



# 支援SAN驅動程式ONTAP Trident

NetApp  
March 02, 2026

# 目錄

支援SAN驅動程式ONTAP .....	1
ONTAP SAN 驅動程式概觀 .....	1
ONTAP SAN 驅動程式詳細資料 .....	1
使用者權限 .....	2
NVMe / TCP 的其他考量事項 .....	2
準備使用ONTAP 支援的SAN驅動程式來設定後端 .....	2
需求 .....	3
驗證 ONTAP 後端 .....	3
使用雙向 CHAP 驗證連接 .....	8
SAN組態選項與範例ONTAP .....	10
後端組態選項 .....	11
用於資源配置磁碟區的後端組態選項 .....	15
最低組態範例 .....	17
虛擬集區的後端範例 .....	21
將後端對應至StorageClass .....	26

# 支援SAN驅動程式ONTAP

## ONTAP SAN 驅動程式概觀

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

### ONTAP SAN 驅動程式詳細資料

Trident 提供下列 SAN 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-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 檔案系統磁碟區模式中無法使用 Rox 和 rwx。	《xfs》、《ext3》、《ext4》
「ONTAP-SAN」	NVMe / TCP  請參閱 <a href="#">NVMe / TCP 的其他考量事項</a> 。	區塊	Rwo、ROX、rwx、RWOP	無檔案系統；原始區塊裝置
「ONTAP-SAN」	NVMe / TCP  請參閱 <a href="#">NVMe / TCP 的其他考量事項</a> 。	檔案系統	RWO、RWOP 檔案系統磁碟區模式中無法使用 Rox 和 rwx。	《xfs》、《ext3》、《ext4》
《ONTAP-san經濟》	iSCSI	區塊	Rwo、ROX、rwx、RWOP	無檔案系統；原始區塊裝置
《ONTAP-san經濟》	iSCSI	檔案系統	RWO、RWOP 檔案系統磁碟區模式中無法使用 Rox 和 rwx。	《xfs》、《ext3》、《ext4》



- 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` 參數將無法與和 `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。

## NVMe / TCP 的其他考量事項

Trident 支援使用驅動程式的非揮發性記憶體高速 (NVMe) 傳輸協定 `ontap-san`、包括：

- IPv6
- NVMe 磁碟區的快照和複本
- 調整 NVMe 磁碟區大小
- 匯入在 Trident 之外建立的 NVMe Volume、以便 Trident 管理其生命週期
- NVMe 原生多重路徑
- K8s 節點正常或不正常關機 (24.06)

Trident 不支援：

- NVMe 原生支援的 DH-HMAC-CHAP
- 裝置對應工具 (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 支援的 SAN 驅動程式來設定後端

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

## 需求

對於所有 ONTAP 後端，Trident 要求至少將一個聚合分配給 SVM。



"ASA r2 系統"與其他ONTAP系統 (ASA、AFF和FAS) 在儲存層的實作上有所不同。在ASA r2 系統中，使用儲存可用區而不是聚合。請參閱["這"](#)知識庫文章，介紹如何在ASA r2 系統中將聚合指派給 SVM。

請記住、您也可以執行多個驅動程式、並建立指向一個或多個驅動程式的儲存類別。例如、您可以設定使用「ONTAP-SAN」驅動程式的「SAN開發」類別、以及使用「ONTAP-SAN經濟」類別的「SAN預設」類別。

您所有的Kubernetes工作節點都必須安裝適當的iSCSI工具。請參閱 ["準備工作節點"](#) 以取得詳細資料。

## 驗證 ONTAP 後端

Trident 提供兩種驗證 ONTAP 後端的模式。

- 認證型：ONTAP 對具備所需權限的使用者名稱和密碼。建議使用預先定義的安全登入角色、例如「admin」或「vsadmin」、以確保與ONTAP 各種版本的最大相容性。
- 憑證型：Trident 也可以使用安裝在後端的憑證與 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\*認證與憑證\*、後端建立將會失敗、並在組態檔中提供多種驗證方法。

### 啟用認證型驗證

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-san
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: password
```

## JSON

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

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

### 啟用基於憑證的身份驗證

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

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

典型的工作流程包括下列步驟。

### 步驟

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

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

- 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>
```

- 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
```



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。

- 確認ONTAP 支援「cert」驗證方法的支援功能。

```
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
```

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

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

- 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
```

- 使用從上一步取得的值建立後端。

```

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

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

```

## 更新驗證方法或旋轉認證資料

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

```

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

#Update backend with tridentctl
tridentctl update backend SanBackend -f cert-backend-updated.json -n
trident
+-----+-----+-----+
+-----+-----+
|   NAME   | STORAGE DRIVER |          UUID          |
STATE | VOLUMES |
+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |      9 |
+-----+-----+-----+
+-----+-----+

```



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

更新後端不會中斷對已建立之磁碟區的存取、也不會影響之後建立的磁碟區連線。成功的後端更新表示 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"](#)

## 使用雙向 CHAP 驗證連接

Trident 可以使用和 `ontap-san-economy` 驅動程式的雙向 CHAP 驗證 iSCSI 工作階段 `ontap-san`。這需要在後端定義中啟用 `useCHAP` 選項。設為 `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。請參閱下列組態範例

:

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



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

除了"useCHAP=true"之外、"chapInitiator Secret (chapInitiator機密)"、"chaptarketatorSecret (chaptarketusername)"、"chaptarketusername (chaptargetuseamuse)"和"chapusername" (chamus在建立後端後端之後、可以執行「tridentctl update」來變更機密。

## 工作原理

儲存管理員會將設定`useCHAP`為 true、指示 Trident 在儲存後端上設定 CHAP。這包括下列項目：

- 在SVM上設定CHAP：
  - 如果 SVM 的預設啟動器安全性類型為無（預設為「無」） \* 且 \* 磁碟區中沒有預先存在的 LUN、則 Trident 會將預設安全性類型設為 CHAP、並繼續設定 CHAP 啟動器和目標使用者名稱和機密。
  - 如果 SVM 包含 LUN、Trident 將不會在 SVM 上啟用 CHAP。這可確保不限制對 SVM 上已存在的 LUN 的存取。
- 設定CHAP啟動器和目標使用者名稱和機密；這些選項必須在後端組態中指定（如上所示）。

建立後端之後、Trident 會建立對應的 tridentbackend CRD、並將 CHAP 機密和使用者名稱儲存為 Kubernetes 機密。Trident 在此後端建立的所有 PV 都會透過 CHAP 掛載及附加。

## 輪換憑證並更新後端

您可以更新「backend.json」檔案中的CHAP參數、以更新CHAP認證。這需要更新CHAP機密、並使用「tridentctl update」命令來反映這些變更。



更新後端的 CHAP 機密時、您必須使用`tridentctl`來更新後端。請勿使用 ONTAP CLI 或 ONTAP 系統管理員更新儲存叢集上的認證，因為 Trident 將無法取得這些變更。

```

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 |
+-----+-----+-----+-----+
+-----+-----+

```

現有連線不會受到影響；如果 Trident 在 SVM 上更新認證、則這些連線將繼續保持作用中狀態。新的連線使用更新的認證資料、而現有的連線會繼續保持作用中。中斷舊PV的連線並重新連線、將會使用更新的認證資料。

## SAN組態選項與範例ONTAP

瞭解如何在 Trident 安裝中建立及使用 ONTAP SAN 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。

"ASA r2 系統"與其他ONTAP系統（ASA、AFF和FAS）在儲存層的實作上有所不同。這些變化會影響某些參數的使用，如註釋中所述。["詳細了解 ASA r2 系統與其他 ONTAP 系統之間的差異"](#)。



只有 `ontap-san` ASA r2 系統支援驅動程式（支援 iSCSI、NVMe/TCP 和 FC 協定）。

在Trident後端設定中，無需指定您的系統是ASA r2。當您選擇 `ontap-san` 作為 `storageDriverName` Trident可自動偵測ASA r2 或其他ONTAP系統。如下表所示，某些後端設定參數不適用於ASA r2 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
「storageDriverName」	儲存驅動程式名稱	ontap-san`或 `ontap-san-economy
「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》	<p>叢集或 SVM 管理 LIF 的 IP 位址。</p> <p>您可以指定完整網域名稱 (FQDN)。</p> <p>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]。</p> <p>如需無縫 MetroCluster 之間的互通性<a href="#">MetroCluster 範例</a>、請參閱。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> 如果您使用的是「vsadmin」認證，則必須是 SVM 的認 managementLIF`證；如果使用的是「admin」認證，則必須是叢集的認證 `managementLIF。</p> </div>	"10.0.0.1"， "[2001:1234:abcd::fefe]"
「DataLIF」	<p>傳輸協定LIF的IP位址。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]。* 請勿指定 iSCSI。Trident 使用"可選擇的LUN對應ONTAP"來探索建立多重路徑工作階段所需的 iSCSI 生命。如果明確定義、就會產生警告 dataLIF。MetroCluster 省略。*請參閱<a href="#">MetroCluster 範例</a>。</p>	源自SVM
《虛擬機器》	<p>要使用的儲存虛擬機器</p> <p>* MetroCluster 請省略。* 請參閱 <a href="#">MetroCluster 範例</a>。</p>	如果指定SVM "managementLIF"則衍生
《使用CHAP》	<p>使用CHAP驗證iSCSI以供ONTAP 支援不支援的SAN驅動程式使用[布林值]。設為 true、讓 Trident 設定並使用雙向 CHAP 做為後端所指定 SVM 的預設驗證。如 "準備使用ONTAP 支援的SAN驅動程式來設定後端" 需詳細資訊、請參閱。*不支援 FCP 或 NVMe/TCP。*</p>	「假」
《chapInitiator機密》	CHAP啟動器密碼。如果是"useCHAP=true"、則為必要項目	"
《標籤》	套用到磁碟區的任意JSON-格式化標籤集	"

參數	說明	預設
《chapTargetInitiator機密》	CHAP目標啟動器機密。如果是"useCHAP=true"、則為必要項目	"
「chapUsername」	傳入使用者名稱。如果是"useCHAP=true"、則為必要項目	"
《chapTargetUsername》	目標使用者名稱。如果是"useCHAP=true"、則為必要項目	"
「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》	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 " <a href="#">使用 Active Directory 憑證向後端 SVM 驗證Trident 的身份</a> "。	"
密碼	與ONTAP集群通訊所需的密碼。用於基於憑證的身份驗證。有關 Active Directory 驗證，請參閱 " <a href="#">使用 Active Directory 憑證向後端 SVM 驗證Trident 的身份</a> "。	"
《虛擬機器》	要使用的儲存虛擬機器	如果指定SVM "managementLIF"則衍生
「storagePrefix」	在SVM中配置新磁碟區時所使用的前置碼。稍後無法修改。若要更新此參數、您需要建立新的後端。	trident
《Aggregate》	<p>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。</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p> 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。</p> </div> <p>不要指定 <b>ASA r2</b> 系統。</p>	"

參數	說明	預設
「限制Aggregateusage」	如果使用率高於此百分比、則無法進行資源配置。如果您使用 Amazon FSX for NetApp ONTAP 後端、請勿指定 limitAggregateUsage。提供的 `fsxadmin` 和 `vsadmin` 不包含使用 Trident 擷取彙總使用量並加以限制所需的權限。不要指定 <b>ASA r2</b> 系統。	"" (預設不強制執行)
《限制Volume大小》	如果要求的磁碟區大小高於此值、則資源配置失敗。也會限制其管理 LUN 的最大磁碟區大小。	"" (預設不會強制執行)
《lunsPerFlexvol》	每FlexVol 個LUN的最大LUN數量、範圍必須在[50、200]	100
「DebugTraceFlags」	疑難排解時要使用的偵錯旗標。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》	<p>使用ONTAP REST API 的布林參數。</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>`useREST` 當設定為 `true`，Trident使用ONTAP REST API 與後端通訊；當設定為 `false`，Trident使用 ONTAPI (ZAPI) 呼叫與後端進行通訊。此功能需要ONTAP 9.11.1 及更高版本。此外，使用的ONTAP登入角色必須具有訪問 `ontapi` 應用。這是透過預定義的 `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；改變 `useREST` 到 `false` 使用 ONTAPI (ZAPI) 呼叫。</p> </div> <p>`useREST` 完全符合 NVMe/TCP 的要求。</p> <div style="display: flex; align-items: center; margin: 10px 0;"> <div style="text-align: center; margin-right: 10px;">  </div> <div> <p>NVMe 僅支援ONTAP REST API，不支援 ONTAPI (ZAPI)。</p> </div> </div> <p>如果指定，則始終設定為 `true` 適用於<b>ASA r2</b> 系統。</p>	true 對於 ONTAP 9.15.1 或更高版本，否則 false。
sanType	用於選擇 iscsi iSCSI、nvme NVMe / TCP 或 fcp SCSI over Fibre Channel (FC)。	iscsi 如果空白

參數	說明	預設
formatOptions	用於 formatOptions 指定命令的命令列引數、每當格式化磁碟區時都會套用這些引數 `mkfs`。這可讓您根據偏好設定來格式化 Volume。請務必指定與 mkfs 命令選項類似的格式選項、但不包括裝置路徑。範例：「-E nobard」  *支援 `ontap-san` 和 `ontap-san-economy` 帶有 iSCSI 協定的驅動程式。 **此外，在使用 iSCSI 和 NVMe/TCP 協定時，支援 ASA r2 系統。 *	
limitVolumePoolSize	在 ONTAP SAN 經濟型後端中使用 LUN 時、可要求的最大 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。只有預先存在的 FlexVols 可用於佈建新的 PV。	

### 使用 formatOptions 的建議

Trident建議採用以下選項來加速格式化流程：

- **-E nodiscard (ext3, ext4):** 不要嘗試在 mkfs 時丟棄區塊（最初丟棄區塊對固態設備和稀疏/精簡配置儲存很有用）。這將取代已棄用的選項“-K”，並且適用於 ext3、ext4 檔案系統。
- **-K (xfs):** 不要在執行 mkfs 時嘗試丟棄區塊。此選項適用於 xfs 檔案系統。

### 使用 Active Directory 憑證向後端 SVM 驗證Trident 的身份

您可以設定Trident以使用 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。對於使用 AD 帳戶進行叢集管理，您必須建立網域隧道。參考 "[在ONTAP中設定 Active Directory 網域控制站存取](#)" 了解詳情。

#### 步驟

1. 為後端 SVM 配置網域名稱系統 (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後端設定檔中，設定 username 和 password 參數分別為 AD 使用者或群組名稱和密碼。

## 用於資源配置磁碟區的后端組態選項

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

參數	說明	預設
"paceAllocate (配置) "	LUN的空間分配	"true" 如果指定，則設定為 `true` 適用於 <b>ASA r2</b> 系統。
《保護區》	空間保留模式；「無」（精簡）或「Volume（大量）」（粗）。設定為 `none` 適用於 <b>ASA r2</b> 系統。	" 無 "
「快照原則」	要使用的 Snapshot 原則。設定為 `none` 適用於 <b>ASA r2</b> 系統。	" 無 "
「qosPolicy」	要指派給所建立磁碟區的QoS原則群組。選擇每個儲存集區/後端的其中一個qosPolicy或adaptiveQosPolicy。搭配 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。	"
《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	"
「快照保留區」	保留給快照的磁碟區百分比。不要為 <b>ASA r2</b> 系統指定。	「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 <a href="#">"Trident 如何與 NVE 和 NAE 搭配運作"</a> ；。	"false" 如果指定，則設定為 `true` 適用於 <b>ASA r2</b> 系統。
luksEncryption	啟用LUKS加密。請參閱 <a href="#">"使用Linux統一金鑰設定 (LUKS) "</a> 。	" 設定為 `false` 適用於 <b>ASA r2</b> 系統。
「分層政策」	分層策略使用「無」 不要為 <b>ASA r2</b> 系統指定。	
nameTemplate	建立自訂磁碟區名稱的範本。	"

### Volume資源配置範例

以下是定義預設值的範例：

```

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

```



對於使用驅動程式建立的所有磁碟區 ontap-san、Trident 會為 FlexVol 額外增加 10% 的容量、以容納 LUN 中繼資料。LUN 的配置大小與使用者在 PVC 中要求的大小完全相同。Trident 將 10% 新增至 FlexVol（在 ONTAP 中顯示為可用大小）。使用者現在可以取得所要求的可用容量。此變更也可防止 LUN 成為唯讀、除非可用空間已充分利用。這不適用於 ONTAP-san 經濟型。

對於定義的後端 snapshotReserve，Trident 將按以下方式計算卷的大小：

$$\text{Total volume size} = [(\text{PVC requested size}) / (1 - (\text{snapshotReserve percentage}) / 100)] * 1.1$$

1.1 是 Trident 為容納 LUN 元資料而額外添加到 FlexVol 的 10%。對於 snapshotReserve = 5%，PVC 請求 = 5 GiB，則總磁碟區大小為 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、只有調整大小、才能將新計算用於現有的 Volume。

## 最低組態範例

下列範例顯示基本組態、讓大部分參數保留預設值。這是定義後端最簡單的方法。



如果您在 NetApp ONTAP 上搭配 Trident 使用 Amazon FSX，NetApp 建議您指定生命體的 DNS 名稱，而非 IP 位址。

### ONTAP SAN 範例

這是使用的基本組態 `ontap-san` 驅動程式：

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

### 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，請使用並省略 `svm`` 參數來指定 `SVM `managementLIF`。例如：

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

## ONTAP SAN 經濟效益範例

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

## 憑證型驗證範例

在此基本組態範例中 `clientCertificate`、`clientPrivateKey` 和 `trustedCACertificate` (選用、如果使用信任的CA) 會填入 `backend.json` 並分別取得用戶端憑證、私密金鑰及信任CA憑證的基礎64編碼值。

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

## 雙向 CHAP 範例

這些範例使用建立後端 useCHAP 設定為 true。

### ONTAP SAN CHAP 範例

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

### ONTAP SAN 經濟 CHAP 範例

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

## NVMe / TCP 範例

您必須在 ONTAP 後端上設定 NVMe 的 SVM 。這是適用於 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

您必須在 ONTAP 後端設定具有 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
```

## 名稱範本的后端組態範例

```
---
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 經濟型驅動程式範例

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

## 虛擬集區的后端範例

在這些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。在 FlexVol volume Trident 上設定的註解會將虛擬集區上的所有標籤複製到資源配置時的儲存磁碟區。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-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"
```

```

---
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StorageClass

下列 StorageClass 定義請參閱 [\[虛擬集區的后端範例\]](#)。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虛擬集區 `ontap-san` 後端：這是唯一提供金級保護的集區。

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

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

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

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

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

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

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: 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-san 中的後端和第四個虛擬集區 ontap-san-economy 後端：這是唯一擁有 5000 個信用點數的集區方案。

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

- my-test-app-sc StorageClass 會對應至 testAPP 中的虛擬集區 ontap-san 驅動程式搭配 sanType: nvme。這是唯一的集區服務項目 testApp。

```
---
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 會決定要選取哪個虛擬集區、並確保符合儲存需求。

## 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 保留隨時變更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。