ONTAP SAN 驅動程式

Trident

NetApp
July 01, 2026

目錄

ONTAP SAN 驅動程式

ONTAP SAN 驅動程式概述

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

ONTAP SAN 驅動程式詳細資料

Trident 提供以下 SAN 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-san`	iSCSI SCSI over FC	區塊	RWO 、 ROX 、 RWX 、 RWOP	無檔案系統；原始區塊裝置
`ontap-san`	iSCSI SCSI over FC	檔案系統	RWO、RWOP ROX 和 RWX 在 Filesystem 磁碟區模式下不可用。	`xfs`, `ext3`, `ext4`
`ontap-san`	NVMe/TCP 請參閱NVMe/TCP 的其他考量事項。	區塊	RWO 、 ROX 、 RWX 、 RWOP	無檔案系統；原始區塊裝置
`ontap-san`	NVMe/TCP 請參閱NVMe/TCP 的其他考量事項。	檔案系統	RWO、RWOP ROX 和 RWX 在 Filesystem 磁碟區模式下不可用。	`xfs`, `ext3`, `ext4`
`ontap-san-economy`	iSCSI	區塊	RWO 、 ROX 、 RWX 、 RWOP	無檔案系統；原始區塊裝置
`ontap-san-economy`	iSCSI	檔案系統	RWO、RWOP ROX 和 RWX 在 Filesystem 磁碟區模式下不可用。	`xfs`, `ext3`, `ext4`

- 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。

NVMe/TCP 的其他考量事項

Trident 支援非揮發性記憶體高速介面（NVMe）協定，使用 `ontap-san` 驅動程式，包括：

- IPv6
- NVMe 磁碟區的快照和複本
- 調整 NVMe Volume 的大小
- 導入在 Trident 外部建立的 NVMe 磁碟區，以便 Trident 管理其生命週期
- NVMe 原生多路徑
- K8s 節點的優雅關閉或非優雅關閉（24.06）

Trident 不支援：

- NVMe 原生支援的 DH-HMAC-CHAP
- 裝置對應程式（DM）多重路徑
- LUKS 加密

NVMe 僅支援 ONTAP REST API ，不支援 ONTAPI （ ZAPI ）。

準備使用 ONTAP SAN 驅動程式配置後端

了解使用 ONTAP SAN 驅動程式配置 ONTAP 後端的要求和驗證選項。

需求

對於所有 ONTAP 後端、 Trident 要求至少將一個 Aggregate 指派給 SVM 。

> "ASA r2 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 ASA r2 系統中，使用儲存可用區而非 Aggregate。請參閱 "這" 知識庫文章，瞭解如何在 ASA r2 系統中將 Aggregate 指派給 SVM。

請記住，您還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，您可以設定一個 `san-dev`類別，使用 `ontap-san`驅動程式，以及一個 `san-default`類別，使用 `ontap-san-economy`驅動程式。

所有 Kubernetes 工作節點都必須安裝適當的 iSCSI 工具。詳情請參閱 "準備工作節點"。

驗證 **ONTAP** 後端

Trident 提供兩種 ONTAP 後端驗證模式。

- 基於憑證：具有所需權限的 ONTAP 使用者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 版本的最大相容性。
- 基於憑證：Trident 也可以使用安裝在後端的憑證與 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

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

JSON

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

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。建立或更新後端是唯一需要瞭解認證資料的步驟。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=admin"
```

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
```

執行此命令後，ONTAP 會提示輸入憑證。貼上步驟 1 中產生的 `k8senv.pem`檔案內容，然後輸入 `END`以完成安裝。

4. 確認 ONTAP 安全登入角色支援 `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。將 <ONTAP Management LIF> 和 <vserver name> 替換為 Management LIF IP 和 SVM 名稱。

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

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"

使用雙向 CHAP 驗證連線

Trident 可以使用雙向 CHAP 對 iSCSI 工作階段進行驗證，適用於 `ontap-san`和 `ontap-san-economy`驅動程式。這需要在後端定義中啟用 `useCHAP`選項。當設定為 `true`時，Trident 會將 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密碼。NetApp 建議使用雙向 CHAP 來驗證連線。請參閱以下範

例組態：

```
---
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 參數為布林值選項，只能配置一次。預設值為 false。將其設為 true 後，無法再將其設為 false。

除了 `useCHAP=true`之外， `chapInitiatorSecret`、 `chapTargetInitiatorSecret`、 `chapTargetUsername`和 `chapUsername`欄位也必須包含在後端定義中。後端建立完成後，可以透過執行 `tridentctl update`來變更金鑰。

運作方式

將 `useCHAP`設為 true 後，儲存管理員會指示 Trident 在儲存後端設定 CHAP。這包括以下內容：

- 在 SVM 上設定 CHAP：
  - 如果 SVM 的預設發起程序安全類型為 none（預設設定）*且*磁碟區中沒有預先存在的 LUN，則 Trident 會將預設安全類型設為 `CHAP`，並繼續設定 CHAP 發起程式和目標使用者名稱及金鑰。
  - 如果 SVM 包含 LUN，Trident 將不會在 SVM 上啟用 CHAP。這確保對 SVM 上已存在的 LUN 的存取不受限制。
- 配置 CHAP 啟動器和目標使用者名稱和密碼；這些選項必須在後端組態中指定（如上所示）。

後端建立完成後， Trident 會建立對應的 `tridentbackend` CRD ，並將 CHAP 金鑰和使用者名稱儲存為 Kubernetes 金鑰。Trident 在此後端建立的所有 PV 都將透過 CHAP 協定進行掛載和連線。

輪換認證資料並更新後端

您可以透過更新 `backend.json` 檔案中的 CHAP 參數來更新 CHAP 憑證。這需要更新 CHAP 金鑰，並使用 `tridentctl update` 命令來反映這些變更。

更新後端的 CHAP 密碼時，您必須使用 `tridentctl`來更新後端。請勿使用 ONTAP CLI 或 ONTAP System Manager 更新儲存叢集上的認證，因為 Trident 將無法識別這些變更。

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

現有連線將不受影響；如果 Trident 在 SVM 上更新了認證資料，這些連線將繼續保持作用中狀態。新連線使用更新的認證資料，現有連線則繼續保持作用中狀態。中斷連線並重新連線舊的 PV 將導致其使用更新的認證資料。

ONTAP SAN 設定選項和範例

了解如何在 Trident 安裝中建立和使用 ONTAP SAN 驅動程式。本節提供後端組態範例以及將後端對應至 StorageClasses 的詳細資訊。"ASA r2 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。這些差異會影響某些參數的使用方式（如註明）。"深入瞭解 ASA r2 系統與其他 ONTAP 系統之間的差異".在 Trident 後端組態中、您不需要指定系統為 ASA r2。當您選擇 `ontap-san`作為 `storageDriverName` 時、Trident 會自動偵測 ASA r2 或其他 ONTAP 系統。如下表所示、某些後端組態參數不適用於 ASA r2 系統。

ASA r2 系統僅支援 `ontap-san`驅動程式（使用 iSCSI、NVMe/TCP 和 FC 協定）。

後端組態選項

請參閱下表以了解後端組態選項：

參數	說明	預設
`version`		始終為 1
`storageDriverName`	儲存驅動程式的名稱	`ontap-san` 或 `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。 可以指定完全限定網域名稱（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 `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`。 如需無縫 MetroCluster 切換、請參閱 MetroCluster 範例。 ⓘ 如果使用「 vsadmin 」認證、`managementLIF`則必須是 SVM 的認證；如果使用「 admin 」認證、`managementLIF`則必須是叢集的認證。	"10.0.0.1", "[2001:1234:abcd::fefe]"
`dataLIF`	協定 LIF 的 IP 位址。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 iSCSI，請勿指定此參數。*Trident 使用"ONTAP Selective LUN Map"來發現建立多路徑會話所需的 iSCSI LIF。如果 `dataLIF`明確定義了此參數，則會產生警告。*對於 MetroCluster，請省略此參數。*請參閱MetroCluster 範例。	由 SVM 導出
`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
`useCHAP`	使用 CHAP 對 ONTAP SAN 驅動程式的 iSCSI 進行驗證 [布林值]。設定為 `true`時、Trident 會將雙向 CHAP 設定並用作後端中指定 SVM 的預設驗證。詳情請參閱"準備使用 ONTAP SAN 驅動程式配置後端"。不支援 **FCP** 或 **NVMe/TCP**。	`false`
`chapInitiatorSecret`	CHAP 啟動器密碼。如果 `useCHAP=true`則為必填項目	""
`labels`	要套用於磁碟區的任意 JSON 格式標籤集	""

參數	說明	預設
`chapTargetInitiatorSecret`	CHAP 目標啟動器密碼。如果 `useCHAP=true`則為必填項目	""
`chapUsername`	入站使用者名稱。如果 `useCHAP=true`則為必填項目	""
`chapTargetUsername`	目標使用者名稱。如果 `useCHAP=true`則為必填項目	""
`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。此參數為可選。用於憑證型驗證。	""
`username`	與 ONTAP 叢集通訊所需的使用者名稱。用於基於憑證的身份驗證。有關 Active Directory 驗證，請參閱 "使用 Active Directory 憑證對後端 SVM 進行 Trident 驗證"。	""
`password`	與 ONTAP 叢集通訊所需的密碼。用於基於憑證的身份驗證。有關 Active Directory 驗證，請參閱 "使用 Active Directory 憑證對後端 SVM 進行 Trident 驗證"。	""
`svm`	要使用的儲存虛擬機器	如果指定了 `managementLIF` SVM，則衍生
`storagePrefix`	在 SVM 中配置新磁碟區時所使用的前綴。無法修改。若要更新此參數、您需要建立新的後端。	`trident`
`aggregate`	用於配置的 Aggregate （選用；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 Aggregate 來配置 FlexGroup Volume。 當 SVM 中的 Aggregate 更新時，Trident 會自動輪詢 SVM 並更新，無需重新啟動 Trident Controller。如果您已在 Trident 中設定用於配置 Volume 的特定 Aggregate，則如果該 Aggregate 被重新命名或從 SVM 中移出，後端將在輪詢 SVM Aggregate 時進入故障狀態。您必須將該 Aggregate 變更為 SVM 中已存在的 Aggregate，或將其完全移除，才能使後端恢復連線狀態。 請勿為 **ASA r2** 系統指定。	""

參數	說明	預設
limitAggregateUsage	如果使用率超過此百分比，則配置失敗。如果您使用的是 Amazon FSx for NetApp ONTAP 後端，請勿指定 limitAggregateUsage。提供的 `fsxadmin`和 `vsadmin`不包含使用 Trident 檢索 Aggregate 使用情況並加以限制所需的權限。請勿為 **ASA r2** 系統指定。	"（預設不強制執行）
limitVolumeSize	如果請求的磁碟區大小超過此值，則配置失敗。此外，也會限制其管理的 LUN 磁碟區大小上限。	"（預設不強制執行）
lunsPerFlexvol	每個 FlexVol 的最大 LUN 數量必須在 [50 、 200] 範圍內	100
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。	null
useREST	布林參數，用於使用 ONTAP REST API。 `useREST`當設定為 `true`時，Trident 使用 ONTAP REST API 與後端通訊；當設定為 `false` 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 `ontapi`應用程式的存取權限。預先定義的 `vsadmin`和 `cluster-admin`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， `useREST`預設設定為 `true`；若要使用 ONTAPI（ZAPI）呼叫，請將 `useREST`變更為 `false`。 useREST 完全符合 NVMe/TCP 標準。 NVMe 僅支援 ONTAP REST API ，不支援 ONTAPI （ ZAPI ）。 如果指定、則一律設為 **true** （適用於 **ASA r2** 系統）。	true 適用於 ONTAP 9.15.1 或更高版本，否則 false。
sanType	用於選擇 iscsi 適用於 iSCSI、 nvme 適用於 NVMe/TCP 或 fcp 適用於 SCSI over Fibre Channel （FC）。	iscsi 如果為空

參數	說明	預設
`formatOptions`	使用 `formatOptions`為 `mkfs`命令指定命令列引數，這些引數將在每次格式化磁碟區時套用。這樣可讓您根據自己的偏好格式化磁碟區。請確保指定的 formatOptions 與 mkfs 命令選項類似，但不包含裝置路徑。範例："-E nodiscard" 支援使用 **iSCSI** 傳輸協定的 **`ontap-san`**和 **`ontap-san-economy`**驅動程式。*此外，使用 iSCSI 和 NVMe/TCP 傳輸協定時，也支援 ASA r2 系統。*	
`limitVolumePoolSize`	在 ontap-san-economy 後端使用 LUN 時可請求的最大 FlexVol 大小。	"（預設不強制執行）
`denyNewVolumePools`	限制 `ontap-san-economy`後端建立新的 FlexVol 磁碟區以包含其 LUN 。僅使用預先存在的 Flexvol 來配置新的 PV 。	

使用 **formatOptions** 的建議

Trident 建議採用以下選項來加速格式化程序：

- **-E nodiscard (ext3, ext4):** 在執行 mkfs 時不要嘗試丟棄資料區塊（在固態裝置和稀疏 / 精簡配置儲存上、初始丟棄資料區塊很有用）。此選項取代了已棄用的「 -K 」選項、適用於 ext3 和 ext4 檔案系統。
- **-K (xfs):** 執行 mkfs 時不要嘗試丟棄資料區塊。此選項適用於 xfs 檔案系統。

使用 **Active Directory** 憑證對後端 **SVM** 進行 **Trident** 驗證

您可以設定 Trident 使用 Active Directory （ AD ）憑證對後端 SVM 進行驗證。在 AD 帳戶可以存取 SVM 之前、您必須設定 AD 網域控制站對叢集或 SVM 的存取權限。若要使用 AD 帳戶進行叢集管理、您必須建立網域通道。詳情請參閱 "在 ONTAP 中設定 Active Directory 網域控制器存取"。

步驟

1. 為後端 SVM 設定網域名稱系統（Domain Name System、DNS）設定：

   ```
   vserver services dns create -vserver <svm_name> -dns-servers
   <dns_server_ip1>,<dns_server_ip2>
   ```

2. 執行下列命令、在 Active Directory 中為 SVM 建立電腦帳戶：

   ```
   vserver active-directory create -vserver DataSVM -account-name ADSERVER1
   -domain demo.netapp.com
   ```

3. 使用此命令建立 AD 使用者或群組來管理叢集或 SVM

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <ad_user_or_group> -application <application> -authentication-method domain
   -role vsadmin
   ```

4. 在 Trident 後端組態檔中，將 `username` 和 `password` 參數分別設定為 AD 使用者或群組名稱和密碼。

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
`spaceAllocation`	LUN 的空間分配	"true" 如果指定、請針對 **ASA r2** 系統設定為 **`true`**。
`spaceReserve`	空間保留模式；「 none 」（精簡）或「 volume 」（完整）。針對 **ASA r2** 系統設為 `none`。	"none"
`snapshotPolicy`	要使用的快照原則。針對 **ASA r2** 系統設定為 **`none`**。	"none"
`qosPolicy`	要為建立的磁碟區指派 QoS 策略群組。每個儲存資源池/後端可選擇 qosPolicy 或 adaptiveQosPolicy 其中之一。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 策略群組，並確保該策略群組單獨套用至每個成員。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。	""
`adaptiveQosPolicy`	為建立的磁碟區指派的自適應 QoS 原則群組。為每個儲存資源池 / 後端選擇 qosPolicy 或 adaptiveQosPolicy 其中之一	""
`snapshotReserve`	為快照預留的磁碟區百分比。請勿為 **ASA r2** 系統指定。	若 `snapshotPolicy`為「none」，則為「0」，否則為「」
`splitOnClone`	建立時將複本從其父項分割	"false"
`encryption`	在新磁碟區上啟用 NetApp Volume Encryption（NVE）；預設值為 `false`。要使用此選項，叢集必須已獲得 NVE 許可並啟用 NVE。如果後端啟用了 NAE，則在 Trident 中佈建的任何磁碟區都會啟用 NAE。如需詳細資訊，請參閱："Trident 與 NVE 和 NAE 的運作方式"。	"false" 如果指定、請針對 **ASA r2** 系統設定為 **`true`**。
`luksEncryption`	啟用 LUKS 加密。請參閱"使用 Linux Unified Key Setup （ LUKS ）"。	"" 設定為 **`false`**適用於 **ASA r2** 系統。
`tieringPolicy`	分層策略使用「無」 請勿為 **ASA r2** 系統指定。	
`nameTemplate`	用於建立自訂磁碟區名稱的範本。	""

Volume 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'
```

對於使用 `ontap-san`驅動程式建立的所有磁碟區、Trident 會額外增加 10% 的容量至 FlexVol 以容納 LUN 中繼資料。LUN 將根據使用者在 PVC 中請求的確切大小進行佈建。Trident 會額外增加 10% 的容量至 FlexVol（在 ONTAP 中顯示為可用大小）。使用者現在將獲得他們請求的可用容量。此變更還可防止 LUN 在可用空間未完全使用之前變為唯讀。此變更不適用於 ontap-san-economy。

對於定義了 `snapshotReserve`的後端， Trident 會依照下列方式計算磁碟區的大小：

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

1.1 是 Trident 為 FlexVol 額外增加的 10% ，以容納 LUN 元資料。對於 `snapshotReserve` = 5% ，且 PVC 請求 = 5 GiB ，總磁碟區大小為 5.79 GiB ，可用大小為 5.5 GiB 。 `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_e42ec6fe_3baa_4af6_996d_134adbbb8e6d
                       online     RW       5.79GB     5.50GB    0%
          _pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba
                       online     RW          1GB    511.8MB    0%
3 entries were displayed.
```

目前，調整大小是將新計算方法應用於現有磁碟區的唯一方法。

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 for NetApp ONTAP 搭配 Trident，NetApp 建議您為 LIF 指定 DNS 名稱而非 IP 位址。

ONTAP SAN 範例

這是使用 `ontap-san` 驅動程式的基本配置。

```
---
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>
```

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回退，請使用 `managementLIF` 指定 SVM 並省略 `svm` 參數。例如：

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

ONTAP SAN 經濟範例

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

基於憑證的驗證範例

在這個基本設定範例中 `clientCertificate`、 `clientPrivateKey` 和 `trustedCACertificate`（選用，如果使用受信任的 CA）會填入 `backend.json` 中，並分別採用用戶端憑證、私密金鑰和受信任的 CA 憑證的 base64 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

這些範例建立了一個後端，並將 `useCHAP`設為 `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 economy 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>
```

NVMe/TCP 範例

您的 ONTAP 後端必須設定一個支援 NVMe 的 SVM。這是 NVMe/TCP 的基本後端組態。

```
---
version: 1
backendName: NVMeBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nvme
username: vsadmin
password: password
sanType: nvme
useREST: true
```

SCSI over FC （ FCP ） 範例

您的 ONTAP 後端必須設定一個支援 FC 的 SVM。這是 FC 的基本後端組態。

```
---
version: 1
backendName: fcp-backend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_fc
username: vsadmin
password: password
sanType: fcp
useREST: true
```

使用 **nameTemplate** 的後端組態範例

```
---
version: 1
storageDriverName: ontap-san
backendName: ontap-san-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}}"
```

formatOptions ontap-san-economy 驅動程式範例

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: ""
svm: svm1
username: ""
password: "!"
storagePrefix: whelk_
debugTraceFlags:
  method: true
  api: true
defaults:
  formatOptions: -E nodiscard
```

具有虛擬資源池的後端範例

在這些範例後端定義檔中，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。備註設置在 FlexVol volume 上。Trident 在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 SAN 範例

```yaml
---
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"
```

NVMe/TCP 範例

```
---
version: 1
storageDriverName: ontap-san
sanType: nvme
managementLIF: 10.0.0.1
svm: nvme_svm
username: vsadmin
password: <password>
useREST: true
defaults:
  spaceAllocation: "false"
  encryption: "true"
storage:
  - labels:
      app: testApp
      cost: "20"
    defaults:
      spaceAllocation: "false"
      encryption: "false"
```

將後端對應至 StorageClasses

以下 StorageClass 定義均與此相關 [具有虛擬資源池的後端範例]。透過該 `parameters.selector` 字段，每個 StorageClass 定義都會指定哪些虛擬池可用於託管磁碟區。磁碟區將具有所選虛擬池中定義的方面。

- 該 `protection-gold` StorageClass 將映射到 `ontap-san`後端中的第一個虛擬資源池。這是唯一提供黃金級保護的資源池。

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

- 該 `protection-not-gold` StorageClass 將對應至 `ontap-san` 後端中的第二個和第三個虛擬資源池。這些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 將對應至 `ontap-san-economy`後端中的第三個虛擬資源池。這是唯一為 mysqldb 類型應用程式提供儲存資源池組態的資源池。

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

- `protection-silver-creditpoints-20k` StorageClass 將對應至 `ontap-san`後端的第二個虛擬資源池。這是唯一提供銀級保護和 20000 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 將對應至 `ontap-san` 後端的第三個虛擬資源池和 `ontap-san-economy` 後端的第四個虛擬資源池。這些是唯一提供 5000 creditpoints 的資源池。

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

- 此 `my-test-app-sc` StorageClass 會對應到 `testAPP` 虛擬資源池，在 `ontap-san` 驅動程式中使用 `sanType: nvme`。這是唯一提供 `testApp` 的資源池。

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

Trident 將決定選擇哪個虛擬資源池，並確保符合儲存需求。