設定後端

Astra Trident

NetApp
April 04, 2024

目錄

設定後端

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。

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。

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。

NFS 和 **SMB** 磁碟區的必要條件

> 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"。

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/writ
e",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/dele
te",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/rea
d",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/wri
te",
```

```
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/del
ete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/Get
Metadata/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/MountTargets/r
ead",
                    "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。

後端組態選項

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。

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	"

參數	說明	預設
`subnet`	委派給的子網路名稱 `Microsoft.Netapp/volumes`	"
`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。	"nfsves=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。	「0.00.0.0/0」
`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

這是絕對最低的後端組態。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、後端會為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** ：虛擬集區組態

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 "三個服務層級"：
  - `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。	

參數	說明	預設
`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"
`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。	「0.00.0.0/0」
`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。

範例**1**：最低組態

這是使用預設「標準」服務層級的預設CVS效能服務類型的最低後端組態。

```
---
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-----
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    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
```

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-----
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    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
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`。

```
---
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-----
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
```

```
    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
```

儲存類別定義

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。

儲存類別範例

```
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。

範例1：最低組態

這是使用的最低後端組態 `storageClass` 指定CVS服務類型和預設值 `standardsw` 服務層級：

```
---
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
storageClass: software
apiRegion: us-east4
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3bl/qp8B4Kws8zX5ojY9m
    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
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
    LLaWOH4VIZQZCAyW5IUp9CAmwqHgdG0uhFNfCgMmED6PBUvVLsLvcq86X+QSWR9k
    ETqElj/sGCenPF7ti1DhGBFafd9hPnxg9PZY29ArEZwY9G/ZjZQX7WPgs0VvxiNR
    DxZRC3GXAgMBAAECggEACn5c59bG/qnVEVI1CwMAalM5M2z09JFhlLlljKwntNPj
    Vilw2eTW2+UE7HbJru/S7KQgA5Dnn9kvCraEahPRuddUMrD0vG4kTl/IODV6uFuk
    Y0sZfbqd4jMUQ21smvGsqFzwloYWS5qzO1W83ivXH/HW/iqkmY2eW+EPRS/hwSSu
    SscR+SojI7PB0BWSJhlV4yqYf3vcD/D95el2CVHfRCkL85DKumeZ+yHEnpiXGZAE
    t8xSs4a5OOPm6NHhevCw2a/UQ95/foXNUR450HtbjieJo5o+FF6EYZQGfU2ZHZO8
    37FBKuaJkdGW5xqaI9TL7aqkGkFMF4F2qvOZM+vy8QKBgQD4oVuOkJDlhkTHP86W
    esFlw1kpWyJR9ZA7LI0g/rVpslnX+XdDq0WQf4umdLNau5hYEH9LU6ZSGs1Xk3/B
    NHwR6OXFuqEKNiu83d0zSlHhTy7PZpOZdj5a/vVvQfPDMz7OvsqLRd7YCAbdzuQ0
    +Ahq0Ztwvg0HQ64hdW0ukpYRRwKBgQDgyHj98oqswoYuIa+pP1yS0pPwLmjwKyNm
    /HayzCp+Qjiyy7Tzg8AUqlH1Ou83XbV428jvg7kDhO7PCCKFq+mMmfqHmTpb0Maq
    KpKnZg4ipsqP1yHNNEoRmcailXbwIhCLewMqMrggUiLOmCw4PscL5nK+4GKu2XE1
    jLqjWAZFMQKBgFHkQ9XXRAJ1kR3XpGHoGN890pZOkCVSrqju6aUef/5KYlFCt8ew
    F/+aIxM2iQSvmWQYOvVCnhuY/F2GFaQ7d0om3decuwI0CX/xy7PjHMkLXa2uaZs4
    WR17sLduj62RqXRLX0c0QkwBiNFyHbRcpdkZJQujbYMhBa+7j7SxT4BtAoGAWMWT
    UucocRXZm/pdvz9wteNH3YDWnJLMxm1KC06qMXbBoYrliY4sm3ywJWMC+iCd/H8A
    Gecxd/xVu5mA2L2N3KMq18Zhz8Th0G5DwKyDRJgOQ0Q46yuNXOoYEjlo4Wjyk8Me
    +tlQ8iK98E0UmZnhTgfSpSNElbz2AqnzQ3MN9uECgYAqdvdVPnKGfvdtZ2DjyMoJ
    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。

開始之前

在建立元素後端之前、您需要下列項目。

- 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"。

Volume 模式

。 `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。
`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

參數	說明	預設
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	
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、有些儲存資源池會自行設定類型、有些資源池則會覆寫上述預設值。

```
---
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"

支援SAN驅動程式ONTAP

ONTAP SAN 驅動程式概觀

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

ONTAP SAN 驅動程式的重要資訊

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

瞭解使用 ONTAP SAN 驅動程式設定 ONTAP 後端的需求和驗證選項。

需求

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 "準備工作節點" 以取得詳細資料。

驗證 ONTAP 後端

Astra Trident提供兩種驗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

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

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CACertifate：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...Vaaalllluuuueeee",
"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。

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
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）。

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",
    "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-economy`、`ontap-nas-flexgroup`、`ontap-san`、`ontap-san-economy`
`backendName`	自訂名稱或儲存後端	驅動程式名稱+「_」+ dataLIF
`managementLIF`	叢集或SVM管理LIF的IP位址 若要進行無縫 MetroCluster 移位、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 "可選擇的LUN對應ONTAP" 探索建立多重路徑工作階段所需的iSCI 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 "準備使用ONTAP 支援的SAN驅動程式來設定後端" 以取得詳細資料。	`false`
`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	「」

參數	說明	預設
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	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
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。	「」（預設不會強制執行）
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、「方法」：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。	null

參數	說明	預設
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。	false

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： "Astra Trident如何與NVE和NAE搭配運作"。	「假」
`luksEncryption`	啟用LUKS加密。請參閱 "使用Linux統一金鑰設定（LUKS）"。	"
`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
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：

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 上搭配 Astra Trident 使用 Amazon FSX 、建議您指定生命的 DNS 名稱、而非 IP 位址。

ONTAP SAN 最小化組態範例

這是使用的基本組態 `ontap-san` 驅動程式：

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
username: vsadmin
password: <password>
```

ONTAP SAN 經濟型最低組態範例

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
username: vsadmin
password: <password>
```

憑證型驗證範例

在此基本組態範例中 `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
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

雙向 CHAP 範例

這些範例使用建立後端 `useCHAP` 設定為 `true`。

ONTAP SAN CHAP 範例

```
---
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
username: vsadmin
password: <password>
```

ONTAP SAN 經濟 CHAP 範例

```
---
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
username: vsadmin
password: <password>
```

虛擬集區的後端範例

在這些後端定義檔案範例中、會針對所有儲存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。

在這些範例中、有些儲存池是自行設定的 `spaceReserve`、 `spaceAllocation`和 `encryption` 值、而某些資源池會覆寫預設值。

ONTAP SAN 範例

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
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'
```

ONTAP SAN 經濟效益範例

```
---
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
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'
- labels:
    department: legal
    creditpoints: '5000'
```

```
  zone: us_east_1c
  defaults:
    spaceAllocation: 'true'
    encryption: 'false'
```

將後端對應至StorageClass

下列 StorageClass 定義請參閱 [虛擬集區的後端範例]。使用 `parameters.selector` 欄位中、每個 StorageClass 都會呼叫哪些虛擬集區可用於主控磁碟區。磁碟區將會在所選的虛擬資源池中定義各個層面。

- 。 `protection-gold` StorageClass 會對應至中的第一個虛擬集區 `ontap-san` 後端：這是唯一提供金級保護的集區。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection=gold"
  fsType: "ext4"
```

- 。 `protection-not-gold` StorageClass 會對應至中的第二個和第三個虛擬集區 `ontap-san` 後端：這是唯一提供金級以外保護層級的集區。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
```

- 。 `app-mysqldb` StorageClass 會對應至中的第三個虛擬集區 `ontap-san-economy` 後端：這是唯一為 mysqldb 類型應用程式提供儲存池組態的集區。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: netapp.io/trident
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
```

- 。 `protection-silver-creditpoints-20k` StorageClass 會對應至中的第二個虛擬集區 `ontap-san` 後端：這是唯一提供銀級保護和 20000 個信用點數的資源池。

```
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"
```

- 。 `creditpoints-5k` StorageClass 會對應至中的第三個虛擬集區 `ontap-san` 中的後端和第四個虛擬集區 `ontap-san-economy` 後端：這是唯一擁有 5000 個信用點數的集區方案。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: netapp.io/trident
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"
```

Astra Trident將決定選取哪個虛擬集區、並確保符合儲存需求。

ASNAS驅動程式ONTAP

ONTAP NAS 驅動程式概述

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

ONTAP NAS 驅動程式的重要資訊

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 中建立更具限制性的角色、讓 Trident 驅動程式可以使用、但我們不建議這樣做。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

瞭解使用 ONTAP NAS 驅動程式設定 ONTAP 後端的需求、驗證選項和匯出原則。

需求

- 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。
- 您可以執行多個驅動程式、並建立指向其中一個或另一個的儲存類別。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。
- Astra Trident僅支援安裝在Windows節點上執行的Pod上的SMB磁碟區。請參閱 準備配置SMB磁碟區 以取得詳細資料。

驗證 ONTAP 後端

Astra Trident提供兩種驗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

```
---
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。

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CACertifate：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...Vaaalllluuuueeee",
"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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

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>
      fileSystemType: 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。

準備配置SMB磁碟區

只需稍加準備、您就可以使用來配置 SMB 磁碟區 `ontap-nas` 驅動程式：

> 您必須在 SVM 上同時設定 NFS 和 SMB/CIFS 通訊協定、才能建立 `ontap-nas-economy` 適用於內部部署 ONTAP 的 SMB Volume 。若未設定上述任一種通訊協定、將導致 SMB 磁碟區建立失敗。

開始之前

在配置 SMB 磁碟區之前、您必須具備下列項目。

- 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。

步驟

1. 對於內部部署 ONTAP 、您可以選擇性地建立 SMB 共用、或是 Astra Trident 可以為您建立一個。

   > Amazon FSX for ONTAP 需要 SMB 共享。

   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` 您可以指定下列其中一項：使用 Microsoft 管理主控台或 ONTAP CLI 建立的 SMB 共用名稱；允許 Astra Trident 建立 SMB 共用的名稱；或將參數保留空白以防止共用磁碟區存取。 對於內部部署 ONTAP 、此參數為選用項目。 Amazon FSX 需要此參數才能支援 ONTAP 後端、且不可為空白。	`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 **`ntfs`** 或 **`mixed`** 適用於**SMB**磁碟區。	`ntfs` 或 `mixed` 適用於SMB磁碟區	`unixPermissions`

列舉**NAS**組態選項與範例**ONTAP**

瞭解如何在 Astra Trident 安裝中建立及使用 ONTAP 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

參數	說明	預設
managementLIF	叢集或SVM管理LIF的IP位址 若要進行無縫 MetroCluster 移位、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」]
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	預設
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。	「」（預設不會強制執行）
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。	「」（預設不會強制執行）
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、「方法」：true } 請勿使用 debugTraceFlags 除非您正在疑難排解並需要詳細的記錄傾印。	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

參數	說明	預設
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。	「」
qtreesPerFlexvol	每FlexVol 個邊的最大qtree數、必須在範圍內[50、300]	「 200 」
smbShare	您可以指定下列其中一項：使用 Microsoft 管理主控台或 ONTAP CLI 建立的 SMB 共用名稱；允許 Astra Trident 建立 SMB 共用的名稱；或將參數保留空白以防止共用磁碟區存取。 對於內部部署 ONTAP 、此參數為選用項目。 Amazon FSX 需要此參數才能支援 ONTAP 後端、且不可為空白。	smb-share
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」

參數	說明	預設
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」
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： "Astra Trident如何與NVE和NAE搭配運作"。	「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 預設值為 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 = 10GiB、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：

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。

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lifs的DNS名稱、而非IP位址。

的最低組態 **<code>ontap-nas-economy</code>**

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

的最低組態 **<code>ontap-nas-flexgroup</code>**

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

SMB 磁碟區的最低組態

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
nasType: smb
securityStyle: ntfs
unixPermissions: ""
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

憑證型驗證

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_
```

自動匯出原則

本範例說明如何指示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：

```
---
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
```

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
```

使用 **SMB Volume** 的 **Amazon FSX for ONTAP**

- `smbShare` 使用 SMB 磁碟區的 ONTAP 需要 FSX 參數。

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

虛擬集區的後端範例

在下面顯示的後端定義檔案範例中、會針對所有儲存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。註解是在的 FlexVol 上設定 `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。

在這些範例中、有些儲存池是自行設定的 `spaceReserve`、 `spaceAllocation`和 `encryption` 值、而某些資源池會覆寫預設值。

ONTAP NAS 範例

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
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:
    department: legal
    creditpoints: '5000'
  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'
```

ONTAP NAS FlexGroup 範例

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
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'
```

ONTAP NAS 經濟效益範例

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
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:
    protection: bronze
    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'
```

將後端對應至StorageClass

請參閱下列 StorageClass 定義 [虛擬集區的後端範例]。使用 `parameters.selector` 欄位中、每個 StorageClass 都會呼叫哪些虛擬集區可用於主控磁碟區。磁碟區將會在所選的虛擬資源池中定義各個層面。

- 。 `protection-gold` StorageClass 會對應至中的第一個和第二個虛擬集區 `ontap-nas-flexgroup` 後端：這是唯一提供金級保護的資源池。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection=gold"
  fsType: "ext4"
```

- 。 `protection-not-gold` StorageClass 會對應至中的第三和第四個虛擬集區 `ontap-nas-flexgroup` 後端：這是唯一提供金級以外保護層級的資源池。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
```

- 。 `app-mysqldb` StorageClass 會對應至中的第四個虛擬集區 `ontap-nas` 後端：這是唯一為 mysqldb 類型應用程式提供儲存池組態的集區。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: netapp.io/trident
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
```

- t `protection-silver-creditpoints-20k` StorageClass 會對應至中的第三個虛擬集區 `ontap-nas-flexgroup` 後端：這是唯一提供銀級保護和 20000 個信用點數的資源池。

```
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"
```

- 。 `creditpoints-5k` StorageClass 會對應至中的第三個虛擬集區 `ontap-nas` 後端和中的第二個虛擬集區 `ontap-nas-economy` 後端：這是唯一擁有 5000 個信用點數的集區方案。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: netapp.io/trident
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"
```

Astra Trident將決定選取哪個虛擬集區、並確保符合儲存需求。

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。

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。

總覽

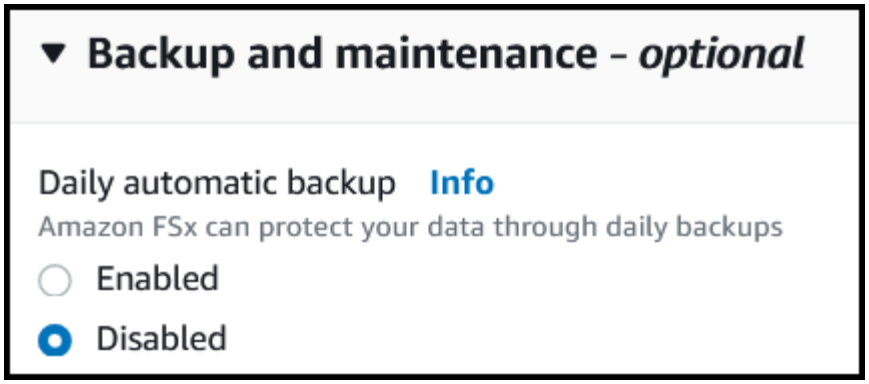
檔案系統是Amazon FSX的主要資源、類似ONTAP 於內部部署的一個叢集。在每個SVM中、您可以建立一個或多個磁碟區、這些磁碟區是儲存檔案系統中檔案和資料夾的資料容器。有了Amazon FSX for NetApp ONTAP 的功能、Data ONTAP 即可在雲端以託管檔案系統的形式提供支援。新的檔案系統類型稱為* NetApp ONTAP Sing*。

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。
- 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。

需求

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 `kubectl` 已安裝。
- 可從叢集工作節點存取的現有 Amazon FSX for NetApp ONTAP 檔案系統和儲存虛擬機器（ SVM ）。
- 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。

- Astra Trident僅支援安裝在Windows節點上執行的Pod上的SMB磁碟區。請參閱 準備配置SMB磁碟區 以取得詳細資料。

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-XXXXXXXXXXXXXXXXX.fs-XXXXXXXXXXXXXXXXX.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-XXXXXXXXXXXXXXXXX.fs-
XXXXXXXXXXXXXXXXX.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。

開始之前

在您使用配置 SMB 磁碟區之前、請先使用 `ontap-nas` 驅動程式、您必須具備下列項目。

- 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。

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`	您可以指定下列其中一項：使用Microsoft 管理主控台或 ONTAP CLI 建立的 SMB 共用名稱、或是允許 Astra Trident 建立 SMB 共用的名稱。 ONTAP 後端的 Amazon FSX 需要此參數。	`smb-share`
`nasType`	*必須設定為 `smb`.*如果為null、則預設為 `nfs`。	`smb`

參數	說明	範例
securityStyle	新磁碟區的安全樣式。 必須設定為 **ntfs** 或 **mixed** 適用於**SMB**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
storageDriverName	儲存驅動程式名稱	ontap-nas、 ontap-nas-economy、 ontap-nas-flexgroup、 ontap-san、 ontap-san-economy
backendName	自訂名稱或儲存後端	驅動程式名稱+「_」+ dataLIF
managementLIF	叢集或SVM管理LIF的IP位址 若要進行無縫 MetroCluster 移位、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]」

參數	說明	範例
dataLIF	傳輸協定LIF的IP位址。 不適用**NAS**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 。 《**SAN**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iSCI 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。	`false`
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	"
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。	

參數	說明	範例
`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。
`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 。 * 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、「方法」：true } 請勿使用 `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 nfs、 smb`或null。  *必須設定為 `smb 對於SMB Volume。*設定為null、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	您可以指定下列其中一項：使用 Microsoft 管理主控台或 ONTAP CLI 建立的 SMB 共用名稱、或是允許 Astra Trident 建立 SMB 共用的名稱。 ONTAP 後端的 Amazon FSX 需要此參數。	smb-share
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：	false

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。

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	`true`
`spaceReserve`	空間保留模式；「無」（精簡）或「Volume」（完整）	`none`
`snapshotPolicy`	要使用的Snapshot原則	`none`
`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` 是 `none`、`else` 「」
`splitOnClone`	建立複本時、從其父複本分割複本	`false`
`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： "Astra Trident如何與NVE和NAE搭配運作"。	`false`
`luksEncryption`	啟用LUKS加密。請參閱 "使用Linux統一金鑰設定（LUKS）"。 僅限 SAN 。	"
`tieringPolicy`	要使用的分層原則 `none`	`snapshot-only` 適用於 ONTAP 9.5 之前的 SVM-DR 組態

參數	說明	預設
unixPermissions	新磁碟區的模式。 如果是**SMB**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 預設值為 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"
```