



ONTAP NAS 驅動程式

Trident

NetApp
October 30, 2026

目錄

ONTAP NAS 驅動程式	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 NAS 驅動程式設定後端	2
需求	2
驗證 ONTAP 後端	2
管理 NFS 匯出原則	7
準備配置 SMB Volume	9
ONTAP NAS 設定選項和範例	13
後端組態選項	13
磁碟區配置的後端組態選項	17
最小組態範例	19
具有虛擬資源池的後端範例	22
將後端對應至 StorageClasses	26
初始配置後更新 dataLIF	28
安全 SMB 範例	28

ONTAP NAS 驅動程式

ONTAP NAS 驅動程式概述

了解如何使用 ONTAP 和 Cloud Volumes ONTAP NAS 驅動程式設定 ONTAP 後端。

ONTAP NAS 驅動程式詳細資料

Trident 提供以下 NAS 儲存驅動程式、用於與 ONTAP 叢集通訊。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	volumeMode	支援的存取模式	支援的檔案系統
ontap-nas	NFS SMB	檔案系統	RWO、ROX、RWX、RWOP	"", nfs, smb
ontap-nas-economy	NFS SMB	檔案系統	RWO、ROX、RWX、RWOP	"", nfs, smb
ontap-nas-flexgroup	NFS SMB	檔案系統	RWO、ROX、RWX、RWOP	"", nfs, smb



- 僅當預期持久性磁碟區使用次數高於"支援的 ONTAP Volume 限制"時，才使用 `ontap-san-economy`。
- 僅當預期持久性磁碟區使用次數高於"支援的 ONTAP Volume 限制"且無法使用 `ontap-san-economy` 驅動程式時，才使用 `ontap-nas-economy`。
- 如果您預計需要資料保護、災難復原或行動性，請勿使用 `ontap-nas-economy`。
- NetApp 除 `ontap-san` 外，不建議在所有 ONTAP 驅動程式中使用 Flexvol 自動增長功能。作為變通方案，Trident 支援使用快照預留，並相應地擴展 Flexvol 磁碟區。

使用者權限

Trident 需要以 ONTAP 或 SVM 管理員身分執行，通常使用 ``admin`` 叢集使用者或 ``vsadmin`` SVM 使用者，或使用具有相同角色但名稱不同的使用者。

對於 Amazon FSx for NetApp ONTAP 部署，Trident 需要以 ONTAP 或 SVM 管理員身分執行，使用叢集 ``fsxadmin`` 使用者或 ``vsadmin`` SVM 使用者，或使用具有相同角色但名稱不同的使用者。``fsxadmin`` 使用者是叢集管理使用者的有限替代方案。



如果使用 ``limitAggregateUsage`` 參數，則需要叢集管理員權限。將 Amazon FSx for NetApp ONTAP 與 Trident 搭配使用時，``limitAggregateUsage`` 參數與 ``vsadmin`` 和 ``fsxadmin`` 使用者帳戶不相容。如果指定此參數，組態作業將失敗。

雖然可以在 ONTAP 中建立更嚴格的角色供 Trident 驅動程式使用，但我們不建議這樣做。大多數新版本的 Trident 都會呼叫額外的 API，這些 API 需要考慮，這會讓升級變得困難且容易出錯。

準備使用 ONTAP NAS 驅動程式設定後端

了解使用 ONTAP NAS 驅動程式配置 ONTAP 後端的要求、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。在 Trident 後端組態中、您無需指定系統為 AFX。當您選擇 `ontap-nas` 作為 `storageDriverName` 時、Trident 會自動偵測 AFX 系統。



AFX 系統僅支援 `ontap-nas` 驅動程式（使用 NFS 協定）；不支援 SMB 協定。

需求

- 對於所有 ONTAP 後端、Trident 要求至少將一個 Aggregate 指派給 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驅動程式的儲存類別。例如，您可以設定使用 `ontap-nas` 驅動程式的 Gold 類別和使用 `ontap-nas-economy` 驅動程式的 Bronze 類別。
- 所有 Kubernetes 工作節點都必須安裝適當的 NFS 工具。如需詳細資訊，請參閱 ["這裡"](#)。
- Trident 僅支援掛載到在 Windows 節點上執行的 Pod 的 SMB 磁碟區。如需詳細資訊，請參閱 [準備配置 SMB Volume](#)。

驗證 ONTAP 後端

Trident 提供兩種 ONTAP 後端驗證模式。

- 基於憑證：此模式需要對 ONTAP 後端擁有足夠的權限。建議使用與預先定義安全登入角色關聯的帳戶，例如 `admin`` 或 ``vsadmin`，以確保與 ONTAP 版本的最大相容性。
- 基於憑證：此模式要求在後端安裝憑證，以便 Trident 與 ONTAP 叢集通訊。在這種情況下，後端定義必須包含客戶端憑證、金鑰以及受信任 CA 憑證（如果使用，建議）的 Base64 編碼值。

您可以更新現有後端，以在基於認證和基於憑證的方法之間移動。但是，一次只支援一種驗證方法。若要切換到不同的驗證方法，您必須從後端組態中移除現有方法。



如果您嘗試同時提供憑證和憑證，則後端建立將會失敗，並出現錯誤，提示組態檔中提供了多個驗證方法。

啟用基於認證的驗證

Trident 需要 SVM 範圍 / 叢集範圍的管理員憑證才能與 ONTAP 後端通訊。建議使用標準預先定義的角色，例如 `admin`` 或 ``vsadmin`。這可確保與未來 ONTAP 版本向前相容，因為未來版本可能會公開供 Trident 版本使用的功能 API。雖然可以建立自訂安全登入角色並將其與 Trident 搭配使用，但不建議這樣做。

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"
  }
}
```

請注意，後端定義是唯一以純文字形式儲存認證資料的地方。建立後端之後，使用者名稱 / 密碼會使用 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，這是僅限管理員執行的作業，由 Kubernetes/ 儲存管理員執行。

啟用基於憑證的驗證

新建和現有後端都可以使用憑證與 ONTAP 後端通訊。後端定義需要三個參數。

- `clientCertificate`：用戶端憑證的 Base64 編碼值。
- `clientPrivateKey`：關聯私密金鑰的 Base64 編碼值。
- `trustedCACertificate`：受信任 CA 憑證的 Base64 編碼值。如果使用受信任的 CA，則必須提供此參數。如果未使用受信任的 CA，則可以忽略此參數。

典型的工作流程包括以下步驟。

步驟

1. 產生客戶端憑證和金鑰。產生時，將 Common Name (CN) 設定為要進行驗證的 ONTAP 使用者。

```
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 憑證新增至 ONTAP 叢集。儲存管理員可能已經處理此作業。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 叢集上安裝用戶端憑證和金鑰（來自步驟 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 安全登入角色支援 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。將 <ONTAP Management LIF> 和 <vserver name> 替換為 Management LIF IP 和 SVM 名稱。您必須確保 LIF 的服務原則已設為 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 對憑證、金鑰和受信任的 CA 憑證進行編碼。

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

7. 使用上一步獲得的值建立後端。

```
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 |
+-----+-----+-----+-----+
+-----+-----+

```

更新驗證方法或輪換認證資料

您可以更新現有後端以使用不同的身份驗證方法或輪換其憑證。此操作雙向有效：使用使用者名稱 / 密碼的後端可以更新為使用憑證；使用憑證的後端可以更新為基於使用者名稱 / 密碼的身份驗證。為此，您必須移除現有的身份驗證方法並新增新的身份驗證方法。然後使用包含所需參數的更新後的 backend.json 檔案來執行 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

```
STATE | VOLUMES |
online | 9 |
```



輪換密碼時，儲存管理員必須先更新 ONTAP 上使用者的密碼。之後，後端需要進行更新。輪換證書時，可以為該使用者新增多個證書。後端隨後會更新以使用新證書，之後即可從 ONTAP 叢集中刪除舊證書。

更新後端不會中斷對已建立磁碟區的存取，也不會影響之後建立的磁碟區連線。後端更新成功表示 Trident 可以與 ONTAP 後端通訊並處理未來的磁碟區作業。

為 Trident 建立自訂 ONTAP 角色

您可以建立一個具有最低權限的 ONTAP 叢集角色，這樣您就不必使用 ONTAP 管理員角色在 Trident 中執行操作。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 叢集角色來執行操作。

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. 使用以下命令建立新角色：

```
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 System Manager 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 **Cluster > Settings**。

(或) 若要在 SVM 層級建立自訂角色、請選取 **Storage > Storage VMs > required SVM > Settings > Users and Roles**。
 - b. 選擇 **Users and Roles** 旁邊的箭頭圖示 (→)。
 - c. 在 **Roles** 下選擇 **+Add**。
 - d. 定義角色規則，然後點選 **Save**。
2. 將角色對應到 Trident 使用者：+ 在 **Users and Roles** 頁面上執行下列步驟：
 - a. 在 **Users** 下方選擇 Add 圖示 +。
 - b. 選擇所需的使用者名稱，然後在 **Role** 下拉式選單中選擇角色。
 - c. 按一下 **Save**。

如需更多資訊、請參閱下列頁面：

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

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 在處理匯出原則時提供兩種選項：

- Trident 可以動態管理匯出策略；在這種模式下，儲存管理員指定 CIDR 區塊列表，這些 CIDR 區塊代表允許的 IP 位址。Trident 會在發佈時自動將落入這些範圍內的適用節點 IP 位址新增至匯出策略。或者，如果沒有指定 CIDR，則會將磁碟區發佈到的節點上找到的所有全域作用域單播 IP 位址新增至匯出策略。
- 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 會使用預設的匯出原則。

動態管理匯出原則

Trident 提供了動態管理 ONTAP 後端匯出原則的功能。這使得儲存管理員能夠為工作節點 IP 指定允許的位址空間，而無需手動定義明確規則。這大大簡化了匯出原則的管理；對匯出原則的修改不再需要在儲存叢集上進行手動干預。此外，這還有助於將對儲存叢集的存取限制在僅掛載磁碟區且 IP 位址在指定範圍內的工作節點上，從而支援精細和自動化管理。



使用動態匯出策略時，請勿使用網路位址轉換（NAT）。啟用 NAT 後，儲存控制器看到的是前端 NAT 位址，而不是實際的 IP 主機位址，因此，如果在匯出規則中找不到符合項，則會拒絕存取。

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，必須確保 SVM 中的根接合點已預先建立匯出原則，且該原則包含允許節點 CIDR 區塊的匯出規則（例如預設匯出原則）。請務必遵循 NetApp 建議的最佳實務做法，為 Trident 專用 SVM。

以下以上述範例為例、說明此功能的工作原理：

- autoExportPolicy 已設定為 true。這表示 Trident 會為使用此後端為 svm1 SVM 配置的每個磁碟區建立一個匯出策略，並使用 autoexportCIDRs 位址區塊處理規則的新增和刪除。在磁碟區連接到節點之前，該磁碟區使用一個空的匯出策略，其中沒有任何規則來防止對該磁碟區的未經授權的存取。當磁碟區發佈到節點時，Trident 會建立一個與底層 qtree 同名的匯出策略，該 qtree 包含指定 CIDR 區塊內的節點 IP 位址。這些 IP 位址也會加入到父 FlexVol 磁碟區使用的匯出策略中。
 - 例如：
 - 後端 UUID 403b5326-8482-40db-96d0-d83fb3f4daec
 - autoExportPolicy 設定為 true
 - 儲存前置詞 trident
 - PVC UUID a79bcf5f-7b6d-4a40-9876-e2551f159c1c
 - 名為 trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c 的 qtree 會為名為 `trident-403b5326-8482-40db96d0-d83fb3f4daec` 的 FlexVol 建立匯出原則、為名為 `trident\_pvc\_a79bcf5f\_7b6d\_4a40\_9876\_e2551f159c1c` 的 qtree 建立匯出原則，並在 SVM 上建立名為 `trident\_empty` 的空白匯出原則。FlexVol 匯出原則的規則將是 qtree 匯出原則中所含任何規則的超集。未附加的磁碟區將重複使用空白匯出原則。
- autoExportCIDRs 包含地址塊列表。此字段為可選字段，預設值為 ["0.0.0.0/0", ":::/0"]。如果未定義，Trident 會新增在已發佈訊息的工作節點上找到的所有全域作用域單播位址。

在本例中，提供了 192.168.0.0/24 位址空間。這表示位於此位址範圍內且具有發佈的 Kubernetes 節點 IP 將新增至 Trident 建立的匯出原則。當 Trident 註冊其執行所在的節點時，會擷取該節點的 IP 位址，並根據 autoExportCIDRs 中提供的位址區塊進行檢查。在發佈時，篩選 IP 後，Trident 會為其發佈目標節點的用戶端 IP 建立匯出原則規則。

建立後端後，您可以更新其 autoExportPolicy 和 autoExportCIDRs。您可以為自動管理的後端附加新

的 CIDR 或刪除現有的 CIDR。刪除 CIDR 時請務必小心，以確保現有連線不會中斷。您也可以選擇停用後端的 `autoExportPolicy`，並回退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 建立或更新後端後、您可以使用 `tridentctl` 或對應的 `tridentbackend` CRD 來檢查後端：

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

當節點被移除時、Trident 會檢查所有匯出原則、以移除與該節點對應的存取規則。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 `tridentctl update backend` 更新後端可確保 Trident 自動管理匯出原則。這會在需要時建立兩個新的匯出原則，分別以後端的 UUID 和 `qtree` 名稱命名。後端上的磁碟區在卸載並重新掛載後，將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刪除動態建立的匯出原則。如果重新建立該後端，則會將其視為新後端，並建立新的匯出原則。

如果正在執行中的節點的 IP 位址更新，您必須重新啟動該節點上的 Trident pod。Trident 隨後會更新其管理的後端匯出原則，以反映此 IP 位址變更。

準備配置 SMB Volume

稍加準備，即可使用 `ontap-nas` 驅動程式配置 SMB Volume。



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。若未設定其中任一通訊協定，將導致 SMB Volume 建立失敗。



autoExportPolicy 不支援 SMB 磁碟區。

開始之前

在配置 SMB 磁碟區之前、您必須具備以下條件。

- Kubernetes 叢集包含一個 Linux 控制器節點和至少一個執行 Windows Server 2022 的 Windows 工作節點。Trident 僅支援掛載到在 Windows 節點上執行的 Pod 的 SMB 磁碟區。
- 至少需要一個包含您的 Active Directory 憑證的 Trident 金鑰。要產生金鑰 smbcreds：

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

- CSI Proxy 設定為 Windows 服務。若要設定 csi-proxy，請參閱["GitHub：CSI Proxy"](#)或["GitHub：適用於 Windows 的 CSI Proxy"](#)以瞭解在 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 共用區、或 Trident 可以為您建立一個。



Amazon FSx for ONTAP 需要 SMB 共用。

您可以透過兩種方式建立 SMB 管理共用：使用 ["Microsoft Management Console"](#) 共用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、請建立共用區的目錄路徑結構。

此 `vserver cifs share create` 指令會檢查在建立共用時透過 `-path` 選項指定的路徑。如果指定的路徑不存在，則命令執行失敗。

- b. 建立與指定 SVM 相關聯的 SMB 共用：

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

- c. 確認共用已建立：

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



詳情請參閱 ["建立 SMB 共用區"](#)。

2. 建立後端時，必須配置以下內容以指定 SMB 磁碟區。有關所有 FSx for ONTAP 後端設定選項，請參閱 ["FSx for ONTAP 設定選項和範例"](#)。

參數	說明	範例
smbShare	您可以指定以下選項之一：使用 Microsoft Management Console 或 ONTAP CLI 建立的 SMB 共用名稱；允許 Trident 建立 SMB 共用的名稱；或者您可以將此參數留空以封鎖對磁碟區的公共共用存取。對於內部部署 ONTAP，此參數為選用項目。對於 Amazon FSx for ONTAP 後端，此參數為必要項目且不能為空白。	smb-share
nasType	* 必須設為 smb。*如果為 null，則預設為 nfs。	smb
securityStyle	新磁碟區的安全樣式。對於 SMB 磁碟區，必須設定為 ntfs 或 mixed 。	ntfs 或 mixed 適用於 SMB 磁碟區
unixPermissions	新磁碟區的模式。 SMB 磁碟區必須保留空白。	""

啟用安全的 SMB

從 25.06 版本開始，NetApp Trident 支援使用 `ontap-nas` 和 `ontap-nas-economy` 後端建立的 SMB 磁碟區的安全性資源配置。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 共用的受控存取權限。

要記住的要點

- 不支援匯入 `ontap-nas-economy` 磁碟區。
- `ontap-nas-economy` 磁碟區僅支援唯讀複本。
- 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。
- 複製 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 中。
- 如果在後端、儲存類別和 PVC 中為同一個 AD 使用者提供不同的權限，則權限優先順序為：PVC、儲存類別，然後是後端。
- 安全 SMB 支援 `ontap-nas` 託管磁碟區匯入，但不適用於非託管磁碟區匯入。

步驟

1. 請在 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. 在儲存類別中新增註解。

將 `trident.netapp.io/smbShareAdUser` 註解新增至儲存類別，以啟用安全 SMB 而不會失敗。為註解 `trident.netapp.io/smbShareAdUser` 指定的使用者值應與 `smbcreds` 密鑰中指定的使用者名稱相同。您可以為 `smbShareAdUserPermission` 選擇下列其中一項：`full_control`、`change` 或 `read`。預設權限為 `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

```

ONTAP NAS 設定選項和範例

在 Trident 安裝中建立和使用 ONTAP NAS 驅動程式。本節提供後端組態範例，以及將後端映射至 StorageClasses 的詳細資訊。從 25.10 版本開始，NetApp Trident 支援["NetApp AFX 儲存系統"](#)。NetApp AFX 儲存系統與其他基於 ONTAP 的系統（ASA、AFF 和 FAS）在儲存層的實作上有所不同。



僅支援 ontap-nas 驅動程式（使用 NFS 協定）用於 NetApp AFX 系統；不支援 SMB 協定。

後端組態選項

在 Trident 後端組態中，您不需要指定系統是 NetApp AFX 儲存系統。當您選取 `ontap-nas` 作為 `storageDriverName` 時，Trident 會自動偵測 AFX 儲存系統。部分後端組態參數不適用於 AFX 儲存系統。

從 26.06 版本開始，您可以啟用 ONTAP 均衡放置，以便 ONTAP 為新 Volume 選擇彙總。ONTAP 9.19.1 或更新版本上的 AFX 儲存系統需要啟用均衡放置功能。請參閱 ["使用 ONTAP 後端進行均衡放置"](#) 以瞭解需求和範例。

下表顯示後端組態選項：

參數	說明	預設
version		始終為 1
storageDriverName	<p>儲存設備驅動程式的名稱。</p> <p>建立後無法修改。若要更新此參數，必須建立新的後端。</p> <div> <p>對於 NetApp AFX 系統，僅支援 ontap-nas。</p> </div>	ontap-nas、ontap-nas-economy 或 ontap-nas-flexgroup
backendName	自訂名稱或儲存後端	驅動程式名稱 + "_" + dataLIF
managementLIF	<p>叢集或 SVM 管理 LIF 的 IP 位址，可以指定完整網域名稱（FQDN）。如果 Trident 是使用 IPv6 旗標安裝的，則可以設定為使用 IPv6 位址。IPv6 位址必須用方括號定義，例如</p> <p>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。如需無縫 MetroCluster 切換，請參閱 MetroCluster 範例。</p>	"10.0.0.1", "[2001:1234:abcd::fefe]"

參數	說明	預設
dataLIF	協定 LIF 的 IP 位址。NetApp 建議指定 dataLIF。如果未提供，Trident 將從 SVM 取得 dataLIF。您可以指定一個完全限定網域名稱 (FQDN) 用於 NFS 掛載作業，從而建立輪詢 DNS 以在多個 dataLIF 之間進行負載平衡。初始設定後可以變更。請參閱。如果 Trident 是使用 IPv6 旗標安裝的，則可以設定為使用 IPv6 位址。IPv6 位址必須用方括號定義，例如 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。*對於 MetroCluster，請省略此參數。*請參閱 MetroCluster 範例 。	指定的位址或從 SVM 衍生（如果未指定）（不建議）
svm	要使用的儲存虛擬機器 *MetroCluster 除外。*請參閱 MetroCluster 範例 。	如果指定了 managementLIF SVM，則衍生
autoExportPolicy	啟用自動匯出原則建立和更新 [布林值]。使用 `autoExportPolicy` 和 `autoExportCIDRs` 選項，Trident 可以自動管理匯出原則。	錯誤
autoExportCIDRs	啟用 `autoExportPolicy` 時用於篩選 Kubernetes 節點 IP 的 CIDR 清單。使用 `autoExportPolicy` 和 `autoExportCIDRs` 選項，Trident 可以自動管理匯出原則。	["0.0.0.0/0", ":::/0"]
labels	要套用於磁碟區的任意 JSON 格式標籤集	""
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	用於連接叢集 / SVM 的使用者名稱。用於基於憑證的驗證。有關 Active Directory 驗證、請參閱 "使用 Active Directory 憑證對後端 SVM 進行 Trident 驗證" 。	
password	連接到叢集 / SVM 的密碼。用於基於憑證的驗證。有關 Active Directory 驗證、請參閱 "使用 Active Directory 憑證對後端 SVM 進行 Trident 驗證" 。	
storagePrefix	在 SVM 中為新 Volume 進行資源配置時所使用的前置詞。設定後無法更新  當使用 ontap-nas-economy 且 storagePrefix 為 24 個或更多字元時，qtree 中不會嵌入儲存設備前綴，但它存在於 Volume 名稱中。	"Trident"

參數	說明	預設
aggregate	<p>用於資源配置的彙總（可選；如果設定，則必須指派給 SVM）。對於 `ontap-nas-flexgroup` 驅動程式，此選項將被忽略。如果未指派，則可以使用任何可用的彙總來資源配置 FlexGroup Volume。</p> <div>  <p>當 SVM 中的彙總更新時，Trident 會自動輪詢 SVM 並更新，無需重新啟動 Trident 控制器。如果您已在 Trident 中設定了特定的彙總來資源配置 Volume，且該彙總被重新命名或從 SVM 移出，則在輪詢 SVM 彙總時，Trident 中的後端將進入故障狀態。您必須將該彙總變更為 SVM 中存在的彙總，或將其完全移除，才能使後端恢復線上。</p> </div> <p>請勿為 AFX 儲存系統指定此規則。</p> <p>請勿指定何時 <code>useBalancedPlacement</code> 設定為 <code>true</code>。</p>	""
useBalancedPlacement	<p>將新 Volume 的彙總選擇委託給 ONTAP [布林值]。需要 ONTAP 9.19.1 或更新版本，且 <code>useREST</code> 設定為 <code>true</code>。不能與 <code>aggregate</code> 組合使用。</p> <p>請參閱 "使用 ONTAP 後端進行均衡放置" 以瞭解需求和範例。</p> <p>如果指定，對於 ONTAP 9.19.1 或更新版本的 AFF 儲存系統，一律設定為 <code>true</code>。</p>	false; true 適用於 ONTAP 9.19.1 或更新版本的 AFX 儲存系統
limitAggregateUsage	<p>如果使用率超過此百分比，則配置失敗。不適用於 Amazon FSx for ONTAP。請勿為 AFX 儲存系統指定此規則。</p>	"（預設不強制執行）
flexgroupAggregateList	<p>用於配置的 Aggregate 清單（選用；如果設定，則必須指派給 SVM）。指派給 SVM 的所有 Aggregate 都將用於配置 FlexGroup Volume。ontap-nas-flexgroup 儲存驅動程式支援此功能。</p> <div>  <p>當 SVM 中的彙總列表更新時，Trident 會自動輪詢 SVM 來更新該列表，無需重新啟動 Trident 控制器。如果您已在 Trident 中設定了特定的彙總清單來資源配置 Volume，則如果該彙總清單已重新命名或從 SVM 中移出，Trident 在輪詢 SVM 彙總時會將後端置於故障狀態。您必須將該彙總列表變更為 SVM 中存在的列表，或將其完全移除，才能使後端恢復線上。</p> </div>	""
limitVolumeSize	<p>如果請求的磁碟區大小超過此值，則配置失敗。</p>	"（預設不強制執行）

參數	說明	預設
debugTraceFlags	用於疑難排解的偵錯旗標。例如、{"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 debugTraceFlags。	null
nasType	配置 NFS 或 SMB 磁碟區的建立。選項為 nfs、smb 或 null。設定為 null 則預設建立 NFS 磁碟區。如果指定，對於 AFX 儲存系統，請始終設定為 nfs 。	nfs
nfsMountOptions	以逗號分隔的 NFS 裝載選項清單。Kubernetes 持久性磁碟區的裝載選項通常在儲存設備類別中指定，但如果儲存設備類別中未指定任何裝載選項，Trident 將回退到使用儲存設備後端組態檔案中指定的裝載選項。如果儲存設備類別和組態檔案中均未指定裝載選項，Trident 將不會在關聯的持久性 Volume 上設定任何裝載選項。	""
qtreesPerFlexvol	每個 FlexVol 的最大 Qtree 數量必須在 [50, 300] 範圍內	"200"
smbShare	您可以指定以下選項之一：使用 Microsoft Management Console 或 ONTAP CLI 建立的 SMB 共用名稱；允許 Trident 建立 SMB 共用的名稱；或者您可以將此參數留空以封鎖對磁碟區的公共共用存取。對於內部部署 ONTAP，此參數為選用項目。對於 Amazon FSx for ONTAP 後端，此參數為必要項目且不能為空白。	smb-share
useREST	布林參數，用於使用 ONTAP REST API。useREST 當設定為 <code>true</code> 時，Trident 使用 ONTAP REST API 與後端通訊；當設定為 <code>false</code> 時，Trident 使用 ONTAPI (ZAPI) 呼叫與後端通訊。此功能需要 ONTAP 9.11.1 或更新版本。此外，使用的 ONTAP 登入角色必須具有 <code>ontapi</code> 應用程式的存取權限。預先定義的 <code>vsadmin</code> 和 <code>cluster-admin</code> 角色可滿足此要求。從 Trident 24.06 版本和 ONTAP 9.15.1 或更高版本開始， <code>useREST</code> 預設設定為 <code>true</code> ；若要使用 ONTAPI (ZAPI) 呼叫，請將 <code>useREST</code> 變更為 <code>false</code> 。如果指定，對於 AFX 儲存系統，請始終設定為 true 。	true 適用於 ONTAP 9.15.1 或更高版本，否則 false。
limitVolumePoolSize	在 ontap-nas-economy 後端中使用 Qtree 時可請求的最大 FlexVol 大小。	"（預設不強制執行）
denyNewVolumePools	限制 <code>ontap-nas-economy</code> 後端建立新 FlexVol 磁碟區來存放其 Qtree。僅使用預先存在的 Flexvols 來佈建新的 PV。	
adAdminUser	擁有對 SMB 共用完全存取權限的 Active Directory 管理員使用者或使用者群組。使用此參數可授予對 SMB 共用的完全控制權限。	

磁碟區配置的後端組態選項

您可以使用 `defaults` 配置部分中的這些選項來控制預設配置。例如、請參閱下面的組態範例。

參數	說明	預設
<code>spaceAllocation</code>	Qtree 的空間分配	"true"
<code>spaceReserve</code>	空間保留模式；「none」（精簡）或「volume」（完整）	"none"
<code>snapshotPolicy</code>	要使用的 Snapshot 原則	"none"
<code>qosPolicy</code>	要為建立的磁碟區指派 QoS 策略群組。為每個儲存資源池 / 後端選擇 <code>qosPolicy</code> 或 <code>adaptiveQosPolicy</code> 其中之一	""
<code>adaptiveQosPolicy</code>	為建立的磁碟區指派的自適應 QoS 原則群組。每個儲存資源池/後端可選擇 <code>qosPolicy</code> 或 <code>adaptiveQosPolicy</code> 其中之一。 <code>ontap-nas-economy</code> 不支援。	""
<code>snapshotReserve</code>	為快照保留的磁碟區百分比	若 <code>snapshotPolicy</code> 為「none」，則為「0」，否則為「1」
<code>splitOnClone</code>	建立時將複本從其父項分割	"false"
<code>encryption</code>	在新 Volume 上啟用 NetApp Volume Encryption (NVE)；預設為 <code>false</code> 。必須在叢集上取得 NVE 授權並啟用，才能使用此選項。如果後端已啟用 NAE，則在 Trident 中資源配置的任何 Volume 都會啟用 NAE。如需詳細資訊，請參閱： "Trident 與 NVE 和 NAE 的運作方式" 。	"false"
<code>tieringPolicy</code>	分層策略使用 "none"	
<code>unixPermissions</code>	新磁碟區模式	NFS 磁碟區為「777」；SMB 磁碟區為空（不適用）
<code>snapshotDir</code>	控制對 <code>.snapshot</code> 目錄的存取	true, false（明確設定）。
<code>exportPolicy</code>	要使用的匯出原則	"default"
<code>securityStyle</code>	新磁碟區的安全樣式。NFS 支援 <code>'mixed'</code> 和 <code>'unix'</code> 安全樣式。SMB 支援 <code>'mixed'</code> 和 <code>'ntfs'</code> 安全樣式。	NFS 預設值為 <code>unix</code> 。SMB 預設值為 <code>ntfs</code> 。
<code>nameTemplate</code>	用於建立自訂磁碟區名稱的範本。	""



搭配 Trident 使用 QoS 策略群組需要 ONTAP 9.8 或更新版本。您應該使用非共享的 QoS 原則群組，並確保該原則群組分別套用於每個成員。共享的 QoS 策略群組會強制限制所有工作負載的總吞吐量上限。

Volume 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"

```

對於 `ontap-nas`` 和 ``ontap-nas-flexgroups``，Trident 現在使用新的計算方法，以確保 FlexVol 的大小與 `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更大的原始 FlexVol。此計算方法可確保使用者在 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，當使用者請求 PVC（例如 5 GiB）且 `snapshotReserve` 百分比為 50% 時，他們只能獲得 2.5 GiB 的可寫空間。這是因為使用者要求的是整個磁碟區，而 `snapshotReserve`` 是其百分比。在 Trident 21.07 中，使用者要求的是可寫入空間，Trident 將該 ``snapshotReserve`` 數值定義為整個磁碟區的百分比。這不適用於 ``ontap-nas-economy``。請參閱以下範例以了解其工作原理：

計算方法如下：

```

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

```

對於 `snapshotReserve = 50%` 以及 PVC 請求 = 5 GiB，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 請求中所要求的大小。``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，對於先前安裝的現有後端，請依照上述說明進行 Volume 資源配置。對於升級前建立的 Volume，您需要調整其大小才能使變更生效。例如，2 GiB 的 PVC 搭配 `snapshotReserve=50` 先前產生的 Volume 僅提供 1 GiB 的可寫入空間。例如，將 Volume 調整為 3 GiB，即可為應用程式在 6 GiB 的 Volume 上提供 3 GiB 的可寫入空間。

最小組態範例

以下範例展示了基本配置，其中大多數參數都保留預設值。這是定義後端最簡單的方法。



如果您在 NetApp ONTAP 上使用 Amazon FSx 搭配 Trident，建議為 LIF 指定 DNS 名稱而非 IP 位址。

▼ ONTAP NAS 經濟範例

```
---
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、以避免在 "SVM 複製與復原" 期間進行切換和切換後手動更新後端定義。

為了實現無縫切換和切換回，請使用 `managementLIF` 指定 SVM 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 磁碟區範例

```
---
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
```

▼ 基於憑證的驗證範例

這是一個最小的後端設定範例。clientCertificate、clientPrivateKey 和 trustedCACertificate（如果使用受信任的 CA，則為可選）分別填充在 backend.json 中，並分別接受客戶端憑證、私鑰和受信任的 CA 憑證的 base64 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

本範例示範如何指示 Trident 使用動態匯出原則來自動建立和管理匯出原則。這對於 `ontap-nas-economy` 和 `ontap-nas-flexgroup` 驅動程式的運作方式相同。

```
---
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

```

▼ 均衡佈局範例

此範例啟用 ONTAP 平衡放置，以便 ONTAP 為新 Volume 選擇彙總。平衡放置需要 ONTAP 9.19.1 或更新版本。如需詳細資訊，請參閱 ["使用 ONTAP 後端進行均衡放置"](#)。

```

---
version: 1
storageDriverName: ontap-nas
backendName: nas-balanced-placement
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
useBalancedPlacement: true

```

▼ IPv6 位址範例

此範例展示 `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** 磁碟區的 **Amazon FSx for ONTAP** 範例

使用 SMB 磁碟區的 FSx for ONTAP 需要 `smbShare` 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_
```

▼ 使用 **nameTemplate** 的後端組態範例

```
---
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}}_{{.volume\
      lume.RequestName}}"
  labels:
    cluster: ClusterA
    PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"
```

具有虛擬資源池的後端範例

在下方所示的範例後端定義檔中，所有儲存池都設定了特定的預設值，例如 `spaceReserve` 為 `none`、`spaceAllocation` 為 `false` 和 `encryption` 為 `false`。虛擬資源池在儲存區段中定義。

Trident 在「備註」欄位中設定配置標籤。備註可以針對 `ontap-nas` 在 `FlexVol` 上設定，或針對 `ontap-nas-flexgroup` 在 `FlexGroup` 上設定。Trident 在配置時會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，儲存管理員可以為每個虛擬資源池定義標籤，並按標籤將磁碟區分組。

在這些範例中，部分儲存資源池設定了自己的 `spaceReserve`、`spaceAllocation` 和 `encryption` 值，而部分儲存資源池則覆寫了預設值。

▼ 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: mysqlldb
  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 **StorageClasses**

以下 StorageClass 定義均參照 [\[具有虛擬資源池的後端範例\]](#)。使用 `parameters.selector` 欄位，每個 StorageClass 都會指出哪些虛擬資源池可用於裝載 Volume。Volume 具有所選虛擬資源池中定義的屬性。

- The `protection-gold` StorageClass 對應至 ``ontap-nas-flexgroup`` 後端中的第一個和第二個虛擬資源池。這些是唯一提供黃金層級保護的資源池。

```

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

```

- The `protection-not-gold` StorageClass 對應至 ``ontap-nas-flexgroup`` 後端中的第三和第四個虛擬資源池。這些是唯一提供黃金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"
```

- The app-mysqldb StorageClass 映射到 `ontap-nas` 後端中的第四個虛擬儲存資源池。這是唯一一個為 mysqldb 類型應用程式提供儲存資源池組態的儲存資源池。

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

- The protection-silver-creditpoints-20k StorageClass 對應至 ontap-nas-flexgroup 後端中的第三個虛擬資源池。這是唯一提供白銀級保護和 20000 信用點的資源池。

```
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"
```

- The creditpoints-5k StorageClass 分別對應 `ontap-nas` 後端中的第三個虛擬資源池和 `ontap-nas-economy` 後端中的第二個虛擬資源池。只有這兩個資源池產品提供 5000 creditpoints。

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

Trident 決定選擇哪個虛擬資源池，並確保符合儲存需求。

初始配置後更新 dataLIF

初始設定完成後，您可以執行以下命令來變更 dataLIF，以提供包含更新 dataLIF 的新後端 JSON 檔案。

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



如果 PVC 連接到一個或多個 Pod、則必須關閉所有對應的 Pod、然後再將其重新啟動、以便讓新的 dataLIF 生效。

安全 SMB 範例

使用 **ontap-nas** 驅動程式進行後端組態

```
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** 驅動程式進行後端組態

```
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

```

後端配置與儲存資源池

```

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

```

使用 **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
```



請務必新增 `annotations` 以啟用安全 SMB。無論後端或 PVC 中如何配置、如果沒有這些註釋、安全 SMB 都無法正常運作。

使用 **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
```

包含單一 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
```

包含多個 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。