



ASNAS驅動程式ONTAP

Trident

NetApp
February 02, 2026

目錄

ASNAS驅動程式ONTAP	1
ONTAP NAS 驅動程式概述	1
ONTAP NAS 驅動程式詳細資料	1
使用者權限	1
準備使用ONTAP 不含NAS的驅動程式來設定後端	2
需求	2
驗證 ONTAP 後端	2
管理NFS匯出原則	7
準備配置SMB磁碟區	10
列舉NAS組態選項與範例ONTAP	13
後端組態選項	13
用於資源配置磁碟區的後端組態選項	17
最低組態範例	19
虛擬集區的後端範例	23
將後端對應至StorageClass	29
更新 dataLIF 初始組態之後	30
安全 SMB 範例	31

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 驅動程式詳細資料

Trident 提供下列 NAS 儲存驅動程式、可與 ONTAP 叢集進行通訊。支援的存取模式包括：*ReadWriteOnce*（*rwo*）、*ReadOnlyMany*（*ROX*）、*_ReadWriteMany*（*rwX*）、*_ReadWriteOncePod*（*RWOP*）。

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-NAS」	NFS 中小企業	檔案系統	Rwo、ROX、rwX、RWOP	"、nfs、smb
《ONTAP-NANAS經濟》	NFS 中小企業	檔案系統	Rwo、ROX、rwX、RWOP	"、nfs、smb
「ONTAP-NAA-flexgroup」	NFS 中小企業	檔案系統	Rwo、ROX、rwX、RWOP	"、nfs、smb



- 使用 `ontap-san-economy` 只有持續磁碟區使用量計數預期會高於 "支援的 ONTAP Volume 限制"。
- 使用 `ontap-nas-economy` 只有持續磁碟區使用量計數預期會高於 "支援的 ONTAP Volume 限制" 和 `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、
- NetApp 不建議在所有 ONTAP 驅動程式中使用 FlexVol 自動擴充，ONTAP SAN 除外。作為因應措施，Trident 支援使用快照保留，並據此擴充 FlexVol 磁碟區。

使用者權限

Trident 預期會以 ONTAP 或 SVM 管理員的身分執行、通常使用叢集使用者或 `vsadmin` SVM 使用者、或是使用 ``admin`` 具有相同角色的不同名稱的使用者。

對於用於 NetApp ONTAP 部署的 Amazon FSX、Trident 預期會以 ONTAP 或 SVM 管理員的身分、使用叢集使用者或 `vsadmin` SVM 使用者、或是具有相同角色的不同名稱的使用者來執行 `fsxadmin`。``fsxadmin`` 使用者只能有限地取代叢集管理使用者。



如果您使用此 ``limitAggregateUsage`` 參數、則需要叢集管理權限。將 Amazon FSX for NetApp ONTAP 搭配 Trident 使用時、此 ``limitAggregateUsage`` 參數將無法與 ``fsxadmin`` 使用者帳戶搭配 ``vsadmin`` 使用。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。

從 25.10 版本開始，NetApp Trident支援"[NetApp AFX儲存系統](#)"。NetApp AFX 儲存系統與其他ONTAP系統（ASA、AFF和FAS）在儲存層的實作方式上有所不同。



只有 `ontap-nas` AFX 系統支援 NFS 協定驅動程式；不支援 SMB 協定。

在Trident後端設定中，您無需指定您的系統是 AFX。當您選擇 `ontap-nas` 作為 `storageDriverName` Trident可自動偵測 AFX 系統。

需求

- 對於所有 ONTAP 後端，Trident 要求至少將一個聚合分配給 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。
- Trident 僅支援掛載至 Windows 節點上執行的 Pod 的 SMB 磁碟區。如 [準備配置SMB磁碟區](#) 需詳細資訊、請參閱。

驗證 ONTAP 後端

Trident 提供兩種驗證 ONTAP 後端的模式。

- 認證型：此模式需要對 ONTAP 後端擁有足夠的權限。建議您使用與預先定義的安全登入角色相關聯的帳戶、例如 admin 或 vsadmin 以確保與ONTAP 更新版本的最大相容性。
- 憑證型：此模式需要在後端安裝憑證、Trident 才能與 ONTAP 叢集通訊。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

Trident 需要 SVM 範圍 / 叢集範圍管理員的認證、才能與 ONTAP 後端通訊。建議您使用標準的預先定義角色、例如 admin 或 vsadmin。如此可確保與未來 ONTAP 版本的前移相容性、這些版本可能會公開未來 Trident 版本所使用的功能 API。自訂安全登入角色可建立並搭配 Trident 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
credentials:
  name: secret-backend-creds
```

JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "credentials": {
    "name": "secret-backend-creds"
  }
}
```

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「cert」驗證方法的支援功能。

```
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「預設資料管理」。

```
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
NasBackend	ontap-nas	98e19b74-aec7-4a3d-8dcf-128e5033b214



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。成功的後端更新表示 Trident 可以與 ONTAP 後端通訊、並處理未來的 Volume 作業。

為 **Trident** 建立自訂 **ONTAP** 角色

您可以使用最低 Privileges 來建立 ONTAP 叢集角色、這樣就不需要使用 ONTAP 管理員角色來執行 Trident 中的作業。當您在 Trident 後端組態中包含使用者名稱時、Trident 會使用您建立的 ONTAP 叢集角色來執行作業。

如需建立 Trident 自訂角色的詳細資訊、請參閱["Trident 自訂角色產生器"](#)。

使用 ONTAP CLI

1. 使用下列命令建立新角色：

```
security login role create <role_name\> -cmddirname "command" -access all  
-vserver <svm_name\>
```

2. 為 Trident 使用者建立使用者名稱：

```
security login create -username <user_name\> -application ontapi  
-authmethod <password\> -role <name_of_role_in_step_1\> -vserver  
<svm_name\> -comment "user_description"
```

3. 將角色對應至使用者：

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod  
<password\>
```

使用 System Manager

在 ONTAP 系統管理員中執行下列步驟：

1. * 建立自訂角色 *：

- a. 若要在叢集層級建立自訂角色、請選取 * 叢集 > 設定 *。

(或) 若要在 SVM 層級建立自訂角色、請選取 * 儲存設備 > 儲存 VM > > required SVM 設定 > 使用者與角色 *。

- b. 選取 * 使用者和角色 * 旁的箭頭圖示 (* → *)。

- c. 在 * 角色 * 下選擇 **+Add**。

- d. 定義角色的規則、然後按一下 * 儲存 *。

2. * 將角色對應至 Trident 使用者 *：+ 在「* 使用者與角色 *」頁面上執行下列步驟：

- a. 在 * 使用者 * 下選取新增圖示 +。

- b. 選取所需的使用者名稱、然後在 * 角色 * 的下拉式功能表中選取角色。

- c. 按一下「* 儲存 *」。

如需詳細資訊、請參閱下列頁面：

- ["用於管理 ONTAP 的自訂角色"或"定義自訂角色"](#)
- ["與角色和使用者合作"](#)

管理 NFS 匯出原則

Trident 使用 NFS 匯出原則來控制對其所配置之磁碟區的存取。

Trident 在使用匯出原則時提供兩個選項：

- Trident 可以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。Trident 會在發佈時自動將屬於這些範圍的適用節點 IP 新增至匯出原則。或者、如果未指定 CIDR、則在要發佈的磁碟區所在節點上找到的所有全域範圍單點傳播 IP 都會新增至匯出原則。
- 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 Trident 會使用預設匯出原則。

動態管理匯出原則

Trident 提供動態管理 ONTAP 後端匯出原則的功能。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、這有助於將儲存叢集的存取限制在裝載磁碟區且指定範圍內有 IP 的工作節點、以支援精細且自動化的管理。



使用動態匯出原則時、請勿使用網路位址轉譯（NAT）。使用 NAT 時、儲存控制器會看到前端 NAT 位址、而非實際 IP 主機位址、因此在匯出規則中找不到相符項目時、就會拒絕存取。

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-economy
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、將 SVM 專用於 Trident。

以下是使用上述範例說明此功能的運作方式：

- `autoExportPolicy` 設定為 `true`。這表示 Trident 會為使用此後端為 SVM 佈建的每個 Volume 建立匯出原則 `svm1`、並使用位址區塊來處理規則的新增和刪除 `autoexportCIDRs`。在磁碟區附加至節點之前、該磁碟區會使用沒有規則的空匯出原則、以防止不必要的存取該磁碟區。當磁碟區發佈至節點 Trident 時、會建立一個匯出原則、其名稱與包含指定 CIDR 區塊內節點 IP 的基礎 `qtree` 相同。這些 IP 也會新增至父 FlexVol volume 所使用的匯出原則
 - 例如：
 - 後端 UUID 403b5326-8482-40der-96d0-d83fb3f4daec
 - `autoExportPolicy` 設定為 `true`

- 儲存字首 trident
- PVC UUID a79bcf5f-7b6d-4a40-9876-e2551f159c1c
- qtree 名稱為 Trident_PVC_a79bcf5f_7b6d_4a40_9876_e2551f159c1c FlexVol、會為命名的 qtree 建立匯出原則、為命名的 qtree 建立匯 trident-403b5326-8482-40db96d0-d83fb3f4daec 出原則、
`trident\_pvc\_a79bcf5f\_7b6d\_4a40\_9876\_e2551f159c1c` 以及在 SVM 上命名的空白匯出原則 `trident\_empty`。FlexVol 匯出原則的規則將是 qtree 匯出原則所包含的任何規則的超集。未附加的任何磁碟區都會重複使用空的匯出原則。
- `autoExportCIDRs` 包含位址區塊清單。此欄位為選用欄位、預設為「0.0.0.0/0」、「:/0」。如果未定義、Trident 會新增所有在工作節點上找到的全域範圍單點傳播位址、並提供出版物。

在此範例中 192.168.0.0/24、會提供位址空間。這表示位於此位址範圍內的 Kubernetes 節點 IP 與出版物將會新增至 Trident 所建立的匯出原則。當 Trident 登錄其執行的節點時，它會擷取節點的 IP 位址，並對照中提供的位址區塊進行檢查 autoExportCIDRs。在發佈時，在篩選 IP 之後，Trident 會為其所發佈節點的用戶端 IP 建立匯出原則規則。

您可以在建立後端後、更新「AutoExportPolicy」和「AutoExportCTR」。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。您也可以選擇停用後端的「autodportPolicy」、然後回到手動建立的匯出原則。這需要在後端組態中設定「exportPolicy」參數。

Trident 建立或更新後端之後、您可以使用或對應的 tridentbackend CRD 來檢查後端 tridentctl：

```
./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
```

移除節點時、Trident 會檢查所有匯出原則、以移除對應於節點的存取規則。透過從受管理後端的匯出原則中移除此節點 IP、Trident 可防止惡意掛載、除非叢集中的新節點重複使用此 IP。

對於先前存在的後端、使用更新後端 `tridentctl update backend` 可確保 Trident 自動管理匯出原則。這會在需要

時建立兩個以後端 UUID 和 qtree 名稱命名的新匯出原則。後端上的磁碟區會在新建立的匯出原則卸載並重新掛載之後、使用這些原則。



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、您必須在節點上重新啟動 Trident Pod。然後 Trident 會更新匯出原則、以反映其所管理的 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，才能為 ONTAP 內部部署叢集建立 `ontap-nas-economy` 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。



`'autoExportPolicy'` 不支援 SMB Volume。

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 2022的Windows工作節點。Trident 僅支援掛載至 Windows 節點上執行的 Pod 的 SMB 磁碟區。
- 至少有一個 Trident 機密包含您的 Active Directory 認證。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 Trident 可以為您建立 SMB 共用。



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 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。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
《生態樣式》	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。*	"

啟用安全 SMB

從 25.06 版本開始，NetApp Trident 支援使用以下方式建立的 SMB 磁碟區的安全性配置 `ontap-nas` 和 `ontap-nas-economy` 後端。啟用安全 SMB 後，您可以使用存取控制清單 (ACL) 為 Active Directory (AD) 使用者和使用者群組提供對 SMB 共用的受控存取。

值得記住的重點

- 輸入 `ontap-nas-economy` 不支援卷。
- 僅支援唯讀克隆 `ontap-nas-economy` 卷。
- 如果啟用了安全 SMB，Trident 將忽略後端提到的 SMB 共用。
- 更新 PVC 註解、儲存類別註解和後端欄位不會更新 SMB 共用 ACL。
- 克隆 PVC 註釋中指定的 SMB 共用 ACL 將優先於來源 PVC 中的 ACL。
- 啟用安全 SMB 時，請確保提供有效的 AD 使用者。無效使用者將不會被加入到 ACL。
- 如果您在後端、儲存類別和 PVC 中為同一個 AD 使用者提供不同的權限，則權限優先權為：PVC、儲存類別、後端。
- 安全 SMB 支持 `ontap-nas` 託管磁碟區匯入，不適用於非託管磁碟區匯入。

步驟

1. 在 TridentBackendConfig 中指定 adAdminUser，如下例所示：

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.193.176.x
  svm: svm0
  useREST: true
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

2. 在儲存類別中加入註解。

添加 `trident.netapp.io/smbShareAdUser` 註解到儲存類，以啟用安全 SMB 而不會失敗。為註釋指定的使用者值 `trident.netapp.io/smbShareAdUser` 應該與 `smbcreds` 秘密。您可以選擇以下其中之一 `smbShareAdUserPermission`： `full_control`， `change`， 或者 `read`。預設權限是 `full_control`。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

1. 建立PVC。

以下範例建立 PVC：

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/snapshotDirectory: "true"
    trident.netapp.io/smbShareAccessControl: |
      read:
        - tridentADtest
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

列舉NAS組態選項與範例ONTAP

瞭解如何在 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及將後端對應至 StorageClasses 的詳細資料。

從 25.10 版本開始，NetApp Trident 支持 ["NetApp AFX 儲存系統"](#)。NetApp AFX 儲存系統與其他基於ONTAP的系統（ASA、AFF和FAS）在儲存層的實作方式上有所不同。



只有 `ontap-nas` NetApp AFX 系統支援 NFS 協定驅動程式；不支援 SMB 協定。

在Trident後端設定中，無需指定您的系統是NetApp AFX 儲存系統。當您選擇 `ontap-nas` 作為 `storageDriverName` Trident會自動偵測 AFX 儲存系統。如下表所示，某些後端組態參數不適用於 AFX 儲存系統。

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
「分度」		永遠為1

參數	說明	預設
「storageDriverName」	儲存驅動程式名稱  僅適用於NetApp AFX 系統 `ontap-nas` 已支援。	ontap-nas、ontap-nas-economy、或 `ontap-nas-flexgroup`
「後端名稱」	自訂名稱或儲存後端	驅動程式名稱 + "_" + dataLIF
《馬納格門達利》	叢集或 SVM 管理 LIF 的 IP 位址可以指定完整網域名稱（FQDN）。如果使用 IPv6 旗標安裝 Trident、則可設定為使用 IPv6 位址。IPv6 位址必須以方括弧定義，例如 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。如需無縫 MetroCluster 之間的互通性MetroCluster 範例、請參閱。	"10.0.0.1"， "[2001:1234:abcd::fefe]"
「DataLIF」	傳輸協定LIF的IP位址。NetApp 建議指定 dataLIF。如果未提供，Trident 會從 SVM 擷取 dataLIFs。您可以指定完整網域名稱（FQDN），以用於 NFS 裝載作業，讓您建立循環 DNS，以便在多個 dataLIFs 之間進行負載平衡。可在初始設定之後變更。請參閱。如果使用 IPv6 旗標安裝 Trident、則可設定為使用 IPv6 位址。IPv6 位址必須以方括弧定義，例如 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。* MetroCluster 省略。*請參閱MetroCluster 範例。	指定位址或從SVM衍生（若未指定）（不建議使用）
《虛擬機器》	要使用的儲存虛擬機器 * MetroCluster 請省略。* 請參閱 MetroCluster 範例。	如果指定SVM "managementLIF"則衍生
「AutoExportPolicy」	啟用自動匯出原則建立及更新[布林值]。使用 `autoExportPolicy` 和 `autoExportCIDRs` 選項、Trident 可以自動管理匯出原則。	錯
《AutoExportCIDR》（自動匯出CTR）	將 Kubernetes 節點 IP 篩選在啟用時的 CIDR 清單 autoExportPolicy。使用 `autoExportPolicy` 和 `autoExportCIDRs` 選項、Trident 可以自動管理匯出原則。	["0.0.0/0"、":/0"]
《標籤》	套用到磁碟區的任意JSON-格式化標籤集	"
「用戶端憑證」	用戶端憑證的Base64編碼值。用於憑證型驗證	"
「clientPrivate Key」	用戶端私密金鑰的Base64編碼值。用於憑證型驗證	"
「可信賴的CACertificate」	受信任CA憑證的Base64編碼值。選用。用於憑證型驗證	"
《使用者名稱》	用於連接到叢集/SVM 的使用者名稱。用於基於憑證的身份驗證。有關 Active Directory 驗證，請參閱 " 使用 Active Directory 憑證向後端 SVM 驗證Trident 的身份 "。	

參數	說明	預設
密碼	連接到叢集/SVM 的密碼。用於基於憑證的身份驗證。有關 Active Directory 驗證，請參閱 "使用 Active Directory 憑證向後端 SVM 驗證 Trident 的身份" 。	
「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  使用 ONTAP NAS 經濟型和 24 個以上字元的 storagePrefix 時，qtree 將不會內嵌儲存前置字元，不過它會位於磁碟區名稱中。	" Trident "
《Aggregate》	用於資源配置的Aggregate（選用；如果已設定、則必須指派給SVM）。對於 `ontap-nas-flexgroup` 驅動程式、此選項會被忽略。如果未指派、任何可用的集合體都可用於佈建 FlexGroup Volume 。  在 SVM 中更新 Aggregate 時、它會透過輪詢 SVM 而無需重新啟動 Trident 控制器、在 Trident 中自動更新。當您在 Trident 中設定特定的 Aggregate 以配置 Volume 時、如果將 Aggregate 重新命名或移出 SVM 、則在輪詢 SVM Aggregate 時、後端將會移至 Trident 中的失敗狀態。您必須將 Aggregate 變更為 SVM 上的 Aggregate 、或是將其全部移除、才能使後端重新上線。 *請勿指定用於 AFX 儲存系統。 *	"
「限制Aggregateusage」	如果使用率超過此百分比，則配置失敗。不適用於 Amazon FSx for ONTAP 。*請勿指定用於 AFX 儲存系統。 *	""（預設不強制執行）

參數	說明	預設
FlexgroupAggregateList	用於資源配置的集合體清單（選用；如果已設定、則必須指派給 SVM）。指派給 SVM 的所有集合體都會用於佈建 FlexGroup Volume。支援 * ONTAP NAS FlexGroup * 儲存驅動程式。  在 SVM 中更新 Aggregate 清單時、會透過輪詢 SVM 而無需重新啟動 Trident 控制器、自動在 Trident 中更新清單。當您在 Trident 中設定特定的 Aggregate 清單來配置 Volume 時、如果將 Aggregate 清單重新命名或移出 SVM、則在輪詢 SVM Aggregate 時、後端將會移至 Trident 中的失敗狀態。您必須將 Aggregate 清單變更為 SVM 上的集合清單、或是將其全部移除以使後端重新上線。	"
《限制Volume大小》	如果請求的磁碟區大小大於此值，則配置失敗。	""（預設不會強制執行）
「DebugTraceFlags」	疑難排解時要使用的偵錯旗標。例如、 { "api" : false 、 "method" : 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	配置 NFS 或 SMB 磁碟區的建立。選項有 nfs，`smb` 或空值。設定為 null 則預設使用 NFS 磁碟區。如果指定，則始終設定為 `nfs` 適用於 AFX 儲存系統。	nfs
「nfsMountOptions」	以逗號分隔的NFS掛載選項清單。Kubernetes-Persistent Volume 的掛載選項通常是在儲存類別中指定、但如果儲存類別中未指定掛載選項、則 Trident 會回復為使用儲存後端組態檔案中指定的掛載選項。如果儲存類別或組態檔案中未指定任何掛載選項、Trident 將不會在關聯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 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。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

參數	說明	預設
《useREST》	使用ONTAP REST API 的布林參數。`useREST`設定為 `true` Trident使用ONTAP REST API 與後端通訊；當設定為 `false` Trident使用 ONTAPI (ZAPI) 呼叫與後端通訊。此功能需要ONTAP 9.11.1 及更高版本。此外，所使用的ONTAP登入角色必須具有存取權限。`ontapi`應用。預定義項滿足了這一點。`vsadmin`和`cluster-admin`角色。從Trident 24.06 版本和ONTAP 9.15.1 或更高版本開始，`useREST`設定為 `true`預設；更改 `useREST`到 `false`使用 ONTAPI (ZAPI) 呼叫。如果指定，則始終設定為 true 適用於 AFX 儲存系統。	true 對於 ONTAP 9.15.1 或更高版本，否則 false。
limitVolumePoolSize	在 ONTAP NAS 經濟型後端使用 qtree 時、可要求的 FlexVol 大小上限。	""（預設不強制執行）
denyNewVolumePools	限制 `ontap-nas-economy`後端建立新的 FlexVol 磁碟區以包含其 qtree。只有預先存在的 FlexVols 可用於佈建新的 PV。	
adAdminUser	具有 SMB 共用完全存取權限的 Active Directory 管理員使用者或使用者群組。使用此參數可為 SMB 共用提供具有完全控制權的管理員權限。	

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
"paceAllocate（配置）"	qtree 的空間分配	"對"
《保護區》	空間保留模式；「無」（精簡）或「Volume」（粗）	"無"
「快照原則」	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。	"
「快照保留區」	保留給快照的磁碟區百分比	「0」如果 snapshotPolicy 為「無」、否則為「」
「PlitOnClone」	建立複本時、從其父複本分割複本	"假"
加密	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 Trident 中配置的任何 Volume 都將啟用 NAE。如需更多資訊、請參閱 "Trident 如何與 NVE 和 NAE 搭配運作" ：	"假"
「分層政策」	分層原則以使用「無」	

參數	說明	預設
「unixPermissions」	新磁碟區的模式	"777" 表示 NFS 磁碟區；SMB 磁碟區為空的（不適用）
「snapshotDir」	控制對的存取 .snapshot 目錄	針對 NFSv3 的 NFSv4 "false" 為 "true"
「匯出政策」	要使用的匯出原則	"預設"
《生態樣式》	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。
nameTemplate	建立自訂磁碟區名稱的範本。	"



搭配 Trident 使用 QoS 原則群組需要 ONTAP 9.8 或更新版本。您應該使用非共用的 QoS 原則群組、並確保個別將原則群組套用至每個成員。共享 QoS 原則群組會強制執行所有工作負載總處理量的上限。

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"

```

為了 ontap-nas`和 `ontap-nas-flexgroups`Trident現在使用新的計算方法，以確保FlexVol 的尺寸

與 `snapshotReserve` 百分比和 PVC 正確匹配。當使用者要求 PVC 時，Trident 會使用新的計算方法建立具有更多空間的原始 FlexVol。此計算可確保使用者在 PVC 中獲得其請求的可寫入空間，而不是少於其請求的空間。在 v21.07 之前，當使用者要求 PVC（例如 5 GiB）時，如果快照預留百分比為 50%，則只能獲得 2.5 GiB 的可寫入空間。這是因為使用者要求的是整個磁碟區。`snapshotReserve` 是其中的百分比。在 Trident 21.07 中，使用者要求的是可寫入空間，而 Trident 定義了該空間。`snapshotReserve` 將數值表示為佔總體積的百分比。這不適用於 `ontap-nas-economy`。請參閱以下範例以了解其工作原理：

計算方式如下：

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

對於快照預留 = 50% 且 PVC 請求 = 5 GiB 的情況，總磁碟區大小為 $5 / 0.5 = 10$ GiB，可用大小為 5 GiB，這正是使用者在 PVC 請求中請求的大小。`volume show` 命令應顯示與此範例類似的結果：

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.

升級 Trident 時，先前安裝的現有後端將以上述方式設定磁碟區。對於升級前建立的捲，您應該調整其大小以觀察到變更。例如，一個 2 GiB 的 PVC 包含 `snapshotReserve=50` 先前的結果是卷提供了 1 GiB 的可寫空間。例如，將磁碟區大小調整為 3 GiB，將在 6 GiB 的磁碟區上為應用程式提供 3 GiB 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。

ONTAP NAS 經濟效益範例

```
---
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 FlexGroup 範例

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

MetroCluster 範例

您可以設定後端、避免在切換和切換期間手動更新後端定義 "SVM 複寫與還原"。

若要無縫切換和切換、請使用指定 SVM managementLIF 並省略 dataLIF 和 svm 參數。例如：

```
---  
version: 1  
storageDriverName: ontap-nas  
managementLIF: 192.168.1.66  
username: vsadmin  
password: password
```

SMB Volume 範例

```
---  
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
```

憑證型驗證範例

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_
```

自動匯出原則範例

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

```
---
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
```

IPv6 位址範例

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
```

Amazon FSX for ONTAP 使用 SMB Volume 範例

- 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_
```



```
---
version: 1
storageDriverName: ontap-nas
backendName: ontap-nas-backend
managementLIF: <ip address>
svm: svm0
username: <admin>
password: <password>
defaults:
  nameTemplate:
    "{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.vo\
      lume.RequestName}}"
labels:
  cluster: ClusterA
PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"
```

虛擬集區的后端範例

在下面顯示的后端定義檔案範例中、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。

Trident 會在「意見」欄位中設定資源配置標籤。註解是在 `FlexVol for` 或 `FlexGroup for ontap-nas-flexgroup` 上設定 `ontap-nas`。Trident 會在資源配置時、將虛擬集區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。

```

---
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: mysqlldb
    cost: "25"
    zone: us_east_1d
    defaults:
      spaceReserve: volume
      encryption: "false"
      unixPermissions: "0775"
```

```

---
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"
```

```

---
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 [\[虛擬集區的后端範例\]](#)。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: csi.trident.netapp.io
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: csi.trident.netapp.io
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: csi.trident.netapp.io
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"

```

- `tprotection-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: csi.trident.netapp.io
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: csi.trident.netapp.io
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

Trident 會決定要選取哪個虛擬集區、並確保符合儲存需求。

更新 dataLIF 初始組態之後

您可以在初始設定後變更 dataLIF，方法是執行下列命令，以更新的 dataLIF 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 PVCS 連接到一個或多個 Pod，您必須關閉所有對應的 Pod，然後重新啟動，新的 dataLIF 才會生效。

安全 SMB 範例

使用 **ontap-nas** 驅動程式的後端配置

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

使用 **ontap-nas-economy** 驅動程式的後端配置

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas-economy
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

具有儲存池的後端配置

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm0
  useREST: false
  storage:
    - labels:
        app: msoffice
      defaults:
        adAdminUser: tridentADuser
  nasType: smb
  credentials:
    name: backend-tbc-ontap-invest-secret

```

採用 **ontap-nas** 驅動程式的儲存類別範例

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADtest
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate

```



確保添加 `annotations` 啟用安全 SMB。如果沒有註釋，安全 SMB 就無法運作，無論後端或 PVC 中設定了什麼配置。

採用 **ontap-nas-economy** 驅動程式的儲存類別範例

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser3
parameters:
  backendType: ontap-nas-economy
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

具有單一 **AD** 使用者的 **PVC** 範例

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      change:
        - tridentADtest
      read:
        - tridentADuser
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

具有多個 **AD** 使用者的 **PVC** 範例

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-test-pvc
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      full_control:
        - tridentTestuser
        - tridentuser
        - tridentTestuser1
        - tridentuser1
      change:
        - tridentADuser
        - tridentADuser1
        - tridentADuser4
        - tridentTestuser2
      read:
        - tridentTestuser2
        - tridentTestuser3
        - tridentADuser2
        - tridentADuser3
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
```

版權資訊

Copyright © 2026 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。