



ONTAP NAS 驱动程序

Trident

NetApp
February 02, 2026

目录

ONTAP NAS 驱动程序	1
ONTAP NAS驱动程序概述	1
ONTAP NAS驱动程序详细信息	1
用户权限	1
准备使用ONTAP NAS驱动程序配置后端	2
要求	2
对ONTAP后端进行身份验证	2
管理 NFS 导出策略	7
准备配置SMB卷	10
ONTAP NAS配置选项和示例	13
后端配置选项	13
用于配置卷的后端配置选项	16
最低配置示例	19
虚拟池后端示例	23
将后端映射到 StorageClasses	29
更新 dataLIF 初始配置后	30
安全 SMB 示例	31

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提供了以下NAS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-nas	NFS SMB	文件系统	Rwo、ROX、rwx、RWOP	""、nfs, smb
ontap-nas-economy.	NFS SMB	文件系统	Rwo、ROX、rwx、RWOP	""、nfs, smb
ontap-nas-flexgroup	NFS SMB	文件系统	Rwo、ROX、rwx、RWOP	""、nfs, smb



- 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。

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）在存储层的实现方式上有所不同。



只有 `ontap-nas` AFX 系统支持 NFS 协议驱动程序；不支持 SMB 协议。

在Trident后端配置中，您无需指定您的系统是 AFX。当您选择 `ontap-nas` 作为 `storageDriverName` Trident可自动检测 AFX 系统。

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，并创建指向其中一个驱动程序的存储类。例如、您可以配置一个使用的黄金类 `ontap-nas` 驱动程序和使用的铜牌类 `ontap-nas-economy` 一个。
- 所有Kubernetes工作节点都必须安装适当的NFS工具。请参见 ["此处"](#) 有关详细信息：
- Trident仅支持挂载到Windows节点上运行的Pod的SMB卷。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提供了两种对ONTAP后端进行身份验证的模式。

- 基于凭据：此模式需要对ONTAP后端具有足够的权限。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）（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

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
credentials:
  name: secret-backend-creds
```

JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "credentials": {
    "name": "secret-backend-creds"
  }
}
```

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 / 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。
- `trustedCACertificate`：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=vsadmin"
```

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
```

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 <SVM 管理 LIF> 和 <SVM 名称> 替换为管理 LIF IP 和 ONTAP 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...Vaaalllluuuuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident

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

更新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、使用更新后的backend.json文件、该文件包含要执行的所需参数 `tridentctl update backend`。

```
cat cert-backend-updated.json
```

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "password",
  "storagePrefix": "myPrefix_"
}
```

```
#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
```

NAME	STORAGE DRIVER	UUID
NasBackend	ontap-nas	98e19b74-aec7-4a3d-8dcf-128e5033b214



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"](#)

管理 NFS 导出策略

Trident使用NFS导出策略控制对其配置的卷的访问。

使用导出策略时、Trident提供了两个选项：

- Trident可以动态管理导出策略本身；在此操作模式下、存储管理员可以指定一个表示可接受IP地址的CIDR块列表。Trident会在发布时自动将这些范围内的适用节点IP添加到导出策略中。或者、如果未指定CIDR、则在要发布卷的节点上找到的所有全局范围单播IP都将添加到导出策略中。
- 存储管理员可以手动创建导出策略和添加规则。除非在配置中指定了其他导出策略名称、否则Trident将使用默认导出策略。

动态管理导出策略

通过Trident、可以动态管理ONTAP后端的导出策略。这样，存储管理员就可以为工作节点 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；修改导出策略不再需要手动干预存储集群。此外、这还有助于将对存储集群的访问限制为仅限正在挂载卷且IP位于指定范围内的工作节点访问、从而支持精细的自动化管理。



使用动态导出策略时、请勿使用网络地址转换(Network Address Translation、NAT)。使用NAT时、存储控制器会看到前端NAT地址、而不是实际IP主机地址、因此、如果在导出规则中找不到匹配项、则会拒绝访问。

示例

必须使用两个配置选项。下面是一个后端定义示例：

```
---
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、您必须确保SVM中的根接合具有先前创建的导出策略、并具有允许节点CIDR块的导出规则(例如默认导出策略)。始终遵循NetApp建议的最佳实践、将SVM专用于Trident。

以下是使用上述示例对此功能的工作原理进行的说明：

- autoExportPolicy` 设置为 `true。这表示Trident会为SVM的使用此后端配置的每个卷创建一个导出策略 svm1、并使用地址块处理规则的添加和删除 autoexportCIDRs。在将卷连接到节点之前、此卷会使用一个空导出策略、此策略不带任何规则来防止对该卷进行不必要的访问。将卷发布到节点后、Trident会创建一个与指定CIDR块中包含节点IP的底层qtree同名的导出策略。这些IP也会添加到父FlexVol volume使用的导出策略中
 - 例如：
 - 后端UUID 403b5326/8482-40db-96d0-d83fb3f4daec
 - autoExportPolicy` 将设置为 `true

- 存储前缀 trident
- pvc UUID a79bcf5f-7b6d-4a40-9876- e2551f159c1c
- 名为svm_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c的qtree会为名为的FlexVol创建一个导出策略、为名为的qtree创建一个导出策略、
trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c`并在Trident上创建
`trident-403b5326-8482-40db96d0-d83fb3f4daec`一个名为的空导出策略
`trident\_empty`。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。空导出策略将由所有未附加的卷重复使用。
- `autoExportCIDRs`包含地址块列表。此字段为可选字段，默认为 "0.0.0.0/0"，": : /0"。如果未定义、则Trident会添加在具有出版物的工作节点上找到的所有全局范围单播地址。

在此示例中、192.168.0.0/24`提供了地址空间。这表示属于此地址范围且发布内容的Kub联网 节点IP将添加到Trident创建的导出策略中。当Trident注册运行该功能的节点时，它将检索该节点的IP地址，并根据中提供的地址块对其进行检查 `autoExportCIDRs`。发布时，在筛选IP之后，Trident将为要发布到的节点的客户端IP创建导出策略规则。

创建后，您可以为后端更新 autosExportPolicy 和 autosExportCIDR。您可以为自动管理的后端附加新的 CIDR，也可以删除现有的 CIDR。删除 CIDR 时请务必小心，以确保现有连接不会断开。您也可以选择对后端禁用 autosExportPolicy，并回退到手动创建的导出策略。这需要在后端配置中设置 exportPolicy 参数。

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

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

删除节点后、Trident会检查所有导出策略以删除与该节点对应的访问规则。通过从受管后端的导出策略中删除此节点IP、Trident可防止恶意挂载、除非集群中的新节点重复使用此IP。

对于以前存在的后端、使用更新后端 `tridentctl update backend` 可确保Trident自动管理导出策略。这样会根据需要创建两个新的导出策略、并以后端的UUID和qtree名称命名。后端上的卷在卸载并重新挂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，则会将其视为新的后端，并会创建新的导出策略。

如果更新了活动节点的IP地址、则必须在此节点上重新启动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

只需稍作准备、您就可以使用配置SMB卷 `ontap-nas` 驱动程序。



您必须在SVM上同时配置NFS和SMB/CCIFS协议、才能为ONTAP内部集群创建 `ontap-nas-economy` SMB卷。如果未能配置其中任一协议、则发生原因 SMB卷创建将失败。



`autoExportPolicy` SMB卷不支持。

开始之前

在配置SMB卷之前、您必须满足以下条件。

- 一个Kubernetes集群、其中包含一个Linux控制器节点以及至少一个运行Windows Server 2022的Windows工作节点。Trident仅支持挂载到Windows节点上运行的Pod的SMB卷。
- 至少一个包含Active Directory凭据的Trident密钥。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。配置 `csi-proxy`、请参见 ["GitHub：CSI代理"](#) 或 ["GitHub：适用于Windows的CSI代理"](#) 适用于在Windows上运行的Kubernetes节点。

步骤

1. 对于内部ONTAP、您可以选择创建SMB共享、也可以选择Trident为您创建一个共享。



Amazon FSx for ONTAP需要SMB共享。

您可以使用以下两种方式之一创建SMB管理共享 ["Microsoft管理控制台"](#) 共享文件夹管理单元或使用ONTAP命令行界面。要使用ONTAP 命令行界面创建SMB共享、请执行以下操作：

- a. 如有必要，为共享创建目录路径结构。

。 `vserver cifs share create` 命令会在创建共享期间检查-path选项中指定的路径。如果指定路径不存在，则命令将失败。

- b. 创建与指定SVM关联的SMB共享：

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

c. 验证是否已创建共享：

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



请参见 ["创建 SMB 共享"](#) 了解完整详细信息。

2. 创建后端时、必须配置以下内容以指定SMB卷。有关适用于ONTAP 后端的所有FSX配置选项、请参见 ["适用于ONTAP 的FSX配置选项和示例"](#)。

参数	Description	示例
smbShare	您可以指定以下选项之一：使用Microsoft管理控制台或ONTAP命令行界面创建的SMB共享的名称；允许Trident创建SMB共享的名称；或者、您可以将参数留空以防止对卷进行通用共享访问。对于内部ONTAP、此参数是可选的。此参数对于Amazon FSx for ONTAP后端为必填项、不能为空。	smb-share
nasType	*必须设置为 smb` 如果为空、则默认为 `nfs。	smb
securityStyle	新卷的安全模式。必须设置为 ntfs 或 mixed 用于 SMB 卷。	ntfs 或 mixed 对于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 支持使用以下方式创建的 SMB 卷的安全配置 `ontap-nas`和 `ontap-nas-economy`后端。启用安全 SMB 后，您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

- 输入 `ontap-nas-economy`不支持卷。
- 仅支持只读克隆 `ontap-nas-economy` 卷。
- 如果启用了安全 SMB，Trident 将忽略后端提到的 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。
- 克隆 PVC 注释中指定的 SMB 共享 ACL 将优先于源 PVC 中的 ACL。
- 启用安全 SMB 时，请确保提供有效的 AD 用户。无效用户将不会被添加到 ACL。
- 如果您在后端、存储类和 PVC 中为同一个 AD 用户提供不同的权限，则权限优先级为：PVC、存储类、后端。
- 安全 SMB 支持 `ontap-nas`托管卷导入，不适用于非托管卷导入。

步骤

1. 在 TridentBackendConfig 中指定 adAdminUser，如以下示例所示：

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.193.176.x
  svm: svm0
  useREST: true
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

2. 在存储类中添加注释。

添加 `trident.netapp.io/smbShareAdUser` 注释到存储类，以启用安全 SMB 而不会失败。为注释指定的用户值 `trident.netapp.io/smbShareAdUser` 应该与 `smbcreds` 秘密。您可以选择以下之一 `smbShareAdUserPermission: full_control`，`change`，或者 `read`。默认权限是 `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 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）在存储层的实现方式上有所不同。



只有 `ontap-nas` NetApp AFX 系统支持 NFS 协议驱动程序；不支持 SMB 协议。

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` Trident会自动检测 AFX 存储系统。如下表所示，某些后端配置参数不适用于 AFX 存储系统。

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

参数	Description	Default
storageDriverName	存储驱动程序的名称  仅适用于NetApp AFX 系统 `ontap-nas` 已支持。	ontap-nas ontap-nas-economy`或`ontap-nas-flexgroup
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。	"10.0.0.1"、"[2001: 1234: abc: : fefe]"
dataLIF	协议 LIF 的 IP 地址。NetApp建议指定 dataLIF。如果未提供此参数、则Trident将从SVM提取数据LIF。您可以指定要用于NFS挂载操作的完全限定域名(FQDN)、以便创建轮叫DNS来在多个dataLIF之间进行负载平衡。可以在初始设置后更改。请参阅。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]。*省略MetroCluster。*请参见MetroCluster示例。	指定的地址或派生自SVM (如果未指定)(不建议)
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
autosExportPolicy	启用自动创建和更新导出策略[布尔值]。使用 `autoExportPolicy` 和 `autoExportCIDRs` 选项、Trident 可以自动管理导出策略。	false
autosExportCIDR	用于筛选KubeNet节点IP的CIDR列表(启用时)。`autoExportPolicy` 使用 `autoExportPolicy` 和 `autoExportCIDRs` 选项、Trident可以自动管理导出策略。	["0.0.0.0/0、": : : /0"]
标签	要应用于卷的一组任意 JSON 格式的标签	""
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	""
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	""
用户名	用于连接到集群/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 的身份" 。	

参数	Description	Default
密码	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 的身份" 。	
s存储前缀	在 SVM 中配置新卷时使用的前缀。设置后无法更新  如果使用的ONTAP是包含24个或更多字符的storagePrefix、则qtrees不会嵌入存储前缀、但会显示在卷名称中。	"三级联"
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。 请勿指定用于 AFX 存储系统。	""
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 。请勿指定用于 AFX 存储系统。	""（默认情况下不强制实施）
FlexgroupGroupRegateList	要配置的聚合列表(可选；如果已设置、则必须将其分配给SVM)。分配给SVM的所有聚合均用于配置FlexGroup卷。支持* ONTAP—NAS—FlexGroup—Storage驱动程序。  在SVM中更新聚合列表后、此列表将在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中配置特定聚合列表以配置卷后、如果聚合列表重命名或移出SVM、则在轮询SVM聚合时、后端将在Trident中变为故障状态。您必须将聚合列表更改为SVM上的聚合列表、或者将其全部删除、以使后端恢复联机。	""
limitVolumeSize	如果请求的卷大小大于此值，则配置失败。	""(默认情况下不强制实施)

参数	Description	Default
debugTraceFlags	故障排除时要使用的调试标志。例如、 {"api": false、"METHO": true} 请勿使用 debugTraceFlags 除非您正在进行故障排除并需要详细的日志转储。	空
nasType	配置 NFS 或 SMB 卷的创建。选项有 nfs, `smb` 或空值。设置为 null 则默认使用 NFS 卷。如果指定, 则始终设置为 `nfs` 适用于 AFX 存储系统。	nfs
nfsMountOptions	NFS挂载选项的逗号分隔列表。通常会在存储类中为Kubernetes-永久性 卷指定挂载选项、但如果在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。如果在存储类或配置文件中未指定挂载选项、则Trident不会在关联的永久性卷上设置任何挂载选项。	""
qtreesPerFlexvol	每个 FlexVol 的最大 qtree 数, 必须在 50 , 300 范围内	"200"
smbShare	您可以指定以下选项之一: 使用Microsoft管理控制台或ONTAP命令行界面创建的SMB共享的名称; 允许Trident创建SMB共享的名称; 或者、您可以将参数留空以防止对卷进行通用共享访问。对于内部ONTAP、此参数是可选的。此参数对于Amazon FSx for ONTAP后端为必填项、不能为空。	smb-share
useREST	使用ONTAP REST API 的布尔参数。`useREST` 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登录角色必须具有访问权限。`ontapi` 应用。预定义项满足了这一点。`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; 更改 `useREST` 到 `false` 使用 ONTAPI (ZAPI) 调用。如果指定, 则始终设置为 `true` 适用于 AFX 存储系统。	true 对于ONTAP 9.151或更高版本, 否则 false。
limitVolumePoolSize	在qtree-NAS ONTAP经济型后端使用qtrees时可请求的最大FlexVol大小。	"" (默认情况下不强制实施)
denyNewVolumePools	限制 `ontap-nas-economy` 后端创建新的FlexVol卷以包含其qtrees。仅会使用已有的FlexVol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。使用此参数可为 SMB 共享提供具有完全控制权的管理员权限。	

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	qtrees的空间分配	"正确"
s页面预留	空间预留模式；"无"(精简)或"卷"(厚)	"无"
sSnapshot 策略	要使用的 Snapshot 策略	"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	""
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。不受 ontap-nas-economy.	""
sSnapshot 预留	为快照预留的卷百分比	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
分层策略	使用"无"的层策略	
unixPermissions	新卷的模式	"777"表示NFS卷；空(不适用)表示SMB卷
snapshotDir	控制对的访问 .snapshot 目录	对于NFSv4、为"TRUE"；对于NFSv3、为"false"
exportPolicy	要使用的导出策略	default
securityStyle	新卷的安全模式。NFS支持 mixed 和 unix 安全模式。SMB支持 mixed 和 ntfs 安全模式。	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。	""



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。

卷配置示例

下面是一个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"

```

为了 ontap-nas 和 ontap-nas-flexgroups Trident 现在使用新的计算方法，以确保 FlexVol 的尺寸与 snapshotReserve 百分比和 PVC 正确匹配。当用户请求 PVC 时，Trident 会使用新的计算方法创建具有更多空间的原始 FlexVol。此计算确保用户在 PVC 中获得其请求的可写空间，而不是少于其请求的空间。在 v21.07 之前，当用户请求 PVC（例如 5 GiB）时，如果快照预留百分比为 50%，则只能获得 2.5 GiB 的可写空间。这是因为用户请求的是整个卷。snapshotReserve 是其中的百分比。在 Trident 21.07 中，用户请求的是可写空间，而 Trident 定义了该空间。snapshotReserve 将数值表示为占总体积的百分比。这不适用于 ontap-nas-economy。请参阅以下示例了解其工作原理：

计算方法如下：

```

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

```

对于快照预留 = 50% 且 PVC 请求 = 5 GiB 的情况，总卷大小为 $5 / 0.5 = 10$ GiB，可用大小为 5 GiB，这正是用户在 PVC 请求中请求的大小。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_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

2 entries were displayed.

升级Trident时，先前安装的现有后端将按上述方式配置卷。对于升级前创建的卷，您应该调整其大小才能观察到更改。例如，一个 2 GiB 的 PVC 包含 `snapshotReserve=50` 之前的结果是卷提供了 1 GiB 的可写空间。例如，将卷大小调整为 3 GiB，将在 6 GiB 的卷上为应用程序提供 3 GiB 的可写空间。

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。



如果在采用 Trident 的 NetApp ONTAP 上使用 Amazon FSx，建议为 LIF 指定 DNS 名称，而不是 IP 地址。

ONTAP NAS经济性示例

```
---
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 dataLIF 和 svm parameters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

这是一个最低后端配置示例。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
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

此示例介绍如何指示Trident使用动态导出策略自动创建和管理导出策略。这对于和 ontap-nas-flexgroup`驱动程序是相同的 `ontap-nas-economy。

```
---
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
```

Amazon FSx for ONTAP使用SMB卷示例

- smbShare 使用SMB卷的FSx for ONTAP需要参数。

```
---
version: 1
backendName: SMBBackend
storageDriverName: ontap-nas
managementLIF: example.mgmt.fqdn.aws.com
nasType: smb
dataLIF: 10.0.0.15
svm: nfs_svm
smbShare: smb-share
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```


使用nameTemplate的后端配置示例

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

虚拟池后端示例

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。注释在FlexVol for或FlexGroup `ontap-nas-flexgroup for`上设置 `ontap-nas`。配置时、Trident会将虚拟池上的所有标签复制到存储卷。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。

```

---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
svm: svm_nfs
username: admin
password: <password>
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: "false"
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      app: msoffice
      cost: "100"
      zone: us_east_1a
      defaults:
        spaceReserve: volume
        encryption: "true"
        unixPermissions: "0755"
        adaptiveQosPolicy: adaptive-premium
  - labels:
      app: slack
      cost: "75"
      zone: us_east_1b
      defaults:
        spaceReserve: none
        encryption: "true"
        unixPermissions: "0755"
  - labels:
      department: legal
      creditpoints: "5000"
      zone: us_east_1b
      defaults:
        spaceReserve: none
        encryption: "true"
        unixPermissions: "0755"
  - labels:

```

```
    app: wordpress
    cost: "50"
    zone: us_east_1c
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0775"
- labels:
    app: mysqlldb
    cost: "25"
    zone: us_east_1d
    defaults:
      spaceReserve: volume
      encryption: "false"
      unixPermissions: "0775"
```

```

---
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"
```

```

---
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定义请参见 [\[虚拟池后端示例\]](#)。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和第二个虚拟池 `ontap-nas-flexgroup` 后端。这些池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将映射到中的第三个和第四个虚拟池 `ontap-nas-flexgroup` 后端。这些池是唯一提供黄金级以外保护级别的池。

```
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将映射到中的第四个虚拟池 `ontap-nas` 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将映射到中的第三个虚拟池 ontap-nas-flexgroup 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-nas 中的后端和第二个虚拟池 ontap-nas-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"

```

Trident将决定选择哪个虚拟池、并确保满足存储要求。

更新 dataLIF 初始配置后

您可以在初始配置后更改dataLIF、方法是运行以下命令、为新的后端JSON文件提供更新后的dataLIF。

```

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

```




如果一个或多个Pod连接了PVC、则必须先关闭所有相应的Pod、然后再将其重新启动、以使新的dataLIF生效。

安全 SMB 示例

使用 **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
```

具有存储池的后端配置

```

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: svm0
  useREST: false
  storage:
    - labels:
        app: msoffice
      defaults:
        adAdminUser: tridentADuser
  nasType: smb
  credentials:
    name: backend-tbc-ontap-invest-secret

```

采用 **ontap-nas** 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: 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

```



确保添加 `annotations` 启用安全 SMB。如果没有注释，安全 SMB 就无法工作，无论后端或 PVC 中设置了什么配置。

采用 **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
```

具有单个 **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
```

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。