ONTAP NAS 驱动程序

Trident

NetApp
July 01, 2026

目录

ONTAP NAS 驱动程序

ONTAP NAS 驱动程序概述

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

ONTAP NAS 驱动程序详细信息

Trident 提供以下 NAS 存储驱动程序以与 ONTAP 集群通信。支持的访问模式有：*ReadWriteOnce* (RWO)、*ReadOnlyMany* (ROX)、*ReadWriteMany* (RWX)、*ReadWriteOncePod* (RWOP)。

驱动程序	协议	**volumeMode**	支持的访问模式	支持的文件系统
`ontap-nas`	NFS SMB	Filesystem	RWO、ROX、RWX、RWOP	", `nfs`, `smb`
`ontap-nas-economy`	NFS SMB	Filesystem	RWO、ROX、RWX、RWOP	", `nfs`, `smb`
`ontap-nas-flexgroup`	NFS SMB	Filesystem	RWO、ROX、RWX、RWOP	", `nfs`, `smb`

- 仅当预期持久卷使用次数高于"支持的 ONTAP 卷限制"时，才使用 `ontap-san-economy`。
- 仅当预期持久卷使用次数高于"支持的 ONTAP 卷限制"且无法使用 `ontap-san-economy`驱动程序时，才使用 `ontap-nas-economy`。
- 如果您预计需要数据保护、灾难恢复或移动性，请勿使用 `ontap-nas-economy`。
- NetApp 不建议在所有 ONTAP 驱动程序中使用 Flexvol 自动增长，除了 ontap-san。作为一种解决方法，Trident 支持使用快照保留并相应地扩展 Flexvol 卷。

用户权限

Trident 希望以 ONTAP 或 SVM 管理员的身份运行，通常使用 `admin`集群用户或 `vsadmin`SVM 用户，或具有相同角色的不同名称的用户。

对于 Amazon FSx for NetApp ONTAP 部署，Trident 希望以 ONTAP 或 SVM 管理员的身份运行，使用集群 `fsxadmin`用户或 `vsadmin`SVM 用户，或具有相同角色的不同名称的用户。 `fsxadmin`用户是集群管理员用户的有限替代品。

如果使用 `limitAggregateUsage` 参数，则需要群集管理员权限。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 Trident 驱动程序可以使用的更具限制性的角色，但我们不建议这样做。大多数新版本的 Trident 会调用必须考虑到的其他 API，这使得升级变得困难且容易出错。

准备使用 ONTAP NAS 驱动程序配置后端

了解使用 ONTAP NAS 驱动程序配置 ONTAP 后端的要求、身份验证选项和导出策略。从 25.10 版本开始，NetApp Trident 支持 "NetApp AFX 存储系统"。NetApp AFX 存储系统与其他 ONTAP 系统（ASA、AFF 和 FAS）在存储层的实现方面有所不同。在 Trident 后端配置中，无需指定您的系统是 AFX。当您选择 `ontap-nas`作为 `storageDriverName`时，Trident 会自动检测 AFX 系统。

AFX 系统仅支持 `ontap-nas`驱动程序（使用 NFS 协议）；不支持 SMB 协议。

要求

- 对于所有 ONTAP 后端，Trident 要求至少将一个聚合分配给 SVM。
- 您可以运行多个驱动程序，并创建指向一个或另一个的存储类。例如，您可以配置一个使用 `ontap-nas`驱动程序的 Gold 类和一个使用 `ontap-nas-economy`驱动程序的 Bronze 类。
- 所有 Kubernetes worker 节点都必须安装相应的 NFS 工具。有关更多详细信息，请参见 "此处"。
- Trident 仅支持将 SMB 卷挂载到在 Windows 节点上运行的 Pod。有关详细信息，请参见 准备配置 SMB 卷。

对 ONTAP 后端进行身份验证

Trident 提供两种身份验证 ONTAP 后端的模式。

- 基于凭据：此模式需要对 ONTAP 后端的足够权限。建议使用与预定义安全登录角色关联的帐户，例如 `admin`或 `vsadmin`，以确保与 ONTAP 版本的最大兼容性。
- 基于证书：此模式需要在后端安装证书，Trident 才能与 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）（推荐）。

您可以更新现有后端以在基于凭据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。

如果您尝试提供*凭据和证书*，则后端创建将失败，错误为配置文件中提供了多个身份验证方法。

启用基于凭据的身份验证

Trident 需要向 SVM 范围/集群范围的管理员提供凭据，以便与 ONTAP 后端进行通信。建议使用标准、预定义的角色，如 `admin`或 `vsadmin`。这确保了与未来 ONTAP 版本的向前兼容性，这些版本可能会公开未来 Trident 版本使用的功能 API。可以创建自定义安全登录角色并与 Trident 一起使用，但不建议这样做。

示例后端定义如下所示：

YAML

```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

```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"
    }
}
```

请记住，后端定义是凭据以纯文本形式存储的唯一位置。后端创建后，用户名/密码使用 Base64 进行编码，并存储为 Kubernetes 密码。创建/更新后端是唯一需要了解凭据的步骤。因此，它是一个仅限管理员的操作，由 Kubernetes/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 后端通信。后端定义中需要三个参数。

- clientCertificate: 客户端证书的 Base64 编码值。
- clientPrivateKey: 关联专用密钥的 Base64 编码值。
- trustedCACertificate：受信任的 CA 证书的 Base64 编码值。如果使用受信任的 CA，则必须提供此参数。如果未使用受信任的 CA，则可以忽略此设置。

典型的工作流程包括以下步骤。

步骤

1. 生成客户端证书和密钥。生成时，将公用名 (CN) 设置为要进行身份验证的 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=vsadmin"
```

2. 将受信任的 CA 证书添加到 ONTAP 集群。这可能已由存储管理员处理。如果未使用受信任的 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（来自步骤 1）。

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

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 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. 使用生成的证书测试身份验证。将 <ONTAP Management LIF> 和 <vserver name> 替换为管理 LIF IP 和 SVM 名称。您必须确保 LIF 的服务策略设置为 `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 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-updated.json
{
"version": 1,
"storageDriverName": "ontap-nas",
"backendName": "NasBackend",
"managementLIF": "1.2.3.4",
"dataLIF": "1.2.3.8",
"svm": "vserver_test",
"clientCertificate": "Faaaakkkkeeee...Vaaalllluuuueeee",
"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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

更新身份验证方法或轮换凭据

您可以更新现有后端以使用不同的身份验证方法或轮换其凭据。这可以双向工作：可以将使用用户名/密码的后端更新为使用证书；可以将使用证书的后端更新为基于用户名/密码。为此，您必须删除现有的身份验证方法并添加新的身份验证方法。然后使用更新的 backend.json 文件，其中包含执行 `tridentctl update backend` 所需的参数。

```
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                 |
STATE   | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |       9 |
+------------+----------------+--------------------------------------
+--------+---------+
```

轮换密码时，存储管理员必须首先更新 ONTAP 上用户的密码。然后进行后端更新。轮换证书时，可以向用户添加多个证书。然后更新后端以使用新证书，之后可以从 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，也不会影响之后建立的卷连接。成功的后端更新表明，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

您可以使用最低权限创建 ONTAP 集群角色，这样您就不必使用 ONTAP 管理员角色在 Trident 中执行操作。在 Trident 后端配置中包含用户名时，Trident 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 CLI**

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

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"

管理 NFS 导出策略

Trident 使用 NFS 导出策略来控制对其提供的卷的访问。

使用出口策略时，Trident 提供两种选择：

- Trident 可以动态管理导出策略本身；在这种操作模式下，存储管理员指定表示可允许 IP 地址的 CIDR 块列表。Trident 会在发布时自动将落在这些范围内的适用节点 IP 添加到导出策略中。或者，当未指定 CIDR 时，在要发布的卷的节点上找到的所有全局范围的单播 IP 都将添加到导出策略中。
- 存储管理员可以创建导出策略并手动添加规则。除非在配置中指定不同的导出策略名称，否则 Trident 使用默认导出策略。

动态管理导出策略

Trident 能够动态管理 ONTAP 后端的导出策略。这使存储管理员能够为工作节点 IP 指定允许的地址空间，而不是手动定义显式规则。它大大简化了导出策略管理；对导出策略的修改不再需要对存储集群进行手动干预。此外，这有助于将对存储集群的访问限制为仅挂载卷且 IP 位于指定范围内的工作节点，从而支持精细化和自动化管理。

> ⓘ 使用动态导出策略时不要使用网络地址转换 (NAT)。对于 NAT，存储控制器看到的是前端 NAT 地址，而不是实际的 IP 主机地址，因此在导出规则中未找到匹配项时将拒绝访问。

示例

必须使用两个配置选项。以下是后端定义示例：

```
---
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
```

> ⓘ 使用此功能时，必须确保 SVM 中的根接合点具有先前创建的导出策略以及允许节点 CIDR 块的导出规则（例如默认导出策略）。始终遵循 NetApp 推荐的最佳实践，为 Trident 专用一个 SVM。

以下是使用上述示例说明此功能工作原理的解释：

- `autoExportPolicy` 设置为 `true`。这表示 Trident 为使用此后端为 `svm1` SVM 配置的每个卷创建导出策略，并使用 `autoexportCIDRs`地址块处理规则的添加和删除。在卷连接到节点之前，该卷使用没有规则的空导出策略来防止对该卷的不必要访问。当卷发布到节点时，Trident 会创建一个与底层 qtree 同名的导出策略，该 qtree 包含指定 CIDR 块中的节点 IP。这些 IP 也将被添加到父 FlexVol 卷使用的导出策略中
  - 例如：
    - 后端 UUID 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy` 设置为 `true`
    - 存储前缀 `trident`

    - PVC UUID a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - 名为 trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c 的 qtree 为名为 `trident-403b5326-8482-40db96d0-d83fb3f4daec`的 FlexVol 创建导出策略，为名为 `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c`的 qtree 创建导出策略，并在 SVM 上创建名为 `trident_empty`的空导出策略。FlexVol 导出策略的规则将是 qtree 导出策略中包含的任何规则的超集。空导出策略将由未附加的任何卷重用。
- `autoExportCIDRs` 包含地址块列表。此字段是可选的，默认为 ["0.0.0.0/0", "::/0"]。如果未定义，Trident 会添加在工作节点上找到的所有全局范围单播地址及其发布。

在此示例中，提供了 `192.168.0.0/24` 地址空间。这表示此地址范围内包含发布的 Kubernetes 节点 IP 将被添加到 Trident 创建的导出策略中。当 Trident 注册其运行的节点时，它会检索节点的 IP 地址，并根据 `autoExportCIDRs` 中提供的地址块进行检查。发布时，过滤 IP 后，Trident 为其发布到的节点的客户端 IP 创建导出策略规则。

您可以在创建后端后对其 `autoExportPolicy`和 `autoExportCIDRs`进行更新。您可以为自动管理的后端追加新的 CIDR 或删除现有的 CIDR。删除 CIDR 时要小心，以确保现有连接不会丢失。您还可以选择对后端禁用 `autoExportPolicy`并回退到手动创建的导出策略。这将需要在后端配置中设置 `exportPolicy`参数。

在 Trident 创建或更新后端后，您可以使用 `tridentctl`或相应的 `tridentbackend` CRD 检查后端：

```
./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>
      fileSystemType: ext4
```

删除节点时，Trident 检查所有导出策略，以删除与该节点对应的访问规则。通过从托管后端的导出策略中删除此节点 IP，Trident 可以防止流氓挂载，除非此 IP 被集群中的新节点重用。

对于以前存在的后端，使用 `tridentctl update backend`更新后端可确保 Trident 自动管理导出策略。这会在需要时创建两个以后端 UUID 和 qtree 名称命名的新导出策略。后端上存在的卷在卸载并再次装载后将使用新创建的导出策略。

删除具有自动管理导出策略的后端将删除动态创建的导出策略。如果重新创建后端，它将被视为新的后端，并将导致创建新的导出策略。

如果实时节点的 IP 地址已更新，则必须在节点上重新启动 Trident pod。然后，Trident 将更新其管理的后端的导出策略，以反映此 IP 更改。

准备配置 SMB 卷

通过一些额外的准备，您可以使用 `ontap-nas` 驱动程序配置 SMB 卷。

必须在 SVM 上配置 NFS 和 SMB/CIFS 协议，才能为 ONTAP 本地群集创建 `ontap-nas-economy` SMB 卷。无法配置这些协议中的任何一个都将导致 SMB 卷创建失败。

`autoExportPolicy` 不支持 SMB 卷。

开始之前

在设置 SMB 卷之前，必须具有下列内容。

- 具有 Linux 控制器节点和至少一个运行 Windows Server 2022 的 Windows worker 节点的 Kubernetes 集群。Trident 仅支持将 SMB 卷挂载到在 Windows 节点上运行的 Pod。
- 至少有一个包含您的 Active Directory 凭据的 Trident 密码。要生成密钥 `smbcreds`：

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

- 配置为 Windows 服务的 CSI 代理。要配置 `csi-proxy`，请参阅"GitHub：CSI Proxy"或"GitHub：适用于 Windows 的 CSI 代理"了解在 Windows 上运行的 Kubernetes 节点。

步骤

1. 对于本地 ONTAP，您可以选择创建 SMB 共享，或者 Trident 可以为您创建一个共享。

   Amazon FSx for ONTAP 需要 SMB 共享。

   您可以使用 "Microsoft 管理控制台" 共享文件夹管理单元或使用 ONTAP CLI 以两种方式之一创建 SMB 管理共享。要使用 ONTAP CLI 创建 SMB 共享：

   a. 如有必要，请为共享创建目录路径结构。

      此 `vserver cifs share create` 命令在共享创建期间检查 -path 选项中指定的路径。如果指定的路径不存在，则命令失败。

   b. 创建与指定 SVM 关联的 SMB 共享：

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

c. 验证是否已创建此共享：

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

有关详细信息，请参见 "创建 SMB 共享"。

2. 创建后端时，必须配置以下内容以指定 SMB 卷。对于所有 FSx for ONTAP 后端配置选项，请参阅 "FSx for ONTAP 配置选项和示例"。

参数	说明	示例
`smbShare`	可以指定以下选项之一：使用 Microsoft Management Console 或 ONTAP CLI 创建的 SMB 共享的名称；允许 Trident 创建 SMB 共享的名称；或者可以将参数留空以阻止对卷的公共共享访问。此参数对于本地 ONTAP 是可选的。此参数是 Amazon FSx for ONTAP 后端所必需的，不能为空。	`smb-share`
`nasType`	*必须设置为 `smb`。*如果为 null，则默认为 `nfs`。	`smb`
`securityStyle`	新卷的安全样式。对于 **SMB** 卷，必须设置为 **`ntfs`** 或 **`mixed`**。	`ntfs` 或 `mixed` 用于 SMB 卷
`unixPermissions`	新卷的模式。对于 **SMB** 卷，必须留空。	""

启用安全 SMB

从 25.06 版本开始，NetApp Trident 支持使用 `ontap-nas`和 `ontap-nas-economy`后端创建的 SMB 卷的安全配置。启用安全 SMB 后，可以使用访问控制列表 (ACL) 为 Active Directory (AD) 用户和用户组提供对 SMB 共享的受控访问。

需要记住的要点

- 不支持导入 `ontap-nas-economy`卷。
- 仅支持 `ontap-nas-economy` 卷的只读克隆。
- 如果启用了安全 SMB，Trident 将忽略后端中提到的 SMB 共享。
- 更新 PVC 注释、存储类注释和后端字段不会更新 SMB 共享 ACL。
- 在克隆 PVC 的注释中指定的 SMB 共享 ACL 将优先于源 PVC 中的 ACL。
- 确保在启用安全 SMB 的同时提供有效的 AD 用户。无效用户将不会添加到 ACL。
- 如果在后端、存储类和 PVC 中为相同的 AD 用户提供不同的权限，则权限优先级为：PVC、存储类，然后是后端。
- 安全 SMB 受 `ontap-nas`托管卷导入支持，不适用于非托管卷导入。

步骤

1. 如下面的示例所示，在 TridentBackendConfig 中指定 adAdminUser：

```
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. 在存储类中添加批注。

   将 `trident.netapp.io/smbShareAdUser` 注释添加到存储类，以始终启用安全的 SMB。为注释 `trident.netapp.io/smbShareAdUser`指定的用户值应与 `smbcreds`密钥中指定的用户名相同。您可以从以下选项中选择一项 `smbShareAdUserPermission`： `full_control`、 `change`或 `read`。默认权限为 `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. 创建 PVC。

以下示例创建了 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 配置选项和示例

了解如何在 Trident 安装中创建和使用 ONTAP NAS 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。从 25.10 版本开始，NetApp Trident 支持 "NetApp AFX 存储系统"。NetApp AFX 存储系统与其他基于 ONTAP 的系统（ASA、AFF 和 FAS）在存储层的实现方面有所不同。

仅支持 `ontap-nas`驱动程序（使用 NFS 协议）用于 NetApp AFX 系统；不支持 SMB 协议。

后端配置选项

在 Trident 后端配置中，无需指定您的系统是 NetApp AFX 存储系统。当您选择 `ontap-nas`作为 `storageDriverName`时，Trident 会自动检测 AFX 存储系统。某些后端配置参数不适用于 AFX 存储系统。

下表显示了后端配置选项：

参数	说明	默认
`version`		始终为 1
`storageDriverName`	存储驱动程序的名称 对于 NetApp AFX 系统，仅支持 `ontap-nas`。	`ontap-nas`， `ontap-nas-economy`，或 `ontap-nas-flexgroup`

参数	说明	默认
backendName	自定义名称或存储后端	驱动程序名称 + "_" + dataLIF
managementLIF	集群或 SVM 管理 LIF 的 IP 地址，也可以指定完全限定域名（FQDN）。如果使用 IPv6 标志安装了 Trident，则可以设置为使用 IPv6 地址。IPv6 地址必须在方括号中定义，例如 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。有关无缝 MetroCluster 切换，请参见 MetroCluster 示例。	“10.0.0.1”，“[2001:1234:abcd::fefe]”
dataLIF	协议 LIF 的 IP 地址。NetApp 建议指定 dataLIF。如果未提供，Trident 将从 SVM 获取 dataLIF。可以指定要用于 NFS 挂载操作的完全限定域名 (FQDN)，允许您创建轮询 DNS 以跨多个 dataLIF 进行负载平衡。可以在初始设置后更改。请参见 。如果使用 IPv6 标志安装了 Trident，则可以设置为使用 IPv6 地址。IPv6 地址必须在方括号中定义，例如 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。*省略 MetroCluster。*请参阅MetroCluster 示例。	指定地址或源自 SVM，如果未指定（不推荐）
svm	要使用的 Storage Virtual Machine *对于 MetroCluster 请省略。*请参阅MetroCluster 示例。	如果指定了 SVM managementLIF，则派生
autoExportPolicy	启用自动导出策略创建和更新 [Boolean]。使用 `autoExportPolicy`和 `autoExportCIDRs`选项，Trident 可以自动管理导出策略。	false
autoExportCIDRs	启用 `autoExportPolicy`时用于过滤 Kubernetes 节点 IP 的 CIDR 列表。使用 `autoExportPolicy`和 `autoExportCIDRs`选项，Trident 可以自动管理导出策略。	["0.0.0.0/0", "::/0"]`
labels	要应用于卷的任意 JSON 格式标签集	""
clientCertificate	客户端证书的 Base64 编码值。用于基于证书的身份验证	""
clientPrivateKey	客户端私钥的 Base64 编码值。用于基于证书的身份验证	""
trustedCACertificate	受信任 CA 证书的 Base64 编码值。可选。用于基于证书的身份验证	""
username	连接到集群/SVM 的用户名。用于基于凭据的身份验证。有关 Active Directory 身份验证，请参阅 "使用 Active Directory 凭据向后端 SVM 验证 Trident"。	
password	连接到集群/SVM 的密码。用于基于凭据的身份验证。有关 Active Directory 身份验证，请参阅 "使用 Active Directory 凭据向后端 SVM 验证 Trident"。	

参数	说明	默认
`storagePrefix`	在 SVM 中配置新卷时使用的前缀。设置后无法更新 当使用 ontap-nas-economy 和 24 个或更多字符的 storagePrefix 时，qtree 将不会嵌入存储前缀，尽管它将位于卷名称中。	“trident”
`aggregate`	用于配置的聚合（可选；如果设置，则必须分配给 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的聚合来配置 FlexGroup 卷。 当聚合在 SVM 中更新时，它会通过轮询 SVM 在 Trident 中自动更新，而无需重新启动 Trident Controller。当您在 Trident 中配置了特定聚合来配置卷时，如果聚合被重命名或移出 SVM，则在轮询 SVM 聚合时，后端将在 Trident 中移至失败状态。您必须将聚合更改为存在于 SVM 上的聚合，或者将其完全删除，以使后端恢复联机。 不要为 **AFF** 存储系统指定。	""
`limitAggregateUsage`	如果使用率超过此百分比，则配置失败。不适用于 **Amazon FSx for ONTAP**。不要为 **AFF** 存储系统指定。	"（默认情况下不强制执行）
flexgroupAggregateList	用于配置的聚合列表（可选；如果设置，则必须分配给 SVM）。分配给 SVM 的所有聚合都用于配置 FlexGroup 卷。支持 **ontap-nas-flexgroup** 存储驱动程序。 在 SVM 中更新聚合列表时，通过轮询 SVM 自动在 Trident 中更新列表，而无需重新启动 Trident Controller。当您在 Trident 中配置了特定的聚合列表来配置卷时，如果聚合列表被重命名或移出 SVM，则在轮询 SVM 聚合时，后端将移至 Trident 中的失败状态。您必须将聚合列表更改为 SVM 上存在的列表，或者将其完全删除，以使后端恢复联机。	""
`limitVolumeSize`	如果请求的卷大小高于此值，则设置失败。	"（默认情况下不强制执行）
`debugTraceFlags`	故障排除时使用的调试标志。例如，{"api":false, "method":true} 除非正在进行故障排除并需要详细的日志转储，否则不要使用 `debugTraceFlags`。	空

参数	说明	默认
nasType	配置 NFS 或 SMB 卷创建。选项为 nfs、 smb`或 null。设置为 null 默认为 NFS 卷。如果指定，对于 **AFF** 存储系统始终设置为 `**nfs**。	nfs
nfsMountOptions	NFS 挂载选项的逗号分隔列表。Kubernetes 持久卷的挂载选项通常在存储类中指定，但如果存储类中未指定挂载选项，则 Trident 将回退到使用存储后端配置文件中指定的挂载选项。如果存储类或配置文件中未指定挂载选项，Trident 将不会在关联的持久卷上设置任何挂载选项。	""
qtreesPerFlexvol	每个 FlexVol 的最大 Qtrees，必须在 [50, 300] 范围内	"200"
smbShare	可以指定以下选项之一：使用 Microsoft Management Console 或 ONTAP CLI 创建的 SMB 共享的名称；允许 Trident 创建 SMB 共享的名称；或者可以将参数留空以阻止对卷的公共共享访问。此参数对于本地 ONTAP 是可选的。此参数是 Amazon FSx for ONTAP 后端所必需的，不能为空。	smb-share
useREST	使用 ONTAP REST API 的布尔参数。 useREST`设置为 `true`时，Trident 使用 ONTAP REST API 与后端通信；设置为 `false`时，Trident 使用 ONTAPI (ZAPI) 调用与后端通信。此功能需要 ONTAP 9.11.1 及更高版本。此外，所使用的 ONTAP 登录角色必须能够访问 `ontapi`应用程序。这通过预定义的 `vsadmin`和 `cluster-admin`角色来满足。从 Trident 24.06 版本和 ONTAP 9.15.1 或更高版本开始， `useREST`默认设置为 `true；将 useREST`更改为 `false`以使用 ONTAPI (ZAPI) 调用。如果指定，对于 **AFF** 存储系统始终设置为 `**true**。	true 适用于 ONTAP 9.15.1 或更高版本，否则 false。
limitVolumePoolSize	在 ontap-nas-economy 后端使用 Qtrees 时的最大可请求 FlexVol 大小。	"（默认情况下不强制执行）
denyNewVolumePools	限制 `ontap-nas-economy`后端创建新 FlexVol 卷以包含其 Qtree。仅预先存在的 FlexVol 用于配置新的 PV。	
adAdminUser	具有 SMB 共享完全访问权限的 Active Directory 管理员用户或用户组。使用此参数为具有完全控制权限的 SMB 共享提供管理员权限。	

用于配置卷的后端配置选项

您可以使用配置的 defaults 部分中的这些选项来控制默认配置。有关示例，请参阅下面的配置示例。

参数	说明	默认
spaceAllocation	Qtree 的空间分配	"true"

参数	说明	默认
spaceReserve	空间预留模式；"none"（精简）或 "volume"（厚）	"无"
snapshotPolicy	要使用的 Snapshot 策略	"无"
qosPolicy	要为创建的卷分配的 QoS 策略组。为每个存储池/后端选择 qosPolicy 或 adaptiveQosPolicy 中的一个	""
adaptiveQosPolicy	要为创建的卷分配的自适应 QoS 策略组。为每个存储池/后端选择 qosPolicy 或 adaptiveQosPolicy 中的一个。ontap-nas-economy 不支持此功能。	""
snapshotReserve	为快照预留的卷百分比	"0" 如果 snapshotPolicy 为 "none"，否则为 "
splitOnClone	创建时从其父级拆分克隆	"false"
encryption	在新卷上启用 NetApp Volume Encryption (NVE)；默认为 false。必须在群集上许可并启用 NVE 才能使用此选项。如果在后端启用了 NAE，则在 Trident 中配置的任何卷都将启用 NAE。有关更多信息，请参阅："Trident 如何与 NVE 和 NAE 配合使用"。	"false"
tieringPolicy	要使用"none"的分层策略	
unixPermissions	新卷的模式	NFS 卷为 "777"；SMB 卷为空（不适用）
snapshotDir	控制对 .snapshot 目录的访问	true, false (显式设置)。
exportPolicy	要使用的导出策略	"default"
securityStyle	新卷的安全样式。NFS 支持 `mixed`和 `unix`安全样式。SMB 支持 `mixed`和 `ntfs`安全样式。	NFS 默认值为 unix。SMB 默认值为 ntfs。
nameTemplate	用于创建自定义卷名称的模板。	""

在 Trident 中使用 QoS 策略组需要 ONTAP 9.8 或更高版本。您应该使用非共享 QoS 策略组，并确保该策略组单独应用于每个组成部分。共享 QoS 策略组强制执行所有工作负载总吞吐量的上限。

卷配置示例

以下是定义了默认值的示例：

```
---
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"
```

对于 `ontap-nas`和 `ontap-nas-flexgroups`，Trident 现在使用新的计算来确保 FlexVol 使用 snapshotReserve 百分比和 PVC 正确调整大小。当用户请求 PVC 时，Trident 使用新的计算创建具有更多空间的原始 FlexVol。此计算可确保用户收到他们在 PVC 中请求的可写空间，而不是少于他们请求的空间。在 v21.07 之前，当用户请求 PVC（例如 5 GiB）时，如果 snapshotReserve 为 50%，则仅获得 2.5 GiB 的可写空间。这是因为用户请求的是整个卷，而 `snapshotReserve`是该卷的百分比。对于 `Trident 21.07`，用户要求的是可写空间，`Trident` 将 `snapshotReserve`数字定义为整个卷的百分比。此情况不适用于 `ontap-nas-economy`。请参见以下示例以了解其工作原理：

计算结果如下所示：

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

对于 snapshotReserve = 50% 和 PVC 请求 = 5 GiB，总体积大小为 5/.5 = 10 GiB，可用大小为 5 GiB，这是用户在 PVC 请求中请求的内容。 `volume show`命令应显示类似于以下示例的结果：

升级 Trident 时，先前安装的现有后端将按上述说明配置卷。对于升级前创建的卷，应调整其卷的大小，以便观察更改。例如，较早的 2 GiB PVC 与 `snapshotReserve=50`导致提供 1 GiB 可写空间的卷。例如，将卷的大小调整为 3 GiB，可在 6 GiB 卷上为应用程序提供 3 GiB 的可写空间。

最小配置示例

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。

> 如果要在 Trident 上使用 Amazon FSx for NetApp ONTAP，建议为 LIF 指定 DNS 名称而不是 IP 地址。

ONTAP NAS 经济示例

```
---
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 示例

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

MetroCluster 示例

您可以配置后端，以避免在 "SVM 复制和恢复" 期间进行切换和切换后手动更新后端定义。

对于无缝切换和切回，使用 `managementLIF` 指定 SVM 并省略 `dataLIF` 和 `svm` 参数。例如：

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

SMB 卷示例

```
---
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
```

基于证书的身份验证示例

这是一个最小后端配置示例。 `clientCertificate`、 `clientPrivateKey` 和 `trustedCACertificate`（可选，如果使用受信任的 CA）分别填充在 `backend.json` 中并获取客户端证书、私钥和可信 CA 证书的 base64 编码值。

```
---
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_
```

自动导出策略示例

此示例演示如何指导 Trident 使用动态导出策略自动创建和管理导出策略。这对 `ontap-nas-economy` 和 `ontap-nas-flexgroup` 驱动程序也同样适用。

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-nasbackend
autoExportPolicy: true
autoExportCIDRs:
- 10.0.0.0/24
username: admin
password: password
nfsMountOptions: nfsvers=4
```

IPv6 地址示例

此示例显示了 `managementLIF`使用 IPv6 地址。

```
---
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** 卷的 **Amazon FSx for ONTAP** 示例

对于使用 SMB 卷的 FSx for ONTAP， `smbShare` 参数是必需的。

```
---
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_
```

带有 **nameTemplate** 的后端配置示例

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

具有虚拟池的后端示例

在下面显示的示例后端定义文件中，为所有存储池设置了特定的默认值，例如 `spaceReserve`为 none、`spaceAllocation`为 false 和 `encryption`为 false。虚拟池在存储部分中定义。

Trident 在"Comments"字段中设置配置标签。Comments 设置在 FlexVol 上用于 `ontap-nas`或 `FlexGroup` 用于 `ontap-nas-flexgroup`。Trident 在配置时将虚拟池上存在的所有标签复制到存储卷。为方便起见，存储管理员可以为每个虚拟池定义标签，并按标签对卷进行分组。

在这些示例中，一些存储池设置了自己的 `spaceReserve`、 `spaceAllocation` 和 `encryption` 值，而一些池覆盖了默认值。

ONTAP NAS 示例

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

ONTAP NAS FlexGroup 示例

```
---
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 经济示例

```
---
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"
```

将后端映射到 StorageClasses

以下 StorageClass 定义参考了 [具有虚拟池的后端示例]。使用 `parameters.selector` 字段，每个 StorageClass 调用哪些虚拟池可用于托管卷。卷将具有所选虚拟池中定义的方面。

- `protection-gold` StorageClass 将映射到 `ontap-nas-flexgroup`后端中的第一个和第二个虚拟池。这些是唯一提供黄金级保护的池。

```
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 `ontap-nas-flexgroup`后端的第三个和第四个虚拟池。这些是唯一提供黄金以外防护等级的池。

```
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 将映射到 `ontap-nas`后端的第四个虚拟池。这是唯一为 mysqldb 类型应用程序提供存储池配置的池。

```
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 `ontap-nas-flexgroup`后端中的第三个虚拟池。这是唯一提供银级保护和 20000 creditpoints 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 `ontap-nas`后端中的第三个虚拟池和 `ontap-nas-economy`后端中的第二个虚拟池。这些是唯一拥有 5000 个信用点的池产品。

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

Trident 将决定选择哪个虚拟池，并确保满足存储要求。

初始配置后更新 `dataLIF`

您可以在初始配置后通过运行以下命令更改 dataLIF，以提供具有更新的 dataLIF 的新后端 JSON 文件。

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

如果 PVC 连接到一个或多个 pod，则必须关闭所有相应的 pod，然后将其重新启动，以使新的 dataLIF 生效。

安全 SMB 示例

带有 ontap-nas 驱动程序的后端配置

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

使用 ontap-nas-economy 驱动程序的后端配置

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

使用存储池的后端配置

```yaml
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
```

带有 **ontap-nas** 驱动程序的存储类示例

```yaml
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
```

请确保添加 `annotations`以启用安全的 SMB。如果没有注释，无论后端或 PVC 中设置的配置如何，Secure SMB 都无法正常工作。

具有 **ontap-nas-economy** 驱动程序的存储类示例

```
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
```

单个 **AD** 用户的 **PVC** 示例

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

具有多个 **AD** 用户的 **PVC** 示例

```
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
```