例 `tridentctl Astra Trident`後端物件的輸出。這會使用 `jq` 公用程式、您可能需要先安裝。

```
tridentctl get storageclass -o json | jq '[.items[] | {storageClass:  
.Config.name, backends: [.storage]|unique}]'
```

## 執行Volume作業

深入瞭解Astra Trident提供的功能、協助您管理磁碟區。

- "使用「[csi拓撲](#)」"
- "使用快照"
- "展開Volume"
- "匯入磁碟區"

### 使用「csi拓撲」

Astra Trident可以利用、選擇性地建立磁碟區、並將磁碟區附加至Kubernetes叢集中的節點 "[「csi拓撲」功能](#)"。使用「csi拓撲」功能、可根據區域和可用性區域、限制對磁碟區的存取、只能存取一部分節點。如今、雲端供應商可讓Kubernetes管理員建立以區域為基礎的節點。節點可位於某個區域內的不同可用度區域、或位於不同區域之間。為了協助在多區域架構中配置工作負載的磁碟區、Astra Trident使用了csi拓撲。



深入瞭解「csi拓撲」功能 "[請按這裡](#)"。

Kubernetes提供兩種獨特的Volume繫結模式：

- 與 `VolumeBindingMode` 設定為 `Immediate` `Astra Trident在沒有任何拓撲感知的情況下建立磁碟區。建立永久虛擬磁碟時、即會處理磁碟區繫結和動態資源配置。這是預設值 `VolumeBindingMode 適用於未強制拓撲限制的叢集。建立永續性磁碟區時、不會對要求的Pod排程需求有任何相依性。
- 與 `VolumeBindingMode` 設定為 `WaitForFirstConsumer`、永久磁碟區的建立與繫結會延遲、直到排程並建立使用該永久磁碟的Pod為止。如此一來、就能建立磁碟區、以符合拓撲需求所強制執行的排程限制。



◦ `WaitForFirstConsumer` 繫結模式不需要拓撲標籤。這可獨立於「csi拓撲」功能使用。



## 您需要的產品

若使用「csi拓撲」、您需要下列項目：

- 執行的Kubernetes叢集 ["支援的Kubernetes版本"](#)

```
kubectl version
Client Version: version.Info{Major:"1", Minor:"19",
GitVersion:"v1.19.3",
GitCommit:"1e11e4a2108024935ecfcb2912226cedaafd99df",
GitTreeState:"clean", BuildDate:"2020-10-14T12:50:19Z",
GoVersion:"go1.15.2", Compiler:"gc", Platform:"linux/amd64"}
Server Version: version.Info{Major:"1", Minor:"19",
GitVersion:"v1.19.3",
GitCommit:"1e11e4a2108024935ecfcb2912226cedaafd99df",
GitTreeState:"clean", BuildDate:"2020-10-14T12:41:49Z",
GoVersion:"go1.15.2", Compiler:"gc", Platform:"linux/amd64"}
```

- 叢集中的節點應該有標籤來介紹拓撲認知 (topology.kubernetes.io/region 和 topology.kubernetes.io/zone) 。在安裝Astra Trident以識別拓撲之前、這些標籤\*應該會出現在叢集\*的節點上。

```
kubectl get nodes -o=jsonpath='{range .items[*]}[{.metadata.name},
{.metadata.labels}][{"\n"}]{end}' | grep --color "topology.kubernetes.io"
[node1,
{"beta.kubernetes.io/arch":"amd64","beta.kubernetes.io/os":"linux","kubernetes.io/arch":"amd64","kubernetes.io/hostname":"node1","kubernetes.io/os":"linux","node-role.kubernetes.io/master":"","topology.kubernetes.io/region":"us-east1","topology.kubernetes.io/zone":"us-east1-a"}]
[node2,
{"beta.kubernetes.io/arch":"amd64","beta.kubernetes.io/os":"linux","kubernetes.io/arch":"amd64","kubernetes.io/hostname":"node2","kubernetes.io/os":"linux","node-role.kubernetes.io/worker":"","topology.kubernetes.io/region":"us-east1","topology.kubernetes.io/zone":"us-east1-b"}]
[node3,
{"beta.kubernetes.io/arch":"amd64","beta.kubernetes.io/os":"linux","kubernetes.io/arch":"amd64","kubernetes.io/hostname":"node3","kubernetes.io/os":"linux","node-role.kubernetes.io/worker":"","topology.kubernetes.io/region":"us-east1","topology.kubernetes.io/zone":"us-east1-c"}]
```

## 步驟1：建立可感知拓撲的後端

Astra Trident儲存後端可根據可用性區域、選擇性地配置磁碟區。每個後端都可隨附選用功能 `supportedTopologies` 代表必須支援之區域和區域清單的區塊。對於使用此類後端的StorageClass、只有在受支援地區/區域中排程的應用程式要求時、才會建立Volume。

以下是後端定義範例：

### YAML

```
---
version: 1
storageDriverName: ontap-san
backendName: san-backend-us-east1
managementLIF: 192.168.27.5
svm: iscsi_svm
username: admin
password: password
supportedTopologies:
- topology.kubernetes.io/region: us-east1
  topology.kubernetes.io/zone: us-east1-a
- topology.kubernetes.io/region: us-east1
  topology.kubernetes.io/zone: us-east1-b
```

### JSON

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "san-backend-us-east1",
  "managementLIF": "192.168.27.5",
  "svm": "iscsi_svm",
  "username": "admin",
  "password": "password",
  "supportedTopologies": [
    {"topology.kubernetes.io/region": "us-east1",
     "topology.kubernetes.io/zone": "us-east1-a"},
    {"topology.kubernetes.io/region": "us-east1",
     "topology.kubernetes.io/zone": "us-east1-b"}
  ]
}
```



`supportedTopologies` 用於提供每個後端的區域和區域清單。這些區域和區域代表StorageClass中可提供的允許值清單。對於包含後端所提供之區域和區域子集的StorageClass、Astra Trident會在後端建立磁碟區。

您可以定義 `supportedTopologies` 也可依儲存資源池。請參閱下列範例：

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas-backend-us-central1
managementLIF: 172.16.238.5
svm: nfs_svm
username: admin
password: password
supportedTopologies:
- topology.kubernetes.io/region: us-central1
  topology.kubernetes.io/zone: us-central1-a
- topology.kubernetes.io/region: us-central1
  topology.kubernetes.io/zone: us-central1-b
storage:
- labels:
    workload: production
    region: Iowa-DC
    zone: Iowa-DC-A
    supportedTopologies:
    - topology.kubernetes.io/region: us-central1
      topology.kubernetes.io/zone: us-central1-a
- labels:
    workload: dev
    region: Iowa-DC
    zone: Iowa-DC-B
    supportedTopologies:
    - topology.kubernetes.io/region: us-central1
      topology.kubernetes.io/zone: us-central1-b
```

在此範例中 `region` 和 `zone` 標籤代表儲存資源池的位置。 `topology.kubernetes.io/region` 和 `topology.kubernetes.io/zone` 指定儲存資源池的使用來源。

## 步驟2：定義可感知拓撲的**StorageClass**

根據提供給叢集中節點的拓撲標籤、可以定義**StorageClass**以包含拓撲資訊。這將決定做為所提出之永久虛擬磁碟要求候選的儲存資源池、以及可以使用Trident所提供之磁碟區的節點子集。

請參閱下列範例：

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: netapp-san-us-east1
provisioner: csi.trident.netapp.io
volumeBindingMode: WaitForFirstConsumer
allowedTopologies:
- matchLabelExpressions:
- key: topology.kubernetes.io/zone
  values:
  - us-east1-a
  - us-east1-b
- key: topology.kubernetes.io/region
  values:
  - us-east1
parameters:
  fsType: "ext4"

```

在上述StorageClass定義中、volumeBindingMode 設為 WaitForFirstConsumer。在Pod中引用此StorageClass所要求的PVCS之前、系統不會對其採取行動。而且、allowedTopologies 提供要使用的區域和區域。netapp-san-us-east1 StorageClass會在上建立PVCS san-backend-us-east1 上述定義的後端。

### 步驟3：建立並使用PVC

建立StorageClass並對應至後端後端後端之後、您現在就可以建立PVCS。

請參閱範例 spec 以下：

```

---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 300Mi
  storageClassName: netapp-san-us-east1

```

使用此資訊清單建立永久虛擬環境可能會產生下列結果：

```

kubect1 create -f pvc.yaml
persistentvolumeclaim/pvc-san created
kubect1 get pvc
NAME          STATUS      VOLUME      CAPACITY    ACCESS MODES    STORAGECLASS
AGE
pvc-san      Pending                                netapp-san-us-east1
2s
kubect1 describe pvc
Name:          pvc-san
Namespace:     default
StorageClass:  netapp-san-us-east1
Status:        Pending
Volume:
Labels:        <none>
Annotations:   <none>
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:
Access Modes:
VolumeMode:    Filesystem
Mounted By:    <none>
Events:
  Type      Reason              Age    From
  ----      -
  Normal    WaitForFirstConsumer  6s     persistentvolume-controller
waiting
for first consumer to be created before binding

```

若要Trident建立磁碟區並將其連結至PVC、請在Pod中使用PVC。請參閱下列範例：

```

apiVersion: v1
kind: Pod
metadata:
  name: app-pod-1
spec:
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
          - matchExpressions:
              - key: topology.kubernetes.io/region
                operator: In
                values:
                  - us-east1
      preferredDuringSchedulingIgnoredDuringExecution:
        - weight: 1
          preference:
            matchExpressions:
              - key: topology.kubernetes.io/zone
                operator: In
                values:
                  - us-east1-a
                  - us-east1-b
    securityContext:
      runAsUser: 1000
      runAsGroup: 3000
      fsGroup: 2000
  volumes:
    - name: vol1
      persistentVolumeClaim:
        claimName: pvc-san
  containers:
    - name: sec-ctx-demo
      image: busybox
      command: [ "sh", "-c", "sleep 1h" ]
      volumeMounts:
        - name: vol1
          mountPath: /data/demo
      securityContext:
        allowPrivilegeEscalation: false

```

此podSpec會指示Kubernetes在中的節點上排程pod us-east1 區域、並從中的任何節點中進行選擇 us-east1-a 或 us-east1-b 區域。

請參閱下列輸出：

```
kubectl get pods -o wide
NAME          READY   STATUS    RESTARTS   AGE   IP              NODE
NOMINATED NODE READINESS GATES
app-pod-1     1/1     Running   0           19s   192.168.25.131  node2
<none>        <none>
kubectl get pvc -o wide
NAME          STATUS    VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS          AGE   VOLUMEMODE
pvc-san       Bound     pvc-ecb1e1a0-840c-463b-8b65-b3d033e2e62b  300Mi
RWO           netapp-san-us-east1   48s   Filesystem
```

更新後端以納入 supportedTopologies

您可以更新現有的後端、以納入清單 supportedTopologies 使用 `tridentctl backend update`。這不會影響已配置的磁碟區、而且只會用於後續的PVCS。

如需詳細資訊、請參閱

- ["管理容器的資源"](#)
- ["節點選取器"](#)
- ["關聯性與反關聯性"](#)
- ["污染與容許"](#)

## 使用快照

您可以建立持續磁碟區 (PV) 的Kubernetes Volume Snapshot (Volume Snapshot)、以維護Astra Trident磁碟區的時間點複本。此外、您也可以從現有的Volume Snapshot建立新的Volume、也稱為`_clon__`。支援Volume Snapshot `ontap-nas`、`ontap-nas-flexgroup`、`ontap-san`、`ontap-san-economy`、`solidfire-san`、`gcp-cvs`和 `azure-netapp-files` 驅動程式：

開始之前

您必須擁有外部快照控制器和自訂資源定義 (CRD)。這是Kubernetes Orchestrator的責任 (例如：Kubeadm、GKE、OpenShift)。

如果您的Kubernetes發佈版本未包含快照控制器和CRD、請參閱 [部署Volume Snapshot控制器](#)。



如果在GKE環境中建立隨需磁碟區快照、請勿建立快照控制器。GKE使用內建的隱藏式快照控制器。

步驟1：建立 VolumeSnapshotClass

此範例會建立Volume Snapshot類別。

```
cat snap-sc.yaml
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: csi-snapclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

◦ `driver` 指向Astra Trident的SCSI驅動程式。◦ `deletionPolicy` 可以 `Delete` 或 `Retain`。◦ 設定為 `Retain`、儲存叢集上的基礎實體快照、即使在 `VolumeSnapshot` 物件已刪除。

如需詳細資訊、請參閱連結：[../Trident參考/objects.html#Kubernetes-volumesnapshotclass-objects\[VolumeSnapshotClass\]](#)。

## 步驟2：建立現有PVC的快照

此範例會建立現有PVC的快照。

```
cat snap.yaml
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshot
metadata:
  name: pvc1-snap
spec:
  volumeSnapshotClassName: csi-snapclass
  source:
    persistentVolumeClaimName: pvc1
```

在此範例中、快照是針對名為的PVC建立 `pvc1` 快照名稱設為 `pvc1-snap`。

```
kubectl create -f snap.yaml
volumesnapshot.snapshot.storage.k8s.io/pvc1-snap created

kubectl get volumesnapshots
NAME                                AGE
pvc1-snap                          50s
```

這會建立一個 `VolumeSnapshot` 物件：`Volume Snapshot`類似於PVC、並與相關聯 `VolumeSnapshotContent` 代表實際快照的物件。

您可以識別 `VolumeSnapshotContent` 的物件 `pvc1-snap` 描述`Volume Snapshot`。



```

kubectl describe volumesnapshots pvcl-snap
Name:          pvcl-snap
Namespace:     default
.
.
.
Spec:
  Snapshot Class Name:    pvcl-snap
  Snapshot Content Name:  snapcontent-e8d8a0ca-9826-11e9-9807-525400f3f660
  Source:
    API Group:
    Kind:      PersistentVolumeClaim
    Name:      pvcl
Status:
  Creation Time:  2019-06-26T15:27:29Z
  Ready To Use:   true
  Restore Size:   3Gi
.
.

```

◦ Snapshot Content Name 識別提供此快照的Volume SnapshotContent物件。◦ Ready To Use 參數表示Snapshot可用於建立新的PVC。

### 步驟3：從Volume Snapshot建立PVCS

此範例使用快照建立一個PVC..

```

cat pvc-from-snap.yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc-from-snap
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: golden
  resources:
    requests:
      storage: 3Gi
  dataSource:
    name: pvcl-snap
    kind: VolumeSnapshot
    apiGroup: snapshot.storage.k8s.io

```

dataSource 顯示必須使用名為的Volume Snapshot建立PVC pvc1-snap 做為資料來源。這會指示Astra Trident從快照建立一個永久虛擬資料。建立好永久虛擬基礎架構之後、就能將它附加到Pod上、就像使用任何其他永久虛擬基礎架構一樣使用。



刪除具有相關快照的持續Volume時、對應的Trident Volume會更新為「刪除狀態」。若要刪除Astra Trident磁碟區、則應移除該磁碟區的快照。

## 部署Volume Snapshot控制器

如果您的Kubernetes發佈版本未包含快照控制器和客戶需求日、您可以依照下列方式進行部署。

### 步驟

1. 建立Volume Snapshot客戶需求日。

```
cat snapshot-setup.sh
#!/bin/bash
# Create volume snapshot CRDs
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-6.1/client/config/crd/snapshot.storage.k8s.io_volumesnapshotclasses.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-6.1/client/config/crd/snapshot.storage.k8s.io_volumesnapshotcontents.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-6.1/client/config/crd/snapshot.storage.k8s.io_volumesnapshots.yaml
```

2. 在所需的命名空間中建立Snapshot控制器。編輯下方的Yaml清單以修改命名空間。

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-6.1/deploy/kubernetes/snapshot-controller/rbac-snapshot-controller.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-6.1/deploy/kubernetes/snapshot-controller/setup-snapshot-controller.yaml
```

### 相關連結

- ["Volume快照"](#)
- ["Volume SnapshotClass"](#)

## 展開Volume

Astra Trident可讓Kubernetes使用者在建立磁碟區之後擴充磁碟區。尋找擴充iSCSI和NFS磁碟區所需組態的相關資訊。

### 展開iSCSI Volume

您可以使用「SCSI資源配置程式」來擴充iSCSI持續磁碟區（PV）。



支援iSCSI Volume擴充 `ontap-san`、`ontap-san-economy`、`solidfire-san` 並需要Kubernetes 1.16及更新版本。

#### 總覽

擴充iSCSI PV包括下列步驟：

- 編輯StorageClass定義以設定 `allowVolumeExpansion` 欄位至 `true`。
- 編輯PVC定義並更新 `spec.resources.requests.storage` 以反映新的所需大小、此大小必須大於原始大小。
- 必須將PV附加至Pod、才能調整其大小。調整iSCSI PV的大小有兩種情況：
  - 如果PV附加至Pod、Astra Trident會在儲存後端擴充磁碟區、重新掃描裝置、並重新調整檔案系統的大小。
  - 嘗試調整未附加PV的大小時、Astra Trident會在儲存後端上擴充磁碟區。在將永久虛擬磁碟綁定至Pod之後、Trident會重新掃描裝置並重新調整檔案系統的大小。然後、Kubernetes會在擴充作業成功完成後、更新PVC大小。

以下範例顯示擴充iSCSI PV的運作方式。

步驟1：設定StorageClass以支援Volume擴充

```
cat storageclass-ontapsan.yaml
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-san
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
allowVolumeExpansion: True
```

對於已存在的StorageClass、請編輯此類以納入 `allowVolumeExpansion` 參數。

步驟2：使用您建立的StorageClass建立一個永久虛擬儲存設備

```

cat pvc-ontapsan.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: san-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-san

```

Astra Trident會建立持續磁碟區（PV）、並將其與此持續磁碟區宣告（PVC）建立關聯。

```

kubectl get pvc

```

NAME	STATUS	VOLUME	CAPACITY
san-pvc	Bound	pvc-8a814d62-bd58-4253-b0d1-82f2885db671	1Gi
RWO		ontap-san	8s

```

kubectl get pv

```

NAME	CAPACITY	ACCESS MODES
pvc-8a814d62-bd58-4253-b0d1-82f2885db671	1Gi	RWO
Delete	Bound	default/san-pvc
		ontap-san
		10s

**步驟3：**定義一個連接至PVC的Pod

在此範例中、會建立使用的Pod san-pvc。

```

kubectll get pod
NAME          READY   STATUS    RESTARTS   AGE
ubuntu-pod    1/1     Running   0           65s

kubectll describe pvc san-pvc
Name:          san-pvc
Namespace:     default
StorageClass:  ontap-san
Status:        Bound
Volume:        pvc-8a814d62-bd58-4253-b0d1-82f2885db671
Labels:        <none>
Annotations:   pv.kubernetes.io/bind-completed: yes
               pv.kubernetes.io/bound-by-controller: yes
               volume.beta.kubernetes.io/storage-provisioner:
               csi.trident.netapp.io
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:      1Gi
Access Modes:  RWO
VolumeMode:    Filesystem
Mounted By:    ubuntu-pod

```

#### 步驟4：展開PV

若要調整從1Gi建立至2Gi的PV大小、請編輯PVC定義並更新 `spec.resources.requests.storage` 至2Gi。

```
kubectl edit pvc san-pvc
# Please edit the object below. Lines beginning with a '#' will be
ignored,
# and an empty file will abort the edit. If an error occurs while saving
this file will be
# reopened with the relevant failures.
#
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  annotations:
    pv.kubernetes.io/bind-completed: "yes"
    pv.kubernetes.io/bound-by-controller: "yes"
    volume.beta.kubernetes.io/storage-provisioner: csi.trident.netapp.io
  creationTimestamp: "2019-10-10T17:32:29Z"
  finalizers:
  - kubernetes.io/pvc-protection
  name: san-pvc
  namespace: default
  resourceVersion: "16609"
  selfLink: /api/v1/namespaces/default/persistentvolumeclaims/san-pvc
  uid: 8a814d62-bd58-4253-b0d1-82f2885db671
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 2Gi
  ...
```

#### 步驟5：驗證擴充

您可以檢查PVC、PV和Astra Trident Volume的大小、以正確驗證擴充作業：

```
kubectl get pvc san-pvc
NAME          STATUS    VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS  AGE
san-pvc      Bound       pvc-8a814d62-bd58-4253-b0d1-82f2885db671  2Gi
RWO           ontap-san    11m

kubectl get pv
NAME          CAPACITY  ACCESS MODES
RECLAIM POLICY STATUS    CLAIM          STORAGECLASS  REASON    AGE
pvc-8a814d62-bd58-4253-b0d1-82f2885db671  2Gi        RWO
Delete              Bound      default/san-pvc  ontap-san    12m

tridentctl get volumes -n trident
+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
|          NAME          | SIZE | STORAGE CLASS |
+-----+-----+-----+-----+-----+-----+
|          BACKEND UUID  | STATE | MANAGED |
+-----+-----+-----+-----+-----+-----+
| pvc-8a814d62-bd58-4253-b0d1-82f2885db671 | 2.0 GiB | ontap-san |
| block | a9b7bfff-0505-4e31-b6c5-59f492e02d33 | online | true |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
```

## 展開NFS Volume

Astra Trident支援在上配置NFS PV的Volume擴充 ontap-nas、ontap-nas-economy、ontap-nas-flexgroup、gcp-cvs和 azure-netapp-files 後端：

步驟1：設定StorageClass以支援Volume擴充

若要調整NFS PV的大小、管理員必須先設定儲存類別、以允許透過設定來擴充磁碟區  
allowVolumeExpansion 欄位至 true：

```
cat storageclass-ontapnas.yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontapnas
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
allowVolumeExpansion: true
```

如果您已建立不含此選項的儲存類別、則只要使用編輯現有的儲存類別即可 kubectl edit storageclass 以允許磁碟區擴充。

步驟2：使用您建立的**StorageClass**建立一個永久虛擬儲存設備

```
cat pvc-ontapnas.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: ontapnas20mb
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 20Mi
  storageClassName: ontapnas
```

Astra Trident應為此PVC建立20MiB NFS PV：

```
kubectl get pvc
NAME                STATUS    VOLUME
CAPACITY            ACCESS MODES  STORAGECLASS  AGE
ontapnas20mb        Bound      pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  20Mi
RWO                  ontapnas      9s

kubectl get pv pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7
NAME                CAPACITY  ACCESS MODES
RECLAIM POLICY      STATUS    CLAIM                STORAGECLASS  REASON
AGE
pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  20Mi      RWO
Delete              Bound     default/ontapnas20mb  ontapnas
2m42s
```

步驟3：展開PV

若要將新建立的20MiB PV調整至1GiB、請編輯該PVC並設定組合 `spec.resources.requests.storage` 至1GB：



```

kubectl edit pvc ontapnas20mb
# Please edit the object below. Lines beginning with a '#' will be
ignored,
# and an empty file will abort the edit. If an error occurs while saving
this file will be
# reopened with the relevant failures.
#
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  annotations:
    pv.kubernetes.io/bind-completed: "yes"
    pv.kubernetes.io/bound-by-controller: "yes"
    volume.beta.kubernetes.io/storage-provisioner: csi.trident.netapp.io
  creationTimestamp: 2018-08-21T18:26:44Z
  finalizers:
  - kubernetes.io/pvc-protection
  name: ontapnas20mb
  namespace: default
  resourceVersion: "1958015"
  selfLink: /api/v1/namespaces/default/persistentvolumeclaims/ontapnas20mb
  uid: c1bd7fa5-a56f-11e8-b8d7-fa163e59eaab
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  ...

```

#### 步驟4：驗證擴充

您可以檢查PVC、PV和Astra Trident Volume的大小、以正確驗證調整大小：

```
kubectl get pvc ontapnas20mb
NAME          STATUS    VOLUME
CAPACITY      ACCESS MODES  STORAGECLASS  AGE
ontapnas20mb  Bound      pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  1Gi
RWO           ontapnas      4m44s

kubectl get pv pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7
NAME          CAPACITY  ACCESS MODES
RECLAIM POLICY STATUS    CLAIM          STORAGECLASS  REASON
AGE
pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  1Gi      RWO
Delete      Bound    default/ontapnas20mb  ontapnas
5m35s

tridentctl get volume pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7 -n trident
+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          | SIZE  | STORAGE CLASS |
+-----+-----+-----+-----+
| PROTOCOL | BACKEND UUID | STATE | MANAGED |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7 | 1.0 GiB | ontapnas      |
file      | c5a6f6a4-b052-423b-80d4-8fb491a14a22 | online | true      |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

## 匯入磁碟區

您可以使用將現有的儲存磁碟區匯入為Kubernetes PV `tridentctl import`。

### 支援**Volume**匯入的驅動程式

下表說明支援匯入磁碟區的驅動程式、以及這些磁碟區所引進的版本。

驅動程式	版本
ontap-nas	19.04
ontap-nas-flexgroup	19.04
solidfire-san	19.04
azure-netapp-files	19.04
gcp-cvs	19.04

驅動程式	版本
ontap-san	19.04

為什麼要匯入磁碟區？

將Volume匯入Trident的使用案例有多種：

- 容器化應用程式、並重新使用現有的資料集
- 將資料集的複本用於暫時性應用程式
- 重建故障的Kubernetes叢集
- 在災難恢復期間移轉應用程式資料

匯入如何運作？

Volume匯入程序會使用持續磁碟區宣告（PVC）檔案來建立PVc。至少、PVc檔案應包含名稱、命名空間、存取模式及storageClassName欄位、如下例所示。

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: my_claim
  namespace: my_namespace
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: my_storage_class
```

◦ tridentctl 用戶端用於匯入現有的儲存磁碟區。Trident會持續儲存Volume中繼資料並建立PVc和PV、以匯入Volume。

```
tridentctl import volume <backendName> <volumeName> -f <path-to-pvc-file>
```

若要匯入儲存磁碟區、請指定包含該磁碟區的Astra Trident後端名稱、以及唯一識別儲存區上該磁碟區的名稱（例如ONTAP FlexVol：Wsel, Element Volume、CVS Volume path）。儲存磁碟區必須允許讀取/寫入存取、且可由指定的Astra Trident後端存取。◦ -f 字串引數為必填、並指定Yaml或Json PVc檔案的路徑。

當Astra Trident收到匯入磁碟區要求時、現有的磁碟區大小會在PVc中決定及設定。儲存驅動程式匯入磁碟區之後、PV會以PVc的ClaimRef建立。回收原則一開始設定為 retain 在PV中。Kubernetes成功繫結了PVc和PV之後、系統會更新回收原則以符合儲存類別的回收原則。如果儲存類別的回收原則為 delete、儲存磁碟區會在PV刪除時刪除。

使用匯入Volume時 --no-manage 引數：Trident不會在物件生命週期的PVc或PV上執行任何其他作業。因為Trident會忽略的PV和PVc事件 --no-manage 物件、儲存磁碟區不會在PV刪除時刪除。此外、也會忽略其他作業、例如Volume Clone和Volume resize。如果您想要將Kubernetes用於容器化工作負載、但想要管理Kubernetes以外儲存磁碟區的生命週期、則此選項非常實用。

將註釋新增至PVC和PV、這有兩種用途、表示已匯入磁碟區、以及是否管理了PVC和PV。不應修改或移除此附註。

Trident 19.07及更新版本可處理PV的附加元件、並在匯入磁碟區時掛載磁碟區。對於使用舊版Astra Trident的匯入、資料路徑不會有任何作業、而且磁碟區匯入不會驗證是否可以掛載磁碟區。如果在匯入磁碟區時發生錯誤（例如、StorageClass不正確）、您可以將PV上的回收原則變更為來恢復 `retain`、刪除PVC和PV、然後重新嘗試Volume匯入命令。

ontap-nas 和 ontap-nas-flexgroup 匯入

使用建立的每個Volume `ontap-nas` 驅動程式FlexVol 是ONTAP 指在整個叢集上執行的功能。使用匯入FlexVols `ontap-nas` 驅動程式的運作方式相同。可將已存在於某個叢集上的一個功能、匯入為FlexVol ONTAP `ontap-nas` PVC。同樣地FlexGroup、也可以將此資訊匯入為 `ontap-nas-flexgroup` PVCs：



若要由Trident匯入某個類型的Rw。ONTAP如果磁碟區是DP類型、則它是SnapMirror目的地磁碟區；在將磁碟區匯入Trident之前、您應該先中斷鏡射關係。



。 `ontap-nas` 驅動程式無法匯入及管理qtree。。 `ontap-nas` 和 `ontap-nas-flexgroup` 驅動程式不允許重複的磁碟區名稱。

例如、匯入名為的磁碟區 `managed_volume` 在名為的後端上 `ontap_nas`，請使用下列命令：

```
tridentctl import volume ontap_nas managed_volume -f <path-to-pvc-file>
```

NAME	SIZE	STORAGE CLASS
pvc-bf5ad463-afbb-11e9-8d9f-5254004dfdb7	1.0 GiB	standard
file	online	true

匯入名為的磁碟區 `unmanaged_volume`（在上 `ontap_nas` backend）（Trident無法管理）、請使用下列命令：

```
tridentctl import volume nas_blog unmanaged_volume -f <path-to-pvc-file>
--no-manage
```

```
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          | SIZE | STORAGE CLASS |
+-----+-----+-----+-----+
|          BACKEND UUID  |      | STATE  | MANAGED |
+-----+-----+-----+-----+
| pvc-df07d542-afbc-11e9-8d9f-5254004dfdb7 | 1.0 GiB | standard      |
+-----+-----+-----+-----+
| file          | c5a6f6a4-b052-423b-80d4-8fb491a14a22 | online | false  |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

使用時 `--no-manage` 引數：Trident不會重新命名磁碟區、也不會驗證磁碟區是否已掛載。如果未手動掛載磁碟區、則磁碟區匯入作業會失敗。



已修正先前使用自訂Unix權限 匯入磁碟區的錯誤。您可以在您的PVC定義或後端組態中指定`unixPermissions`、並指示Astra Trident依此匯入磁碟區。

## ontap-san 匯入

Astra Trident也能匯入ONTAP 包含單一LUN的SAN FlexVols。這與一致 `ontap-san` 驅動程式、為FlexVol 每個實體磁碟和FlexVol 一個LUN建立一個實體。您可以使用 `tridentctl import` 命令的方式與其他情況相同：

- 包括的名稱 `ontap-san` 後端：
- 請提供FlexVol 需要匯入的名稱。請記住FlexVol、這個功能只包含一個必須匯入的LUN。
- 提供必須搭配使用的PVC定義路徑 `-f` 旗標。
- 您可以選擇管理或不受管理的永久虛擬網路。根據預設、Trident會管理PVC、並在FlexVol 後端重新命名該LUN。若要匯入為未受管理的Volume、請傳遞 `--no-manage` 旗標。



匯入未受管理的時 `ontap-san` Volume中的LUN FlexVol 名稱 `lun0` 並對應至具有所需啟動器的`igroup`。Astra Trident會自動處理這項作業、以便進行託管匯入。

然後Astra Trident會匯入FlexVol 該等物件、並將其與PVC定義建立關聯。Astra Trident也將FlexVol 該等功能重新命名為 `pvc-<uuid>` 格式化及FlexVol LUN在功能區內 `lun0`。



建議匯入沒有現有作用中連線的磁碟區。如果您要匯入使用中的Volume、請先複製該Volume、然後再執行匯入。

## 範例

以匯入 `ontap-san-managed` 上的顯示FlexVol `ontap_san_default` 後端、執行 `tridentctl import` 命令形式：

```
tridentctl import volume ontapsan_san_default ontap-san-managed -f pvc-
basic-import.yaml -n trident -d
```

```
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS |
PROTOCOL |          BACKEND UUID          |  STATE  | MANAGED |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| pvc-d6ee4f54-4e40-4454-92fd-d00fc228d74a | 20 MiB | basic          |
block    | cd394786-ddd5-4470-adc3-10c5ce4ca757 | online | true          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```



若要由Astra Trident匯入某個類型的RW磁碟區。ONTAP如果磁碟區為DP類型、則為SnapMirror目的地磁碟區；您應該先中斷鏡射關係、再將磁碟區匯入Astra Trident。

#### element 匯入

您可以使用NetApp Element Trident將支援功能的軟體/NetApp HCI磁碟區匯入Kubernetes叢集。您需要Astra Trident後端的名稱、以及磁碟區的唯一名稱和Pvc檔案做為的引數 `tridentctl import` 命令。

```
tridentctl import volume element_default element-managed -f pvc-basic-
import.yaml -n trident -d
```

```
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS |
PROTOCOL |          BACKEND UUID          |  STATE  | MANAGED |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| pvc-970ce1ca-2096-4ecd-8545-ac7edc24a8fe | 10 GiB | basic-element |
block    | d3ba047a-ea0b-43f9-9c42-e38e58301c49 | online | true          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```



Element驅動程式支援重複的Volume名稱。如果有重複的Volume名稱、Trident的Volume匯入程序會傳回錯誤。因應措施是複製磁碟區、並提供唯一的磁碟區名稱。然後匯入複製的Volume。

#### gcp-cvs 匯入



若要匯入以NetApp Cloud Volumes Service 支援的GCP磁碟區、請使用磁碟區路徑來識別該磁碟區、而非其名稱。

若要匯入 gcp-cvs 後端上的Volume稱為 gcpcvs\_YEppr 的磁碟區路徑 adroit-jolly-swift，請使用下列命令：

```
tridentctl import volume gcpcvs_YEppr adroit-jolly-swift -f <path-to-pvc-file> -n trident
```

```
+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS |
PROTOCOL |          BACKEND UUID          | STATE | MANAGED |
+-----+-----+-----+
+-----+-----+-----+-----+
| pvc-a46ccab7-44aa-4433-94b1-e47fc8c0fa55 | 93 GiB | gcp-storage   | file
| e1a6e65b-299e-4568-ad05-4f0a105c888f | online | true         |
+-----+-----+-----+
+-----+-----+-----+-----+
```



Volume路徑是Volume匯出路徑的一部分、位於：/之後。例如、如果匯出路徑為 10.0.0.1:/adroit-jolly-swift、磁碟區路徑為 adroit-jolly-swift。

azure-netapp-files 匯入

若要匯入 azure-netapp-files 後端上的Volume稱為 azurenetappfiles\_40517 磁碟區路徑 importvol1，執行下列命令：

```
tridentctl import volume azurenetappfiles_40517 importvol1 -f <path-to-pvc-file> -n trident
```

```
+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          |  SIZE  | STORAGE CLASS |
PROTOCOL |          BACKEND UUID          | STATE | MANAGED |
+-----+-----+-----+
+-----+-----+-----+-----+
| pvc-0ee95d60-fd5c-448d-b505-b72901b3a4ab | 100 GiB | anf-storage   |
file      | 1c01274f-d94b-44a3-98a3-04c953c9a51e | online | true         |
+-----+-----+-----+
+-----+-----+-----+-----+
```



anf磁碟區的磁碟區路徑會出現在裝載路徑中的：/之後。例如、如果掛載路徑為 10.0.0.2:/importvol1、磁碟區路徑為 importvol1。

# 跨命名空間共用NFS磁碟區

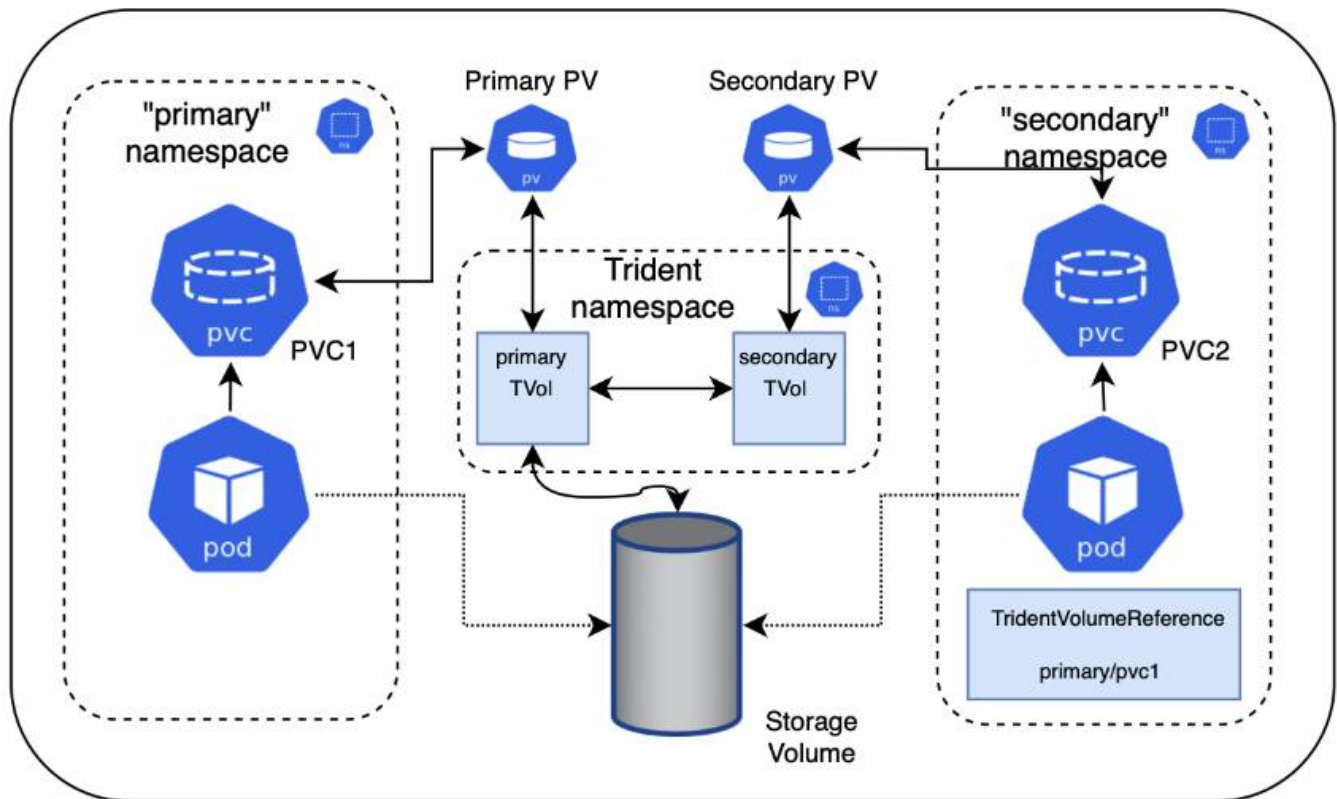
使用Astra Trident、您可以在主要命名空間中建立磁碟區、並將其共用於一或多個次要命名空間中。

## 功能

Astra TridentVolume Reference CR可讓您在一或多個Kubernetes命名空間中安全地共用ReadWriteMany (rwx) NFS磁碟區。此Kubernetes原生解決方案具有下列優點：

- 多層存取控制、確保安全性
- 可搭配所有Trident NFS Volume驅動程式使用
- 不依賴tridentctl或任何其他非原生Kubernetes功能

此圖說明兩個Kubernetes命名空間之間的NFS Volume共用。



## 快速入門

您只需幾個步驟就能設定NFS Volume共享。

1

設定來源**PVc**以共用磁碟區

來源命名空間擁有者授予存取來源PVc中資料的權限。



2

授予在目的地命名空間中建立**CR**的權限

叢集管理員授予目的地命名空間擁有者建立TridentVolume Reference CR的權限。

3

在目的地命名空間中建立**TridentVolume Reference**

目的地命名空間的擁有者會建立TridentVolume Reference CR來參照來源PVC。

4

在目的地命名空間中建立從屬的**PVC**

目的地命名空間的擁有者會建立從屬的PVC、以使用來源PVC的資料來源。

## 設定來源和目的地命名空間

為了確保安全性、跨命名空間共用需要來源命名空間擁有者、叢集管理員和目的地命名空間擁有者的協同作業與行動。使用者角色會在每個步驟中指定。

### 步驟

1. \*來源命名空間擁有者：\*建立PVC (pvc1) (namespace2) 使用 shareToNamespace 註釋：

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc1
  namespace: namespace1
  annotations:
    trident.netapp.io/shareToNamespace: namespace2
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: trident-csi
  resources:
    requests:
      storage: 100Gi
```

Astra Trident會建立PV及其後端NFS儲存磁碟區。



- 您可以使用以逗號分隔的清單、將永久虛擬儲存設備共用至多個命名空間。例如、  
trident.netapp.io/shareToNamespace:  
namespace2, namespace3, namespace4 ◦
- 您可以使用共用至所有命名空間 \*。例如、  
trident.netapp.io/shareToNamespace: \*
- 您可以更新PVC,以納入 shareToNamespace 隨時註釋。

2. \*叢集管理：\*建立自訂角色和KUBEconfig、以授予目的地命名空間擁有者權限、以便在目的地命名空間中建立TridentVolume Reference CR。
3. \*目的地命名空間擁有者：\*在參照來源命名空間的目的地命名空間中建立TridentVolume Reference CR pvc1。

```
apiVersion: trident.netapp.io/v1
kind: TridentVolumeReference
metadata:
  name: my-first-tvr
  namespace: namespace2
spec:
  pvcName: pvc1
  pvcNamespace: namespace1
```

4. \*目的地命名空間擁有者：\*建立一個PVC (pvc2) (namespace2) 使用 shareFromPVC 註釋以指定來源PVC。

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  annotations:
    trident.netapp.io/shareFromPVC: namespace1/pvc1
  name: pvc2
  namespace: namespace2
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: trident-csi
  resources:
    requests:
      storage: 100Gi
```



目的地PVC的大小必須小於或等於來源PVC。

## 結果

Astra Trident讀取 shareFromPVC 在目的地永久虛擬磁碟上註釋、並將目的地PV建立為從屬磁碟區、而其本身並無儲存資源指向來源PV並共用來源PV儲存資源。目的地的PVC和PV似乎正常連結。

## 刪除共享Volume

您可以刪除跨多個命名空間共用的磁碟區。Astra Trident會移除對來源命名空間上磁碟區的存取權、並維持對其他共用該磁碟區的命名空間的存取權。當所有參照磁碟區的命名空間都移除時、Astra Trident會刪除該磁碟區。

## 使用 `tridentctl get` 查詢從屬Volume

使用[`tridentctl` 公用程式、您可以執行 `get` 取得從屬磁碟區的命令。如需詳細資訊、請參閱連結：[../ Trident 參考/ tridentctl.html](#)[`tridentctl` 命令與選項]。

```
Usage:
  tridentctl get [option]
```

旗標：

- `-h, --help`：Volume的說明。
- `--parentOfSubordinate string`：將查詢限制在從屬來源Volume。
- `--subordinateOf string`：將查詢限制在Volume的下屬。

### 限制

- Astra Trident無法防止目的地命名空間寫入共用磁碟區。您應該使用檔案鎖定或其他程序來防止覆寫共用Volume資料。
- 您無法藉由移除來撤銷對來源PVC的存取權 `shareToNamespace` 或 `shareFromNamespace` 註釋或刪除 `TridentVolumeReference CR`。若要撤銷存取權、您必須刪除從屬的PVC。
- 在從屬磁碟區上無法執行快照、複製和鏡射。

### 以取得更多資訊

若要深入瞭解跨命名空間Volume存取：

- 請造訪 ["在命名空間之間共用磁碟區：歡迎使用跨命名空間磁碟區存取"](#)。
- 觀看示範 ["NetAppTV"](#)。

## 監控Astra Trident

Astra Trident提供一組Prometheus指標端點、可用來監控Astra Trident的效能。

Astra Trident提供的指標可讓您執行下列作業：

- 隨時掌握Astra Trident的健全狀況與組態。您可以檢查作業的成功程度、以及是否能如預期般與後端進行通訊。
- 檢查後端使用資訊、並瞭解後端上配置的磁碟區數量、以及所耗用的空間量等。
- 維護可用後端配置的磁碟區數量對應。
- 追蹤效能。您可以查看Astra Trident與後端及執行作業所需的時間。



根據預設、Trident的度量會顯示在目標連接埠上 8001 在 `/metrics` 端點：安裝Trident時\*預設會啟用這些度量。

您需要的產品

- 安裝Astra Trident的Kubernetes叢集。
- Prometheus執行個體。這可以是 ["容器化Prometheus部署"](#) 或者、您也可以選擇以執行Prometheus ["原生應用程式"](#)。

## 步驟1：定義Prometheus目標

您應該定義Prometheus目標、以收集指標並取得有關後端Astra Trident管理的資訊、以及其建立的磁碟區等資訊。這 ["部落格"](#) 說明如何使用Prometheus和Grafana搭配Astra Trident來擷取指標。部落格說明如何在Kubernetes叢集中以營運者的形式執行Prometheus、以及建立ServiceMonitor來取得Astra Trident的指標。

## 步驟2：建立Prometheus ServiceMonitor

若要使用Trident指標、您應該建立監控的Prometheus ServiceMonitor `trident-csi` 服務並傾聽 `metrics` 連接埠。ServiceMonitor範例如下所示：

```
apiVersion: monitoring.coreos.com/v1
kind: ServiceMonitor
metadata:
  name: trident-sm
  namespace: monitoring
  labels:
    release: prom-operator
spec:
  jobLabel: trident
  selector:
    matchLabels:
      app: controller.csi.trident.netapp.io
  namespaceSelector:
    matchNames:
      - trident
  endpoints:
    - port: metrics
      interval: 15s
```

此ServiceMonitor定義會擷取由傳回的度量 `trident-csi` 服務、並特別尋找 `metrics` 服務的端點。因此、Prometheus現在已設定為瞭解Astra Trident的指標。

除了直接從Astra Trident取得的指標之外、Kubelet也公開了許多指標 `kubelet_volume_*` 透過IT本身的指標端點來建立指標。Kubelet可提供有關所附加磁碟區、Pod及其處理的其他內部作業的資訊。請參閱 ["請按這裡"](#)。

## 步驟3：使用PromQL查詢Trident度量

PromQL適用於建立傳回時間序列或表格資料的運算式。

以下是一些您可以使用的PromQL查詢：

## 取得Trident健全狀況資訊

- 來自Astra Trident的HTTP 2XX回應百分比\*

```
(sum (trident_rest_ops_seconds_total_count{status_code=~"2.."} OR on()  
vector(0)) / sum (trident_rest_ops_seconds_total_count)) * 100
```

- 透過狀態代碼\*來自Astra Trident的休息回應百分比

```
(sum (trident_rest_ops_seconds_total_count) by (status_code) / scalar  
(sum (trident_rest_ops_seconds_total_count))) * 100
```

- 由Astra Trident執行的平均營運持續時間

```
sum by (operation)  
(trident_operation_duration_milliseconds_sum{success="true"}) / sum by  
(operation)  
(trident_operation_duration_milliseconds_count{success="true"})
```

## 取得Astra Trident使用資訊

- 平均Volume大小\*

```
trident_volume_allocated_bytes/trident_volume_count
```

- 每個後端配置的Volume空間總計\*

```
sum (trident_volume_allocated_bytes) by (backend_uuid)
```

## 取得個別Volume使用量



只有同時收集kubelet度量時、才會啟用此功能。

- 每個Volume的已用空間百分比\*

```
kubelet_volume_stats_used_bytes / kubelet_volume_stats_capacity_bytes *  
100
```

## 深入瞭解Astra Trident AutoSupport 遙測技術

依預設、Astra Trident會每日傳送Prometheus指標和基本後端資訊給NetApp。

- 若要停止Astra Trident將Prometheus指標和基本後端資訊傳送給NetApp、請通過 `--silence -autosupport` Astra Trident安裝期間的旗標。
- Astra Trident也可透過傳送容器記錄至NetApp Support隨選服務 `tridentctl send autosupport`。您需要觸發Astra Trident來上傳記錄。在您提交記錄之前、您應該接受NetApp的<https://www.netapp.com/company/legal/privacy-policy/>["隱私權政策"]。
- 除非另有說明、Astra Trident會從過去24小時擷取記錄。
- 您可以使用指定記錄保留時間範圍 `--since` 旗標。例如：`tridentctl send autosupport --since=1h`。此資訊會透過收集和傳送 `trident-autosupport` 安裝於Astra Trident旁的容器。您可以從取得Container映像 "[Trident AutoSupport](#) 的"。
- Trident AutoSupport 無法收集或傳輸個人識別資訊 (PII) 或個人資訊。隨附a "[EULA](#)" 這不適用於Trident Container映像本身。您可以深入瞭解NetApp對資料安全性與信任的承諾 "[請按這裡](#)"。

Astra Trident傳送的有效負載範例如下：

```
---
items:
- backendUUID: ff3852e1-18a5-4df4-b2d3-f59f829627ed
  protocol: file
  config:
    version: 1
    storageDriverName: ontap-nas
    debug: false
    debugTraceFlags:
    disableDelete: false
    serialNumbers:
    - nwkvzfanek_SN
    limitVolumeSize: ''
  state: online
  online: true
```

- 此資訊將傳送至NetApp的「不只是」端點。AutoSupport AutoSupport如果您使用私有登錄來儲存容器映像、可以使用 `--image-registry` 旗標。
- 您也可以產生安裝Yaml檔案來設定Proxy URL。您可以使用來完成這項作業 `tridentctl install --generate-custom-yaml` 以建立Yaml檔案並新增 `--proxy-url` 的引數 `trident-autosupport` 中的Container `trident-deployment.yaml`。

## 停用Astra Trident度量

若要在報告中停用\*指標、您應該產生自訂YAM（使用 `--generate-custom-yaml` 標記）並加以編輯以移除 `--metrics` 無法為呼叫旗標 `trident-main` 容器。

# 適合Docker的Astra Trident

## 部署的先決條件

您必須先在主機上安裝並設定必要的傳輸協定先決條件、才能部署Astra Trident。

### 驗證需求

- 確認您的部署符合所有的 "需求"。
- 確認您安裝的Docker版本受支援。如果您的Docker版本過時、"安裝或更新"。

```
docker --version
```

- 確認已在您的主機上安裝及設定通訊協定先決條件：

傳輸協定	作業系統	命令
NFS	RHEL 8以上	sudo yum install -y nfs-utils
NFS	Ubuntu	sudo apt-get install -y nfs-common

傳輸協定	作業系統	命令
iSCSI	RHEL 8以上	<ol style="list-style-type: none"> <li>安裝下列系統套件： <pre>sudo yum install -y lsscsi iscsi-initiator- utils sg3_utils device- mapper-multipath</pre> </li> <li>檢查iscsite-initier-utils版本是否為6.6.0.874-2.el7或更新版本： <pre>rpm -q iscsi-initiator- utils</pre> </li> <li>將掃描設為手動： <pre>sudo sed -i 's/^\(node.session.scan \).*\/\1 = manual/' /etc/iscsi/iscsid.conf</pre> </li> <li>啟用多重路徑： <pre>sudo mpathconf --enable --with_multipathd y --find_multipaths n</pre> <div>  <p>確保 etc/multipath.conf 包含 find_multipaths no 低於 defaults。</p> </div> </li> <li>請確保如此 iscsid 和 multipathd 執行中： <pre>sudo systemctl enable --now iscsid multipathd</pre> </li> <li>啟用並啟動 iscsi： <pre>sudo systemctl enable --now iscsi</pre> </li> </ol>



傳輸協定	作業系統	命令
iSCSI	Ubuntu	<p>1. 安裝下列系統套件：</p> <pre>sudo apt-get install -y open-iscsi lsscsi sg3- utils multipath-tools scsitools</pre> <p>2. 檢查開放式iSCSI版本是否為2.0.874-5ubuntu2.10或更新版本（適用於雙聲網路）或2.0.874-7.1ubuntu6.1或更新版本（適用於焦點）：</p> <pre>dpkg -l open-iscsi</pre> <p>3. 將掃描設為手動：</p> <pre>sudo sed -i 's/^\(node.session.scan \).*\/1 = manual/' /etc/iscsi/iscsid.conf</pre> <p>4. 啟用多重路徑：</p> <pre>sudo tee /etc/multipath.conf &lt; ←'EOF' defaults { user_friendly_names yes find_multipaths no } EOF sudo systemctl enable --now multipath- tools.service sudo service multipath- tools restart</pre> <div>  <p>確保 etc/multipath.conf 包含 find_multipaths no 低於 defaults。</p> </div> <p>5. 請確保如此 open-iscsi 和 multipath-tools 已啟用並執行：</p> <pre>sudo systemctl status multipath-tools sudo systemctl enable --now open- iscsi.service</pre>

# 部署Astra Trident

`sudo systemctl status`

適用於Docker的Astra Trident可直接整合適用於NetApp儲存平台的Docker生態系統。它支援從儲存平台到Docker主機的儲存資源資源配置與管理、並提供架構、可在未來新增更多平台。

多個Astra Trident執行個體可同時在同一個主機上執行。這可同時連線至多個儲存系統和儲存類型、並可自訂Docker磁碟區所使用的儲存設備。

您需要的產品

請參閱 ["部署的先決條件"](#)。在您確定已符合先決條件之後、就可以開始部署Astra Trident。

## Docker託管外掛程式方法（1.1/17.03版及更新版本）



開始之前

如果您在傳統精靈方法中使用Astra Trident preer Docker 1.3/17.03、請務必先停止Astra Trident 程序、然後重新啟動Docker精靈、再使用託管外掛方法。

1. 停止所有執行中的執行個體：

```
pkill /usr/local/bin/netappdvp
pkill /usr/local/bin/trident
```

2. 重新啟動Docker。

```
systemctl restart docker
```

3. 請確定您已安裝Docker Engine 17.03（全新1.13）或更新版本。

```
docker --version
```

如果您的版本過時、["安裝或更新安裝"](#)。

### 步驟

1. 建立組態檔並指定下列選項：

- config：預設檔案名稱為 config.json、不過您可以指定來使用您選擇的任何名稱、config 選項及檔案名稱。組態檔必須位於中 /etc/netappdvp 主機系統上的目錄。
- log-level：指定記錄層級 (debug、info、warn、error、fatal)。預設值為 info。
- debug：指定是否啟用偵錯記錄。預設值為假。如果為true、則會置換記錄層級。

- i. 建立組態檔的位置：

```
sudo mkdir -p /etc/netappdvp
```

ii. 建立組態檔：

```
cat << EOF > /etc/netappdvp/config.json
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "managementLIF": "10.0.0.1",
    "dataLIF": "10.0.0.2",
    "svm": "svm_nfs",
    "username": "vsadmin",
    "password": "password",
    "aggregate": "aggr1"
}
EOF
```

2. 使用託管外掛系統啟動Astra Trident。更換 <version> 使用您所使用的外掛程式版本（xxx.xxx.xx）。

```
docker plugin install --grant-all-permissions --alias netapp
netapp/trident-plugin:<version> config=myConfigFile.json
```

3. 開始使用Astra Trident來消耗已設定系統的儲存空間。

a. 建立名為「firstVolume」的Volume：

```
docker volume create -d netapp --name firstVolume
```

b. 在容器啟動時建立預設Volume：

```
docker run --rm -it --volume-driver netapp --volume
secondVolume:/my_vol alpine ash
```

c. 移除Volume「firstVolume」：

```
docker volume rm firstVolume
```

## 傳統方法（1.12版或更早版本）

開始之前

1. 請確定您擁有Docker 1.10版或更新版本。

```
docker --version
```

如果您的版本已過時、請更新安裝。

```
curl -fsSL https://get.docker.com/ | sh
```

或者、"請依照您的經銷指示進行"。

2. 確保已為您的系統設定NFS和/或iSCSI。

#### 步驟

1. 安裝及設定NetApp Docker Volume外掛程式：

- a. 下載並解壓縮應用程式：

```
wget  
https://github.com/NetApp/trident/releases/download/v23.01.1/trident-  
installer-23.01.1.tar.gz  
tar xzf trident-installer-23.01.1.tar.gz
```

- b. 移至Bin路徑中的位置：

```
sudo mv trident-installer/extras/bin/trident /usr/local/bin/  
sudo chown root:root /usr/local/bin/trident  
sudo chmod 755 /usr/local/bin/trident
```

- c. 建立組態檔的位置：

```
sudo mkdir -p /etc/netappdvp
```

- d. 建立組態檔：

```
cat << EOF > /etc/netappdvp/ontap-nas.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1"
}
EOF
```

2. 放置二進位檔並建立組態檔之後、請使用所需的組態檔來啟動Trident精靈。

```
sudo trident --config=/etc/netappdvp/ontap-nas.json
```



除非指定、否則Volume驅動程式的預設名稱為「NetApp」。

精靈啟動後、您可以使用Docker CLI介面來建立及管理磁碟區

3. 建立Volume：

```
docker volume create -d netapp --name trident_1
```

4. 在啟動容器時配置Docker Volume：

```
docker run --rm -it --volume-driver netapp --volume trident_2:/my_vol
alpine ash
```

5. 移除Docker Volume：

```
docker volume rm trident_1
docker volume rm trident_2
```

## 在系統啟動時啟動Astra Trident

如需系統型系統的單元檔案範例、請參閱 `contrib/trident.service.example` 在Git repo中。若要搭配RHEL使用檔案、請執行下列步驟：

1. 將檔案複製到正確的位置。

如果執行多個執行個體、則應使用單元檔案的唯一名稱。

```
cp contrib/trident.service.example  
/usr/lib/systemd/system/trident.service
```

2. 編輯檔案、變更說明（第2行）以符合驅動程式名稱和組態檔案路徑（第9行）、以反映您的環境。
3. 重新載入系統d以擷取變更：

```
systemctl daemon-reload
```

4. 啟用服務。

此名稱會根據您在主命名檔案的內容而有所不同 `/usr/lib/systemd/system` 目錄。

```
systemctl enable trident
```

5. 啟動服務。

```
systemctl start trident
```

6. 檢視狀態。

```
systemctl status trident
```



每當您修改單元檔案時、請執行 `systemctl daemon-reload` 命令、讓IT知道變更。

## 升級或解除安裝Astra Trident

您可以安全地升級適用於Docker的Astra Trident、而不會對使用中的磁碟區造成任何影響。在升級過程中、我們會在短時間內完成 `docker volume` 導向外掛程式的命令將不會成功、應用程式將無法掛載磁碟區、直到外掛程式再次執行為止。在大多數情況下、這是幾秒鐘的事。

### 升級

執行下列步驟以升級適用於Docker的Astra Trident。

#### 步驟

1. 列出現有的磁碟區：

```
docker volume ls
DRIVER          VOLUME NAME
netapp:latest   my_volume
```

## 2. 停用外掛程式：

```
docker plugin disable -f netapp:latest
docker plugin ls
ID                NAME                DESCRIPTION
ENABLED
7067f39a5df5     netapp:latest       nDVP - NetApp Docker Volume
Plugin    false
```

## 3. 升級外掛程式：

```
docker plugin upgrade --skip-remote-check --grant-all-permissions
netapp:latest netapp/trident-plugin:21.07
```



18.01版的Astra Trident取代了nDVP。您應該直接從升級 netapp/ndvp-plugin 映像到 netapp/trident-plugin 映像。

## 4. 啟用外掛程式：

```
docker plugin enable netapp:latest
```

## 5. 確認外掛程式已啟用：

```
docker plugin ls
ID                NAME                DESCRIPTION
ENABLED
7067f39a5df5     netapp:latest       Trident - NetApp Docker Volume
Plugin    true
```

## 6. 確認磁碟區可見：

```
docker volume ls
DRIVER          VOLUME NAME
netapp:latest   my_volume
```



如果您要從舊版的Astra Trident（20.10之前版本）升級至Astra Trident 20.10或更新版本、可能會發生錯誤。如需詳細資訊、請參閱 ["已知問題"](#)。如果您遇到錯誤、應該先停用外掛程式、然後移除外掛程式、再傳遞額外的組態參數來安裝所需的Astra Trident版本：`docker plugin install netapp/trident-plugin:20.10 --alias netapp --grant -all-permissions config=config.json`

## 解除安裝

執行下列步驟以解除安裝適用於Docker的Astra Trident。

### 步驟

1. 移除外掛程式所建立的任何磁碟區。
2. 停用外掛程式：

```
docker plugin disable netapp:latest
docker plugin ls
```

ID	NAME	DESCRIPTION
ENABLED		
7067f39a5df5	netapp:latest	nDVP - NetApp Docker Volume
Plugin	false	

3. 移除外掛程式：

```
docker plugin rm netapp:latest
```

## 使用Volume

您可以使用標準輕鬆建立、複製及移除磁碟區 `docker volume` 需要時指定Astra Trident 驅動程式名稱的命令。

### 建立Volume

- 使用預設名稱建立具有驅動程式的磁碟區：

```
docker volume create -d netapp --name firstVolume
```

- 建立具有特定Astra Trident執行個體的Volume：

```
docker volume create -d ntap_bronze --name bronzeVolume
```





如果您未指定任何 "選項"，將使用驅動程式的預設值。

- 覆寫預設的Volume大小。請參閱下列範例、以使用驅動程式建立20GiB磁碟區：

```
docker volume create -d netapp --name my_vol --opt size=20G
```



Volume大小以包含整數值的字串表示、並提供選用單位（例如：10g、20GB、3TiB）。如果未指定單位、則預設值為G大小單位可以表示為2（B、KiB、MiB、GiB、TiB）或10（B、KB、MB、GB、TB）的冪。簡寫單元使用2（G = GiB、T = TiB、...）的權力。

## 移除Volume

- 移除Volume就像移除任何其他Docker Volume一樣：

```
docker volume rm firstVolume
```



使用時 `solidfire-san` 驅動程式、上述範例會刪除及清除磁碟區。

執行下列步驟以升級適用於Docker的Astra Trident。

## 複製磁碟區

使用時 `ontap-nas`、`ontap-san`、`solidfire-san` 和 `gcp-cvs storage drivers`、Astra Trident可以複製磁碟區。使用時 `ontap-nas-flexgroup` 或 `ontap-nas-economy` 驅動程式、不支援複製。從現有磁碟區建立新磁碟區、將會產生新的快照。

- 檢查磁碟區以列舉快照：

```
docker volume inspect <volume_name>
```

- 從現有的Volume建立新的Volume。這將會產生新的快照：

```
docker volume create -d <driver_name> --name <new_name> -o  
from=<source_docker_volume>
```

- 從磁碟區上現有的快照建立新磁碟區。這不會建立新的快照：

```
docker volume create -d <driver_name> --name <new_name> -o  
from=<source_docker_volume> -o fromSnapshot=<source_snap_name>
```

```

docker volume inspect firstVolume

[
  {
    "Driver": "ontap-nas",
    "Labels": null,
    "Mountpoint": "/var/lib/docker-volumes/ontap-
nas/netappdvp_firstVolume",
    "Name": "firstVolume",
    "Options": {},
    "Scope": "global",
    "Status": {
      "Snapshots": [
        {
          "Created": "2017-02-10T19:05:00Z",
          "Name": "hourly.2017-02-10_1505"
        }
      ]
    }
  }
]

docker volume create -d ontap-nas --name clonedVolume -o from=firstVolume
clonedVolume

docker volume rm clonedVolume
docker volume create -d ontap-nas --name volFromSnap -o from=firstVolume
-o fromSnapshot=hourly.2017-02-10_1505
volFromSnap

docker volume rm volFromSnap

```

## 存取外部建立的磁碟區

如果容器沒有分割區、而且其檔案系統受Astra Trident支援（例如：an）、您可以使用Trident \* Only \*來存取外部建立的區塊裝置（或其複製） ext4`格式化` /dev/sdc1 無法透過Astra Trident存取）。

## 驅動程式專屬的Volume選項

每個儲存驅動程式都有一組不同的選項、您可以在建立磁碟區時指定、以自訂結果。請參閱下方、以瞭解適用於您所設定儲存系統的選項。

在磁碟區建立作業期間使用這些選項非常簡單。使用提供選項和值 -o 在CLI作業期間、這會覆寫Json組態檔中的任何等效值。

## 選購的選購配備ONTAP

NFS和iSCSI的Volume建立選項包括：

選項	說明
size	Volume的大小、預設為1 GiB。
spaceReserve	精簡或完整配置磁碟區、預設為精簡。有效值為 none（資源隨需配置）和 volume（完整配置）。
snapshotPolicy	這會將快照原則設定為所需的值。預設值為 none（表示不會自動為磁碟區建立快照）。除非您的儲存管理員加以修改、否則ONTAP 所有的各種系統都會有一個名為「預設」的原則、用來建立並保留六個每小時、每天兩個和每週兩個快照。瀏覽至、即可恢復快照中保留的資料 .snapshot 磁碟區中任何目錄的目錄。
snapshotReserve	這會將快照保留設定為所需的百分比。預設值為無值、表示ONTAP 如果您已選取snapshotPolicy、將選取snapshotReserve（通常為5%）、如果snapshotPolicy為無、則選取0%。您可以在組態檔中為所有ONTAP 的支援項目設定預設的snapshotReserve值、也可以將其用作所有ONTAP 不支援ONTAP-NAS-經濟功能的支援項目、作為所有支援項目的磁碟區建立選項。
splitOnClone	當複製Volume時、ONTAP 這會導致停止實體複本、立即將其從父複本分割開來。預設值為 false。部分複製磁碟區的使用案例、最好是在建立時立即將複本從父複本分割出來、因為不太可能有提高儲存效率的機會。例如，複製空白資料庫可節省大量時間，但儲存空間卻很少，因此最好立即分割實體複本。
encryption	<p>在新磁碟區上啟用NetApp Volume Encryption（NVE）；預設為 false。必須在叢集上授權並啟用NVE、才能使用此選項。</p> <p>如果在後端啟用NAE、則Astra Trident中配置的任何磁碟區都會啟用NAE。</p> <p>如需詳細資訊、請參閱：<a href="#">"Astra Trident如何與NVE和NAE搭配運作"</a>。</p>
tieringPolicy	設定要用於磁碟區的分層原則。這會決定資料在非作用中（冷）時是否移至雲端層。

下列其他選項適用於NFS \* Only \*：

選項	說明
unixPermissions	這會控制Volume本身的權限設定。依預設、權限會設為 `---rwxr-xr-x` 或是以數字表示法 0755、和 `root` 將成為擁有者。文字或數字格式皆可運作。
snapshotDir	設定為 true 將會製作 .snapshot 存取磁碟區的用戶端可看到的目錄。預設值為 false、表示的可見度 .snapshot 目錄預設為停用。某些影像（例如官方MySQL映像）在執行時無法如預期般運作 .snapshot 目錄可見。
exportPolicy	設定要用於磁碟區的匯出原則。預設值為 default。
securityStyle	設定用於存取磁碟區的安全樣式。預設值為 unix。有效值為 unix 和 mixed。

下列其他選項僅適用於iSCSI \*：

選項	說明
fileSystemType	設定用於設定iSCSI磁碟區格式的檔案系統。預設值為 ext4。有效值為 ext3、ext4 和 xfs。
spaceAllocation	設定為 false 將關閉LUN的空間分配功能。預設值為 true、表示ONTAP 當磁碟區空間不足、且磁碟區中的LUN無法接受寫入作業時、此功能會通知主機。此選項也可讓ONTAP 支援功能在主機刪除資料時自動回收空間。

## 範例

請參閱下列範例：

- 建立10GiB Volume：

```
docker volume create -d netapp --name demo -o size=10G -o encryption=true
```

- 使用快照建立100GiB磁碟區：

```
docker volume create -d netapp --name demo -o size=100G -o snapshotPolicy=default -o snapshotReserve=10
```

- 建立已啟用setuid位元的磁碟區：

```
docker volume create -d netapp --name demo -o unixPermissions=4755
```

最小Volume大小為20MiB。

如果未指定快照保留、則快照原則為 `none`、Trident將使用快照保留0%。

- 建立沒有快照原則且無快照保留的磁碟區：

```
docker volume create -d netapp --name my_vol --opt snapshotPolicy=none
```

- 建立不含快照原則的磁碟區、以及自訂快照保留10%的磁碟區：

```
docker volume create -d netapp --name my_vol --opt snapshotPolicy=none  
--opt snapshotReserve=10
```

- 建立具有快照原則和10%自訂快照保留的磁碟區：

```
docker volume create -d netapp --name my_vol --opt  
snapshotPolicy=myPolicy --opt snapshotReserve=10
```

- 使用快照原則建立磁碟區、並接受ONTAP的預設快照保留（通常為5%）：

```
docker volume create -d netapp --name my_vol --opt  
snapshotPolicy=myPolicy
```

## Element軟體Volume選項

元素軟體選項會顯示與磁碟區相關的服務品質（QoS）原則大小和品質。建立磁碟區時、會使用指定與其相關的QoS原則 `-o type=service_level` 命名法。

使用元素驅動程式定義QoS服務層級的第一步、是建立至少一種類型、並在組態檔中指定與名稱相關的最小、最大和尖峰IOPS。

其他元素軟體磁碟區建立選項包括：

選項	說明
size	磁碟區大小、預設為1GiB或組態項目... 「預設值」： {"Size": "5G"}。

選項	說明
blocksize	使用512或4096、預設為512或組態項目預設BlockSizes。

## 範例

請參閱下列QoS定義範例組態檔：

```
{
  "...": "...",
  "Types": [
    {
      "Type": "Bronze",
      "Qos": {
        "minIOPS": 1000,
        "maxIOPS": 2000,
        "burstIOPS": 4000
      }
    },
    {
      "Type": "Silver",
      "Qos": {
        "minIOPS": 4000,
        "maxIOPS": 6000,
        "burstIOPS": 8000
      }
    },
    {
      "Type": "Gold",
      "Qos": {
        "minIOPS": 6000,
        "maxIOPS": 8000,
        "burstIOPS": 10000
      }
    }
  ]
}
```

在上述組態中、我們有三種原則定義：銅級、銀級和金級。這些名稱為任意名稱。

- 建立10GiB Gold Volume：

```
docker volume create -d solidfire --name sfGold -o type=Gold -o size=10G
```

- 建立100GiB銅級磁碟區：

```
docker volume create -d solidfire --name sfBronze -o type=Bronze -o size=100G
```

## 收集記錄

您可以收集記錄以協助疑難排解。收集記錄的方法會因執行Docker外掛程式的方式而有所不同。

### 收集記錄以進行疑難排解

#### 步驟

1. 如果您使用建議的託管外掛程式方法執行Astra Trident（例如、使用） `docker plugin` 命令）、請依下列方式檢視：

```
docker plugin ls
ID                                NAME                                DESCRIPTION
ENABLED
4fb97d2b956b                    netapp:latest                      nDVP - NetApp Docker Volume
Plugin    false
journalctl -u docker | grep 4fb97d2b956b
```

標準記錄層級應可讓您診斷大多數問題。如果您發現這還不夠、可以啟用偵錯記錄。

2. 若要啟用除錯記錄、請安裝已啟用除錯記錄的外掛程式：

```
docker plugin install netapp/trident-plugin:<version> --alias <alias>
debug=true
```

或者、當外掛程式已安裝時、請啟用偵錯記錄功能：

```
docker plugin disable <plugin>
docker plugin set <plugin> debug=true
docker plugin enable <plugin>
```

3. 如果您在主機上執行二進位檔本身、則可在主機中使用記錄檔 `/var/log/netappdvp` 目錄。若要啟用偵錯記錄、請指定 `-debug` 當您執行外掛程式時。

## 一般疑難排解秘訣

- 新使用者最常遇到的問題是組態錯誤、導致外掛程式無法初始化。發生這種情況時、當您嘗試安裝或啟用外掛程式時、可能會看到如下訊息：

```
Error response from daemon: dial unix /run/docker/plugins/<id>/netapp.sock:
connect: no such file or directory
```

這表示外掛程式無法啟動。幸運的是、外掛程式是以全方位的記錄功能打造而成、可協助您診斷大部分可能遇到的問題。

- 如果在將PV安裝至容器時發生問題、請確定 `rpcbind` 已安裝並執行。使用主機作業系統所需的套件管理程式、並檢查是否有 `rpcbind` 正在執行。您可以執行來檢查 `rpcbind` 服務的狀態 `systemctl status rpcbind` 或同等產品。

## 管理多個Astra Trident執行個體

當您想要同時使用多個儲存組態時、需要多個Trident執行個體。多個執行個體的關鍵是使用為它們指定不同的名稱 `--alias` 可搭配容器化外掛程式使用的選項、或 `--volume-driver` 在主機上具現化Trident時的選項。

### Docker託管外掛程式（1.3/17.03版或更新版本）的步驟

1. 啟動第一個指定別名和組態檔的執行個體。

```
docker plugin install --grant-all-permissions --alias silver
netapp/trident-plugin:21.07 config=silver.json
```

2. 啟動第二個執行個體、指定不同的別名和組態檔。

```
docker plugin install --grant-all-permissions --alias gold
netapp/trident-plugin:21.07 config=gold.json
```

3. 建立磁碟區、將別名指定為驅動程式名稱。

例如、黃金Volume：

```
docker volume create -d gold --name ntapGold
```

例如、對於銀級Volume：

```
docker volume create -d silver --name ntapSilver
```



## 傳統的步驟（1.12版或更早版本）

1. 使用自訂驅動程式ID以NFS組態啟動外掛程式：

```
sudo trident --volume-driver=netapp-nas --config=/path/to/config  
-nfs.json
```

2. 使用自訂驅動程式ID以iSCSI組態啟動外掛程式：

```
sudo trident --volume-driver=netapp-san --config=/path/to/config  
-iscsi.json
```

3. 為每個驅動程式執行個體配置Docker磁碟區：

例如、對於NFS：

```
docker volume create -d netapp-nas --name my_nfs_vol
```

例如、對於iSCSI：

```
docker volume create -d netapp-san --name my_iscsi_vol
```

## 儲存組態選項

請參閱Astra Trident組態的可用組態選項。

### 全域組態選項

這些組態選項適用於所有Astra Trident組態、無論使用何種儲存平台。

選項	說明	範例
version	組態檔版本編號	1
storageDriverName	儲存驅動程式名稱	ontap-nas、ontap-san、 ontap-nas-economy、 ontap-nas-flexgroup、 solidfire-san
storagePrefix	Volume名稱的選用首碼。預設： netappdvp_。	staging_

選項	說明	範例
limitVolumeSize	Volume大小的選擇性限制。預設值：「」（未強制執行）	10g



請勿使用 `storagePrefix` 元素後端的（包括預設值）。依預設 `solidfire-san` 驅動程式將忽略此設定、而不使用前置碼。我們建議使用特定的TenantId進行Docker Volume對應、或是使用Docker版本、驅動程式資訊和原始名稱填入的屬性資料、以便在可能使用任何名稱標示的情況下使用。

您可以使用預設選項、避免在每個建立的Volume上指定這些選項。。 `size` 選項適用於所有控制器類型。如ONTAP 需如何設定預設Volume大小的範例、請參閱「功能區組態」一節。

選項	說明	範例
size	新磁碟區的選用預設大小。預設：1G	10G

## 組態ONTAP

除了上述全域組態值之外、使用ONTAP 時還提供下列頂層選項。

選項	說明	範例
managementLIF	IP位址ONTAP：您可以指定完整網域名稱（FQDN）。	10.0.0.1
dataLIF	<p>傳輸協定LIF的IP位址。</p> <p>《NAS驅動程式》：建議您指定ONTAP <code>dataLIF</code>。如果未提供、Astra Trident會從SVM擷取資料lifs。您可以指定要用於NFS掛載作業的完整網域名稱（FQDN）、讓您建立循環配置資源DNS、以便在多個資料生命期之間達到負載平衡。</p> <p>《SAN驅動程式：請勿指定用於iSCSI》ONTAP。Astra Trident的用途 "可選擇的LUN對應ONTAP" 探索建立多重路徑工作階段所需的iSCSI LIF。如果發生此情況、將會產生警告 <code>dataLIF</code> 已明確定義。</p>	10.0.0.2
svm	要使用的儲存虛擬機器（如果管理LIF是叢集LIF、則為必要）	svm_nfs

選項	說明	範例
username	連線至儲存設備的使用者名稱	vsadmin
password	連線至儲存設備的密碼	secret
aggregate	用於資源配置的Aggregate（選用；如果已設定、則必須指派給SVM）。適用於 <code>ontap-nas-flexgroup</code> 驅動程式、此選項會被忽略。指派給SVM的所有集合體均可用來配置FlexGroup 一個SVolume。	aggr1
limitAggregateUsage	如果使用率高於此百分比、則可選用、失敗的資源配置	75%
nfsMountOptions	精細控制NFS掛載選項；預設為「 <code>-o nfsver=3</code> 」。僅適用於 <b>ontap-nas</b> 和 <b>ontap-nas-economy</b> 驅動程式。 <a href="#">"請參閱此處的NFS主機組態資訊"</a> 。	<code>-o nfsvers=4</code>
igroupName	外掛程式使用的 igroup；預設為 <code>netappdvp</code> 。僅適用於「 <b>ONTAP-San'driver</b> 」。	myigroup
limitVolumeSize	可申請的Volume大小上限和qtree父Volume大小上限。適用於 <b>ontap-nas-economy</b> 驅動程式、此選項還會限制其所建立的FlexVols的大小。	300g
qtreesPerFlexvol	每FlexVol 個邊區最多qtree數、範圍必須為[50、300]、預設值為200。適用於 <b>ontap-nas-economy</b> 驅動程式、此選項可自訂每FlexVol 個版本的qtree數量上限。	300

您可以使用預設選項、避免在您建立的每個Volume上指定這些選項：

選項	說明	範例
spaceReserve	空間保留模式；none（精簡配置）或 volume（粗）	none

選項	說明	範例
snapshotPolicy	要使用的 Snapshot 原則、預設為 none	none
snapshotReserve	Snapshot 保留百分比、預設為「」接受 ONTAP 預設值	10
splitOnClone	建立複本時、將其父複本分割成預設值 false	false
encryption	<p>在新磁碟區上啟用NetApp Volume Encryption (NVE) ；預設為 false。必須在叢集上授權並啟用NVE、才能使用此選項。</p> <p>如果在後端啟用NAE、則Astra Trident中配置的任何磁碟區都會啟用NAE。</p> <p>如需詳細資訊、請參閱：<a href="#">"Astra Trident如何與NVE和NAE搭配運作"</a>。</p>	是的
unixPermissions	NAS 選項適用於已佈建的 NFS 磁碟區、預設為 777	777
snapshotDir	NAS選項、可存取 .snapshot 目錄、預設為 false	true
exportPolicy	NFS 匯出原則使用的 NAS 選項、預設為 default	default
securityStyle	<p>NAS選項、可存取已配置的NFS Volume。</p> <p>NFS支援 mixed 和 unix 安全樣式：預設值為 unix。</p>	unix
fileSystemType	SAN 選項可選擇檔案系統類型、預設為 ext4	xfs
tieringPolicy	要使用的分層原則、預設為 none ； snapshot-only 適用於 ONTAP 9.5 之前的 SVM-DR 組態	none

## 擴充選項

◦ `ontap-nas` 和 `ontap-san` 驅動程式會為ONTAP FlexVol 每個Docker Volume建立一個支援功能。支援每個叢集節點最多1000個FlexVols、叢集最多12、000個FlexVols。ONTAP如果您的Docker Volume需求符合該限制 `ontap-nas` 由於FlexVols提供的其他功能（例如Docker Volume精細快照和複製）、因此驅動程式是首選的NAS解決方案。

如果您需要的Docker磁碟區數量超過FlexVol 了《支援範圍 `ontap-nas-economy` 或 `ontap-san-economy` 驅動程式：

◦ `ontap-nas-economy` 驅動程式會在ONTAP 自動管理的FlexVols資源池中、將Docker Volume建立為架構樹狀結構。`qtree`的擴充能力大幅提升、每個叢集節點最多可達100、000個、每個叢集最多可達2、400、000個、而犧牲了部分功能。◦ `ontap-nas-economy` 驅動程式不支援Docker Volume精細的快照或複製。



◦ `ontap-nas-economy` Docker swarm目前不支援驅動程式、因為swarm不會協調跨多個節點建立磁碟區。

◦ `ontap-san-economy` 驅動程式會在ONTAP 自動管理的FlexVols共用集區內、將Docker Volume建立為如此FlexVol 一來、每個支援不只侷限於一個LUN、而且能為SAN工作負載提供更好的擴充性。根據儲存陣列的不同、ONTAP 每個叢集最多可支援16384個LUN。由於磁碟區是下方的LUN、因此此驅動程式支援Docker磁碟區精細快照和複製。

選擇 `ontap-nas-flexgroup` 將平行處理能力提升至單一磁碟區、以數十億個檔案擴充至PB範圍。FlexGroups的一些理想使用案例包括AI / ML / DL、Big Data和分析、軟體建置、串流、檔案儲存庫等。Trident在配置FlexGroup 完一套SVM時、會使用指派給SVM的所有集合體。支援Trident也有下列考量：  
FlexGroup

- 需要ONTAP 9.2版或更新版本。
- 截至本文撰寫時、FlexGroups僅支援NFS v3。
- 建議啟用SVM的64位元NFSv3識別碼。
- 建議FlexGroup 的最小內存區大小為100GB。
- 不支援FlexGroup 將複製複製用於實體磁碟區。

如需適用於FlexGroups的FlexGroups與工作負載相關資訊、請參閱 "[NetApp FlexGroup](#) 《NetApp》《最佳實務做法與實作指南》"。

若要在同一個環境中獲得進階功能和大規模擴充、您可以使用執行多個Docker Volume外掛程式執行個體 `ontap-nas` 和另一個使用 `ontap-nas-economy`。

## 範例ONTAP：功能組態檔

- NFS範例 `ontap-nas` 驅動程式\*

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1",
  "defaults": {
    "size": "10G",
    "spaceReserve": "none",
    "exportPolicy": "default"
  }
}
```

• NFS範例 ontap-nas-flexgroup 驅動程式\*

```
{
  "version": 1,
  "storageDriverName": "ontap-nas-flexgroup",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password",
  "defaults": {
    "size": "100G",
    "spaceReserve": "none",
    "exportPolicy": "default"
  }
}
```

• NFS範例 ontap-nas-economy 驅動程式\*

```
{
  "version": 1,
  "storageDriverName": "ontap-nas-economy",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1"
}
```

• iSCSI範例 ontap-san 驅動程式\*

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1",
  "igroupName": "myigroup"
}
```

• NFS範例 ontap-san-economy 驅動程式\*

```
{
  "version": 1,
  "storageDriverName": "ontap-san-economy",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi_eco",
  "username": "vsadmin",
  "password": "password",
  "aggregate": "aggr1",
  "igroupName": "myigroup"
}
```

## 元件軟體組態

除了全域組態值之外、使用Element軟體（NetApp HCI / SolidFire）時、也可使用這些選項。

選項	說明	範例
Endpoint	https://<login>:<password>@<mvip>/json-rpc/<element-version>	https://admin:admin@192.168.160.3/json-rpc/8.0
SVIP	iSCSI IP位址和連接埠	10.0.0.7 : 3260
TenantName	要使用的SolidFireF租戶（如果找不到、請建立）	docker
InitiatorIFace	將iSCSI流量限制為非預設介面時、請指定介面	default
Types	QoS規格	請參閱以下範例
LegacyNamePrefix	升級版Trident安裝的首碼。如果您使用1.3.2版之前的Trident版本、並使用現有磁碟區執行升級、則必須設定此值、才能存取透過Volume名稱方法對應的舊磁碟區。	netappdvp-

◦ solidfire-san 驅動程式不支援Docker Swarm。

## 元素軟體組態檔範例



```

{
  "version": 1,
  "storageDriverName": "solidfire-san",
  "Endpoint": "https://admin:admin@192.168.160.3/json-rpc/8.0",
  "SVIP": "10.0.0.7:3260",
  "TenantName": "docker",
  "InitiatorIFace": "default",
  "Types": [
    {
      "Type": "Bronze",
      "Qos": {
        "minIOPS": 1000,
        "maxIOPS": 2000,
        "burstIOPS": 4000
      }
    },
    {
      "Type": "Silver",
      "Qos": {
        "minIOPS": 4000,
        "maxIOPS": 6000,
        "burstIOPS": 8000
      }
    },
    {
      "Type": "Gold",
      "Qos": {
        "minIOPS": 6000,
        "maxIOPS": 8000,
        "burstIOPS": 10000
      }
    }
  ]
}

```

## 已知問題與限制

尋找使用Astra Trident搭配Docker時已知問題和限制的相關資訊。

從舊版升級**Trident Docker Volume**外掛程式至**20.10**及更新版本、會導致升級失敗、且不會發生此類檔案或目錄錯誤。

因應措施

1. 停用外掛程式。

```
docker plugin disable -f netapp:latest
```

2. 移除外掛程式。

```
docker plugin rm -f netapp:latest
```

3. 提供額外的、重新安裝外掛程式 config 參數。

```
docker plugin install netapp/trident-plugin:20.10 --alias netapp --grant  
-all-permissions config=config.json
```

**Volume**名稱長度必須至少**2**個字元。



這是Docker用戶端的限制。用戶端會將單一字元名稱解譯為Windows路徑。"請參閱錯誤25773"。

**Docker swarm**具有某些行為、可防止**Astra Trident**在每個儲存設備和驅動程式組合中支援它。

- Docker swarm目前使用Volume名稱、而非Volume ID做為其唯一的Volume識別碼。
- Volume要求會同時傳送至swarm叢集中的每個節點。
- Volume外掛程式（包括Astra Trident）必須在swarm叢集中的每個節點上獨立執行。因為功能不一ONTAP `ontap-nas` 和 `ontap-san` 驅動程式功能、是唯一能夠在這些限制範圍內運作的驅動程式。

其餘的驅動程式可能會受到競爭狀況等問題的影響、導致在單一要求中建立大量磁碟區、而不需要明確的「贏家」；例如、Element的功能可讓磁碟區擁有相同名稱但不同ID。

NetApp已向Docker團隊提供意見回饋、但沒有任何未來追索的跡象。

如果配置的是某個功能區、則如果第二個功能區的一個或多個集合體與要配置的功能區相同、則不提供第二個功能區。**FlexGroup ONTAP FlexGroup FlexGroup FlexGroup**

# 常見問題集

尋找有關安裝、設定、升級及疑難排解Astra Trident的常見問題解答。

## 一般問題

### Astra Trident多久發佈一次？

Astra Trident每三個月發佈一次：1月、4月、7月和10月。這是Kubernetes發表後的一個月。

### Astra Trident是否支援特定Kubernetes版本中發行的所有功能？

Astra Trident通常不支援Kubernetes的Alpha功能。Trident可能支援Kubernetes試用版之後的兩個Trident版本中的試用版功能。

### Astra Trident是否因其運作而依賴其他NetApp產品？

Astra Trident並不依賴其他NetApp軟體產品、而是以獨立應用程式的形式運作。不過、您應該擁有NetApp後端儲存設備。

### 如何取得完整的Astra Trident組態詳細資料？

使用 `tridentctl get` 命令以取得Astra Trident組態的詳細資訊。

### 我可以取得Astra Trident如何配置儲存設備的指標嗎？

是的。Trident 20.01推出Prometheus端點、可用來收集有關Astra Trident作業的資訊、例如受管理的後端數目、已配置的磁碟區數目、已用位元組等。您也可以使用Cloud Insights 此功能進行監控與分析。

### 使用Astra Trident做為「csi資源配置工具」時、使用者是否會有變更？

不可以就使用者體驗和功能而言、沒有任何改變。使用的資源配置程式名稱為 `csi.trident.netapp.io`。如果您想要使用目前和未來版本所提供的所有新功能、建議使用這種安裝Astra Trident的方法。

## 在Kubernetes叢集上安裝及使用Astra Trident

### 支援的版本為何 etcd？

Astra Trident不再需要 etcd。它使用客戶需求日來維持狀態。

### Astra Trident是否支援從私有登錄進行離線安裝？

可以、Astra Trident可以離線安裝。請參閱 ["請按這裡"](#)。

## 我可以從遠端安裝**Astra Trident**嗎？

是的。Astra Trident 18.10及更新版本可從任何擁有的機器支援遠端安裝功能 `kubectl` 存取叢集。之後 `kubectl` 存取已驗證（例如：啟動 `kubectl get nodes` 遠端機器的命令進行驗證）、請遵循安裝指示。

## 我可以使用**Astra Trident**設定高可用度嗎？

Astra Trident是以單一執行個體安裝為Kubernetes部署（ReplicaSet）、因此內建HA。您不應增加部署中的複本數量。如果安裝Astra Trident的節點遺失、或Pod無法存取、Kubernetes會自動將Pod重新部署至叢集中的健全節點。Astra Trident僅適用於控制面板、因此若重新部署Astra Trident、目前安裝的Pod不會受到影響。

## **Astra Trident**是否需要存取**Kube**系統命名空間？

Astra Trident從Kubernetes API伺服器讀取、以判斷應用程式何時要求新的PVCS、因此需要存取Kube-system。

## **Astra Trident**使用哪些角色和權限？

Trident安裝程式會建立Kubernetes ClusterRole、該叢集具有特定存取權、可存取叢集的PersistentVolume、PersistentVolume Claim、StorageClass及Kubernetes叢集的Secret資源。請參閱 ["請按這裡"](#)。

## 我可以在本機產生安裝所用的確切資訊清單檔案嗎？

如有需要、您可以在本機產生及修改安裝所使用的確切資訊清單檔案Astra Trident。請參閱 ["請按這裡"](#)。

## 我是否可以針對**ONTAP** 兩個獨立**Kubernetes**叢集的兩個**Astra Trident**執行個體、共用相同的支援功能後端**SVM**？

雖然不建議使用、但您可以針對兩個Astra Trident執行個體使用相同的後端SVM。在安裝期間為每個執行個體指定唯一的Volume名稱、及（或）指定唯一的Volume名稱 `StoragePrefix` 中的參數 `setup/backend.json` 檔案：這是為了確保FlexVol 兩個執行個體都不會使用相同的功能。

## 是否能在**ContainerLinux**（前身為**CoreOS**）下安裝**Astra Trident**？

Astra Trident只是Kubernetes Pod、可安裝在Kubernetes執行的任何位置。

## 我可以將**Astra Trident**搭配**NetApp Cloud Volumes ONTAP** 功能嗎？

是的、AWS、Google Cloud和Azure均支援Astra Trident。

## **Astra Trident**是否能與**Cloud Volumes Services**搭配運作？

是的、Astra Trident不僅支援Azure NetApp Files Azure中的「不二」服務、Cloud Volumes Service 也支援GCP中的「不二」功能。

## 疑難排解與支援

## NetApp是否支援Astra Trident？

儘管Astra Trident是開放原始碼且免費提供、但只要您的NetApp後端受到支援、NetApp就能提供完整支援。

## 如何提出支援案例？

若要提出支援案例、請執行下列其中一項：

1. 請聯絡您的支援客戶經理、以取得索取機票的協助。
2. 請聯絡以提出支援案例 ["NetApp支援"](#)。

## 如何產生支援記錄套裝組合？

您可以執行來建立支援服務組合 `tridentctl logs -a`。除了在套裝組合中擷取的記錄之外、請擷取kubelet記錄、以診斷Kubernetes端的掛載問題。取得Kubernetes記錄的指示會根據Kubernetes的安裝方式而有所不同。

## 如果我需要提出新功能的要求、該怎麼辦？

在上建立問題 ["Astra Trident Github"](#) 並在問題的主題和說明中提及\* RFE\*。

## 我該在哪裡提出瑕疵？

在上建立問題 ["Astra Trident Github"](#)。請務必附上與問題相關的所有必要資訊和記錄。

## 如果我有關於Astra Trident的快速問題、而我需要澄清、會發生什麼情況？是否有社群或論壇？

如果您有任何問題、問題或要求、請透過我們的Astra與我們聯絡 ["不和通路"](#) 或GitHub。

## 我的儲存系統密碼已變更、Astra Trident已無法運作、我該如何恢復？

使用更新後端的密碼 `tridentctl update backend myBackend -f </path/to_new_backend.json> -n trident`。更換 myBackend 在範例中、使用您的後端名稱、和 `</path/to_new_backend.json>` 並將路徑移至正確位置 `backend.json` 檔案：

## Astra Trident找不到Kubernetes節點。如何修正此問題？

Astra Trident找不到Kubernetes節點的原因可能有兩種。這可能是因為Kubernetes內的網路問題或DNS問題。在每個Kubernetes節點上執行的Trident節點取消影像集、必須能夠與Trident控制器通訊、才能在Trident中登錄節點。如果在安裝Astra Trident之後發生網路變更、您只會遇到新增至叢集的Kubernetes節點的問題。

## 如果Trident Pod毀損、我會遺失資料嗎？

如果Trident Pod遭到破壞、資料將不會遺失。Trident的中繼資料儲存在CRD物件中。所有由Trident提供的PV均可正常運作。

# 升級Astra Trident

我可以直接從舊版本升級至新版本（跳過幾個版本）嗎？

NetApp支援將Astra Trident從一個重大版本升級至下一個重大版本。您可以從11.xx版升級至19.xx、19.xx版升級至20.xx版、依此類推。在正式作業部署之前、您應該先在實驗室中測試升級。

是否能將Trident降級至先前的版本？

如果您想要降級、有許多因素需要評估。請參閱 ["降級一節"](#)。

## 管理後端和磁碟區

我是否需要在ONTAP 一個後端定義檔案中定義管理和資料生命期？

管理LIF為必填項目。資料LIF會有所不同：

- 支援SAN：請勿指定iSCSI ONTAP。Astra Trident的用途 ["可選擇的LUN對應ONTAP"](#) 探索建立多重路徑工作階段所需的iSCSI LIF。如果發生此情況、將會產生警告 dataLIF 已明確定義。請參閱 ["SAN組態選項與範例ONTAP"](#) 以取得詳細資料。
- ASNAS：建議您指定ONTAP dataLIF。如果未提供、Astra Trident會從SVM擷取資料lifs。您可以指定要用於NFS掛載作業的完整網域名稱（FQDN）、讓您建立循環配置資源DNS、以便在多個資料生命期之間達到負載平衡。請參閱 ["列舉NAS組態選項與範例ONTAP"](#) 以取得詳細資料

Astra Trident是否能設定CHAP以ONTAP 供後端使用？

是的。從20.04開始、Astra Trident支援雙向CHAP以利ONTAP 實現後端。這需要設定 `useCHAP=true` 在後端組態中。

如何使用Astra Trident管理匯出原則？

Astra Trident可從20.04版起、動態建立及管理匯出原則。如此一來、儲存管理員就能在其後端組態中提供一或多個CIDR區塊、並將位於這些範圍內的Trident新增節點IP、加入其所建立的匯出原則。如此一來、Astra Trident就能自動管理新增和刪除在指定CIDR內具有IP的節點規則。此功能需要「csi Trident」。

我們可以在DataLIF中指定連接埠嗎？

Astra Trident 19.01及更新版本支援在DataLIF中指定連接埠。在中設定 `backend.json` 檔案格式 `"managementLIF": <ip address>:<port>"`。例如、如果管理LIF的IP位址為192.0.2.1、而連接埠為1000、請進行設定 `"managementLIF": "192.0.2.1:1000"`。

IPv6位址是否可用於管理和資料生命量？

Astra Trident支援定義IPv6位址：

- `managementLIF` 和 `dataLIF` 適用於不支援NAS的後端ONTAP。
- `managementLIF` 適用於SAN後端ONTAP。您無法指定 `dataLIF` 在SAN後端ONTAP。

必須使用安裝Astra Trident `--use-ipv6` 旗標可讓IT透過IPv6運作。

## 是否能在後端更新管理LIF？

是的、您可以使用更新後端管理LIF `tridentctl update backend` 命令。

## 是否能在後端更新Data LIF？

您可以在上更新Data LIF `ontap-nas` 和 `ontap-nas-economy` 僅限。

## 我可以在Astra Trident中為Kubernetes建立多個後端嗎？

Astra Trident可同時支援多個後端、無論是使用相同的驅動程式或不同的驅動程式。

## Astra Trident如何儲存後端認證資料？

Astra Trident將後端認證儲存為Kubernetes Secrets。

## Astra Trident如何選擇特定的後端？

如果無法使用後端屬性自動選取類別的適當資源池、則會使用 `storagePools` 和 `additionalStoragePools` 參數用於選擇一組特定的資源池。

## 如何確保Astra Trident不會從特定後端進行資源配置？

◦ `excludeStoragePools` 參數用於篩選Astra Trident將用於資源配置的資源池集區集區集區、並移除任何符合的資源池。

## 如果有多個相同類型的後端、Astra Trident如何選擇要使用的後端？

如果有多個相同類型的已設定後端、則Astra Trident會根據中的參數選取適當的後端 `StorageClass` 和 `PersistentVolumeClaim`。例如、如果有多個ONTAP-NAS驅動程式後端、Astra Trident會嘗試比對中的參數 `StorageClass` 和 `PersistentVolumeClaim` 結合並符合後端、以滿足中所列的需求 `StorageClass` 和 `PersistentVolumeClaim`。如果有多個後端符合要求、則Astra Trident會隨機從其中一個後端選取。

## Astra Trident是否支援採用Element / SolidFire的雙向CHAP？

是的。

## Astra Trident如何將qtree部署在ONTAP 一個邊角捲上？單一磁碟區可部署多少qtree？

◦ `ontap-nas-economy` 驅動程式可在同FlexVol 一個範圍內建立多達200個qtree（可設定為50到300個）、每個叢集節點可建立100、000個qtree、每個叢集可建立2.4公尺。當您輸入新的時 `PersistentVolumeClaim` 這是經濟型驅動程式所提供的服務、駕駛會查看FlexVol 是否已存在可為新Qtree提供服務的功能。如果FlexVol 不存在能夠服務Qtree的功能、FlexVol 就會建立新的功能。

我要如何為**ONTAP** 以**NAS**配置的**Volume**設定**Unix**權限？

您可以在後端定義檔中設定參數、以設定Astra Trident所佈建的Volume上的Unix權限。

如何在**ONTAP** 配置**Volume**時、設定一組明確的靜態**NFS**掛載選項？

依預設、Astra Trident不會使用Kubernetes將掛載選項設為任何值。若要在Kubernetes儲存類別中指定掛載選項、請遵循所提供的範例 "[請按這裡](#)"。

如何將已配置的磁碟區設定為特定的匯出原則？

若要允許適當的主機存取磁碟區、請使用 `exportPolicy` 後端定義檔中設定的參數。

如何透過**Astra Trident**搭配**ONTAP** 使用才能設定**Volume**加密？

您可以使用後端定義檔中的加密參數、在Trident所提供的磁碟區上設定加密。如需詳細資訊、請參閱：["Astra Trident如何與NVE和NAE搭配運作"](#)

什麼是透過**ONTAP Astra Trident**實作**QoS for Sfor Sfor Sfor the S**星？

使用 `StorageClasses` 實作ONTAP QoS for Sfor

如何透過**Astra Trident**指定精簡或完整的資源配置？

支援精簡或密集資源配置的支援。ONTAP此功能預設為精簡配置。ONTAP如果需要完整資源配置、您應該設定後端定義檔或 `StorageClass`。如果兩者都已設定、`StorageClass` 優先。設定ONTAP 下列項目以供參考：

1. 開啟 `StorageClass`、設定 `provisioningType` 屬性為`thick`。
2. 在後端定義檔中、透過設定來啟用厚磁碟區 `backend spaceReserve parameter` 作為Volume。

如何確保即使意外刪除了**PVC**,也不會刪除使用中的磁碟區？

Kubernetes從1.10版開始自動啟用PVC保護。

我可以擴充由**Astra Trident**所建立的**NFS PVCs**嗎？

是的。您可以擴充由Astra Trident所建立的永久虛電路。請注意、Volume自動擴充ONTAP 是不適用於Trident的功能。

如果我的磁碟區是在**Astra Trident**以外建立的、我可以將它匯入**Astra Trident**嗎？

從19.04開始、您可以使用Volume匯入功能將磁碟區帶入Kubernetes。

我可以在磁碟區處於**SnapMirror**資料保護（**DP**）或離線模式時匯入該磁碟區嗎？

如果外部磁碟區處於DP模式或離線、則磁碟區匯入會失敗。您會收到下列錯誤訊息：



```
Error: could not import volume: volume import failed to get size of
volume: volume <name> was not found (400 Bad Request) command terminated
with exit code 1.
Make sure to remove the DP mode or put the volume online before importing
the volume.
```

## 我可以擴充由Astra Trident建立的iSCSI PVCs嗎？

Trident 19.10支援使用csi資源配置程式擴充iSCSI PV。

## 資源配額如何轉譯至NetApp叢集？

只要NetApp儲存設備具備容量、Kubernetes儲存資源配額就能運作。當NetApp儲存設備因為容量不足而無法遵守Kubernetes配額設定時、Astra Trident會嘗試進行資源配置、但卻發生錯誤。

## 我可以使用Astra Trident建立Volume Snapshot嗎？

是的。Astra Trident支援從快照建立隨需磁碟區快照和持續磁碟區。若要從快照建立PV、請確定VolumeSnapshotDataSource 功能閘道已啟用。

## 哪些驅動程式支援Astra Trident Volume快照？

目前、我們提供隨需快照支援 `ontap-nas`、`ontap-nas-flexgroup`、`ontap-san`、`ontap-san-economy`、`solidfire-san`、`gcp-cvs`和 `azure-netapp-files` 後端驅動程式：

## 我要如何針對Astra Trident提供ONTAP 的含有「支援」功能的磁碟區進行快照備份？

可在上取得 `ontap-nas`、`ontap-san`和 `ontap-nas-flexgroup` 驅動程式：您也可以指定 `snapshotPolicy` 適用於 `ontap-san-economy` 驅動程式FlexVol。

也可在上取得 `ontap-nas-economy` 驅動程式、但FlexVol在「不」於「不」於「不」於「qtree」層級精細度的情況下。若要讓Astra Trident提供的磁碟區能夠快照、請設定後端參數選項 `snapshotPolicy` 到ONTAP 所需的Snapshot原則、如在功能不完整的後端上所定義。Astra Trident不知道儲存控制器所拍攝的任何快照。

## 我可以為透過Astra Trident佈建的磁碟區設定快照保留百分比嗎？

是的、您可以設定、保留特定百分比的磁碟空間、以便透過Astra Trident來儲存快照複本 `snapshotReserve` 後端定義檔中的屬性。如果您已設定 `snapshotPolicy` 和 `snapshotReserve` 在後端定義檔中、快照保留百分比是根據設定 `snapshotReserve` 後端檔案中提及的百分比。如果是 `snapshotReserve` 未提及百分比數、ONTAP 根據預設、此為快照保留百分比5。如果是 `snapshotPolicy` 選項設為無、快照保留百分比設為0。

## 我可以直接存取Volume Snapshot目錄並複製檔案嗎？

是的、您可以設定Trident來存取Volume上的Snapshot目錄 `snapshotDir` 後端定義檔中的參數。

## 我可以透過Astra Trident為磁碟區設定SnapMirror嗎？

目前、SnapMirror必須使用ONTAP CLI或OnCommand 《系統管理程式》從外部設定。

## 如何將持續磁碟區還原至特定ONTAP 的不還原快照？

若要將磁碟區還原ONTAP 成一個無法修復的快照、請執行下列步驟：

1. 靜止使用持續磁碟區的應用程式Pod。
2. 透過ONTAP NetApp CLI或OnCommand 《系統管理程式》回復至所需的快照。
3. 重新啟動應用程式Pod。

## 是否能在已設定負載共享鏡射的SVM上、對磁碟區進行Trident資源配置？

您可以為透過NFS提供資料的SVM根磁碟區建立負載共享鏡像。針對Trident所建立的磁碟區、自動更新負載共享鏡像。ONTAP這可能會導致掛載磁碟區延遲。使用Trident建立多個磁碟區時、資源配置磁碟區會仰賴ONTAP於更新負載共享鏡像。

## 如何區分每位客戶/租戶的儲存類別使用量？

Kubernetes不允許命名空間中的儲存類別。不過、您可以使用Kubernetes來限制每個命名空間的特定儲存類別使用量、方法是使用儲存資源配額（每個命名空間）。若要拒絕特定儲存設備的特定命名空間存取、請將該儲存類別的資源配額設為0。

# 支援

Astra Trident是正式支援的NetApp專案。您可以使用任何標準機制聯絡NetApp、取得所需的企業級支援。

我們的Astra還有一個充滿活力的公共社群、由容器使用者（包括Astra Trident開發人員）所共同參與 ["不和通路"](#)。這是您提出專案相關一般問題、並與志同道合的同儕討論相關主題的好地方。

# 疑難排解

請使用此處提供的指標來疑難排解安裝及使用Astra Trident時可能遇到的問題。



如需Astra Trident的協助、請使用建立支援套裝組合 `tridentctl logs -a -n trident` 並傳送至 NetApp Support <Getting Help>。



如需疑難排解文章的完整清單、請參閱 ["NetApp知識庫（需要登入）"](#)。您也可以找到Astra相關疑難排解問題的相關資訊 ["請按這裡"](#)。

## 一般疑難排解

- 如果Trident Pod無法正常顯示（例如、當Trident Pod卡在中時） ContainerCreating 階段、只需不到兩個就緒容器）、就能執行 `kubectl -n trident describe deployment trident` 和 `kubectl -n trident describe pod trident--**` 可提供更多洞見。取得Kubelet記錄（例如、透過 `journalctl -xeu kubelet`）也很有幫助。
- 如果Trident記錄中沒有足夠的資訊、您可以透過傳遞來嘗試啟用Trident的偵錯模式 `-d` 根據您的安裝選項標示安裝參數。

然後確認是否使用設定偵錯 `./tridentctl logs -n trident` 和搜尋 `level=debug msg` 在記錄中。

與營運者一起安裝

```
kubectl patch torc trident -n <namespace> --type=merge -p
'{"spec":{"debug":true}}'
```

這會重新啟動所有Trident Pod、可能需要數秒鐘的時間。您可以查看的輸出中的「年齡」欄來檢查 `kubectl get pod -n trident`。

使用Astra Trident 20.07和20.10 tprov 取代 torc。

與Helm一起安裝

```
helm upgrade <name> trident-operator-21.07.1-custom.tgz --set
tridentDebug=true`
```

安裝試用版

```
./tridentctl uninstall -n trident
./tridentctl install -d -n trident
```

- 您也可以取得每個後端的除錯記錄、方法是加入 `debugTraceFlags` 在後端定義中。例如、包括 `debugTraceFlags: {"api":true, "method":true,}` 取得Trident記錄中的API呼叫和方法反向。現有的後端可以有 `debugTraceFlags` 設定為 `tridentctl backend update`。

- 使用RedHat CoreOS時、請務必確認 `iscsid` 在工作節點上啟用、預設為啟動。您可以使用OpenShift機器組態或修改點火模板來完成此作業。
- 使用Trident時可能會遇到的常見問題 ["Azure NetApp Files"](#) 當租戶和用戶端機密來自權限不足的應用程式登錄時。如需Trident需求的完整清單、請參閱 ["Azure NetApp Files"](#) 組態：
- 如果在將PV安裝至容器時發生問題、請確定 `rpcbind` 已安裝並執行。使用主機作業系統所需的套件管理程式、並檢查是否有 `rpcbind` 正在執行。您可以檢查的狀態 `rpcbind` 執行 `systemctl status rpcbind` 或同等產品。
- 如果Trident後端報告其位於 `failed` 狀態儘管以前曾經工作過、但可能是因為變更與後端相關的SVM/admin認證資料所致。使用更新後端資訊 `tridentctl update backend` 或是退回Trident Pod即可解決此問題。
- 如果您要升級Kubernetes叢集和（或）Trident以使用beta Volume Snapshot、請確定已完全移除所有現有的Alpha Snapshot CRS。然後您就可以使用 `tridentctl obliviante alpha-snapshot-crd` 刪除Alpha Snapshot CRD的命令。請參閱 ["這篇部落格"](#) 瞭解移轉Alpha快照所需的步驟。
- 如果在容器執行時間安裝Trident with Docker時遇到權限問題、請嘗試使用安裝Trident `--in-cluster=false` 旗標。這不會使用安裝程式pod、也會避免因為而發生權限問題 `trident-installer` 使用者：
- 使用 `uninstall parameter <Uninstalling Trident>` 用於在執行失敗後進行清理。根據預設、指令碼不會移除Trident所建立的客戶需求日、即使在執行中的部署中、也能安全地解除安裝及再次安裝。
- 如果您想要降級至舊版Trident、請先執行 `tridentctl uninstall` 移除Trident的命令。下載所需的 ["Trident版本"](#) 並使用安裝 `tridentctl install` 命令。只有在沒有建立新的PV、且尚未對現有的PV/後端/儲存類別進行任何變更時、才考慮降級。由於Trident現在使用CRD來維護狀態、因此所有建立的儲存實體（後端、儲存類別、PV和Volume Snapshot）都擁有 associated CRD objects <Kubernetes CustomResourceDefinition Objects> 而非寫入先前安裝版本Trident所使用之PV的資料。移回舊版時、新建立的**PV**將無法使用。\*對物件所做的變更、例如後端、PV、儲存類別和Volume快照（已建立/更新/刪除）、在降級\*時、Trident將無法看到。Trident安裝的舊版Trident所使用的PV、仍可供Trident查看。返回舊版不會中斷已使用舊版建立之PV的存取、除非已升級。
- 若要完全移除Trident、請執行 `tridentctl obliviante crd` 命令。這會移除所有CRD物件、並取消定義客戶需求日。Trident將不再管理任何已配置的PV。



之後需要從頭重新設定Trident。

- 成功安裝之後、如果有一個PVC卡在中 `Pending` 階段、執行中 `kubectl describe pvc` 可提供有關Trident為何無法為此PVC配置PV的其他資訊。

## 使用操作員疑難排解不成功的Trident部署

如果您使用運算子部署Trident、則狀態為 `TridentOrchestrator` 變更來源 `Installing` 至 `Installed`。如果您觀察到 `Failed` 狀態、而且操作員無法自行恢復、您應該執行下列命令來檢查操作員的記錄：

```
tridentctl logs -l trident-operator
```

追蹤Trident運算子容器的記錄可以指出問題所在。例如、其中一個問題可能是無法從無線環境中的上游登錄擷取所需的容器映像。

若要瞭解Trident安裝失敗的原因、請參閱 `TridentOrchestrator` 狀態。

```
kubectl describe torc trident-2
Name:          trident-2
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:   trident.netapp.io/v1
Kind:          TridentOrchestrator
...
Status:
  Current Installation Params:
    IPv6:
    Autosupport Hostname:
    Autosupport Image:
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:
    Image Pull Secrets:          <nil>
    Image Registry:
    k8sTimeout:
    Kubelet Dir:
    Log Format:
    Silence Autosupport:
    Trident Image:
  Message:          Trident is bound to another CR 'trident'
  Namespace:        trident-2
  Status:           Error
  Version:
Events:
  Type      Reason  Age                From              Message
  ----      -
Warning    Error    16s (x2 over 16s)  trident-operator.netapp.io  Trident
is bound to another CR 'trident'
```

此錯誤表示已存在 `TridentOrchestrator` 用於安裝 `Trident`。由於每個 `Kubernetes` 叢集只能有一個 `Trident` 執行個體、因此操作員可確保在任何指定時間只有一個作用中的執行個體存在 `TridentOrchestrator` 它可以建立的。

此外、觀察 `Trident Pod` 的狀態、通常會指出是否有不正確的情況。

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

NAME	READY	STATUS	RESTARTS
trident-csi-4p5kq 5m18s	1/2	ImagePullBackOff	0
trident-csi-6f45bfd8b6-vfrkw 5m19s	4/5	ImagePullBackOff	0
trident-csi-9q5xc 5m18s	1/2	ImagePullBackOff	0
trident-csi-9v95z 5m18s	1/2	ImagePullBackOff	0
trident-operator-766f7b8658-ldzsv 8m17s	1/1	Running	0

您可以清楚看到、由於未擷取一或多個容器映像、所以Pod無法完全初始化。

若要解決此問題、您應該編輯 `TridentOrchestrator` CR.或者、您也可以刪除 `TridentOrchestrator`，然後建立新的定義，以修改且準確的定義。

## 使用疑難排解不成功的**Trident**部署 `tridentctl`

為了協助您找出錯誤所在、您可以使用再次執行安裝程式 `-d` 引數、可開啟偵錯模式、協助您瞭解問題所在：

```
./tridentctl install -n trident -d
```

解決此問題之後、您可以依照下列方式清理安裝、然後執行 `tridentctl install` 再次命令：

```
./tridentctl uninstall -n trident
INFO Deleted Trident deployment.
INFO Deleted cluster role binding.
INFO Deleted cluster role.
INFO Deleted service account.
INFO Removed Trident user from security context constraint.
INFO Trident uninstallation succeeded.
```

# 最佳實務做法與建議

## 部署

部署Astra Trident時、請使用此處列出的建議。

### 部署至專屬命名空間

"命名空間" 在不同的應用程式之間提供管理分離、是資源共用的障礙。例如、某個命名空間的某個永久虛電路無法從另一個命名空間使用。Astra Trident為Kubernetes叢集中的所有命名空間提供PV資源、並因此運用具有較高權限的服務帳戶。

此外、存取Trident Pod可能會讓使用者存取儲存系統認證和其他敏感資訊。請務必確保應用程式使用者和管理應用程式無法存取Trident物件定義或Pod本身。

### 使用配額和範圍限制來控制儲存使用量

Kubernetes有兩項功能、一旦結合、就能提供強大的機制來限制應用程式的資源使用量。。 "儲存配額機制" 可讓系統管理員針對每個命名空間來實作全域和儲存類別的容量和物件數使用限制。此外、請使用 "範圍限制" 確保在將要求轉送至資源配置程式之前、永久虛擬機器要求的最小值和最大值都在內。

這些值是以每個命名空間為基礎來定義、這表示每個命名空間都應該定義符合其資源需求的值。如需相關資訊、請參閱此處 "如何運用配額"。

## 儲存組態

NetApp產品組合中的每個儲存平台都有獨特的功能、無論應用程式是否為容器化的應用程式帶來好處。

### 平台總覽

Trident可搭配ONTAP 使用沒有一個平台比其他平台更適合所有應用程式和案例、不過在選擇平台時、應考慮應用程式和管理裝置團隊的需求。

您應該遵循主機作業系統的基礎最佳實務做法、以及您所使用的傳輸協定。或者、您可能想要考慮在可用的情況下、將應用程式最佳實務做法與後端、儲存類別和永久虛擬基礎架構設定整合、以最佳化特定應用程式的儲存。

### 最佳實務做法ONTAP Cloud Volumes ONTAP

瞭解設定ONTAP 適用於Cloud Volumes ONTAP Trident的功能性及功能性的最佳實務做法。

以下建議是設定ONTAP 以容器化工作負載為基礎的功能指南、這些功能會消耗Trident動態配置的磁碟區。每個項目都應考量及評估是否適合您的環境。

### 使用Trident專用的SVM

儲存虛擬機器（SVM）可隔離ONTAP 及管理各個客戶在一個系統上的區隔。將SVM專用於應用程式可委派權限、並可套用最佳實務做法來限制資源使用量。



SVM管理有多種選項可供選擇：

- 在後端組態中提供叢集管理介面、以及適當的認證、然後指定SVM名稱。
- 使用ONTAP 支援功能的支援中心或CLI、為SVM建立專屬的管理介面。
- 與NFS資料介面共用管理角色。

在每種情況下、介面都應該位於DNS中、而且在設定Trident時、應該使用DNS名稱。這有助於推動一些DR案例、例如不使用網路身分保留功能的SVM-DR。

不過、您並不偏好為SVM設定專屬或共享的管理LIF、不過您應該確保網路安全性原則符合您選擇的方法。無論如何、管理LIF都應透過DNS存取、以達到最大的靈活性 **"SVM-DR"** 與Trident搭配使用。

### 限制最大Volume數

根據軟體版本和硬體平台、系統可提供最大的Volume數。ONTAP請參閱 **"NetApp Hardware Universe"** 針對您的特定平台和ONTAP 版本、決定確切的限制。當磁碟區數用盡時、資源配置作業不僅會針對Trident、也會針對所有儲存要求失敗。

Trident的 `ontap-nas` 和 `ontap-san` 驅動程式會針對所建立的每個Kubernetes持續Volume (PV) 來配置FlexVolume。◦ `ontap-nas-economy` 每200個PV約需建立一個FlexVolume (可設定為50至300)。◦ `ontap-san-economy` 每100個PV約需建立一個FlexVolume (可設定為50到200)。若要避免Trident佔用儲存系統上的所有可用磁碟區、您應該在SVM上設定限制。您可以從命令列執行此動作：

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

的價值 `max-volumes` 視您環境的幾項特定條件而異：

- 在叢集中現有的Volume數量ONTAP
- 您預期在Trident外部配置其他應用程式的Volume數量
- Kubernetes應用程式預期會使用的持續磁碟區數量

◦ `max-volumes` 值是ONTAP 指在整個叢集中所有節點上配置的總Volume、而非在個別ONTAP 的節點上配置的總Volume。因此ONTAP、您可能會遇到一些情況、例如、某個叢集節點的資源配置量可能遠高於或低於其他節點。

舉例ONTAP 來說、雙節點的「叢集」最多可裝載2000個FlexVolumes。將最大Volume數設為1250似乎非常合理。不過、如果只有 **"集合體"** 從某個節點指派給SVM、或是從某個節點指派的集合體無法根據（例如、由於容量）進行資源配置、則另一個節點會成為所有Trident資源配置磁碟區的目標。這表示該節點可能會在之前達到磁碟區限制 `max-volumes` 達到該值、會影響Trident和其他使用該節點的Volume作業。您可以確保叢集中每個節點的集合體都指派給**Trident**使用的**SVM**、數量相等、藉此避免這種情況。

### 限制Trident所建立的Volume大小上限

若要設定Trident可建立之磁碟區的最大大小、請使用 `limitVolumeSize` 中的參數 `backend.json` 定義。

除了控制儲存陣列的磁碟區大小、您也應該善用Kubernetes功能。

## 設定Trident使用雙向CHAP

您可以在後端定義中指定CHAP啟動器和目標使用者名稱和密碼、並在SVM上啟用Trident啟用CHAP。使用 useCHAP 後端組態中的參數、Trident會驗證iSCSI連線ONTAP、以CHAP作為後端。Trident 20.04及更新版本提供雙向CHAP支援。

## 建立並使用SVM QoS原則

運用ONTAP 套用至SVM的SVM的SQoS原則、限制Trident佈建磁碟區所耗用的IOPS數量。這對我們有幫助 "[預防欺凌](#)" 或失控的容器、避免影響Trident SVM以外的工作負載。

您可以在幾個步驟中建立SVM的QoS原則。如ONTAP 需最準確的資訊、請參閱您的版次更新文件。以下範例建立QoS原則、將SVM可用的總IOPS限制為5000。

```
# create the policy group for the SVM
qos policy-group create -policy-group <policy_name> -vserver <svm_name>
-max-throughput 5000iops

# assign the policy group to the SVM, note this will not work
# if volumes or files in the SVM have existing QoS policies
vserver modify -vserver <svm_name> -qos-policy-group <policy_name>
```

此外、如果ONTAP 您的版本支援此功能、您可以考慮使用QoS下限來保證容器化工作負載的處理量。調適性QoS與SVM層級原則不相容。

容器化工作負載專用的IOPS數量取決於許多層面。其中包括：

- 使用儲存陣列的其他工作負載。如果有其他工作負載與Kubernetes部署無關、請善用儲存資源、確保這些工作負載不會意外受到不良影響。
- 預期的工作負載會在容器中執行。如果將在容器中執行高IOPS需求的工作負載、低QoS原則會導致不良體驗。

請務必記住、在SVM層級指派的QoS原則會導致所有已配置給SVM的磁碟區共用相同的IOPS集區。如果其中一種或少數幾種容器化應用程式的IOPS需求較高、可能會成為其他容器化工作負載的一大功臣。如果是這種情況、您可能需要考慮使用外部自動化來指派每個Volume QoS原則。



如果您的版本早於ONTAP 9.8、您應該將QoS原則群組指派給SVM \* Only \*。

## 為Trident建立QoS原則群組

服務品質（QoS）可確保關鍵工作負載的效能不會因競爭工作負載而降級。支援QoS原則群組的QoS選項可用於磁碟區、並可讓使用者定義一或多個工作負載的處理量上限。ONTAP如需QoS的詳細資訊、請參閱 "[保證QoS的處理量](#)"。您可以在後端或儲存資源池中指定QoS原則群組、並將其套用至該資源池或後端中建立的每個磁碟區。

包含兩種QoS原則群組：傳統和可調適。ONTAP傳統原則群組可在IOPS中提供最大（或最小）的單位處理量（在較新版本中）。調適性QoS會自動將處理量調整至工作負載大小、並隨著工作負載大小變更、維持IOPS與TBs的比率。當您在大型部署中管理數百個或數千個工作負載時、這項優勢就相當顯著。

建立QoS原則群組時、請考量下列事項：

- 您應該設定 qosPolicy 鍵入 defaults 後端組態區塊。請參閱下列後端組態範例：

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 0.0.0.0
dataLIF: 0.0.0.0
svm: svm0
username: user
password: pass
defaults:
  qosPolicy: standard-pg
storage:
- labels:
  performance: extreme
  defaults:
    adaptiveQosPolicy: extremely-adaptive-pg
- labels:
  performance: premium
  defaults:
    qosPolicy: premium-pg
```

- 您應該為每個Volume套用原則群組、以便每個Volume都能獲得原則群組指定的整個處理量。不支援共用原則群組。

如需QoS原則群組的詳細資訊、請參閱 ["Sof 9.8 QoS命令ONTAP"](#)。

### 限制Kubernetes叢集成員存取儲存資源

限制存取Trident所建立的NFS磁碟區和iSCSI LUN、是Kubernetes部署安全態勢的重要元件。這樣做可防止非Kubernetes叢集一部分的主機存取磁碟區、並可能意外修改資料。

請務必瞭解命名空間是Kubernetes中資源的邏輯邊界。假設相同命名空間中的資源可以共用、但重要的是、沒有跨命名空間功能。這表示即使PV是全域物件、但只有在同一個命名空間中的Pod才能存取它們。確保命名空間在適當時用於提供分隔是非常重要的。

大多數組織對於Kubernetes內容中的資料安全性、主要關注的是、容器中的程序可以存取掛載到主機의儲存設備、但不適用於容器。["命名空間"](#) 旨在防止這類入侵。不過、有一個例外：特殊權限容器。

與正常情況相比、特權容器的執行主機層級權限大幅增加。依預設不會拒絕這些功能、因此請務必使用停用該功能 ["Pod安全性原則"](#)。

對於需要從Kubernetes和外部主機存取的磁碟區、儲存設備應以傳統方式進行管理、由系統管理員引進PV、而非由Trident管理。這可確保只有在Kubernetes和外部主機中斷連線且不再使用磁碟區時、才會銷毀儲存磁碟區。此外、也可以套用自訂匯出原則、以便從Kubernetes叢集節點和Kubernetes叢集以外的目標伺服器存取。

對於具有專用基礎架構節點（例如OpenShift）或其他節點無法排程使用者應用程式的部署、應使用個別的匯出原則、進一步限制對儲存資源的存取。這包括為部署至這些基礎架構節點的服務（例如OpenShift Metrics和記錄服務）、以及部署至非基礎架構節點的標準應用程式建立匯出原則。

## 使用專屬的匯出原則

您應該確保每個後端都有一個匯出原則、只允許存取Kubernetes叢集中的節點。Trident可從20.04版開始自動建立及管理匯出原則。如此一來、Trident就能限制對Kubernetes叢集中節點所配置之磁碟區的存取、並簡化節點的新增/刪除作業。

或者、您也可以手動建立匯出原則、並以一或多個匯出規則填入、以處理每個節點存取要求：

- 使用 `vserver export-policy create` 建立匯出原則的CLI命令。ONTAP
- 使用新增規則至匯出原則 `vserver export-policy rule create` CLI命令。ONTAP

執行這些命令可讓您限制哪些Kubernetes節點可以存取資料。

## 停用 `showmount` 適用於應用程式SVM

◦ `showmount` 功能可讓NFS用戶端查詢SVM、取得可用NFS匯出的清單。部署至Kubernetes叢集的Pod可能會發出問題 `showmount -e` 針對資料LIF執行命令、並接收可用掛載的清單、包括無法存取的掛載。雖然這本身並不是安全威脅、但它確實提供不必要的資訊、可能有助於未獲授權的使用者連線至NFS匯出。

您應該停用 `showmount` 使用SVM層級ONTAP 的SVM CLI命令：

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```

## 最佳實務做法SolidFire

瞭解設定SolidFire Trident之用的功能完善的功能。

### 建立SolidFire 支援帳戶

每SolidFire 個驗證帳戶都代表唯一的磁碟區擁有者、並會收到自己的挑戰握手驗證傳輸協定（CHAP）認證資料。您可以使用帳戶名稱和相對CHAP認證、或是透過Volume存取群組、來存取指派給帳戶的磁碟區。帳戶最多可指派2、000個磁碟區、但一個磁碟區只能屬於一個帳戶。

### 建立QoS原則

如果您想建立並儲存可套用至許多Volume的標準化服務品質設定、請使用SolidFire 「服務品質（QoS）」原則。

您可以設定每個Volume的QoS參數。設定三個可設定的參數來定義QoS、以確保每個Volume的效能：最小IOPS、最大IOPS和爆發IOPS。

以下是4KB區塊大小的可能最小、最大和尖峰IOPS值。

IOPS參數	定義	最小價值	預設值	最大價值（4KB）
最小IOPS	保證磁碟區效能等級。	50	50	15000

IOPS參數	定義	最小價值	預設值	最大價值 (4KB)
最大IOPS	效能不會超過此限制。	50	15000	20萬
暴增IOPS	在短時間暴增案例中允許的最大IOPS。	50	15000	20萬



雖然最大IOPS和爆發IOPS可設定為高達20、000、但實際的Volume最大效能卻受到叢集使用量和每節點效能的限制。

區塊大小和頻寬會直接影響IOPS的數量。隨著區塊大小增加、系統會將頻寬增加至處理較大區塊大小所需的層級。隨著頻寬增加、系統能夠達到的IOPS數量也隨之減少。請參閱 ["服務品質SolidFire"](#) 如需QoS和效能的詳細資訊、請參閱。

## 驗證SolidFire

Element支援兩種驗證方法：CHAP和Volume Access Groups (VAG)。CHAP使用CHAP傳輸協定驗證主機到後端的驗證。Volume存取群組可控制對其所配置之Volume的存取。NetApp建議使用CHAP進行驗證、因為它更簡單、而且沒有擴充限制。



Trident搭配增強的csi佈置程式、可支援使用CHAP驗證。VAG只能在傳統的非csi操作模式下使用。

CHAP驗證（驗證啟動器是否為預定的Volume使用者）僅支援帳戶型存取控制。如果您使用CHAP進行驗證、則有兩個選項可供使用：單向CHAP和雙向CHAP。單向CHAP使用SolidFire 驗證帳戶名稱和啟動器密碼來驗證Volume存取。雙向CHAP選項提供最安全的驗證磁碟區方法、因為磁碟區會透過帳戶名稱和啟動器密碼來驗證主機、然後主機會透過帳戶名稱和目標密碼來驗證磁碟區。

但是、如果無法啟用CHAP且需要VAG、請建立存取群組、然後將主機啟動器和磁碟區新增至存取群組。您新增至存取群組的每個IQN都可以使用或不使用CHAP驗證來存取群組中的每個磁碟區。如果iSCSI啟動器設定為使用CHAP驗證、則會使用帳戶型存取控制。如果iSCSI啟動器未設定為使用CHAP驗證、則會使用Volume Access Group存取控制。

## 哪裡可以找到更多資訊？

以下列出部分最佳實務做法文件。搜尋 ["NetApp資料庫"](#) 適用於最新版本。

### 《》 ONTAP

- ["NFS最佳實務與實作指南"](#)
- ["SAN管理指南"](#)（適用於iSCSI）
- ["適用於RHEL的iSCSI Express組態"](#)

### 元件軟體

- ["設定SolidFire 適用於Linux的功能"](#)

### 《》 NetApp HCI

- ["部署先決條件NetApp HCI"](#)
- ["存取NetApp部署引擎"](#)

應用程式最佳實務做法資訊

- ["MySQL ONTAP 的最佳實務做法"](#)
- ["MySQL SolidFire 的最佳實務做法"](#)
- ["NetApp SolidFire 的功能與Cassandra"](#)
- ["Oracle SolidFire 的最佳實務做法"](#)
- ["PostgreSQL SolidFire 的最佳實務做法"](#)

並非所有應用程式都有特定的準則、請務必與您的NetApp團隊合作並使用 ["NetApp資料庫"](#) 以尋找最新的文件。

## 整合Astra Trident

若要整合Astra Trident、下列設計與架構元素需要整合：驅動程式選擇與部署、儲存類別設計、虛擬集區設計、持續磁碟區宣告（PVC）、使用Astra Trident對儲存資源配置、磁碟區作業及OpenShift服務部署的影響。

### 驅動程式選擇與部署

為您的儲存系統選取並部署後端驅動程式。

#### 背後驅動程式ONTAP

以使用的傳輸協定和儲存系統上的磁碟區配置方式來區分後端驅動程式ONTAP。因此、在決定要部署的驅動程式時、請謹慎考量。

較高層級的應用程式若有需要共用儲存設備的元件（多個Pod存取相同的PVC）、則以NAS為基礎的驅動程式將是預設選擇、而區塊型iSCSI驅動程式則可滿足非共用儲存設備的需求。根據應用程式的需求、以及儲存設備和基礎架構團隊的舒適度來選擇傳輸協定。一般而言、大多數應用程式的差異不大、因此通常是根據是否需要共用儲存設備（如果有多個Pod需要同時存取）來決定。

可用ONTAP 的支援功能包括：

- `ontap-nas`：配置的每個PV都是ONTAP 完整的FlexVolume。
- `ontap-nas-economy`：每個配置的PV都是qtree、每個FlexVolume可設定的qtree數量（預設值為200）。
- `ontap-nas-flexgroup`：每個PV均配置為完整ONTAP FlexGroup 的功能、並使用指派給SVM的所有集合體。
- `ontap-san`：每個已配置的PV都是其FlexVolume中的LUN。
- `ontap-san-economy`：配置的每個PV都是一個LUN、每個FlexVolume有可設定的LUN數量（預設值為100）。

在這三種NAS驅動程式之間選擇、會對應用程式可用的功能產生一些影響。

請注意、在下表中、並非所有功能都透過Astra Trident公開。如果需要這些功能、儲存管理員必須在資源配置後



套用部分功能。上標註可區分每項功能和驅動程式的功能。

ASNAS驅動程式ONTAP	快照	複製	動態匯出原則	多重附加	QoS	調整大小	複寫
ontap-nas	是的	是的	是註腳：5[]	是的	是註腳：1[]	是的	是註腳：1[]
ontap-nas-economy	是註腳：3[]	是註腳：3[]	是註腳：5[]	是的	是註腳：3[]	是的	是註腳：3[]
ontap-nas-flexgroup	是註腳：1[]	否	是註腳：5[]	是的	是註腳：1[]	是的	是註腳：1[]

Astra Trident提供2個ONTAP SAN驅動程式來支援功能如下所示。

支援SAN驅動程式ONTAP	快照	複製	多重附加	雙向CHAP	QoS	調整大小	複寫
ontap-san	是的	是的	是註腳：4[]	是的	是註腳：1[]	是的	是註腳：1[]
ontap-san-economy	是的	是的	是註腳：4[]	是的	是註腳：3[]	是的	是註腳：3[]

上表的註腳：是註腳：1[]：不受Astra Trident管理是註腳：2[]：由Astra Trident管理、但不受PV精細控制是註腳：3[]：不受Astra Trident管理而非PV精細控制是註腳：4[]：支援原始區塊Volume是註腳：5[]：受Ci Trident支援

非PV精細的功能會套用至整個FlexVolume、而所有PV（即共享FlexVols中的qtree或LUN）都會共用一個共同排程。

如上表所示、兩者之間的大部分功能 ontap-nas 和 ontap-nas-economy 相同。不過、因為 ontap-nas-economy 驅動程式會限制以每個PV精細度控制排程的能力、這可能會特別影響您的災難恢復與備份規劃。如果開發團隊想要在ONTAP 不支援的儲存設備上使用永久虛擬複製功能、只有在使用時才有可能做到這一點 ontap-nas、ontap-san 或 ontap-san-economy 驅動程式：



。solidfire-san 驅動程式也能複製PVCS。

## 背後驅動程式Cloud Volumes ONTAP

支援資料控管功能、並提供企業級的儲存功能、適用於各種使用案例、包括檔案共用、區塊層級儲存設備（NFS、SMB / CIFS及iSCSI）Cloud Volumes ONTAP。Cloud Volume ONTAP 的相容驅動程式就是 ontap-nas、ontap-nas-economy、ontap-san 和 ontap-san-economy。適用於ONTAP Azure的Cloud Volume供應、適用於ONTAP GCP的Cloud Volume供應。

## Amazon FSXfor ONTAP Sendbackend驅動程式

Amazon FSX ONTAP for VMware可讓客戶運用熟悉的NetApp功能、效能和管理功能、同時充分發揮儲存AWS資料的簡易性、敏捷度、安全性和擴充性。FSX ONTAP for FSfor支援ONTAP的許多檔案系統功能和管理API。Cloud Volume ONTAP 的相容驅動程式就是 ontap-nas、ontap-nas-economy、ontap-nas-flexgroup、ontap-san 和 ontap-san-economy。

## NetApp HCI / SolidFire後端驅動程式

◦ `solidfire-san` 與NetApp HCI / SolidFire平台搭配使用的驅動程式、可協助管理員根據QoS限制、設定Trident的元素後端。如果您想要設計後端、以便針對Trident提供的磁碟區設定特定的QoS限制、請使用 `type` 後端檔案中的參數。管理員也可以使用來限制儲存設備上可建立的磁碟區大小 `limitVolumeSize` 參數。目前、不支援磁碟區大小調整和磁碟區複寫等元素儲存功能 `solidfire-san` 驅動程式：這些作業應透過Element Software Web UI手動完成。

驅動程式SolidFire	快照	複製	多重附加	CHAP	QoS	調整大小	複寫
<code>solidfire-san</code>	是的	是的	是註腳：2[]	是的	是的	是的	是註腳：1[]

註腳：是註腳：1[]：不受Astra Trident管理是註腳：2[]：支援原始區塊磁碟區

## 背後驅動程式Azure NetApp Files

Astra Trident使用 `azure-netapp-files` 管理的驅動程式 "[Azure NetApp Files](#)" 服務：

如需此驅動程式及其設定方式的詳細資訊、請參閱 "[Astra Trident的Azure NetApp Files 後端組態、適用於](#)"。

驅動程式Azure NetApp Files	快照	複製	多重附加	QoS	展開	複寫
<code>azure-netapp-files</code>	是的	是的	是的	是的	是的	是註腳：1[]

註腳：是註腳：1[]：不由Astra Trident管理

## 在Google Cloud後端驅動程式上執行Cloud Volumes Service

Astra Trident使用 `gcp-cvs` 在Cloud Volumes Service Google Cloud上連結至該解決方案的驅動程式。

◦ `gcp-cvs` 驅動程式使用虛擬資源池來抽象化後端、並允許Astra Trident決定磁碟區放置。系統管理員會在主目錄中定義虛擬資源池 `backend.json` 檔案：儲存類別會使用選取器來依標籤識別虛擬資源池。

- 如果在後端定義了虛擬資源池、Astra Trident會嘗試在Google Cloud儲存資源池中建立該虛擬資源池所限制的磁碟區。
- 如果後端未定義虛擬資源池、Astra Trident會從該地區可用的儲存資源池中選取Google Cloud儲存資源池。

若要在Astra Trident上設定Google Cloud後端、您必須指定 `projectNumber`、`apiRegion`和 `apiKey` 在後端檔案中。您可以在Google Cloud主控台找到專案編號。API金鑰取自您在Google Cloud Volumes Service Cloud上設定API存取功能時所建立的服務帳戶私密金鑰檔案。

如需Cloud Volumes Service 有關Google Cloud服務類型與服務層級的詳細資訊、請參閱 "[瞭解Astra Trident對CVS for GCP的支援](#)"。



適用於Google Cloud驅動程式Cloud Volumes Service	快照	複製	多重附加	QoS	展開	複寫
gcp-cvs	是的	是的	是的	是的	是的	僅適用於CVS效能服務類型。



#### 複寫附註

- 複寫不由Astra Trident管理。
- 該實體複本會建立在與來源Volume相同的儲存資源池中。

## 儲存層級設計

需要設定並套用個別的儲存類別、才能建立Kubernetes儲存類別物件。本節將討論如何為應用程式設計儲存類別。

### 特定後端使用率

篩選功能可在特定的儲存類別物件內使用、以決定要搭配該特定儲存類別使用的儲存資源池或集區集區集區。可在儲存類別中設定三組篩選器： `storagePools`、`additionalStoragePools` 和/或 `excludeStoragePools`。

◦ `storagePools` 參數有助於將儲存區限制在符合任何指定屬性的集區集合。◦ `additionalStoragePools` 參數可用來擴充Astra Trident將用於資源配置的集區集區集區集區、以及由屬性和所選的集區集區集區集區集區集區集區集區 `storagePools` 參數。您可以單獨使用參數或同時使用兩者、以確保已選取適當的儲存資源池集區集區。

◦ `excludeStoragePools` 參數用於明確排除所列的符合屬性的集區集區集區集區。

### 模擬QoS原則

如果您想要設計儲存類別來模擬服務品質原則、請使用建立儲存類別 `media` 屬性為 `hdd` 或 `ssd`。根據 `media` 儲存類別中提及的屬性Trident會選取適當的後端來提供服務 `hdd` 或 `ssd` 集合體以符合媒體屬性、然後將磁碟區的資源配置導向特定的集合體。因此、我們可以建立一個儲存等級Premium `media` 屬性設為 `ssd` 可歸類為優質QoS原則。我們可以建立另一個儲存類別標準、將媒體屬性設為「HDD」、並將其歸類為標準QoS原則。我們也可以使用儲存類別中的「IOPS」屬性、將資源配置重新導向至可定義為QoS原則的元素應用裝置。

### 根據特定功能使用後端

儲存類別可設計用於將Volume資源配置導向特定後端、啟用精簡與完整資源配置、快照、複製及加密等功能。若要指定要使用的儲存設備、請建立儲存設備類別、以指定啟用所需功能的適當後端。

### 虛擬資源池

所有Astra Trident後端均可使用虛擬資源池。您可以使用Astra Trident提供的任何驅動程式、為任何後端定義虛擬資源池。

虛擬集區可讓系統管理員在後端建立抽象層級、以便透過「儲存類別」加以參考、以提高磁碟區在後端的靈活性與效率。不同的後端可以使用相同的服務類別來定義。此外、您也可以相同的後端上建立多個儲存資源池、但

其特性不同。當儲存類別設定為具有特定標籤的選取器時、Astra Trident會選擇符合所有選取器標籤的後端來放置磁碟區。如果儲存類別選取器標籤符合多個儲存資源池、Astra Trident會選擇其中一個來配置磁碟區。

## 虛擬資源池設計

建立後端時、您通常可以指定一組參數。系統管理員無法以相同的儲存認證和一組不同的參數來建立另一個後端。隨著虛擬資源池的推出、這個問題已經減輕。虛擬集區是後端與Kubernetes儲存類別之間的層級抽象、可讓系統管理員定義參數及標籤、並以不受後端限制的方式透過Kubernetes儲存類別做為選取元來參考。可使用Astra Trident為所有支援的NetApp後端定義虛擬資源池。這份清單包括SolidFire/NetApp HCI、ONTAP 《關於Cloud Volumes Service GCP的功能、功能、功能、功能Azure NetApp Files 、功能、以及



定義虛擬資源池時、建議您不要嘗試重新排列後端定義中現有虛擬資源池的順序。此外、建議您不要編輯/修改現有虛擬資源池的屬性、改為定義新的虛擬資源池。

## 模擬不同的服務層級/QoS

您可以設計虛擬集區來模擬服務類別。使用適用於Azure NetApp Files 支援功能的Cloud Volume Service for效益的虛擬資源池實作、讓我們來看看如何設定不同的服務類別。使用代表不同效能等級的多個標籤來設定ANF後端。設定 `servicelevel` 並在每個標籤下新增其他必要的層面。現在請建立不同的Kubernetes儲存類別、以便對應至不同的虛擬資源池。使用 `parameters.selector` 欄位中、每個StorageClass會呼叫哪些虛擬資源池可用於裝載Volume。

## 指派特定的層面組合

可從單一儲存後端設計多個具有特定層面的虛擬集區。若要這麼做、請使用多個標籤來設定後端、並在每個標籤下設定所需的層面。現在、請使用建立不同的Kubernetes儲存類別 `parameters.selector` 對應至不同虛擬資源池的欄位。在後端上進行資源配置的磁碟區、將會在所選的虛擬資源池中定義各個層面。

## 會影響儲存資源配置的永久儲存設備特性

在建立永久虛擬儲存設備時、超出所要求儲存類別的部分參數可能會影響Astra Trident的資源配置決策程序。

## 存取模式

透過永久虛擬網路申請儲存時、其中一個必填欄位是存取模式。所需的模式可能會影響所選的後端、以裝載儲存要求。

Astra Trident會嘗試將所使用的儲存傳輸協定與根據下列對照表所指定的存取方法配對。這與基礎儲存平台無關。

	ReadWriteOnce	ReadOnlyMany	ReadWriteMany
iSCSI	是的	是的	是（原始區塊）
NFS	是的	是的	是的

如果要求將ReadWriteMany永久虛擬磁碟提交至Trident部署、但未設定NFS後端、則不會配置任何磁碟區。因此、申請者應使用適合其應用程式的存取模式。

## Volume作業

## 修改持續磁碟區

持續磁碟區除了兩個例外、都是Kubernetes中不可變的物件。建立後、即可修改回收原則和大小。不過、這並不妨礙在Kubernetes外部修改磁碟區的某些部分。這可能是理想的做法、以便針對特定應用程式自訂磁碟區、確保容量不會意外耗用、或是單純地將磁碟區移至不同的儲存控制器。



Kubernetes樹狀目錄內建資源配置程式目前不支援NFS或iSCSI PV的磁碟區大小調整作業。Astra Trident支援同時擴充NFS和iSCSI磁碟區。

PV的連線詳細資料無法在建立後修改。

## 建立隨需磁碟區快照

Astra Trident支援隨需磁碟區快照建立、並使用csi架構從快照建立PVCS。Snapshot提供便利的方法來維護資料的時間點複本、並使Kubernetes中的來源PV在生命週期上獨立不受影響。這些快照可用於複製PVCS。

## 從快照建立磁碟區

Astra Trident也支援從Volume快照建立PersistentVolumes。為達成此目的、只要建立一個PersistentVolume Claim並提及即可 `datasource` 所需的快照、以便建立磁碟區。Astra Trident會利用快照上的資料建立磁碟區、以處理此永久虛擬磁碟。有了這項功能、您可以跨區域複製資料、建立測試環境、完整取代毀損或毀損的正式作業磁碟區、或擷取特定檔案和目錄、然後將它們傳輸到其他附加磁碟區。

## 在叢集中移動磁碟區

儲存管理員能夠在ONTAP 整個叢集中的集合體和控制器之間、不中斷營運地將磁碟區移至儲存使用者。此作業不會影響Astra Trident或Kubernetes叢集、只要目的地Aggregate是Astra Trident所使用的SVM能夠存取的集合體。重要的是、如果新將Aggregate新增至SVM、則需要重新將其新增至Astra Trident來重新整理後端。這會觸發Astra Trident重新清查SVM、以便辨識新的Aggregate。

然而、Astra Trident並不支援跨後端移動磁碟區。這包括在同一個叢集內的SVM之間、叢集之間或不同的儲存平台（即使該儲存系統是連接至Astra Trident的儲存系統）。

如果將磁碟區複製到其他位置、則磁碟區匯入功能可用於將目前的磁碟區匯入Astra Trident。

## 展開Volume

Astra Trident支援調整NFS和iSCSI PV的大小。這可讓使用者透過Kubernetes層直接調整磁碟區大小。所有主要的NetApp儲存平台皆可進行Volume擴充、包括ONTAP：NetApp、SolidFire/NetApp HCI及Cloud Volumes Service 背後端點。若要允許稍後擴充、請設定 `allowVolumeExpansion` 至 `true` 在與磁碟區相關的StorageClass中。每當需要調整持續Volume的大小時、請編輯 `spec.resources.requests.storage` 持續Volume中的註釋會宣告為所需的Volume大小。Trident會自動調整儲存叢集上的磁碟區大小。

## 將現有磁碟區匯入Kubernetes

Volume匯入功能可將現有的儲存磁碟區匯入Kubernetes環境。目前支援此功能 `ontap-nas`、`ontap-nas-flexgroup`、`solidfire-san`、`azure-netapp-files` 和 `gcp-cvs` 驅動程式：當將現有應用程式移轉至Kubernetes或發生災難恢復時、此功能非常實用。

使用ONTAP the功能時 `solidfire-san` 驅動程式、請使用命令 `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` 將現有磁碟區匯入Kubernetes、由Astra Trident管理。匯入Volume命令中使用的PVC Yaml或Json檔案會指向儲存類別、以將Astra Trident識別為資源配置程式。使

用NetApp HCI / SolidFire後端時、請確定磁碟區名稱是唯一的。如果磁碟區名稱重複、請將磁碟區複製成唯一名稱、以便磁碟區匯入功能能夠區分它們。

如果是 azure-netapp-files 或 gcp-cvs 使用驅動程式時、請使用命令 `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` 將磁碟區匯入要由Astra Trident管理的Kubernetes。如此可確保唯一的Volume參考。

執行上述命令時、Astra Trident會在後端找到磁碟區並讀取其大小。它會自動新增（必要時覆寫）設定的PVc Volume大小。Astra Trident接著會建立新的PV、Kubernetes則會將PVc繫結至PV。

如果部署的容器需要特定匯入的PVc、則會保持擱置狀態、直到PVC/PV配對透過Volume匯入程序繫結為止。在PVC/PV配對繫結之後、如果沒有其他問題、則應啟動容器。

## 部署OpenShift服務

OpenShift加值叢集服務可為叢集管理員和託管的應用程式提供重要功能。這些服務所使用的儲存設備可以使用節點本機資源進行資源配置、但這通常會限制服務的容量、效能、可恢復性及永續性。運用企業儲存陣列來提供這些服務的容量、可大幅改善服務品質、不過OpenShift和儲存管理員應該密切合作、以決定每個服務的最佳選項。Red Hat文件應充分運用、以判斷需求、並確保符合規模調整與效能需求。

### 登錄服務

登錄的儲存設備部署與管理已記錄在中 ["NetApp.IO"](#) 在中 ["部落格"](#)。

### 記錄服務

如同其他OpenShift服務、記錄服務是使用Ansible搭配庫存檔案所提供的組態參數（即k.a.）來部署主機、提供給教戰手冊。其中包括兩種安裝方法：在初始OpenShift安裝期間部署記錄、以及在安裝OpenShift之後部署記錄。



從Red Hat OpenShift版本3.9起、官方文件建議您不要使用NFS來執行記錄服務、因為您擔心資料毀損。這是以Red Hat測試其產品為基礎。ONTAP的NFS伺服器沒有這些問題、可以輕鬆地回溯記錄部署。最後、記錄服務的通訊協定選擇取決於您、只要知道兩者在使用NetApp平台時都能順利運作、而且如果您偏好NFS、就沒有理由不使用NFS。

如果您選擇使用NFS搭配記錄服務、則必須設定Ansible變數

`openshift_enable_unsupported_configurations` 至 `true` 以避免安裝程式失敗。

### 開始使用

記錄服務可選擇性地同時部署給應用程式、以及OpenShift叢集本身的核心作業。如果您選擇部署作業記錄、請指定變數 `openshift_logging_use_ops` 做為 `true`、將會建立兩個服務執行個體。控制作業記錄執行個體的變數包含「ops」、而應用程式執行個體則不包含。

根據部署方法設定Ansible變數非常重要、因為這樣才能確保基礎服務使用正確的儲存設備。讓我們來看看每種部署方法的選項。



下表僅包含與記錄服務相關的儲存組態變數。您可以在中找到其他選項 ["RedHat OpenShift記錄文件"](#) 應根據您的部署情況來審查、設定及使用。

下表中的變數會使用提供的詳細資料、產生Ansible教戰手冊、為記錄服務建立PV和PVc。這種方法的彈性遠低於OpenShift安裝後使用元件安裝方針、不過如果您有現有的磁碟區可用、這是一個選項。

變動	詳細資料
<code>openshift_logging_storage_kind</code>	設定為 <code>nfs</code> 若要讓安裝程式為記錄服務建立NFS PV。
<code>openshift_logging_storage_host</code>	NFS主機的主機名稱或IP位址。這應該設定為虛擬機器的資料LIF。
<code>openshift_logging_storage_nfs_directory</code>	NFS匯出的掛載路徑。例如、如果該磁碟區的輔助狀態為 <code>/openshift_logging</code> 您可以將該路徑用於此變數。
<code>openshift_logging_storage_volume_name</code>	名稱、例如 <code>pv_ose_logs</code> 的。
<code>openshift_logging_storage_volume_size</code>	例如、NFS匯出的大小 100Gi。

如果您的OpenShift叢集已在執行中、因此已部署及設定Trident、則安裝程式可以使用動態資源配置來建立磁碟區。需要設定下列變數。

變動	詳細資料
<code>openshift_logging_es_pvc_dynamic</code>	設為 <code>true</code> 可使用動態資源配置的磁碟區。
<code>openshift_logging_es_pvc_storage_class_name</code>	將在PVC中使用的儲存類別名稱。
<code>openshift_logging_es_pvc_size</code>	在永久虛擬磁碟中要求的磁碟區大小。
<code>openshift_logging_es_pvc_prefix</code>	記錄服務使用的PVCS前置詞。
<code>openshift_logging_es_ops_pvc_dynamic</code>	設定為 <code>true</code> 使用動態資源配置的磁碟區來執行作業記錄執行個體。
<code>openshift_logging_es_ops_pvc_storage_class_name</code>	作業記錄執行個體的儲存類別名稱。
<code>openshift_logging_es_ops_pvc_size</code>	作業執行個體的Volume要求大小。
<code>openshift_logging_es_ops_pvc_prefix</code>	ops執行個體PVCS的前置詞。

## 部署記錄堆疊

如果您將記錄部署為初始OpenShift安裝程序的一部分、則只需遵循標準部署程序即可。Ansible會設定及部署所需的服務和OpenShift物件、以便在可執行的完成後立即提供服務。

不過、如果您在初始安裝之後進行部署、Ansible將需要使用元件方針。不同版本的OpenShift可能會稍微改變此程序、因此請務必閱讀並遵循 ["RedHat OpenShift Container Platform 3.11文件"](#) 適用於您的版本。

## 度量服務

度量服務可針對OpenShift叢集的狀態、資源使用率及可用度、提供寶貴的資訊給系統管理員。此外、也需要Pod自動擴充功能、許多組織會使用指標服務的資料來支付費用和/或顯示應用程式。

如同記錄服務和OpenShift整體、Ansible可用於部署度量服務。此外、如同記錄服務、度量服務也可在叢集初始設定期間或使用元件安裝方法運作之後進行部署。下表包含在設定度量服務的持續儲存時、重要的變數。



下表僅包含與度量服務相關的儲存組態相關變數。文件中還有許多其他選項、您應該根據部署情況來檢閱、設定及使用。



變動	詳細資料
<code>openshift_metrics_storage_kind</code>	設定為 <code>nfs</code> 若要讓安裝程式為記錄服務建立NFS PV。
<code>openshift_metrics_storage_host</code>	NFS主機的主機名稱或IP位址。這應該設定為SVM的資料LIF。
<code>openshift_metrics_storage_nfs_directory</code>	NFS匯出的掛載路徑。例如、如果該磁碟區的輔助狀態為 <code>/openshift_metrics</code> 您可以將該路徑用於此變數。
<code>openshift_metrics_storage_volume_name</code>	名稱、例如 <code>pv_ose_metrics</code> 的。
<code>openshift_metrics_storage_volume_size</code>	例如、NFS匯出的大小 100Gi。

如果您的OpenShift叢集已在執行中、因此已部署及設定Trident、則安裝程式可以使用動態資源配置來建立磁碟區。需要設定下列變數。

變動	詳細資料
<code>openshift_metrics_cassandra_pvc_prefix</code>	用於度量PVCS的前置詞。
<code>openshift_metrics_cassandra_pvc_size</code>	要要求的磁碟區大小。
<code>openshift_metrics_cassandra_storage_type</code>	用於度量的儲存類型、必須設定為動態、Ansible才能建立具有適當儲存類別的PVCS。
<code>openshift_metrics_cassandra_pvc_storage_class_name</code>	要使用的儲存類別名稱。

## 部署度量服務

在您的主機/庫存檔案中定義適當的可Ansible變數後、使用Ansible部署服務。如果您是在OpenShift安裝時間進行部署、則會自動建立及使用PV。如果您使用元件教戰手冊進行部署、則在OpenShift安裝之後、Ansible會建立任何需要的PVCS、並在Astra Trident為其配置儲存設備之後、部署該服務。

上述變數及部署程序可能會隨OpenShift的每個版本而變更。請務必檢閱並遵循 ["RedHat的OpenShift部署指南"](#) 以供您的環境使用。

## 資料保護

瞭解NetApp儲存平台提供的資料保護與恢復選項。Astra Trident可配置磁碟區、以充分利用其中的部分功能。對於每個應用程式、您都應該有持續性需求的資料保護與還原策略。

### 備份 etcd 叢集資料

Astra Trident將其中繼資料儲存在Kubernetes叢集中 etcd 資料庫。定期備份 etcd 叢集資料對於在災難案例中還原Kubernetes叢集非常重要。

#### 步驟

1. `etcdctl snapshot save` 命令可讓您擷取的時間點快照 etcd 叢集：

```
sudo docker run --rm -v /backup:/backup \
  --network host \
  -v /etc/kubernetes/pki/etcd:/etc/kubernetes/pki/etcd \
  --env ETCDCTL_API=3 \
  registry.k8s.io/etcd-amd64:3.2.18 \
  etcdctl --endpoints=https://127.0.0.1:2379 \
  --cacert=/etc/kubernetes/pki/etcd/ca.crt \
  --cert=/etc/kubernetes/pki/etcd/healthcheck-client.crt \
  --key=/etc/kubernetes/pki/etcd/healthcheck-client.key \
  snapshot save /backup/etcd-snapshot.db
```

此命令可藉由旋轉etcd容器來建立etcd快照、並將其儲存在中 /backup 目錄。

- 發生災難時、您可以使用etcd快照來啟動Kubernetes叢集。使用 `etcdctl snapshot restore` 命令來還原所擷取的特定快照 /var/lib/etcd 資料夾。還原之後、請確認是否有 /var/lib/etcd 資料夾已填入 member 資料夾。以下是的範例 `etcdctl snapshot restore` 命令：

```
etcdctl snapshot restore '/backup/etcd-snapshot-latest.db' ; mv
/default.etcd/member/ /var/lib/etcd/
```

- 初始化Kubernetes叢集之前、請複製所有必要的憑證。
- 使用建立叢集 `--ignore-preflight-errors=DirAvailable-var-lib-etcd` 旗標。
- 叢集啟動後、請確定已啟動kube系統Pod。
- 使用 `kubectl get crd` 命令來驗證Trident所建立的自訂資源是否存在、並擷取Trident物件、以確保所有資料都可用。

## 使用ONTAP 不含資訊的快照來恢復日期

快照提供應用程式資料的時間點還原選項、因此扮演著重要角色。不過、快照本身並不是備份、因此無法防止儲存系統故障或其他災難。但是、在大多數情況下、它們都是一種方便、快速且簡單的資料恢復方法。瞭ONTAP 解如何使用「支援資料快照」技術來備份磁碟區、以及如何還原。

- 如果未在後端定義快照原則、則會預設使用 `none` 原則。如此一ONTAP 來、我們便無法自動擷取快照。不過、儲存管理員可以手動擷取快照、或是透過ONTAP 功能完善的管理介面變更快照原則。這不會影響Trident作業。
- Snapshot目錄預設為隱藏。這有助於最大程度地相容於使用配置的磁碟區 `ontap-nas` 和 `ontap-nas-economy` 驅動程式：啟用 `.snapshot` 使用時的目錄 `ontap-nas` 和 `ontap-nas-economy` 可讓應用程式直接從快照恢復資料的驅動程式。
- 使用將磁碟區還原至先前快照中記錄的狀態 `volume snapshot restore` CLI命令。ONTAP還原快照複本時、還原作業會覆寫現有的Volume組態。建立Snapshot複本之後、對磁碟區中資料所做的任何變更都會遺失。

```
cluster1::*> volume snapshot restore -vserver vs0 -volume vol3 -snapshot  
vol3_snap_archive
```

## 使用ONTAP 功能複寫資料

複寫資料對於防止儲存陣列故障所造成的資料遺失、扮演著重要的角色。



如需ONTAP 深入瞭解有關資訊複寫技術的資訊、請參閱 ["本文檔 ONTAP"](#)。

### SnapMirror儲存虛擬機器 (SVM) 複寫

您可以使用 **"SnapMirror"** 複寫完整的SVM、其中包括其組態設定及其磁碟區。發生災難時、您可以啟動SnapMirror目的地SVM、開始提供資料服務。還原系統時、您可以切換回主要系統。

Astra Trident無法自行設定複寫關係、因此儲存管理員可以使用ONTAP的SnapMirror SVM複寫功能、將磁碟區自動複寫到災難恢復 (DR) 目的地。

如果您打算使用SnapMirror SVM複寫功能、或是目前正在使用此功能、請考慮下列事項：

- 您應該為每個啟用SVM災難恢復的SVM建立不同的後端。
- 您應該設定儲存類別、以便在需要時、不要選取複寫的後端。這一點非常重要、因為如此一來、您就不必將不需要保護複寫關係的磁碟區配置到支援SVM-DR的後端。
- 應用程式管理員應瞭解複寫資料所需的額外成本與複雜度、並在使用資料複寫之前、先決定恢復計畫。
- 啟動SnapMirror目的地SVM之前、請先停止所有排程的SnapMirror傳輸、中止所有進行中的SnapMirror傳輸、中斷複寫關係、停止來源SVM、然後啟動SnapMirror目的地SVM。
- Astra Trident不會自動偵測SVM故障。因此、當系統管理員發生故障時、應執行 `tridentctl backend update` 觸發Trident容錯移轉至新後端的命令。

以下是SVM設定步驟的總覽：

- 在來源與目的地叢集與SVM之間設定對等關係。
- 使用建立目的地SVM `-subtype dp-destination` 選項。
- 建立複寫工作排程、以確保複寫會在所需的時間間隔執行。
- 使用建立SnapMirror複寫、從目的地SVM複寫到來源SVM `-identity-preserve true` 可確保來源SVM組態和來源SVM介面複製到目的地的選項。從目的地SVM初始化SnapMirror SVM複寫關係。





#### Trident的災難恢復工作流程

Astra Trident 19.07及更新版本使用Kubernetes CRD來儲存及管理自己的狀態。它使用Kubernetes叢集 etcd 以儲存其中繼資料。我們在此假設Kubernetes etcd 資料檔案和憑證會儲存在NetApp FlexVolume上。此FlexVolume位於SVM中、與次要站台的目的地SVM有SnapMirror SVM-DR關係。

下列步驟說明如何在發生災難時、使用Astra Trident來還原單一主Kubernetes叢集：

1. 如果來源SVM故障、請啟動SnapMirror目的地SVM。為達成此目的、您應該停止排程的SnapMirror傳輸、中止進行中的SnapMirror傳輸、中斷複寫關係、停止來源SVM、以及啟動目的地SVM。
2. 從目的地SVM掛載包含Kubernetes的磁碟區 etcd 將設定為主節點的主機上的資料檔案和憑證。
3. 複製下Kubernetes叢集所需的所有憑證 /etc/kubernetes/pki 和etcd member 下的檔案 /var/lib/etcd。
4. 使用建立Kubernetes叢集 `kubeadm init` 命令 `--ignore-preflight-errors=DirAvailable--var-lib-etcd` 旗標。Kubernetes節點使用的主機名稱應與來源Kubernetes叢集相同。
5. 執行 `kubectl get crd` 命令來驗證所有Trident自訂資源是否都已啟動並擷取Trident物件、以驗證所有資料是否可用。
6. 執行以更新所有必要的後端、以反映新的目的地SVM名稱 `./tridentctl update backend <backend-name> -f <backend-json-file> -n <namespace>` 命令。



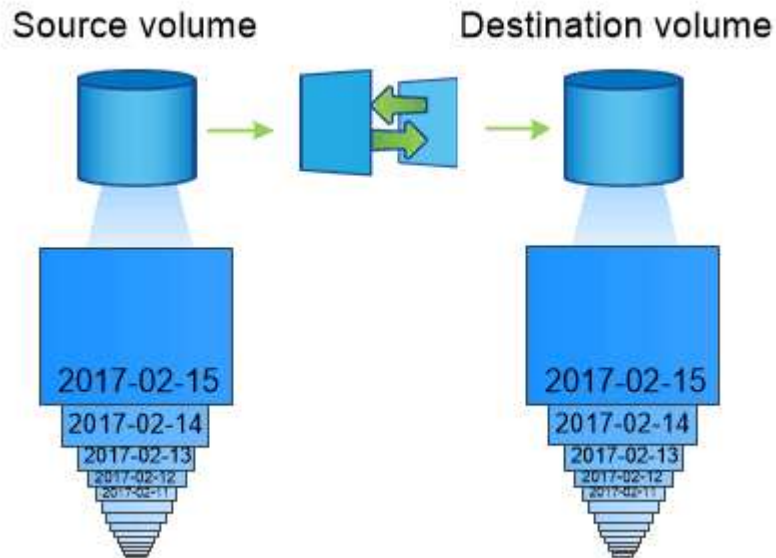
對於應用程式持續磁碟區、當目的地SVM啟動時、Trident所配置的所有磁碟區都會開始提供資料。使用上述步驟在目的地端設定Kubernetes叢集之後、所有的部署和Pod都會啟動、而且容器化應用程式應該能順利執行、不會發生任何問題。

#### SnapMirror Volume複寫

SnapMirror Volume複寫是一項災難恢復功能、可從Volume層級的主要儲存設備進行容錯移轉至目的地儲存設備。ONTAPSnapMirror透過同步快照、在次要儲存設備上建立主要儲存設備的Volume複本或鏡射。

以下是ONTAP 關於SnapMirror Volume複寫設定步驟的總覽：

- 在磁碟區所在的叢集與從磁碟區提供資料的SVM之間設定對等關係。
- 建立SnapMirror原則、以控制關係的行為、並指定該關係的組態屬性。
- 使用建立目的地Volume與來源Volume之間的SnapMirror關係[`snapmirror create` 命令]並指派適當的SnapMirror原則。
- 建立SnapMirror關係之後、請初始化關係、以便完成從來源磁碟區到目的地磁碟區的基礎傳輸。



適用於Trident的SnapMirror Volume災難恢復工作流程

下列步驟說明如何使用Astra Trident來復原單一主Kubernetes叢集。

1. 發生災難時、請停止所有排程的SnapMirror傳輸、並中止所有進行中的SnapMirror傳輸。中斷目的地與來源磁碟區之間的複寫關係、使目的地磁碟區變成讀取/寫入。
2. 從目的地SVM掛載包含Kubernetes的磁碟區 `etcd` 主機上的資料檔案和憑證、將設定為主節點。
3. 複製下Kubernetes叢集所需的所有憑證 `/etc/kubernetes/pki` 和 `etcd member` 下的檔案 `/var/lib/etcd`。
4. 執行以建立Kubernetes叢集 `kubeadm init` 命令 `--ignore-preflight-errors=DirAvailable-  
var-lib-etcd` 旗標。主機名稱應與來源Kubernetes叢集相同。
5. 執行 `kubectl get crd` 命令來驗證是否所有Trident自訂資源都已啟動並擷取Trident物件、以確保所有資料都可用。
6. 清理先前的後端、並在Trident上建立新的後端。指定目的地SVM的新管理LIF、新SVM名稱和密碼。

應用程式持續磁碟區的災難恢復工作流程

下列步驟說明在發生災難時、如何為容器化工作負載提供SnapMirror目的地磁碟區：

1. 停止所有排程的SnapMirror傳輸、並中止所有進行中的SnapMirror傳輸。中斷目的地與來源磁碟區之間的複寫關係、使目的地磁碟區變成讀取/寫入。清除使用與來源SVM上磁碟區連結之PVC的部署。

2. 使用上述步驟在目的地端設定Kubernetes叢集之後、請從Kubernetes叢集清除部署、PVCS和PV。
3. 指定新的管理與資料LIF、新的SVM名稱和目的地SVM密碼、在Trident上建立新的後端。
4. 使用「Trident匯入」功能、將所需的磁碟區匯入為與新的PVc繫結的PV。
5. 使用新建立的PVCS重新部署應用程式部署。

## 使用元素快照來恢復資料

設定磁碟區的快照排程、並確保每隔一段時間擷取快照、以備份元素磁碟區上的資料。您應該使用元素UI或API來設定快照排程。目前無法透過設定快照排程至磁碟區 `solidfire-san` 驅動程式：

在資料毀損的情況下、您可以使用元素UI或API、選擇特定的快照、然後手動將磁碟區復原至快照。這會還原自建立快照以來對磁碟區所做的任何變更。

## 安全性

### 安全性

請使用此處列出的建議、確保您的Astra Trident安裝安全無虞。

在自己的命名空間中執行**Astra Trident**

防止應用程式、應用程式管理員、使用者及管理應用程式存取Astra Trident物件定義或Pod、以確保可靠的儲存並封鎖潛在的惡意活動、這一點非常重要。

若要將其他應用程式和使用者與Astra Trident區隔開、請務必在自己的Kubernetes命名空間中安裝Astra Trident (`trident`)。將Astra Trident放在自己的命名空間中、可確保只有Kubernetes管理人員能夠存取Astra Trident Pod、以及儲存在命名式CRD物件中的成品（例如後端和CHAP機密）。您應確保只允許系統管理員存取Astra Trident命名空間、進而存取 `tridentctl` 應用程式：

使用**CHAP**驗證搭配**ONTAP** 使用支援**SAN**的功能

Astra Trident支援ONTAP 以CHAP為基礎的驗證功能、適用於各種不實的SAN工作負載（使用 `ontap-san` 和 `ontap-san-economy` 驅動程式）。NetApp建議使用雙向CHAP搭配Astra Trident進行主機與儲存後端之間的驗證。

針對使用SAN儲存驅動程式的幕後作業、Astra Trident可設定雙向CHAP、並透過管理CHAP使用者名稱和機密ONTAP `tridentctl`。請參閱 ["請按這裡"](#) 瞭解Astra Trident如何在ONTAP 不景點上設定CHAP。



Trident 20.04及更新版本提供對支援不支援的CHAP ONTAP。

使用**CHAP**驗證**NetApp HCI** 搭配不景和**SolidFire** 不景的後端

NetApp建議部署雙向CHAP、以確保主機與NetApp HCI 支援功能及SolidFire 支援功能之間的驗證。Astra Trident使用每個租戶包含兩個CHAP密碼的秘密物件。當Trident安裝為「倡議」資源配置程式時、它會管理CHAP機密並將其儲存在中 `tridentvolume` 對應PV的CR物件。建立PV時、「csi Astra Trident」會使用CHAP機密來啟動iSCSI工作階段、NetApp HCI 並透過CHAP與該系統進行通訊SolidFire。



由csi Trident建立的磁碟區不會與任何Volume存取群組相關聯。

在非csi前端中、磁碟區作為工作節點上的裝置附加作業是由Kubernetes處理。建立磁碟區之後、Astra Trident會呼叫NetApp HCI / SolidFire系統、以便在該租戶的機密資訊尚未存在時擷取機密資訊。然後、Astra Trident將機密傳給Kubernetes。位於每個節點上的Kubelet可透過Kubernetes API存取機密資料、並使用它們在存取磁碟區的每個節點與磁碟區所在的NetApp HCI / SolidFire系統之間執行/啟用CHAP。

### 使用Astra Trident搭配NVE和NAE

NetApp ONTAP 支援閒置資料加密、可在磁碟遭竊、退回或重新使用時、保護敏感資料。如需詳細資訊、請參閱 ["設定NetApp Volume Encryption總覽"](#)。

- 如果在後端啟用NAE、則Astra Trident中配置的任何磁碟區都將啟用NAE。
- 如果後端未啟用NAE、則在Astra Trident中配置的任何Volume都會啟用NVE、除非您將NVE加密旗標設為 `false` 在後端組態中。

在啟用NAE的後端Astra Trident中建立的磁碟區、必須加密NVE或NAE。



- 您可以將NVE加密旗標設為 `true` 在Trident後端組態中、覆寫NAE加密、並以每個磁碟區為基礎使用特定的加密金鑰。
- 將NVE加密旗標設定為 `false` 在啟用NAE的後端上、將會建立啟用NAE的Volume。您無法將NVE加密旗標設為、以停用NAE加密 `false`。

- 您可以在Astra Trident中手動建立NVE磁碟區、方法是將NVE加密旗標明確設定為 `true`。

如需後端組態選項的詳細資訊、請參閱：

- ["支援SAN組態選項ONTAP"](#)
- ["ASNAS組態選項ONTAP"](#)

### Linux統一化金鑰設定 (LUKS)

您可以在ONTAP Astra Trident上啟用Linux Unified Key Setup (LUKS) 來加密支援的SAN和ONTAP 支援的SAN經濟版磁碟區。Astra Trident支援使用密碼的輪替和磁碟區擴充、適用於使用LUKS加密的磁碟區。

在Astra Trident中、LUKS加密的磁碟區會依照所建議的方式使用AES-XTS-plain64 cypher和模式 **"NIST"**。

開始之前

- 工作者節點必須安裝密碼設定2.1或更高版本（但低於3.0）。如需詳細資訊、請造訪 ["Gitlab：密碼設定"](#)。
- 基於效能考量、我們建議工作節點支援進階加密標準新增指令（AES-NI）。若要驗證AES-NI支援、請執行下列命令：

```
grep "aes" /proc/cpuinfo
```

如果沒有歸還任何內容、您的處理器就不支援AES-NI。如需AES-NI的詳細資訊、請造訪：["Intel：進階加密"](#)

標準指令 (AES-NI) "。

## 啟用LUKS加密

您可以使用Linux Unified Key Setup (LUKS) 來啟用每個Volume、主機端的加密功能、以利ONTAP 執行SAN 和ONTAP 支援SAN經濟效益的磁碟區。

### 步驟

1. 在後端組態中定義LUKS加密屬性。如需ONTAP 有關支援不支援SAN的後端組態選項的詳細資訊、請參閱 "[支援SAN組態選項ONTAP](#)"。

```
"storage": [  
  {  
    "labels":{"luks": "true"},  
    "zone":"us_east_1a",  
    "defaults": {  
      "luksEncryption": "true"  
    }  
  },  
  {  
    "labels":{"luks": "false"},  
    "zone":"us_east_1a",  
    "defaults": {  
      "luksEncryption": "false"  
    }  
  },  
]
```

2. 使用 `parameters.selector` 使用LUKS加密定義儲存資源池。例如：

```
apiVersion: storage.k8s.io/v1  
kind: StorageClass  
metadata:  
  name: luks  
provisioner: netapp.io/trident  
parameters:  
  selector: "luks=true"  
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}  
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

3. 建立包含LUKS通關密碼的秘密。例如：

```
kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA
```

## 限制

LUKS加密磁碟區無法利用ONTAP 重複資料刪除技術與壓縮技術。

## 旋轉LUKS複雜密碼

您可以旋轉LUKS複雜密碼並確認輪調。



請勿忘記密碼、除非您已驗證它不再被任何磁碟區、快照或機密所引用。如果參考的通關密碼遺失、您可能無法掛載磁碟區、而且資料將保持加密且無法存取。

## 關於這項工作

如果在指定新的LUKS通關密碼之後建立裝載磁碟區的Pod、則會發生LUKS通關密碼循環。建立新的Pod時、Astra Trident會比較磁碟區上的LUKS通關密碼與機密中的作用中通關密碼。

- 如果磁碟區上的通關密碼與機密中的作用中通關密碼不相符、就會發生輪調。
- 如果磁碟區上的通關密碼與機密中的作用中通關密碼相符 `previous-luks-passphrase` 參數被忽略。

## 步驟

1. 新增 `node-publish-secret-name` 和 `node-publish-secret-namespace` `StorageClass`參數。例如：

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}
```

2. 識別磁碟區或快照上的現有密碼。

## Volume

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["A"]
```

## Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["A"]
```

3. 更新磁碟區的LUKS機密、以指定新的和先前的密碼。確保 `previous-luke-passphrase-name` 和 `previous-luks-passphrase` 請與先前的通關密碼相符。

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. 建立新的Pod以掛載Volume。這是啟動旋轉所需的。
5. 確認複雜密碼已旋轉。

## Volume

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["B"]
```

## Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["B"]
```



## 結果

只有在磁碟區和快照上傳回新的通關密碼時、才會旋轉通關密碼。



例如、如果傳回兩個複雜密碼 `luksPassphraseNames: ["B", "A"]`、旋轉不完整。您可以觸發新的Pod以嘗試完成旋轉。

## 啟用Volume擴充

您可以在LUKS加密的Volume上啟用Volume擴充。

### 步驟

1. 啟用 `CSINodeExpandSecret` 功能閘道 (beta 1.25 +)。請參閱 ["Kubernetes 1.25：使用Secrets進行節點導向的SCSI Volume擴充"](#) 以取得詳細資料。
2. 新增 `node-expand-secret-name` 和 `node-expand-secret-namespace` `StorageClass` 參數。例如：

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: netapp.io/trident
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

## 結果

當您啟動線上儲存擴充時、kubelet會將適當的認證資料傳遞給驅動程式。



# 參考資料

## Astra Trident連接埠

深入瞭解Astra Trident用於通訊的連接埠。

### Astra Trident連接埠

Astra Trident透過下列連接埠進行通訊：

連接埠	目的
8443.	後端通道HTTPS
8001	Prometheus指標端點
8000	Trident REST伺服器
17546	Trident取消安裝套件所使用的活動/整備度探針連接埠



您可以在安裝期間使用變更活動力/整備度探針連接埠 `--probe-port` 旗標。請務必確認工作節點上的其他程序並未使用此連接埠。

## Astra Trident REST API

而 "[tridentctl命令和選項](#)" 這是與Astra Trident REST API互動最簡單的方法、您可以視需要直接使用REST端點。

### 何時使用REST API

REST API適用於在非Kubernetes部署中使用Astra Trident做為獨立二進位元的進階安裝。

為了提升安全性、Astra Trident REST API 在Pod內部執行時、預設限制為localhost。若要變更此行為、您必須設定Astra Trident的 `-address` 其Pod組態中的引數。

### 使用REST API

API的運作方式如下：

GET

- `GET <trident-address>/trident/v1/<object-type>`：列出該類型的所有對象。
- `GET <trident-address>/trident/v1/<object-type>/<object-name>`：獲取命名對象的詳細信息。

POST

`POST <trident-address>/trident/v1/<object-type>`：創建指定類型的對象。

- 需要Json組態才能建立物件。如需每種物件類型的規格、請參閱連結：[tridentctl.html](#)[tridentctl 命令與選項]。
- 如果物件已經存在、行為會有所不同：後端會更新現有物件、而其他所有物件類型都會使作業失敗。

DELETE

DELETE <trident-address>/trident/v1/<object-type>/<object-name>：刪除命名資源。



與後端或儲存類別相關聯的磁碟區將繼續存在、必須分別刪除。如需詳細資訊、請參閱連結：[tridentctl.html](#)[tridentctl 命令與選項]。

如需如何呼叫這些API的範例、請通過偵錯 (-d) 旗標。如需詳細資訊、請參閱連結：[tridentctl.html](#)[tridentctl 命令與選項]。

## 命令列選項

Astra Trident提供Trident Orchestrator的數個命令列選項。您可以使用這些選項來修改部署。

### 記錄

- -debug：啟用偵錯輸出。
- -loglevel <level>：設定記錄層級（偵錯、資訊、警告、錯誤、嚴重）。預設為資訊。

### Kubernetes

- -k8s\_pod：使用此選項或 -k8s\_api\_server 以啟用Kubernetes支援。設定此選項會使Trident使用內含Pod的Kubernetes服務帳戶認證、來聯絡API伺服器。這只有當Trident在Kubernetes叢集中以Pod形式執行、且已啟用服務帳戶時才會運作。
- -k8s\_api\_server <insecure-address:insecure-port>：使用此選項或 -k8s\_pod 以啟用Kubernetes支援。如果指定、Trident會使用提供的不安全位址和連接埠、連線至Kubernetes API伺服器。這可讓Trident部署在Pod外部、但它只支援不安全的API伺服器連線。若要安全地連線、請將Trident部署在Pod中 -k8s\_pod 選項。
- -k8s\_config\_path <file>：必要；您必須指定KubeConfig檔案的路徑。

### Docker

- -volume\_driver <name>：註冊Docker外掛程式時使用的驅動程式名稱。預設為 netapp。
- -driver\_port <port-number>：偵聽此連接埠而非UNIX網域通訊端。
- -config <file>：必要；您必須指定後端組態檔的路徑。

### 休息

- -address <ip-or-host>：指定Trident的REST伺服器應接聽的位址。預設為localhost。當偵聽localhost並在Kubernetes Pod內部執行時、無法從Pod外部直接存取REST介面。使用 -address "" 可讓REST介面從Pod IP位址存取。



Trident REST介面可設定為偵聽、僅適用於127.0.0.1（適用於IPV4）或[:1]（適用於IPv6）。

- `-port <port-number>`：指定Trident的REST伺服器應偵聽的連接埠。預設為8000。
- `-rest`：啟用REST介面。預設為true。

## 與Kubernetes整合的NetApp產品

NetApp儲存產品組合可與Kubernetes叢集的許多不同層面整合、提供進階資料管理功能、強化Kubernetes部署的功能、功能、效能及可用度。

### Astra

"Astra" 讓企業更輕鬆地管理、保護及搬移在公有雲內部及內部部署的Kubernetes上執行的資料豐富的容器化工作負載。Astra採用NetApp在公有雲和內部部署環境中備受肯定且廣泛的儲存產品組合Trident、提供持續的容器儲存設備。此外、它還提供一組豐富的進階應用程式感知資料管理功能、例如Snapshot、備份與還原、活動記錄、以及資料保護、災難/資料恢復、資料稽核、以及Kubernetes工作負載的移轉使用案例的主動複製。

### ONTAP

NetApp的多重傳輸協定、統一化儲存作業系統可為任何應用程式提供進階資料管理功能。ONTAP支援所有Flash、混合式或全硬碟組態的系統、可提供多種不同的部署模式、包括工程設計硬體（英文版）、白箱（英文版）和僅雲端（英文版）ONTAP FAS AFF ONTAP Select Cloud Volumes ONTAP。



Trident支援上述ONTAP 所有的功能齊全的部署模式。

### Cloud Volumes ONTAP

"Cloud Volumes ONTAP" 是一款純軟體的儲存應用裝置、可在ONTAP 雲端上執行功能完善的資料管理軟體。您可以使用Cloud Volumes ONTAP 支援功能來執行正式作業工作負載、災難恢復、DevOps、檔案共享和資料庫管理。它提供儲存效率、高可用度、資料複製、資料分層和應用程式一致性、將企業儲存設備延伸至雲端。

### Amazon FSX for NetApp ONTAP 產品

"Amazon FSX for NetApp ONTAP 產品" 是一項完整管理的AWS服務、可讓客戶啟動及執行採用NetApp ONTAP的一套資訊儲存作業系統的檔案系統。FSX for ONTAP VMware可讓客戶運用熟悉的NetApp功能、效能和管理功能、同時充分發揮儲存AWS資料的簡易性、敏捷度、安全性和擴充性。FSX ONTAP for FSfor支援ONTAP的許多檔案系統功能和管理API。

### Element軟體

"元素" 儲存管理員可藉由保證效能、並簡化及簡化儲存設備佔用空間、來整合工作負載。搭配API來實現儲存管理所有層面的自動化、Element可讓儲存管理員以更少的心力完成更多工作。

### NetApp HCI

"NetApp HCI" 將例行工作自動化、讓基礎架構管理員能夠專注於更重要的功能、進而簡化資料中心的管理與規模。

Trident完全支援此功能。NetApp HCI Trident可直接針對底層NetApp HCI 的資訊儲存平台、為容器化應用程式配置及管理儲存設備。

## Azure NetApp Files

"[Azure NetApp Files](#)" 是採用NetApp技術的企業級Azure檔案共享服務。您可以在Azure原生環境中執行最嚴苛的檔案型工作負載、並享有NetApp所提供的效能與豐富資料管理功能。

## 適用於 Google Cloud Cloud Volumes Service

"[適用於Cloud Volumes Service Google Cloud的NetApp解決方案](#)" 是雲端原生檔案服務、可透過NFS和SMB提供NAS磁碟區的All Flash效能。此服務可讓任何工作負載（包括舊版應用程式）在GCP雲端上執行。它提供完整的託管服務、提供一致的高效能、即時複製、資料保護、以及安全存取Google Compute Engine（GCE）執行個體。

## Kubernetes和Trident物件

您可以透過讀取和寫入資源物件、使用REST API與Kubernetes和Trident互動。Kubernetes與Trident、Trident與Storage、Kubernetes與儲存設備之間有幾個資源物件、分別是它們之間的關係。其中有些物件是透過Kubernetes進行管理、其他物件則是透過Trident進行管理。

### 物件如何彼此互動？

瞭解物件、物件的適用範圍及其互動方式、最簡單的方法可能是遵循Kubernetes使用者的單一儲存要求：

1. 使用者會建立 `PersistentVolumeClaim` 正在申請新的 `PersistentVolume` Kubernetes的特定尺寸 `StorageClass` 這是先前由系統管理員設定的。
2. Kubernetes `StorageClass` 將Trident識別為其資源配置程式、並包含可告知Trident如何為所要求的類別資源配置Volume的參數。
3. Trident會自行決定 `StorageClass` 使用識別相符項目的相同名稱 `Backends` 和 `StoragePools` 可用來為類別配置磁碟區。
4. Trident會在相符的後端上配置儲存設備、並建立兩個物件：a `PersistentVolume` Kubernetes告訴Kubernetes如何尋找、掛載及處理Volume、以及Trident中保留兩者關係的Volume `PersistentVolume` 以及實際儲存設備。
5. Kubernetes會連結 `PersistentVolumeClaim` 新的 `PersistentVolume`。包含的Pod `PersistentVolumeClaim` 將該`PersistentVolume`掛載到其執行的任何主機上。
6. 使用者會建立 `VolumeSnapshot` 現有的PVC,使用 `VolumeSnapshotClass` 這是Trident的重點。
7. Trident會識別與該PVC相關聯的磁碟區、並在其後端建立磁碟區快照。也會建立 `VolumeSnapshotContent` 這會指示Kubernetes如何識別快照。
8. 使用者可以建立 `PersistentVolumeClaim` 使用 `VolumeSnapshot` 來源：
9. Trident會識別所需的快照、並執行建立所需的相同步驟集 `PersistentVolume` 和答 `Volume`。



如需進一步瞭解Kubernetes物件、我們強烈建議您閱讀 "[持續磁碟區](#)" Kubernetes文件的一節。

## Kubernetes PersistentVolumeClaim 物件

Kubernetes PersistentVolumeClaim 物件是Kubernetes叢集使用者所提出的儲存要求。

除了標準規格之外、Trident還可讓使用者指定下列Volume專屬附註、以覆寫您在後端組態中設定的預設值：

註釋	Volume選項	支援的驅動程式
trident.netapp.io/fileSystem	檔案系統	ONTAP-SAN、solidfire-san 、ONTAP-san經濟型
trident.netapp.io/cloneFromPVC	cloneSourceVolume	ONTAP-NAS、ONTAP-SAN 、solidfire-san、azure-NetApp- Files、GCP-CVS、ONTAP-san經 濟型
trident.netapp.io/splitOnClone	分岔OnClone	ONTAP-NAS、ONTAP-SAN
trident.netapp.io/protocol	傳輸協定	任何
trident.netapp.io/exportPolicy	匯出原則	ONTAP-NAS、ONTAP-NAS-經濟 型、ONTAP-NAS- Flexgroup
trident.netapp.io/snapshotPolicy	Snapshot原則	ONTAP-NAS、ONTAP-NAS-經濟 型、ONTAP-NAS-flexgroup 、ONTAP-SAN
trident.netapp.io/snapshotReserve	Snapshot保留區	ONTAP-NAS、ONTAP-NAs- flexgroup、ONTAP-SAN、GCP- CVS
trident.netapp.io/snapshotDirectory	Snapshot目錄	ONTAP-NAS、ONTAP-NAS-經濟 型、ONTAP-NAS- Flexgroup
trident.netapp.io/unixPermissions	unix權限	ONTAP-NAS、ONTAP-NAS-經濟 型、ONTAP-NAS- Flexgroup
trident.netapp.io/blockSize	區塊大小	solidfire-san

如果建立的PV具有 Delete 回收原則：Trident會在PV發行時（亦即使用者刪除PVC時）同時刪除PV和備用Volume。如果刪除動作失敗、Trident會將PV標示為這樣、並定期重試該作業、直到成功或手動刪除PV為止。如果PV使用 Retain 原則、Trident會忽略它、並假設系統管理員會從Kubernetes和後端進行清理、以便在移除磁碟區之前、先備份或檢查該磁碟區。請注意、刪除PV並不會導致Trident刪除背板Volume。您應該使用REST API將其移除 (tridentctl)。

Trident支援使用csi規格建立Volume Snapshot：您可以建立Volume Snapshot、並將其作為資料來源來複製現有的PVCS。如此一來、PV的時間點複本就能以快照形式呈現給Kubernetes。快照可用來建立新的PV。請看一下 On-Demand Volume Snapshots 以瞭解這項功能的運作方式。

Trident也提供 cloneFromPVC 和 splitOnClone 建立複本的附註。您可以使用這些附註來複製一個PVC,而不需要使用csi實作（在Kubernetes 1.13及更早版本上）或Kubernetes版本不支援beta Volume Snapshot（Kubernetes 1.16及更早版本）。請記住、Trident 19.10支援從PVC複製的csi工作流程。



您可以使用 cloneFromPVC 和 splitOnClone 附有「csi Trident」和傳統非csi前端的註釋。

以下是一個範例：如果使用者已經有一個名為的PVC mysql、使用者可以建立名為的新永久虛擬環境

mysqlclone 使用註釋、例如 `trident.netapp.io/cloneFromPVC: mysql`。使用此註釋集、Trident 會複製對應於 MySQL PVC 的磁碟區、而非從頭開始配置磁碟區。

請考量以下幾點：

- 我們建議您複製閒置的 Volume。
  - 一個 PVC 及其複本應位於相同的 Kubernetes 命名空間中、且具有相同的儲存類別。
  - 使用 `ontap-nas` 和 `ontap-san` 驅動程式、可能需要設定 PVC 註釋 `trident.netapp.io/splitOnClone` 與搭配使用 `trident.netapp.io/cloneFromPVC`。與 `trident.netapp.io/splitOnClone` 設定為 `true`、Trident 將複製的磁碟區從父磁碟區分割出來、因此將複製的磁碟區生命週期與父磁碟區完全分離、而犧牲部分儲存效率。未設定 `trident.netapp.io/splitOnClone` 或設定為 `false` 減少後端的空間使用量、而犧牲父磁碟區與複製磁碟區之間的相依性、因此除非先刪除複本、否則無法刪除父磁碟區。分割實體複製是合理的做法、是將空的資料庫磁碟區複製到磁碟區及其實體複製環境、以大幅分散差異、而非 ONTAP 受益於由 NetApp 提供的儲存效率。
- `sample-input` 目錄包含用於 Trident 的 PVC 定義範例。請參閱 Trident Volume 物件、以取得與 Trident Volume 相關的參數和設定完整說明。

## Kubernetes PersistentVolume 物件

Kubernetes PersistentVolume 物件代表 Kubernetes 叢集可用的一部分儲存設備。它的生命週期與使用它的 Pod 無關。



Trident 會建立 PersistentVolume 根據資源配置的磁碟區、自動在 Kubernetes 叢集中登錄物件。您不需要自行管理。

當您建立參照 Trident 型的 PVC 時 StorageClass、Trident 會使用對應的儲存類別來配置新的 Volume、並針對該 Volume 登錄新的 PV。在設定已配置的 Volume 和對應的 PV 時、Trident 遵循下列規則：

- Trident 會產生 Kubernetes 的 PV 名稱、以及用來配置儲存設備的內部名稱。在這兩種情況下、都是確保名稱在其範圍內是唯一的。
- 磁碟區的大小會盡可能接近在室早中所要求的大小、不過視平台而定、磁碟區可能會四捨五入至最接近的可分配數量。

## Kubernetes StorageClass 物件

Kubernetes StorageClass 物件是以中的名稱來指定 PersistentVolumeClaims 以一組內容來配置儲存設備。儲存類別本身會識別要使用的資源配置程式、並根據資源配置程式所瞭解的方式來定義該組內容。

這是需要由系統管理員建立及管理的兩個基本物件之一。另一個是 Trident 後端物件。

Kubernetes StorageClass 使用 Trident 的物件看起來像這樣：



```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: <Name>
provisioner: csi.trident.netapp.io
mountOptions: <Mount Options>
parameters:
  <Trident Parameters>
allowVolumeExpansion: true
volumeBindingMode: Immediate

```

這些參數是Trident專屬的、可告訴Trident如何為類別配置Volume。

儲存類別參數包括：

屬性	類型	必要	說明
屬性	map[string]string	否	請參閱以下「屬性」一節
storagePools	map[string]string	否	將後端名稱對應至中的儲存資源池清單
其他StoragePools	map[string]string	否	將後端名稱對應至中的儲存資源池清單
排除StoragePools	map[string]string	否	將後端名稱對應至中的儲存資源池清單

儲存屬性及其可能值可分類為儲存資源池選擇屬性和Kubernetes屬性。

儲存資源池選擇屬性

這些參數決定應使用哪些Trident託管儲存資源池來配置特定類型的磁碟區。

屬性	類型	價值	優惠	申請	支援者
媒體 <sup>1</sup>	字串	HDD、混合式、SSD	資源池包含此類型的媒體、混合式表示兩者	指定的媒體類型	ONTAP-NAS、ONTAP-NAS-經濟型、ONTAP-NAS-flexgroup、ONTAP-SAN、solidfire-san
資源配置類型	字串	纖薄、厚實	Pool支援此資源配置方法	指定的資源配置方法	厚：全ONTAP 是邊、薄：全ONTAP 是邊、邊、邊、邊、邊、邊、邊、邊

屬性	類型	價值	優惠	申請	支援者
後端類型	字串	ONTAP-NAS 、ONTAP-NAS- 經濟 型、ONTAP- NAS-flexgroup 、ONTAP- SAN、solidfire- san、GCP- CVS、azure- NetApp-Files 、ONTAP-san經 濟	集區屬於此類型 的後端	指定後端	所有驅動程式
快照	布爾	對、錯	集區支援具有快 照的磁碟區	已啟用快照 的Volume	ONTAP-NAS 、ONTAP- SAN、Solidfire- SAN、GCP-CVS
複製	布爾	對、錯	資源池支援複製 磁碟區	已啟用複本 的Volume	ONTAP-NAS 、ONTAP- SAN、Solidfire- SAN、GCP-CVS
加密	布爾	對、錯	資源池支援加密 磁碟區	已啟用加密 的Volume	ONTAP-NAS 、ONTAP-NAS- 經濟型、ONTAP- NAS- FlexGroups、ON TAP-SAN
IOPS	內部	正整數	集區能夠保證此 範圍內的IOPS	Volume保證這 些IOPS	solidfire-san

#### 1：ONTAP Select 不受支援

在大多數情況下、所要求的值會直接影響資源配置、例如、要求完整資源配置會導致資源配置較為密集的Volume。不過、元素儲存資源池會使用其提供的IOPS下限和上限來設定QoS值、而非所要求的值。在此情況下、要求的值僅用於選取儲存資源池。

理想情況下、您可以使用 `attributes` 只有模型、才能建立儲存設備的品質、滿足特定類別的需求。Trident會自動探索並選取符合 `_all_` 的儲存集區 `attributes` 您指定的。

如果您發現自己無法使用 `attributes` 若要自動為類別選取適當的資源池、您可以使用 `storagePools` 和 `additionalStoragePools` 用於進一步精簡集區或甚至選取特定集區集區的參數。

您可以使用 `storagePools` 參數以進一步限制符合任何指定之集區的集合 `attributes`。換句話說、Trident會使用由所識別的資源池交會 `attributes` 和 `storagePools` 資源配置參數。您可以單獨使用參數、也可以同時使用兩者。

您可以使用 `additionalStoragePools` 此參數可延伸Trident用於資源配置的集區集區集區集區集區集區、無論所選取的任何集區為何 `attributes` 和 `storagePools` 參數。

您可以使用 `excludeStoragePools` 篩選Trident用於資源配置的資源池集區集合的參數。使用此參數會移除任



何相符的集區。

在中 `storagePools` 和 `additionalStoragePools` 參數、每個項目都採用格式

`<backend>:<storagePoolList>`、其中 `<storagePoolList>` 是指定後端的儲存資源池清單、以英文分隔。例如、的值 `additionalStoragePools` 看起來可能是這樣

`ontapnas_192.168.1.100:aggr1,aggr2;solidfire_192.168.1.101:bronze`。這些清單接受後端值和清單值的`regex`值。您可以使用 `tridentctl get backend` 以取得後端及其資源池清單。

## Kubernetes屬性

這些屬性在動態資源配置期間、不會影響Trident選擇儲存資源池/後端。相反地、這些屬性只會提供Kubernetes持續磁碟區所支援的參數。工作節點負責檔案系統建立作業、可能需要檔案系統公用程式、例如`xfspgms`。

屬性	類型	價值	說明	相關驅動因素	Kubernetes版本
FSType	字串	ext4、ext3、xfs等	區塊磁碟區的檔案系統類型	solidfire-san 、ontap、nap、nap、nas經濟、ontap、nas、flexgroup、ontap、san、ONTAP-san經濟型	全部
owVolume擴充	布林值	對、錯	啟用或停用對增加PVc大小的支援	ONTAP-NAS 、ONTAP-NAS-經濟型、ONTAP-NAS-flexgroup 、ONTAP-SAN、ONTAP-san經濟型、solidfire-san 、gcp-CVS 、azure-netapp檔案	1.11+
Volume BindingMode	字串	立即、WaitForFirst消費者	選擇何時進行磁碟區繫結和動態資源配置	全部	1.19 - 1.26



- `fsType` 參數用於控制SAN LUN所需的檔案系統類型。此外、Kubernetes也會使用的 `fsType` 在儲存類別中、表示檔案系統存在。您可以使用來控制Volume擁有權 `fsGroup` 只有在下列情況下、Pod的安全內容才會出現 `fsType` 已設定。請參閱 "[Kubernetes：設定Pod或Container的安全內容](#)" 如需使用設定Volume擁有權的總覽 `fsGroup` 背景。Kubernetes將套用 `fsGroup` 只有在下列情況下才有

- `fsType` 在儲存類別中設定。

- PVC存取模式為`rwo`。

對於NFS儲存驅動程式、檔案系統已存在做為NFS匯出的一部分。以供使用 `fsGroup` 儲存類別仍需指定 `fsType`。您可以將其設定為 `nfs` 或任何非`null`值。

- 請參閱 "[展開Volume](#)" 如需磁碟區擴充的詳細資料、
- Trident安裝程式套件提供數個範例儲存類別定義、可與中的Trident搭配使用 `sample-input/storage-class-*.yaml`。刪除Kubernetes儲存類別也會刪除對應的Trident儲存類別。

## Kubernetes VolumeSnapshotClass 物件

Kubernetes `VolumeSnapshotClass` 物件類似 `StorageClasses`。它們有助於定義多種儲存類別、並由Volume Snapshot參考、以將快照與所需的Snapshot類別建立關聯。每個Volume Snapshot都與單一Volume Snapshot類別相關聯。

答 `VolumeSnapshotClass` 應由系統管理員定義以建立快照。建立具有下列定義的Volume Snapshot類別：

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: csi-snapclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

◦ `driver` 指定要要求的Kubernetes磁碟區快照 `csi-snapclass` 類別由Trident處理。◦ `deletionPolicy` 指定必須刪除快照時要採取的動作。何時 `deletionPolicy` 設為 `Delete`、刪除快照時、會移除儲存叢集上的Volume Snapshot物件及基礎快照。或者、將其設定為 `Retain` 也就是說 `VolumeSnapshotContent` 並保留實體快照。

## Kubernetes VolumeSnapshot 物件

Kubernetes `VolumeSnapshot` 物件是建立磁碟區快照的要求。就像使用者針對磁碟區所提出的要求一樣、磁碟區快照是使用者建立現有虛擬磁碟快照的要求。

當磁碟區快照要求出現時、Trident會在後端自動管理磁碟區的快照建立、並建立唯一的快照來公開快照 `VolumeSnapshotContent` 物件：您可以從現有的PVCS建立快照、並在建立新的PVCS時、將快照作為DataSource使用。



Volume Snapshot的生命週期與來源PVCs無關：即使刪除來源PVCs、快照仍會持續存在。刪除具有相關快照的永久虛擬磁碟時、Trident會將此永久虛擬磁碟的備份磁碟區標示為\*刪除\*狀態、但不會將其完全移除。刪除所有相關的快照時、即會移除該磁碟區。

## Kubernetes VolumeSnapshotContent 物件

Kubernetes VolumeSnapshotContent 物件代表從已配置的磁碟區擷取的快照。類似於 PersistentVolume 並表示儲存叢集上已配置的快照。類似 PersistentVolumeClaim 和 PersistentVolume 建立快照時的物件 VolumeSnapshotContent 物件會將一對一的對應維持在上 VolumeSnapshot 物件、要求建立快照。



Trident會建立 VolumeSnapshotContent 根據資源配置的磁碟區、自動在Kubernetes叢集中登錄物件。您不需要自行管理。

◦ VolumeSnapshotContent 物件包含可唯一識別快照的詳細資料、例如 snapshotHandle。這 snapshotHandle 是PV名稱與名稱的獨特組合 VolumeSnapshotContent 物件：

當快照要求出現時、Trident會在後端建立快照。建立快照之後、Trident會設定 VolumeSnapshotContent 然後將快照公開給Kubernetes API。

## Kubernetes CustomResourceDefinition 物件

Kubernetes自訂資源是Kubernetes API中由系統管理員定義的端點、用於將類似物件分組。Kubernetes支援建立自訂資源來儲存物件集合。您可以執行來取得這些資源定義 `kubectl get crds`。

自訂資源定義（CRD）及其相關的物件中繼資料會由Kubernetes儲存在其中繼資料儲存區中。如此一來、您就不需要另外建立Trident的儲存區。

從19.07版開始、Trident使用了許多 CustomResourceDefinition 保留Trident物件身分的物件、例如Trident後端、Trident儲存類別和Trident Volume。這些物件由Trident管理。此外、「csi Volume Snapshot」架構也引進了定義Volume快照所需的部分CRD。

CRD是Kubernetes建構。上述資源的物件是由Trident所建立。例如、使用建立後端時 `tridentctl`、對應的 `tridentbackends` CRD物件是由Kubernetes所建立、供其使用。

以下是Trident客戶需求日的幾點重點：

- 安裝Trident時、會建立一組客戶需求日、並可像使用任何其他資源類型一樣使用。
- 從先前版本的Trident（使用的Trident）升級時 `etcd` 為了維持狀態）、Trident安裝程式會從移轉資料 `etcd` 金鑰值資料儲存區、並建立對應的CRD物件。
- 使用解除安裝Trident時 `tridentctl uninstall` 命令、Trident Pod會刪除、但建立的客戶需求日不會清除。請參閱 ["解除安裝Trident"](#) 瞭解如何徹底移除Trident並從頭重新設定。

## Trident StorageClass 物件

Trident為Kubernetes建立相符的儲存類別 StorageClass 指定的物件 `csi.trident.netapp.io/netapp.io/trident` 在他們的資源配置工具欄位中。儲存類別名稱與Kubernetes名稱相符 StorageClass 所代表的物件。



使用Kubernetes時、這些物件會在Kubernetes時自動建立 StorageClass 使用Trident做為資源配置程式的功能已登錄。

儲存類別包含一組磁碟區需求。Trident會將這些需求與每個儲存資源池中的屬性相符；如果符合、則該儲存資源池是使用該儲存類別來配置磁碟區的有效目標。

您可以使用REST API建立儲存類別組態、以直接定義儲存類別。不過、在Kubernetes部署中、我們預期在登錄新Kubernetes時會建立這些部署 StorageClass 物件：

## Trident後端物件

後端代表儲存供應商、其中Trident會配置磁碟區；單一Trident執行個體可管理任何數量的後端。



這是您自己建立和管理的兩種物件類型之一。另一個是Kubernetes StorageClass 物件：

如需如何建構這些物件的詳細資訊、請參閱 ["設定後端"](#)。

## Trident StoragePool 物件

儲存資源池代表可在每個後端上進行資源配置的不同位置。就支援而言ONTAP、這些項目對應於SVM中的集合體。對於NetApp HCI / SolidFire、這些服務會對應到系統管理員指定的QoS頻段。就架構而言、這些項目對應於雲端供應商所在的地區。Cloud Volumes Service每個儲存資源池都有一組獨特的儲存屬性、可定義其效能特性和資料保護特性。

與此處的其他物件不同、儲存資源池候選項目一律會自動探索及管理。

## Trident Volume 物件

Volume是資源配置的基本單位、包含NFS共用和iSCSI LUN等後端端點。在Kubernetes中、這些項目會直接對應至 PersistentVolumes。建立磁碟區時、請確定它有一個儲存類別、決定該磁碟區可以配置的位置及大小。



在Kubernetes中、會自動管理這些物件。您可以檢視這些資源、以查看資源配置的Trident內容。



刪除具有相關快照的PV時、對應的Trident Volume會更新為\*刪除\*狀態。若要刪除Trident磁碟區、您應該移除該磁碟區的快照。

Volume組態會定義已配置磁碟區應具備的內容。

屬性	類型	必要	說明
版本	字串	否	Trident API版本（「1」）
名稱	字串	是的	要建立的Volume名稱
storageClass	字串	是的	配置Volume時使用的儲存類別
尺寸	字串	是的	要配置的磁碟區大小（以位元組為單位）

屬性	類型	必要	說明
傳輸協定	字串	否	要使用的傳輸協定類型；「檔案」或「區塊」
內部名稱	字串	否	儲存系統上的物件名稱；由Trident產生
cloneSourceVolume	字串	否	Sname (NAS、SAN) & S--*：要複製的磁碟區名稱ONTAP SolidFire
分岔OnClone	字串	否	例 (NAS、SAN)：從父實體分割複本ONTAP
Snapshot原則	字串	否	S--*：快照原則ONTAP
Snapshot保留區	字串	否	Sing-*：保留給快照的磁碟區百分比ONTAP
匯出原則	字串	否	ONTAP-NAS*：要使用的匯出原則
Snapshot目錄	布爾	否	ONTAP-NAS*：快照目錄是否可見
unix權限	字串	否	ONTAP-NAS*：初始UNIX權限
區塊大小	字串	否	S--*：區塊/區段大小SolidFire
檔案系統	字串	否	檔案系統類型

Trident會產生 `internalName` 建立Volume時。這包括兩個步驟。首先、它會預先加上儲存前置詞（預設值之一 `trident` 或是後端組態中的前置字元）到磁碟區名稱、產生表單名稱 `<prefix>-<volume-name>`。然後、它會繼續清理名稱、取代後端不允許的字元。對於後端、它會以底線取代連字號（因此內部名稱會變成ONTAP `<prefix>_<volume-name>`）。對於元素後端、它會以連字號取代底線。

您可以使用Volume組態、使用REST API直接配置磁碟區、但在Kubernetes部署中、我們預期大多數使用者都會使用標準Kubernetes `PersistentVolumeClaim` 方法。Trident會自動建立此Volume物件、做為資源配置程序的一部分。

## Trident Snapshot 物件

快照是磁碟區的時間點複本、可用來配置新的磁碟區或還原狀態。在Kubernetes中、這些項目會直接對應至 `VolumeSnapshotContent` 物件：每個快照都與一個Volume相關聯、該磁碟區是快照資料的來源。

每個 Snapshot 物件包含下列內容：

屬性	類型	必要	說明
版本	字串	是的	Trident API版本（「1」）
名稱	字串	是的	Trident Snapshot物件的名稱

屬性	類型	必要	說明
內部名稱	字串	是的	儲存系統上Trident Snapshot物件的名稱
Volume名稱	字串	是的	為其建立快照的持續Volume名稱
Volume內部名稱	字串	是的	儲存系統上相關Trident Volume物件的名稱



在Kubernetes中、會自動管理這些物件。您可以檢視這些資源、以查看資源配置的Trident內容。

當Kubernetes時 VolumeSnapshot 物件要求已建立、Trident可在備份儲存系統上建立Snapshot物件。。  
 internalName 此快照物件的產生方式為結合前置詞 snapshot- 使用 UID 的 VolumeSnapshot 物件（例如、snapshot-e8d8a0ca-9826-11e9-9807-525400f3f660）。 volumeName 和 volumeInternalName 會透過取得備用磁碟區的詳細資料來填入。

## Astra Trident ResourceQuota 物件

Trident去除會耗用a system-node-critical 優先級類別是Kubernetes中最高的優先級類別、可確保Astra Trident在正常節點關機期間識別並清理磁碟區、並允許Trident的取消安裝Pod在資源壓力較高的叢集中預先配置優先級較低的工作負載。

為了達成此目標、Astra Trident採用 ResourceQuota 確保在Trident取消程式集上達到「系統節點關鍵」優先順序類別的物件。在部署和建立實體化設定之前、Astra Trident會先尋找 ResourceQuota 物件、如果未探索到、則套用它。

如果您需要更多控制預設資源配額和優先順序類別、可以產生 custom.yaml 或設定 ResourceQuota 使用Helm圖表的物件。

以下是「資源配額」物件優先處理Trident的範例。

```
apiVersion: <version>
kind: ResourceQuota
metadata:
  name: trident-csi
  labels:
    app: node.csi.trident.netapp.io
spec:
  scopeSelector:
    matchExpressions:
      - operator : In
        scopeName: PriorityClass
        values: ["system-node-critical"]
```

如需資源配額的詳細資訊、請參閱 "[Kubernetes：資源配額](#)"。

清理 ResourceQuota 如果安裝失敗

在極少數情況下、安裝會在之後失敗 ResourceQuota 物件已建立、請先嘗試 ["正在解除安裝"](#) 然後重新安裝。

如果這不管用、請手動移除 ResourceQuota 物件：

移除 ResourceQuota

如果您偏好控制自己的資源配置、可以移除Astra Trident ResourceQuota 使用命令的物件：

```
kubectl delete quota trident-csi -n trident
```

## tridentctl命令和選項

◦ ["Trident安裝程式套裝組合"](#) 包括命令列公用程式、`tridentctl`可讓您輕鬆存取Astra Trident。擁有足夠權限的Kubernetes使用者可以使用它來安裝Astra Trident、以及直接與它互動、以管理包含Astra Trident Pod的命名空間。

### 可用的命令和選項

如需使用資訊、請執行 `tridentctl --help`。

可用的命令和全域選項包括：

```
Usage:
  tridentctl [command]
```

可用命令：

- `create`：將資源新增至Astra Trident。
- `delete`：從Astra Trident移除一或多個資源。
- `get`：從Astra Trident取得一或多項資源。
- `help`：有關任何命令的幫助。
- `images`：列印容器影像Astra Trident需求的表格。
- `import`：將現有資源導入Astra Trident。
- `install`：安裝Astra Trident。
- `logs`：從Astra Trident列印記錄。
- `send`：從Astra Trident傳送資源。
- `uninstall`：卸載Astra Trident。
- `update`：修改Astra Trident中的資源。

- upgrade：升級Astra Trident中的資源。
- version：列印Astra Trident的版本。

旗標：

- `-d, --debug`：除錯輸出。
- `-h, --help`：幫助 `tridentctl`。
- `-n, --namespace string`：Astra Trident部署的命名空間。
- `-o, --output string`：輸出格式。json之一| yaml| name| w| ps（預設）。
- `-s, --server string`：Astra Trident REST介面的位址/連接埠。



Trident REST介面可設定為偵聽、僅適用於127.0.0.1（適用於IPV4）或[:1]（適用於IPv6）。



Trident REST介面可設定為偵聽、僅適用於127.0.0.1（適用於IPV4）或[:1]（適用於IPv6）。

## create

您可以使用執行 `create` 命令以新增資源至Astra Trident。

```
Usage:
tridentctl create [option]
```

可用選項：

backend：將後端新增至Astra Trident。

## delete

您可以執行 `delete` 從Astra Trident移除一或多個資源的命令。

```
Usage:
tridentctl delete [option]
```

可用選項：

- backend：從Astra Trident刪除一個或多個儲存後端。
- snapshot：從Astra Trident刪除一個或多個Volume快照。
- storageclass：從Astra Trident刪除一個或多個儲存類別。
- volume：從Astra Trident刪除一個或多個儲存磁碟區。



## get

您可以執行 `get` 從Astra Trident取得一或多個資源的命令。

```
Usage:
  tridentctl get [option]
```

可用選項：

- `backend`：從Astra Trident取得一或多個儲存後端。
- `snapshot`：從Astra Trident取得一或多個快照。
- `storageclass`：從Astra Trident取得一或多個儲存課程。
- `volume`：從Astra Trident取得一或多個磁碟區。

`volume` 旗標：`* -h, --help`：Volume的說明。`* --parentOfSubordinate string`：將查詢限制在從屬來源Volume。`* --subordinateOf string`：將查詢限制在Volume的下屬。

## images

您可以執行 `images` 標記以列印容器影像Astra Trident需求的表格。

```
Usage:
  tridentctl images [flags]
```

旗標：`* -h, --help``：Help for images。  
`* -v, --k8s-version stru``：語義版本的Kubernetes叢集。

## import volume

您可以執行 `import volume` 將現有磁碟區匯入Astra Trident的命令。

```
Usage:
  tridentctl import volume <backendName> <volumeName> [flags]
```

別名：

`volume, v`

旗標：

- `-f, --filename string`：Yaml或Json PVc檔案的路徑。
- `-h, --help`：Volume的說明。
- `--no-manage`：僅建立PV/PVc。不要假設磁碟區生命週期管理。

## install

您可以執行 `install` 安裝Astra Trident的旗標。

```
Usage:
  tridentctl install [flags]
```

旗標：

- `--autosupport-image string`: AutoSupport 適用於遙測的容器影像（預設為「NetApp/Trident autosupport:20.07.0」）。
- `--autosupport-proxy string`: 代理伺服器的位址/連接埠、用於傳送AutoSupport「遙測」功能。
- `--csi`: 安裝csi Trident（僅適用於Kubernetes 1.13的置換功能、需要功能閘道）。
- `--enable-node-prep`: 嘗試在節點上安裝所需的套件。
- `--generate-custom-yaml`: 在不安裝任何內容的情況下生成Yaml文件。
- `-h, --help`: 安裝說明。
- `--http-request-timeout`: 覆蓋Trident控制器REST API的HTTP要求逾時時間（預設值為1m30s）。
- `--image-registry string`: 內部映像登錄的位址/連接埠。
- `--k8s-timeout duration`: 所有Kubernetes作業的逾時時間（預設為3個月）。
- `--kubelet-dir string`: Kubelet內部狀態的主機位置（預設為「/var/lib/kubelet」）。
- `--log-format string`: Astra Trident記錄格式（text、json）（預設「text」）。
- `--pv string`: Astra Trident使用的舊PV名稱、確保不存在（預設為「Trident」）。
- `--pvc string`: Astra Trident使用的舊版永久虛擬卷名稱、確保不存在（預設為「Trident」）。
- `--silence-autosupport`: 請勿AutoSupport 自動將不實的套裝組合傳送至NetApp（預設為true）。
- `--silent`: 安裝期間禁用大多數輸出。
- `--trident-image string`: 要安裝的Astra Trident映像。
- `--use-custom-yaml`: 使用安裝目錄中現有的任何Yaml檔案。
- `--use-ipv6`: 使用IPv6進行Astra Trident的通訊。

## logs

您可以執行 `logs` 用於列印Astra Trident記錄的旗標。

```
Usage:
  tridentctl logs [flags]
```

旗標：

- ``-a, --archive`：除非另有說明、否則請使用所有記錄建立支援歸檔。
- ``-h, --help`：日誌幫助。
- ``-l, --log string`：要顯示的Astra Trident記錄。其中一個trident | auto| trident運算子| all（預設為「自動」）。
- ``--node string`：Kubernetes節點名稱、用於收集節點Pod記錄。
- ``-p, --previous`：獲取先前容器實例的日誌（如果存在）。
- ``--sidecars`：取得邊側邊容器的記錄。

## send

您可以執行 `send` 從Astra Trident傳送資源的命令。

```
Usage:
  tridentctl send [option]
```

可用選項：

`autosupport`：將AutoSupport 一份不適用的歸檔文件傳送給NetApp。

## uninstall

您可以執行 `uninstall` 解除安裝Astra Trident的旗標。

```
Usage:
  tridentctl uninstall [flags]
```

旗標：`* -h, --help`：解除安裝說明。`* --silent`：卸載期間禁用大多數輸出。

## update

您可以執行 `update` 用於修改Astra Trident中資源的命令。

```
Usage:
  tridentctl update [option]
```

可用選項：

`backend`：更新Astra Trident的後端。

## upgrade

您可以執行 `upgrade` 用於升級Astra Trident資源的命令。

```
Usage:
tridentctl upgrade [option]
```

可用選項：

volume：將一個或多個持續磁碟區從NFS/iSCSI升級至csi。

version

您可以執行 `version` 用於列印版本的旗標 `tridentctl` 以及執行中的Trident服務。

```
Usage:
tridentctl version [flags]
```

旗標：\* `--client`：僅限用戶端版本（不需要伺服器）。\* `-h`, `--help`：版本說明。

## Pod安全標準（PSS）與安全內容限制（SCC）

Kubernetes Pod安全標準（Ps）和Pod安全政策（Ps）定義權限等級、並限制Pod的行為。OpenShift Security內容限制（SCC）同樣定義OpenShift Kubernetes Engine特有的Pod限制。為了提供此自訂功能、Astra Trident可在安裝期間啟用特定權限。以下各節詳細說明Astra Trident設定的權限。



PSS-取代Pod安全性原則（PSP）。在Kubernetes v1.21中、已不再使用PSP、將在v1.25中移除。如需詳細資訊、請參閱 "[Kubernetes：安全性](#)"。

### 必要的Kubernetes安全內容和相關欄位

權限	說明
權限	SCSI需要雙向裝載點、這表示Trident節點Pod必須執行特殊權限容器。如需詳細資訊、請參閱 " <a href="#">Kubernetes：掛載傳播</a> "。
主機網路	iSCSI精靈所需。 <code>iscsiadm</code> 管理iSCSI掛載、並使用主機網路與iSCSI精靈進行通訊。
主機IPC	NFS使用程序間通訊（IPC）與 <code>nfdsd</code> 通訊。
主機PID	必須啟動 <code>rpc-statd</code> NFS：Astra Trident會查詢主機程序以判斷是否 <code>rpc-statd</code> 在掛載NFS磁碟區之前執行。
功能	<ul style="list-style-type: none"><li>◦ <code>SYS_ADMIN</code> 此功能是專為特殊權限容器提供的預設功能之一。例如、<code>Docker</code>會針對特殊權限容器設定下列功能：</li></ul> <pre>CapPrm: 0000003fffffffffff CapEff: 0000003fffffffffff</pre>

權限	說明
Seccomp	Seccomp設定檔在特殊權限容器中一律為「未限制」、因此無法在Astra Trident中啟用。
SELinux	在OpenShift上、有權限的容器會在中執行 <code>spc_t</code> （「超級權限容器」）網域和無權限容器會在中執行 <code>container_t</code> 網域：開啟 <code>containerd</code> 、搭配 <code>container-selinux</code> 安裝後、所有的容器都會在中執行 <code>spc_t</code> 網域、有效停用SELinux。因此、Astra Trident並未新增 <code>seLinuxOptions</code> 至容器。
DAC	權限容器必須以root身分執行。非權限容器會以root身分執行、以存取csi所需的UNIX通訊端。

## Pod安全標準（PSS）

標籤	說明	預設
<code>pod-security.kubernetes.io/enforce</code>	允許Trident控制器和節點進入安裝命名空間。請勿變更命名空間標籤。	<code>enforce: privileged</code>
<code>pod-security.kubernetes.io/enforce-version</code>		<code>enforce-version: &lt;version of the current cluster or highest version of PSS tested.&gt;</code>



變更命名空間標籤可能會導致無法排程Pod、「建立錯誤：...」或「警告：Trident：Cig-...」。如果發生這種情況、請檢查命名空間標籤是否適用於 `privileged` 已變更。如果是、請重新安裝Trident。

## Pod安全原則（PSP）

欄位	說明	預設
<code>allowPrivilegeEscalation</code>	特殊權限容器必須允許權限提高。	<code>true</code>
<code>allowedCSIDrivers</code>	Trident不使用即時的csi暫時性磁碟區。	空白
<code>allowedCapabilities</code>	非權限Trident容器不需要比預設集更多的功能、而且會將所有可能的功能授予權限容器。	空白
<code>allowedFlexVolumes</code>	Trident並未使用 " <a href="#">FlexVolume驅動程式</a> " 因此，它們不會包含在允許的磁碟區清單中。	空白
<code>allowedHostPaths</code>	Trident節點Pod會掛載節點的根檔案系統、因此設定此清單沒有任何好處。	空白
<code>allowedProcMountTypes</code>	Trident不使用任何 <code>ProcMountTypes</code> 。	空白

欄位	說明	預設
allowedUnsafeSysctls	Trident不需要任何不安全的項目 sysctls。	空白
defaultAddCapabilities	不需要將任何功能新增至權限容器。	空白
defaultAllowPrivilegeEscalation	每個Trident Pod都會處理允許權限提高的問題。	false
forbiddenSysctls	否 sysctls 允許。	空白
fsGroup	Trident容器以root執行。	RunAsAny
hostIPC	掛載NFS磁碟區需要主機IPC才能與進行通訊 nfsd	true
hostNetwork	iscsiadm要求主機網路與iSCSI精靈進行通訊。	true
hostPID	需要主機PID才能檢查是否有 rpc-statd 正在節點上執行。	true
hostPorts	Trident不使用任何主機連接埠。	空白
privileged	Trident節點Pod必須執行特殊權限容器、才能掛載磁碟區。	true
readOnlyRootFilesystem	Trident節點Pod必須寫入節點檔案系統。	false
requiredDropCapabilities	Trident節點Pod執行特殊權限容器、無法丟棄功能。	none
runAsGroup	Trident容器以root執行。	RunAsAny
runAsUser	Trident容器以root執行。	runAsAny
runtimeClass	Trident不使用 RuntimeClasses。	空白
seLinux	未設定Trident seLinuxOptions 因為目前容器執行時間與Kubernetes發行版本處理SELinux的方式有差異。	空白
supplementalGroups	Trident容器以root執行。	RunAsAny
volumes	Trident Pod需要這些Volume外掛程式。	hostPath, projected, emptyDir

## 安全內容限制（SCC）

標籤	說明	預設
allowHostDirVolumePlugin	Trident節點Pod會掛載節點的根檔案系統。	true
allowHostIPC	掛載NFS磁碟區需要主機IPC才能與進行通訊 nfsd。	true

標籤	說明	預設
allowHostNetwork	iscsiadm要求主機網路與iSCSI精靈進行通訊。	true
allowHostPID	需要主機PID才能檢查是否有 rpc-statd 正在節點上執行。	true
allowHostPorts	Trident不使用任何主機連接埠。	false
allowPrivilegeEscalation	特殊權限容器必須允許權限提高。	true
allowPrivilegedContainer	Trident節點Pod必須執行特殊權限容器、才能掛載磁碟區。	true
allowedUnsafeSysctls	Trident不需要任何不安全的項目 sysctls。	none
allowedCapabilities	非權限Trident容器不需要比預設集更多的功能、而且會將所有的功能授予權限容器。	空白
defaultAddCapabilities	不需要將任何功能新增至權限容器。	空白
fsGroup	Trident容器以root執行。	RunAsAny
groups	此SCC僅適用於Trident、並與其使用者有關。	空白
readOnlyRootFilesystem	Trident節點Pod必須寫入節點檔案系統。	false
requiredDropCapabilities	Trident節點Pod執行特殊權限容器、無法丟棄功能。	none
runAsUser	Trident容器以root執行。	RunAsAny
seLinuxContext	未設定Trident seLinuxOptions 因為目前容器執行時間與Kubernetes發行版本處理SELinux的方式有差異。	空白
seccompProfiles	特殊權限容器永遠都會執行「未限制」。	空白
supplementalGroups	Trident容器以root執行。	RunAsAny
users	提供一個項目來將此SCC繫結至Trident命名空間中的Trident使用者。	不適用
volumes	Trident Pod需要這些Volume外掛程式。	hostPath, downwardAPI, projected, emptyDir

# 較早版本的文件

如果您未執行 Astra Trident 23.01 、則可取得先前版本的文件。

- ["Astra Trident 22.10"](#)
- ["Astra Trident 22.07"](#)
- ["Astra Trident 22.04"](#)
- ["Astra Trident 22.01"](#)
- ["Astra Trident 21.10"](#)
- ["Astra Trident 21.07"](#)



# 法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

## 版權

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## 商標

NetApp、NetApp 標誌及 NetApp 商標頁面上列出的標章均為 NetApp、Inc. 的商標。其他公司與產品名稱可能為其各自所有者的商標。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## 專利

如需最新的 NetApp 擁有專利清單、請參閱：

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## 隱私權政策

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## 開放原始碼

您可以在每個版本的通知檔案中檢閱 NetApp 軟體中用於 Astra Trident 的協力廠商版權與授權、網址為 <https://github.com/NetApp/trident/>。

## 版權資訊

Copyright © 2024 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。