ONTAP SAN 驱动程序

Trident

NetApp
February 02, 2026

目录

ONTAP SAN 驱动程序 . . . 1
- ONTAP SAN驱动程序概述 . . . 1
  - ONTAP SAN驱动程序详细信息 . . . 1
  - 用户权限 . . . 2
  - NVMe/TCP的其他注意事项 . . . 2
- 准备使用ONTAP SAN驱动程序配置后端 . . . 2
  - 要求 . . . 3
  - 对ONTAP后端进行身份验证 . . . 3
  - 使用双向 CHAP 验证连接 . . . 8
- ONTAP SAN配置选项和示例 . . . 10
  - 后端配置选项 . . . 11
  - 用于配置卷的后端配置选项 . . . 15
  - 最低配置示例 . . . 17
  - 虚拟池后端示例 . . . 21
  - 将后端映射到 StorageClasses . . . 26

ONTAP SAN 驱动程序

ONTAP SAN驱动程序概述

了解如何使用 ONTAP 和 Cloud Volumes ONTAP SAN 驱动程序配置 ONTAP 后端。

ONTAP SAN驱动程序详细信息

Trident提供了以下SAN存储驱动程序来与ONTAP集群进行通信。支持的访问模式包括：*ReadWriteOnce*(RWO)、*ReadOnlyMany*(ROX)、*ReadWriteMany*(rwx)、*ReadWriteOncePod*(RWOP)。

驱动程序	协议	卷模式	支持的访问模式	支持的文件系统
`ontap-san`	基于FC的iSCSI SCSI	块	Rwo、ROX、rwx、RWOP	无文件系统；原始块设备
`ontap-san`	基于FC的iSCSI SCSI	文件系统	Rwo、RWO1. Rox和rwx在文件系统卷模式下不可用。	`xfs`， `ext3`， `ext4`
`ontap-san`	NVMe/TCP 请参见NVMe/TCP的其他注意事项。	块	Rwo、ROX、rwx、RWOP	无文件系统；原始块设备
`ontap-san`	NVMe/TCP 请参见NVMe/TCP的其他注意事项。	文件系统	Rwo、RWO1. Rox和rwx在文件系统卷模式下不可用。	`xfs`， `ext3`， `ext4`
`ontap-san-economy.`	iSCSI	块	Rwo、ROX、rwx、RWOP	无文件系统；原始块设备
`ontap-san-economy.`	iSCSI	文件系统	Rwo、RWO1. Rox和rwx在文件系统卷模式下不可用。	`xfs`， `ext3`， `ext4`

- 使用 … `ontap-san-economy` 只有当永久性卷使用量计数预期高于时、才会显示此值 "支持的ONTAP卷限制"。
- 使用 … `ontap-nas-economy` 只有当永久性卷使用量计数预期高于时、才会显示此值 "支持的ONTAP卷限制" 和 `ontap-san-economy` 无法使用驱动程序。
- 请勿使用 `ontap-nas-economy` 预测数据保护、灾难恢复或移动性的需求。
- NetApp不建议在所有ONTAP驱动程序中使用FlexVol自动增长、但ONTAP SAN除外。解决方法是、Trident支持使用快照预留并相应地扩展FlexVol卷。

用户权限

Trident应以ONTAP或SVM管理员身份运行、通常使用集群用户 `vsadmin`或SVM用户、或者使用 `admin`具有相同角色的其他名称的用户。对于Amazon FSx for NetApp ONTAP部署、Trident应使用集群用户 `vsadmin`或SVM用户以ONTAP或SVM管理员身份运行、或者使用具有相同角色的其他名称的用户运行 `fsxadmin`。此 `fsxadmin`用户只能有限地替代集群管理员用户。

如果使用 `limitAggregateUsage`参数、则需要集群管理员权限。将Amazon FSx for NetApp ONTAP与Trident结合使用时、 `limitAggregateUsage`参数不适用于 `vsadmin`和 `fsxadmin`用户帐户。如果指定此参数，配置操作将失败。

虽然可以在ONTAP中创建一个可以由三端驱动程序使用的限制性更强的角色、但我们不建议这样做。大多数新版本的 Trident 都会调用需要考虑的其他 API ，从而使升级变得困难且容易出错。

NVMe/TCP的其他注意事项

Trident使用以下驱动程序支持非易失性内存快速(NVMe)协议 `ontap-san`：

- IPv6
- NVMe卷的快照和克隆
- 调整NVMe卷大小
- 导入在Trident外部创建的NVMe卷、以便Trident可以管理其生命周期
- NVMe本机多路径
- 正常或非正常关闭K8s节点(24.06)

Trident不支持：

- NVMe 原生支持的 DH-HMAC-CHAP
- 设备映射程序(Device maper、DM)多路径
- 进行了加密

NVMe 仅支持ONTAP REST API，不支持 ONTAPI (ZAPI)。

准备使用ONTAP SAN驱动程序配置后端

了解使用ONTAP SAN驱动程序配置ONTAP后端的要求和身份验证选项。

要求

对于所有 ONTAP 后端，Trident 要求至少将一个聚合分配给 SVM。

> "ASA r2系统"与其他ONTAP系统（ASA、 AFF和FAS）在存储层的实现上有所不同。在ASA r2系统中，使用存储可用区而不是聚合。请参阅"这"知识库文章，介绍如何在ASA r2 系统中将聚合分配给 SVM。

请记住，您还可以运行多个驱动程序，并创建指向其中一个驱动程序的存储类。例如，您可以配置使用 `ontap-san` 驱动程序的 `san-dev` 类和使用 `ontap-san-economy-one` 的 `san-default` 类。

所有Kubernetes工作节点都必须安装适当的iSCSI工具。请参见 "准备工作节点" 了解详细信息。

对**ONTAP**后端进行身份验证

Trident提供了两种对ONTAP后端进行身份验证的模式。

- Credential Based ： 具有所需权限的 ONTAP 用户的用户名和密码。建议使用 `admin` 或 `vsadmin` 等预定义的安全登录角色，以确保与 ONTAP 版本的最大兼容性。
- 基于证书：Trident还可以使用后端安装的证书与ONTAP集群进行通信。此处，后端定义必须包含客户端证书，密钥和可信 CA 证书的 Base64 编码值（如果使用）（建议）。

您可以更新现有后端、以便在基于凭据的方法和基于证书的方法之间移动。但是、一次仅支持一种身份验证方法。要切换到其他身份验证方法、必须从后端配置中删除现有方法。

> 如果您尝试同时提供*凭据和证书*、则后端创建将失败、并显示一条错误、指出配置文件中提供了多种身份验证方法。

启用基于凭据的身份验证

Trident需要SVM范围/集群范围的管理员的凭据才能与ONTAP后端进行通信。建议使用标准的预定义角色，如 `admin`或 `vsadmin`。这样可以确保与未来ONTAP版本的正向兼容性、这些版本可能会公开未来Trident版本要使用的功能API。可以创建自定义安全登录角色并将其用于Trident、但不建议这样做。

后端定义示例如下所示：

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"
}
```

请注意，后端定义是凭据以纯文本格式存储的唯一位置。创建后端后，用户名 / 密码将使用 Base64 进行编码并存储为 Kubernetes 密钥。创建或更新后端是唯一需要了解凭据的步骤。因此，这是一项仅由管理员执行的操作，由 Kubernetes 或存储管理员执行。

启用基于证书的身份验证

新的和现有的后端可以使用证书并与 ONTAP 后端进行通信。后端定义需要三个参数。

- clientCertificate ： 客户端证书的 Base64 编码值。
- clientPrivateKey ： 关联私钥的 Base64 编码值。
- trustedCACertifate ： 受信任 CA 证书的 Base64 编码值。如果使用可信 CA ，则必须提供此参数。如果不使用可信 CA ，则可以忽略此设置。

典型的工作流包括以下步骤。

步骤

1. 生成客户端证书和密钥。生成时，将公用名（ Common Name ， CN ）设置为要作为身份验证的 ONTAP 用户。

```
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. 将可信 CA 证书添加到 ONTAP 集群。此问题可能已由存储管理员处理。如果未使用可信 CA ，则忽略。

```
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 集群上安装客户端证书和密钥（从步骤 1 开始）。

```
security certificate install -type client-ca -cert-name <certificate-
name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

运行此命令后，ONTAP 提示输入证书。粘贴步骤 1 中生成的 `k8senv.pem`文件内容，然后输入 `END`以完成安装。

4. 确认 ONTAP 安全登录角色支持 `cert` 身份验证方法。

```
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. 使用生成的证书测试身份验证。将 <SVM 管理 LIF> 和 <SVM 名称 > 替换为管理 LIF IP 和 ONTAP 名称。

```
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 对证书，密钥和可信 CA 证书进行编码。

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

7. 使用从上一步获得的值创建后端。

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

更新身份验证方法或轮换凭据

您可以更新现有后端以使用其他身份验证方法或轮换其凭据。这两种方式都适用：使用用户名 / 密码的后端可以更新为使用证书；使用证书的后端可以更新为基于用户名 / 密码的后端。为此、您必须删除现有身份验证方法并添加新的身份验证方法。然后、使用包含所需参数的更新后端.json文件执行`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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

轮换密码时，存储管理员必须先在 ONTAP 上更新用户的密码。然后进行后端更新。轮换证书时，可以向用户添加多个证书。之后，后端将更新以使用新证书，然后可以从 ONTAP 集群中删除旧证书。

更新后端不会中断对已创建卷的访问，也不会影响在之后建立的卷连接。后端更新成功表示Trident可以与ONTAP后端通信并处理未来的卷操作。

为**Trident**创建自定义**ONTAP**角色

您可以创建Privileges最低的ONTAP集群角色、这样就不必使用ONTAP管理员角色在Trident中执行操作。如果在Trident后端配置中包含用户名、则Trident将使用您创建的ONTAP集群角色来执行操作。

有关创建Trident自定义角色的详细信息、请参见"Trident自定义角色生成器"。

使用**ONTAP**命令行界面

1. 使用以下命令创建新角色：

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

2. 为Trident用户创建用户名：

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

3. 将角色映射到用户：

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

使用 **System Manager**

在ONTAP系统管理器中执行以下步骤：

1. 创建自定义角色：
   a. 要在集群级别创建自定义角色，请选择*Cluster > Settings*。

      (或)要在SVM级别创建自定义角色、请选择*存储> Storage VM `required SVM` >>设置>用户和角色*。

   b. 选择*用户和角色*旁边的箭头图标(→)。
   c. 在*角色*下选择*+添加*。
   d. 定义角色的规则，然后单击*Save*。
2. 将角色映射到**Trident user**：+在*Users and Roles*页面上执行以下步骤：
   a. 在*用户*下选择添加图标*+*。
   b. 选择所需的用户名，然后在下拉菜单中为*rouser*选择一个角色。
   c. 单击 * 保存 * 。

有关详细信息、请参见以下页面：

- "用于管理ONTAP的自定义角色"或"定义自定义角色"
- "使用角色和用户"

使用双向 **CHAP** 验证连接

Trident可以使用和 `ontap-san-economy`驱动程序的双向CHAP对iSCSI会话进行身份验证 `ontap-san`。这需要在后端定义中启用此 `useCHAP`选项。设置为时 `true`，Trident会将SVM的默认启动程序安全性配置为双向CHAP，并设置后端文件中的用户名和密钥。NetApp 建议使用双向 CHAP 对连接进行身份验证。请参见以

下配置示例：

```
---
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 参数是一个布尔选项，只能配置一次。默认情况下，此参数设置为 false 。将其设置为 true 后，无法将其设置为 false 。

除了 useCHAP=true 之外，后端定义还必须包括 chapInitiatorSecret ， chapTargetInitiatorSecret ， chapTargetUsername 和 chapUsername 字段。通过运行 tridentctl update 创建后端，可以更改这些密钥。

工作原理

如果将设置 `useCHAP`为true、则存储管理员将指示Trident在存储后端配置CHAP。其中包括：

- 在 SVM 上设置 CHAP ：
  - 如果SVM的默认启动程序安全类型为none (默认设置)*和*卷中已没有已有的LUN、则Trident会将默认安全类型设置为 CHAP、并继续配置CHAP启动程序以及目标用户名和密码。
  - 如果SVM包含LUN、则Trident不会在此SVM上启用CHAP。这样可确保对SVM上已存在的LUN的访问不受限制。
- 配置 CHAP 启动程序以及目标用户名和密码；必须在后端配置中指定这些选项（如上所示）。

创建后端后、Trident会创建相应的 `tridentbackend`CRD并将CHAP密码和用户名存储为Kubbernetes密码。Trident在此后端创建的所有PV,都将通过CHAP进行挂载和连接。

轮换凭证并更新后端

您可以通过更新 backend.json 文件中的 CHAP 参数来更新 CHAP 凭据。这需要更新 CHAP 密码并使用 tridentctl update 命令反映这些更改。

更新后端的CHAP密码时、必须使用 `tridentctl`更新后端。请勿使用ONTAP命令行界面或ONTAP系统管理器更新存储集群上的凭据、因为Trident将无法接受这些更改。

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

现有连接不会受到影响；如果Trident在SVM上更新凭据、这些连接将继续保持活动状态。新连接将使用更新后的凭据、现有连接将继续保持活动状态。断开并重新连接旧的 PV 将导致它们使用更新后的凭据。

ONTAP SAN配置选项和示例

了解如何在Trident安装中创建和使用ONTAP SAN驱动程序。本节提供了将后端映射到StorageClasses的后端配置示例和详细信息。

"ASA r2系统"与其他ONTAP系统（ASA、 AFF和FAS）在存储层的实现上有所不同。这些变化会影响某些参数的使用，如注释中所述。"详细了解 ASA r2 系统与其他 ONTAP 系统之间的差异"。

只有 `ontap-san`ASA r2 系统支持驱动程序（支持 iSCSI、NVMe/TCP 和 FC 协议）。

在Trident后端配置中，无需指定您的系统是ASA r2。当您选择 `ontap-san`作为 `storageDriverName`Trident可自动检测ASA r2 或其他ONTAP系统。如下表所示，某些后端配置参数不适用于ASA r2 系统。

后端配置选项

有关后端配置选项，请参见下表：

参数	Description	Default
ve版本		始终为 1
storageDriverName	存储驱动程序的名称	ontap-san`或 `ontap-san-economy
backendName	自定义名称或存储后端	驱动程序名称+"_"+ dataLIF
m年 月 日	集群或SVM管理LIF的IP地址。 可以指定完全限定域名(FQDN)。 如果Trident是使用IPv6标志安装的、则可以设置为使用IPv6地址。IPv6地址必须用方括号定义，例如[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。 有关无缝MetroCluster切换的信息，请参见MetroCluster示例。 如果您使用的是"vsadmin"凭据、managementLIF`则必须是SVM的凭据；如果使用的是"admin"凭据、则必须是集群的凭据 `managementLIF。	"10.0.0.1"、"[2001：1234：abc：：：fefe]"
dataLIF	协议 LIF 的 IP 地址。如果Trident是使用IPv6标志安装的、则可以设置为使用IPv6地址。IPv6地址必须用方括号定义，例如[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。*不指定iSCSI。*Trident使用"ONTAP 选择性LUN映射"发现建立多路径会话所需的iSCSI LUN。如果明确定义、则会生成警告 dataLIF。*省略MetroCluster。*请参见MetroCluster示例。	由SVM派生
sVM	要使用的 Storage Virtual Machine *对于MetroCluster省略。*请参见 MetroCluster示例。	如果指定了 SVM managementLIF，则派生
使用 CHAP	使用CHAP对iSCSI的ONTAP SAN驱动程序进行身份验证[布尔值]。将设置为 true、以便Trident配置双向CHAP并将其用作后端中给定SVM的默认身份验证。有关详细信息、请参见 "准备使用ONTAP SAN驱动程序配置后端" 。不支持 **FCP** 或 **NVMe/TCP**。	false
chapInitiatorSecret	CHAP 启动程序密钥。如果为 useCHAP=true ，则为必需项	""
标签	要应用于卷的一组任意 JSON 格式的标签	""

参数	Description	Default
chapTargetInitiatorSecret	CHAP 目标启动程序密钥。如果为 useCHAP=true ，则为必需项	""
chapUsername	入站用户名。如果为 useCHAP=true ，则为必需项	""
chapTargetUsername	目标用户名。如果为 useCHAP=true ，则为必需项	""
客户端证书	客户端证书的 Base64 编码值。用于基于证书的身份验证	""
clientPrivateKey	客户端专用密钥的 Base64 编码值。用于基于证书的身份验证	""
trustedCACertifate	受信任 CA 证书的 Base64 编码值。可选。用于基于证书的身份验证。	""
用户名	与ONTAP集群通信所需的用户名。用于基于凭证的身份验证。有关 Active Directory 身份验证，请参阅 "使用 Active Directory 凭据向后端 SVM 验证Trident 的身份"。	""
密码	与ONTAP集群通信所需的密码。用于基于凭证的身份验证。有关 Active Directory 身份验证，请参阅 "使用 Active Directory 凭据向后端 SVM 验证Trident 的身份"。	""
sVM	要使用的 Storage Virtual Machine	如果指定了 SVM managementLIF ，则派生
s存储前缀	在 SVM 中配置新卷时使用的前缀。无法稍后修改。要更新此参数、您需要创建一个新的后端。	trident
聚合	要配置的聚合（可选；如果设置了聚合，则必须将其分配给 SVM ）。对于 `ontap-nas-flexgroup`驱动程序、此选项将被忽略。如果未分配、则 可以使用任何可用聚合来配置FlexGroup卷。 在SVM中更新聚合后、该聚合将在Trident中自动更新、方法是轮询SVM、而无需重新启动Trident控制器。在Trident中配置了特定聚合以配置卷后、如果将该聚合重命名或移出SVM、则在轮询SVM聚合时、后端将在Trident中变为故障状态。您必须将聚合更改为SVM上的聚合、或者将其全部删除、以使后端恢复联机。 不要指定 **ASA r2** 系统。	""

参数	Description	Default
limitAggregateUsage	如果使用量超过此百分比，则配置失败。如果您使用的是Amazon FSx for NetApp ONTAP后端，请勿指定 limitAggregateUsage。提供的和 `vsadmin`不包含使用Trident检索聚合使用情况并对其进行限制所需的 `fsxadmin`权限。不要指定 **ASA r2** 系统。	"" （默认情况下不强制实施）
limitVolumeSize	如果请求的卷大小超过此值、则配置失败。此外、还会限制它为LUN管理的卷的大小上限。	""(默认情况下不强制实施)
lunsPerFlexvol	每个 FlexVol 的最大 LUN 数，必须在 50 ， 200 范围内	100
debugTraceFlags	故障排除时要使用的调试标志。例如、 {"api"：false、"METHO"：true} 除非正在进行故障排除并需要详细的日志转储、否则请勿使用。	null
useREST	使用ONTAP REST API 的布尔参数。 `useREST`当设置为 `true`，Trident使用ONTAP REST API与后端通信；当设置为 `false`，Trident使用 ONTAPI （ZAPI）调用与后端进行通信。此功能需要ONTAP 9.11.1 及更高版本。此外，使用的ONTAP登录角色必须具有访问 `ontapi`应用。这是通过预定义的 `vsadmin`和 `cluster-admin`角色。从Trident 24.06 版本和ONTAP 9.15.1 或更高版本开始，`useREST`设置为 `true`默认；改变 `useREST`到 `false`使用 ONTAPI (ZAPI) 调用。 `useREST`完全符合 NVMe/TCP 的要求。 NVMe 仅支持ONTAP REST API，不支持 ONTAPI (ZAPI)。 如果指定，则始终设置为 **`true`**适用于**ASA r2** 系统。	true 对于ONTAP 9.151或更高版本，否则 false。
sanType	用于为iSCSI、 nvme`NVMe/TCP或基于光纤通道的 `fcp`SCSI (FC)选择 `iscsi。	iscsi 如果为空

参数	Description	Default
formatOptions	`formatOptions`用于指定命令的命令行参数、每当对卷进行格式化时、都会应用这些参数`mkfs`。这样、您可以根据偏好格式化卷。请确保指定与mkfs命令选项类似的格式选项，但不包括设备路径。示例："-E nobdiscard" 支持 **`ontap-san`**和 **`ontap-san-economy`**带有 **iSCSI** 协议的驱动程序。*此外，在使用 iSCSI 和 NVMe/TCP 协议时，支持 ASA r2 系统。*	
limitVolumePoolSize	在LUS-SAN-Economy后端使用ONTAP时可要求的最大FlexVol大小。	""（默认情况下不强制实施）
denyNewVolumePools	限制 `ontap-san-economy`后端创建新的FlexVol卷以包含其LUN。仅会使用已有的FlexVol配置新的PV.	

有关使用**formatOptions**的建议

Trident建议采用以下选项来加快格式化过程：

- **-E nodiscard (ext3, ext4):** 不要尝试在 mkfs 时丢弃块（最初丢弃块对固态设备和稀疏/精简配置存储很有用）。这将取代已弃用的选项"-K"，并且适用于 ext3、ext4 文件系统。
- **-K (xfs):** 不要在执行 mkfs 时尝试丢弃块。此选项适用于 xfs 文件系统。

使用 **Active Directory** 凭据向后端 **SVM** 验证**Trident** 的身份

您可以配置Trident以使用 Active Directory (AD) 凭据对后端 SVM 进行身份验证。在 AD 帐户可以访问 SVM 之前，您必须配置 AD 域控制器对集群或 SVM 的访问权限。对于使用 AD 帐户进行集群管理，您必须创建域隧道。参考 "在ONTAP中配置 Active Directory 域控制器访问" 了解详情。

步骤

1. 为后端 SVM 配置域名系统 (DNS) 设置：

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

2. 运行以下命令在 Active Directory 中为 SVM 创建计算机帐户：

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

3. 使用此命令创建 AD 用户或组来管理集群或 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后端配置文件中，设置 `username` 和 `password` 参数分别为 AD 用户或组名称和密码。

用于配置卷的后端配置选项

您可以在中使用这些选项控制默认配置 `defaults` 配置部分。有关示例，请参见以下配置示例。

参数	Description	Default
`spaceAllocation`	LUN 的空间分配	"true" 如果指定，则设置为 **`true`**适用于 **ASA r2** 系统。
s页面预留	空间预留模式；"无"(精简)或"卷"(厚)。设置为 **`none`** 适用于 **ASA r2** 系统。	"无"
`sSnapshot` 策略	要使用的Snapshot策略。设置为 **`none`**适用于 **ASA r2** 系统。	"无"
`qosPolicy`	要为创建的卷分配的 QoS 策略组。选择每个存储池 / 后端的 qosPolicy 或 adaptiveQosPolicy 之一。将QoS策略组与Trident结合使用需要使用ONTAP 9™8或更高版本。您应使用非共享QoS策略组、并确保此策略组分别应用于每个成分卷。共享QoS策略组会对所有工作负载的总吞吐量实施上限。	""
`adaptiveQosPolicy`	要为创建的卷分配的自适应 QoS 策略组。选择每个存储池 / 后端的 qosPolicy 或 adaptiveQosPolicy 之一	""
`sSnapshot` 预留	为快照预留的卷百分比。不要为 **ASA r2** 系统指定。	如果为"0"、则为"0" `snapshotPolicy` 为"none"、否则为""
`splitOnClone`	创建克隆时，从其父级拆分该克隆	false
加密	在新卷上启用NetApp卷加密(NVE)；默认为 `false`。要使用此选项，必须在集群上获得 NVE 的许可并启用 NVE 。如果在后端启用了NAE、则在Trident中配置的任何卷都将启用NAE。有关详细信息，请参阅：“Trident如何与NVE和NAE配合使用”。	“false” 如果指定，则设置为 **`true`**适用于 **ASA r2** 系统。
`luksEncryption`	启用LUKS加密。请参阅 “使用Linux统一密钥设置(LUKS)”。	"" 设置为 **`false`**适用于 **ASA r2** 系统。
分层策略	分层策略使用“无” 不要为 **ASA r2** 系统指定。	
`nameTemplate`	用于创建自定义卷名称的模板。	""

卷配置示例

下面是一个定义了默认值的示例：

```
---
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'
```

对于使用驱动程序创建的所有卷 `ontap-san`、Trident会向FlexVol额外添加10%的容量、以容纳LUN元数据。LUN 将使用用户在 PVC 中请求的确切大小进行配置。Trident会将10%的空间添加到FlexVol中(在ONTAP中显示为可用大小)。用户现在将获得所请求的可用容量。此更改还可防止 LUN 变为只读状态，除非已充分利用可用空间。这不适用于 ontap-san-economy.

对于定义的后端 `snapshotReserve`，Trident将按如下所示计算卷的大小：

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

1.1 是Trident为容纳 LUN 元数据而额外添加到FlexVol 的10%。对于 `snapshotReserve` = 5%，PVC 请求 = 5 GiB，则总卷大小为 5.79 GiB，可用大小为 5.5 GiB。 `volume show`命令应显示与此示例类似的结果：

```
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，调整大小是对现有卷使用新计算的唯一方法。

最低配置示例

以下示例显示了将大多数参数保留为默认值的基本配置。这是定义后端的最简单方法。

> 如果您在NetApp ONTAP上使用Amazon FSx和、NetApp建议您为Trident指定DNS名称、而不是IP地址。

ONTAP SAN示例

这是使用的基本配置 `ontap-san` 驱动程序。

```
---
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示例

您可以对后端进行配置、以避免在切换和切回后手动更新后端定义 "SVM复制和恢复"。

要进行无缝切换和切回、请使用指定SVM `managementLIF`、并省略这些 `svm`参数。例如：

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

ONTAP SAN经济性示例

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

基于证书的身份验证示例

在本基本配置示例中 `clientCertificate`， `clientPrivateKey`，和 `trustedCACertificate` (如果使用可信CA、则可选)将填充 `backend.json` 和分别采用客户端证书、专用密钥和可信CA证书的base64编码值。

```
---
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
```

双向CHAP示例

这些示例使用创建后端 `useCHAP` 设置为 `true`。

ONTAP SAN CHAP示例

```
---
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经济性CHAP示例

```
---
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示例

您必须在ONTAP后端为SVM配置NVMe。这是NVMe/TCP的基本后端配置。

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

基于FC的SCSI (FCP)示例

您必须在ONTAP后端为SVM配置FC。这是FC的基本后端配置。

```
---
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**的后端配置示例

```
---
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的**ONTAP SAN**经济驱动程序示例

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

虚拟池后端示例

在这些示例后端定义文件中、为所有存储池设置了特定默认值、例如 `spaceReserve` 无、 `spaceAllocation` 为false、和 `encryption` 为false。虚拟池在存储部分中进行定义。

Trident会在"Comments"字段中设置配置标签。在配置时、FlexVol volume Trident会将虚拟池上的所有标签复制到存储卷上、从而设置注释。为了方便起见、存储管理员可以按标签为每个虚拟池和组卷定义标签。

在这些示例中、某些存储池会自行设置 `spaceReserve`， `spaceAllocation`，和 `encryption` 值、而某些

池会覆盖默认值。

ONTAP SAN示例

```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经济性示例

```
---
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示例

```
---
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"
```

将后端映射到 StorageClasses

以下StorageClass定义涉及 [虚拟池后端示例]。使用 `parameters.selector` 字段中、每个StorageClass都会指出可用于托管卷的虚拟池。卷将在选定虚拟池中定义各个方面。

- 。 `protection-gold` StorageClass将映射到中的第一个虚拟池 `ontap-san` 后端。这是唯一提供金牌保护的池。

```
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将映射到中的第二个和第三个虚拟池 `ontap-san` 后端。只有这些池提供的保护级别不是gold。

```
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将映射到中的第三个虚拟池 `ontap-san-economy` 后端。这是为mysqldb类型的应用程序提供存储池配置的唯一池。

```
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将映射到中的第二个虚拟池 `ontap-san` 后端。这是唯一提供银牌保护和20000个信用点的池。

```
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将映射到中的第三个虚拟池 `ontap-san` 中的后端和第四个虚拟池 `ontap-san-economy` 后端。这是唯一一款信用点数为5000的池产品。

```
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将映射到 `testAPP` 中的虚拟池 `ontap-san` 驱动程序 `sanType: nvme`。这是唯一的池产品 `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将决定选择哪个虚拟池、并确保满足存储要求。