ONTAP NAS 驱动程序

Trident

NetApp
January 15, 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 驱动程序详情

Trident提供以下 NAS 存储驱动程序，用于与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	音量模式	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`

- 使用 `ontap-san-economy`仅当预计持续卷使用量高于……时"支持的ONTAP容量限制"。
- 使用 `ontap-nas-economy`仅当预计持续卷使用量高于……时"支持的ONTAP容量限制"以及 `ontap-san-economy`驱动程序无法使用。
- 请勿使用 `ontap-nas-economy`如果您预计需要数据保护、灾难恢复或移动办公。
- NetApp不建议在所有ONTAP驱动程序中使用 Flexvol 自动增长，ontap-san 除外。作为一种变通方法， Trident支持使用快照储备，并相应地调整 Flexvol 容量。

用户权限

Trident预期以ONTAP或 SVM 管理员身份运行，通常使用以下方式： `admin`集群用户或 `vsadmin`SVM 用户，或者具有相同角色但名称不同的用户。

对于Amazon FSx for NetApp ONTAP部署， Trident需要以ONTAP或 SVM 管理员身份运行，并使用集群。`fsxadmin`用户或 `vsadmin`SVM 用户，或者具有相同角色但名称不同的用户。这 `fsxadmin`用户是集群管理员用户的有限替代品。

如果你使用 `limitAggregateUsage`需要参数和集群管理员权限。当使用Amazon FSx for NetApp ONTAP和Trident时， `limitAggregateUsage`参数将无法与 `vsadmin`和 `fsxadmin`用户账户。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Trident驱动程序可以使用的限制性更强的角色，但我们不建议这样做。 Trident的大多数新版本都会调用额外的 API，这些 API 必须加以考虑，这使得升级变得困难且容易出错。

准备配置带有ONTAP NAS 驱动程序的后端

了解配置带有ONTAP NAS 驱动程序的ONTAP后端的要求、身份验证选项和导出策略。

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或另一个驱动程序的存储类。例如，您可以配置一个使用以下方式的 Gold 类： `ontap-nas`驾驶员和使用青铜级的驾驶员 `ontap-nas-economy`一。
- 所有 Kubernetes 工作节点都必须安装相应的 NFS 工具。请参阅"此处"更多详情请见下文。
- Trident仅支持挂载到运行在 Windows 节点上的 pod 的 SMB 卷。参考 准备配置SMB卷 了解详情。

对ONTAP后端进行身份验证

Trident提供两种ONTAP后端身份验证方式。

- 基于凭证：此模式需要对ONTAP后端拥有足够的权限。建议使用与预定义的安全登录角色关联的帐户，例如： `admin`或者 `vsadmin`确保与ONTAP版本最大程度兼容。
- 基于证书：此模式要求后端安装证书， Trident才能与ONTAP集群通信。此处，后端定义必须包含客户端证书、密钥和受信任 CA 证书（如果使用，建议使用）的 Base64 编码值。

您可以更新现有后端，以在基于凭据的方法和基于证书的方法之间进行切换。但是，一次只能支持一种身份验证方法。要切换到不同的身份验证方法，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，并出现错误，提示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 SVM 范围/集群范围管理员的凭据才能与ONTAP后端通信。建议使用标准的、预定义的角色，例如： `admin`或者 `vsadmin`。这样可以确保与未来ONTAP版本向前兼容，这些版本可能会公开一些功能 API，供未来的Trident版本使用。虽然可以创建自定义安全登录角色并将其与Trident一起使用，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-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"
    }
}
```

请注意，后端定义是唯一以纯文本形式存储凭据的地方。后端创建完成后，用户名/密码将使用 Base64 进行编码，并存储为 Kubernetes 密钥。后端创建/更新是唯一需要了解凭据的步骤。因此，这是一项仅限管理员执行的操作，由 Kubernetes/存储管理员执行。

启用基于证书的身份验证

新的和现有的后端都可以使用证书与ONTAP后端通信。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。如果使用受信任的 CA，则必须提供此参数。如果没有使用受信任的证书颁发机构，则可以忽略此步骤。

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，将通用名称 (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. 向ONTAP集群添加受信任的 CA 证书。这可能已经由存储管理员处理了。如果没有使用受信任的证书颁发机构，则忽略此操作。

```
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. 使用生成的证书进行身份验证。请将 < ONTAP管理 LIF> 和 <vserver 名称> 替换为管理 LIF IP 地址和 SVM 名称。您必须确保 LIF 的服务策略已设置为 `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、密钥和受信任的 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。这种方法是双向的：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，您必须删除现有的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的 backend.json 文件来执行 `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                 |
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。接下来将进行后端更新。轮换证书时，可以为用户添加多个证书。然后更新后端以使用新证书，之后即可从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。后端更新成功表明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

您可以创建一个具有最低权限的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将使用您创建的ONTAP集群角色来执行操作。

请参阅"Trident自定义角色生成器"有关创建Trident自定义角色的更多信息。

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\>
```

使用系统管理器

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“集群 > 设置”。

      （或者）要在 SVM 级别创建自定义角色，请选择“存储”>“存储虚拟机”> `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. 定义角色规则，然后点击“保存”。
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. 在“用户”下方选择“添加”图标 **+**。
   b. 选择所需的用户名，然后在“角色”下拉菜单中选择角色。
   c. 单击“保存”。

更多信息请参阅以下页面：

- "用于管理ONTAP的自定义角色"或者"定义自定义角色"
- "与角色和用户协作"

管理 NFS 导出策略

Trident使用 NFS 导出策略来控制对其所配置卷的访问。

Trident在处理出口策略时提供两种选择：

- Trident可以动态管理导出策略本身；在这种操作模式下，存储管理员指定一个 CIDR 块列表，这些 CIDR 块代表可接受的 IP 地址。 Trident会在发布时自动将属于这些范围内的适用节点 IP 添加到导出策略中。或者，如果没有指定 CIDR，则会将发布卷的节点上找到的所有全局范围的单播 IP 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。除非在配置中指定了不同的导出策略名称，否则Trident将使用默认导出策略。

动态管理出口策略

Trident提供了动态管理ONTAP后端导出策略的功能。这样，存储管理员就可以指定工作节点 IP 的允许地址空间，而无需手动定义明确的规则。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人工干预。此外，这有助于将对存储集群的访问限制在仅允许挂载卷且 IP 地址在指定范围内的节点上，从而支持细粒度和自动化管理。

> ⓘ 使用动态导出策略时，请勿使用网络地址转换（NAT）。使用 NAT 时，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，因此当在导出规则中找不到匹配项时，访问将被拒绝。

示例

必须使用两种配置选项。以下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，必须确保 SVM 中的根连接点具有先前创建的导出策略，该策略的导出规则允许节点 CIDR 块（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。

下面以上述示例为例，解释此功能的工作原理：

- `autoExportPolicy`设置为 `true`。这表明Trident会为使用此后端配置的每个卷创建一个导出策略。`svm1`使用 SVM 处理规则的添加和删除 `autoexportCIDRs`地址块。在卷连接到节点之前，该卷使用空的导出策略，没有任何规则来防止对该卷的未经授权的访问。当卷发布到节点时， Trident会创建一个导出策略，该策略的名称与包含指定 CIDR 块内节点 IP 的底层 qtree 的名称相同。这些 IP 地址也将添加到父FlexVol volume使用的导出策略中。
  - 例如：
    - 后端 UUID 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy`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FlexVol的 FlexVol 创建了一个导出策略。 `trident-403b5326-8482-40db96d0-d83fb3f4daec` ，名为 qtree 的导出策略 `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c`以及一个名为“空的导出策略”的 `trident_empty`在支持向量机上。 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。任何未附加的卷都将重用空导出策略。

- `autoExportCIDRs`包含地址块列表。此字段为可选字段，默认值为 ["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具有发布的全局作用域的单播地址。

在这个例子中， `192.168.0.0/24`已提供地址空间。这意味着，位于此地址范围内且已发布 Kubernetes 节点 IP 的节点将被添加到Trident创建的导出策略中。当Trident注册它运行所在的节点时，它会检索该节点的 IP 地址，并将其与提供的地址块进行比对。 `autoExportCIDRs`在发布时， Trident在过滤 IP 地址后，会为它要发布到的节点的客户端 IP 地址创建导出策略规则。

您可以更新 `autoExportPolicy`和 `autoExportCIDRs`创建后端之后，需要进行以下操作。您可以为自动管理的后端添加新的 CIDR，或者删除现有的 CIDR。删除 CIDR 时要格外小心，确保现有连接不会断开。您也可以选择禁用 `autoExportPolicy`对于后端，如果出现问题，则回退到手动创建的导出策略。这将需要进行设置 `exportPolicy`后端配置中的参数。

Trident创建或更新后端后，您可以使用以下命令检查后端： `tridentctl`或相应的 `tridentbackend`CRD：

```
./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
```

当一个节点被移除时， Trident会检查所有导出策略，以移除与该节点对应的访问规则。通过从受管后端导出策略中移除此节点 IP， Trident可以防止恶意挂载，除非集群中的新节点重新使用此 IP。

对于先前存在的后端，使用以下方式更新后端： `tridentctl update backend`确保Trident自动管理出口策略。这样，当需要时，就会创建两个以后端 UUID 和 qtree 名称命名的新导出策略。后端存在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。如果后端被重新创建，它将被视为一个新的后端，并将导致创建一个新的导出策略。

如果运行中的节点的 IP 地址更新，则必须重启该节点上的Trident pod。 Trident随后将更新其管理的后端的导出策略，以反映此 IP 变更。

准备配置SMB卷

稍作准备，您就可以使用以下方式配置 SMB 卷 `ontap-nas`司机。

> 您必须在 SVM 上同时配置 NFS 和 SMB/CIFS 协议才能创建 `ontap-nas-economy`适用于ONTAP本地集群的 SMB 卷。如果未能配置这些协议中的任何一个，都会导致 SMB 卷创建失败。

> `autoExportPolicy`不支持 SMB 卷。

开始之前

在配置 SMB 卷之前，您必须具备以下条件。

- 一个 Kubernetes 集群，包含一个 Linux 控制器节点和至少一个运行 Windows Server 2022 的 Windows 工作节点。 Trident仅支持挂载到运行在 Windows 节点上的 pod 的 SMB 卷。
- 至少有一个包含您的 Active Directory 凭据的Trident密钥。生成秘密 `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代理"或者"GitHub：适用于 Windows 的 CSI 代理"适用于在 Windows 上运行的 Kubernetes 节点。

步骤

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

   > Amazon FSx for ONTAP需要 SMB 共享。

   您可以通过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 CLI。使用ONTAP CLI 创建 SMB 共享：

   a. 如有必要，请创建共享的目录路径结构。

      这 `vserver cifs share create`该命令检查在创建共享时 -path 选项中指定的路径。如果指定的路径不存在，则命令执行失败。

   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. 确认共享已创建：

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

请参阅"创建 SMB 共享"了解详细信息。

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	描述	示例
`smbShare`	您可以指定以下一项：使用 Microsoft 管理控制台或ONTAP CLI 创建的 SMB 共享的名称；允许Trident创建 SMB 共享的名称；或者您可以将参数留空以防止对卷的公共共享访问。对于本地部署的ONTAP，此参数是可选的。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`.*如果为空，则默认为空。 `nfs` 。	`smb`
`securityStyle`	新卷的安全样式。 必须设置为 `**ntfs**`或者 `**mixed**`适用于 **SMB** 卷。	`ntfs`或者 `mixed`适用于 SMB 卷
`unixPermissions`	新卷模式。 对于 **SMB** 卷，此项必须留空。	""

启用安全的 **SMB**

从 25.06 版本开始， NetApp Trident支持使用以下方式安全配置创建的 SMB 卷： `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 注解、存储类注解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访问控制列表 (ACL) 中。
- 如果在后端、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，然后是后端。
- 支持安全 SMB `ontap-nas`仅适用于托管卷导入，不适用于非托管卷导入。

步骤

1. 在 TridentBackendConfig 中指定 adAdminUser，如下例所示：

```
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. 在存储类中添加注解。

   添加 `trident.netapp.io/smbShareAdUser`对存储类进行注解，以启用安全可靠的 SMB 连接。用户为注释指定的值 `trident.netapp.io/smbShareAdUser`应该与指定的用户名相同 `smbcreds`秘密。您可以从以下选项中选择一项 `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

学习如何在Trident系统中创建和使用ONTAP NAS 驱动程序。本节提供后端配置示例以及将后端映射到 StorageClasses 的详细信息。

后端配置选项

请参阅下表了解后端配置选项：

参数	描述	默认
`version`		始终为 1
`storageDriverName`	存储驱动程序的名称	`ontap-nas`， `ontap-nas-economy` ， 或者 `ontap-nas-flexgroup`
`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 地址可以指定完全限定域名 (FQDN)。如果Trident安装时使用了 IPv6 标志，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]` 。为了实现MetroCluster 的无缝切换，请参阅MetroCluster示例。	"10.0.0.1", "[2001:1234:abcd::fefe]"

参数	描述	默认
dataLIF	LIF协议的IP地址。 NetApp建议指定 dataLIF。如果未提供， Trident将从 SVM 获取 dataLIF。您可以指定一个完全限定域名 (FQDN) 用于 NFS 挂载操作，从而创建轮询 DNS 以在多个 dataLIF 之间进行负载均衡。初始设置后可以更改。参考。如果Trident安装时使用了 IPv6 标志，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] 。 *Metrocluster 除外。*查看MetroCluster示例。	指定地址或从 SVM 派生，如果未指定（不推荐）
svm	要使用的存储虚拟机 *Metrocluster 除外。*查看MetroCluster示例。	如果是 SVM 则推导而来 `managementLIF`已指定
autoExportPolicy	启用自动导出策略创建和更新 [布尔值]。使用 `autoExportPolicy`和 `autoExportCIDRs`可选功能包括： Trident可以自动管理出口策略。	false
autoExportCIDRs	用于过滤 Kubernetes 节点 IP 的 CIDR 列表 `autoExportPolicy`已启用。使用 `autoExportPolicy`和 `autoExportCIDRs`可选功能包括： Trident可以自动管理出口策略。	["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	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"。	
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 的身份"。	
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，尽管它会包含在卷名称中。	“三叉戟”

参数	描述	默认
`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 SVM 中的聚合数据更新时， Trident会自动轮询 SVM 进行更新，而无需重启Trident控制器。当您在Trident中配置特定聚合以配置卷时，如果该聚合被重命名或移出 SVM，则在轮询 SVM 聚合时， Trident中的后端将变为失败状态。您必须将聚合更改为 SVM 上存在的聚合，或者将其完全删除，才能使后端恢复联机。	""
`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**。	（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。 当 SVM 中的聚合列表更新时， Trident会通过轮询 SVM 自动更新该列表，而无需重新启动Trident控制器。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， Trident中的后端将进入失败状态。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，才能使后端恢复联机。	""
`limitVolumeSize`	如果请求的卷大小大于此值，则配置失败。此外，它还限制了 qtree 管理的卷的最大大小，以及 `qtreesPerFlexvol`此选项允许自定义每个FlexVol volume的最大 qtree 数量。	（默认情况下不强制执行）
`debugTraceFlags`	故障排除时要使用的调试标志。例如，{"api":false, "method":true} 请勿使用 `debugTraceFlags`除非您正在进行故障排除并且需要详细的日志转储。	无效的
`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。	`nfs`
`nfsMountOptions`	以逗号分隔的 NFS 挂载选项列表。 Kubernetes 持久卷的挂载选项通常在存储类中指定，但如果存储类中没有指定挂载选项， 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任何挂载选项， Trident将不会在关联的持久卷上设置任何挂载选项。	""

参数	描述	默认
`qtreesPerFlexvol`	每个FlexVol 的最大 Qtree 数量必须在 [50, 300] 范围内	“200”
`smbShare`	您可以指定以下一项：使用 Microsoft 管理控制台或ONTAP CLI 创建的 SMB 共享的名称；允许Trident 创建 SMB 共享的名称；或者您可以将参数留空以防止对卷的公共共享访问。对于本地部署的ONTAP，此参数是可选的。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`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`默认值；更改 `useREST`到 `false`使用 ONTAPI (ZAPI) 调用。	`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 时可请求的最大FlexVol大小。	（默认情况下不强制执行）
`denyNewVolumePools`	限制 `ontap-nas-economy`后端创建新的FlexVol卷来包含它们的 Qtree。只有预先存在的 Flexvol 才能用于配置新的 PV。	
`adAdminUser`	具有对 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 共享提供管理员权限，并赋予其完全控制权限。	

卷配置的后端配置选项

您可以使用以下选项控制默认配置。 `defaults`配置部分。例如，请参见下面的配置示例。

参数	描述	默认
`spaceAllocation`	Q树的空间分配	“真的”
`spaceReserve`	空间预留模式；“无”（细）或“大量”（粗）	“没有任何”
`snapshotPolicy`	要使用的快照策略	“没有任何”
`qosPolicy`	要为创建的卷分配的 QoS 策略组。每个存储池/后端选择 qosPolicy 或 adaptiveQosPolicy 之一	""
`adaptiveQosPolicy`	要为创建的卷分配的自适应 QoS 策略组。每个存储池/后端选择 qosPolicy 或 adaptiveQosPolicy 之一。ontap-nas-economy 不支持此功能。	""
`snapshotReserve`	快照预留的卷百分比	如果为“0”， `snapshotPolicy`为“无”，否则为“

参数	描述	默认
splitOnClone	创建时将克隆体从其母体中分离出来	"false"
encryption	在新卷上启用NetApp卷加密 (NVE)；默认设置为 false。要使用此选项，必须在集群上获得 NVE 许可并启用 NVE。如果后端启用了 NAE，则在Trident中配置的任何卷都将启用 NAE。更多信息，请参阅：“Trident如何与 NVE 和 NAE 协同工作”。	"false"
tieringPolicy	分层策略使用“无”	
unixPermissions	新卷模式	NFS 卷的端口号为“777”；SMB 卷的端口号为空（不适用）。
snapshotDir	控制对以下方面的访问 `.snapshot`目录	NFSv4 为“true”，NFSv3 为“false”。
exportPolicy	出口政策的使用	“默认”
securityStyle	新卷的安全样式。 NFS 支持 `mixed`和 `unix`安全措施。中小企业支持 `mixed`和 `ntfs`安全措施。	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ONTAP 9.8 或更高版本。您应该使用非共享的 QoS 策略组，并确保该策略组单独应用于每个成员。共享的 QoS 策略组强制规定所有工作负载的总吞吐量上限。

卷配置示例

以下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 。此计算方法可确保用户在 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/.5 = 10 GiB，可用大小为 5 GiB，这正是用户在 PVC 请求中请求的大小这 `volume show`该命令应显示与此示例类似的结果：

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 `snapshotReserve=50`之前的结果是一个提供 1 GiB 可写空间的卷。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。

最小配置示例

以下示例展示了基本配置，其中大多数参数都保留默认值。这是定义后端最简单的方法。

> 如果您在NetApp ONTAP上使用Amazon FSx和Trident，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，以避免在切换和切换回后端后手动更新后端定义。"SVM复制和恢复" 。

为了实现无缝切换和切换回，请指定 SVM `managementLIF`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`（如果使用受信任的 CA，则为可选） `backend.json`分别取客户端证书、私钥和受信任 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_
```

自动出口政策示例

本示例向您展示如何指示Trident使用动态导出策略来自动创建和管理导出策略。这对于以下情况也适用：`ontap-nas-economy`和 `ontap-nas-flexgroup`司机。

```
---
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

这个例子表明 `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

这 `smbShare`使用 SMB 卷的 FSx for ONTAP需要此参数。

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

具有虚拟池的后端示例

在下方所示的示例后端定义文件中，所有存储池都设置了特定的默认值，例如： `spaceReserve`没有，`spaceAllocation`为假，并且 `encryption`错误。虚拟池在存储部分中定义。

Trident在“备注”字段中设置配置标签。 FlexVol上已设置评论 `ontap-nas`或`FlexGroup `ontap-nas-flexgroup`。 Trident在配置时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，一些存储池会设置自己的参数。 `spaceReserve`， `spaceAllocation`， 和 `encryption`有些值会覆盖默认值，有些池会覆盖默认值。

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"
```

将后端映射到存储类

以下 StorageClass 定义指的是[具有虚拟池的后端示例]。使用 `parameters.selector`字段中，每个 StorageClass 都会指定哪些虚拟池可用于托管卷。卷将具有所选虚拟池中定义的各个方面。

- 这 `protection-gold`StorageClass 将映射到第一个和第二个虚拟池。 `ontap-nas-flexgroup`后端。只有这些泳池提供黄金级保护。

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

- 这 `protection-not-gold`StorageClass 将映射到第三个和第四个虚拟池。 `ontap-nas-flexgroup`后端。除了黄金之外，只有这些金池提供其他级别的保护。

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

- 这 `app-mysqldb`StorageClass 将映射到第四个虚拟池。 `ontap-nas`后端。这是唯一一个为mysqldb类型应用程序提供存储池配置的存储池。

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

- 该 `protection-silver-creditpoints-20k`StorageClass 将映射到第三个虚拟池。 `ontap-nas-flexgroup`后端。这是唯一提供银级保护和 20000 积分的彩池。

```
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"
```

- 这 `creditpoints-5k`StorageClass 将映射到第三个虚拟池。 `ontap-nas`后端和第二个虚拟池 `ontap-nas-economy`后端。这是唯一提供 5000 积分的彩池产品。

```
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，并确保满足存储需求。

更新 `dataLIF`初始配置后

初始配置完成后，您可以通过运行以下命令来更改 dataLIF，从而为新的后端 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 PVC 连接到一个或多个舱体，则必须将所有相应的舱体放下，然后再将它们重新升起，以便新的 dataLIF 生效。

安全的中小企业示例

使用 **ontap-nas** 驱动程序进行后端配置

```
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** 驱动程序进行后端配置

```
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
```

后端配置及存储池

```
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
```

使用 **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
```

请确保添加 `annotations`实现安全的SMB。如果没有注释，无论后端或 PVC 中设置了什么配置，安全 SMB 都无法工作。

使用 **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
```

包含单个 **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
```

包含多个 **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
```