



使用 **ONTAP** 或 **Cloud Volumes ONTAP NAS** 驱动程序配置后端 Astra Trident

NetApp
April 16, 2024

目录

- 使用 ONTAP NAS 驱动程序配置后端 1
 - 用户权限 1
 - 准备 1
 - 配置选项和示例 7

使用 ONTAP NAS 驱动程序配置后端

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

- ["准备"](#)
- ["配置和示例"](#)

用户权限

Astra Trident 应以 ONTAP 或 SVM 管理员身份运行，通常使用 `admin cluster` 用户或 `vsadmin SVM` 用户，或者使用具有相同角色的其他名称的用户。对于适用于 NetApp ONTAP 的 Amazon FSx 部署，Astra Trident 应使用集群 `fsxadmin user` 或 `vsadmin SVM` 用户或具有相同角色的其他名称的用户作为 ONTAP 或 SVM 管理员运行。`fsxadmin` 用户是集群管理员用户的有限替代用户。



如果使用 `limitAggregateUsage` 参数，则需要集群管理员权限。将适用于 NetApp ONTAP 的 Amazon FSx 与 Astra 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。

准备

了解如何准备使用 ONTAP NAS 驱动程序配置 ONTAP 后端。对于所有 ONTAP 后端，Astra Trident 需要至少为 SVM 分配一个聚合。

对于所有 ONTAP 后端，Astra Trident 需要至少为 SVM 分配一个聚合。

请记住，您还可以运行多个驱动程序，并创建指向其中一个驱动程序的存储类。例如，您可以配置一个使用 `ontap-nas` 驱动程序`的金牌类和一个使用 `ontap-nas-economy-one` 的铜牌类。

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：

身份验证

Astra Trident 提供了两种对 ONTAP 后端进行身份验证的模式。

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

用户还可以选择更新现有后端，选择从基于凭据迁移到基于证书，反之亦然。如果 * 同时提供了凭据和证书 *，则 Astra Trident 将在发出警告以从后端定义中删除凭据时默认使用证书。

启用基于凭据的身份验证

Astra 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，例如 `admin` 或 `vsadmin`。这样可以确保与未来的 ONTAP 版本向前兼容，这些版本可能会使功能 API 公开供未来的 Astra Trident 版本使用。可以创建自定义安全登录角色并将其用于 Astra Trident，但不建议使用。

后端定义示例如下所示：

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret"
}
```

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，请使用更新后的 `backend.json` 文件，该文件包含执行 `tridentctl` 后端更新 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": "secret",
  "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。成功的后端更新表明，Astra Trident 可以与 ONTAP 后端进行通信并处理未来的卷操作。

管理 NFS 导出策略

Astra Trident 使用 NFS 导出策略来控制对其配置的卷的访问。

使用导出策略时，Astra Trident 提供了两个选项：

- Astra Trident 可以动态管理导出策略本身；在此操作模式下，存储管理员会指定一个表示可接受 IP 地址的 CIDR 块列表。Astra Trident 会自动将属于这些范围的节点 IP 添加到导出策略中。或者，如果未指定任何 CIDR，则在节点上找到的任何全局范围的单播 IP 都将添加到导出策略中。
- 存储管理员可以手动创建导出策略和添加规则。除非在配置中指定了不同的导出策略名称，否则 Astra Trident 将使用默认导出策略。

动态管理导出策略

CSI Trident 20.04 版可以动态管理 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，这有助于将对存储集群的访问限制为仅允许 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。



只有 CSI Trident 才支持动态管理导出策略。请务必确保工作节点未被 NAT 处理。

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",
  "backendName": "ontap_nas_auto_export",
  "managementLIF": "192.168.0.135",
  "svm": "svm1",
  "username": "vsadmin",
  "password": "FaKePaSsWoRd",
  "autoExportCIDRs": ["192.168.0.0/24"],
  "autoExportPolicy": true
}
```



使用此功能时，您必须确保 SVM 中的根接合具有预先创建的导出策略，并具有允许节点 CIDR 块的导出规则（例如默认导出策略）。请始终遵循 NetApp 建议的最佳实践，为 Astra Trident 专用 SVM。

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 Astra Trident 将为 `svm1` SVM 创建导出策略，并使用 `autoExportCIDRs` 地址块处理规则的添加和删除。例如，UUID 为 `403b5326-8482-40db-96d0-d83fb3f4daec` 且 `autoExportPolicy` 设置为 `true` 的后端会在 SVM 上创建一个名为 `trident-403b5326-8482-40db-96d0-d83fb3f4daec` 的导出策略。
- `autoExportCIDR` 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 Astra Trident 会添加在工作节点上找到的所有全局范围的单播地址。

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的 Kubernetes 节点 IP 将添加到 Astra Trident 创建的导出策略中。当 Astra Trident 注册其运行的节点时，它会检索该节点的 IP 地址，并根据 `autoExportCIDRs` 中提供的地址块对其进行检查。筛选 IP 后，Astra Trident 会为其发现的客户端 IP 创建导出策略规则，并为其标识的每个节点创建一个规则。

创建后，您可以为后端更新 `autoExportPolicy` 和 `autoExportCIDR`。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 `autoExportPolicy`，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 Astra 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: ""
    autoExportCIDsRs:
    - 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
```

当节点添加到 Kubernetes 集群并向 Astra Trident 控制器注册后，现有后端的导出策略将会更新（前提是它们位于后端的 `autoExportCIDR` 中指定的地址范围内）。

删除节点后，Astra Trident 会检查所有联机后端，以删除该节点的访问规则。通过从受管后端的导出策略中删除此节点 IP，Astra Trident 可防止恶意挂载，除非此 IP 可由集群中的新节点重复使用。

对于以前存在的后端，使用 `tridentctl update backend` 更新后端可确保 Astra Trident 自动管理导出策略。这将创建一个以后端 UUID 命名的新导出策略，后端上存在的卷将在重新挂载时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 Astra Trident Pod。然后，Astra Trident 将更新其管理的后端的导出策略，以反映此 IP 更改。

配置选项和示例

了解如何在您的 Astra Trident 安装中创建和使用 ONTAP NAS 驱动程序。本节提供了后端配置示例以及有关如何将后端映射到 `StorageClasses` 的详细信息。

后端配置选项

有关后端配置选项，请参见下表：

参数	Description	Default
ve版本		始终为 1
storageDriverName	存储驱动程序的名称	"ontap-nas" , "ontap-nas-economy-" , "ontap-nas-flexgroup" , "ontap-san" , "ontap-san-economy-"
backendName	自定义名称或存储后端	驱动程序名称 + "_" + dataLIF
m年月日	集群或 SVM 管理 LIF 的 IP 地址	"10.0.0.1" , "2001 : 1234 : abcd : : : fefe]"
dataLIF	协议 LIF 的 IP 地址。对于 IPv6 , 请使用方括号。设置后无法更新	由 SVM 派生, 除非另有说明
autosExportPolicy	启用自动创建和更新导出策略 [布尔值]	false
autosExportCIDR	启用 AutoExportPolicy 时用于筛选 Kubernetes 节点 IP 的 CIDR 列表	["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	
密码	连接到集群 /SVM 的密码。用于基于凭据的身份验证	
sVM	要使用的 Storage Virtual Machine	如果指定了 SVM managementLIF , 则派生
igroupName	要使用的 SAN 卷的 igroup 的名称	"trident — < 后端 UUID >"
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	Trident
limitAggregateUsage	如果使用量超过此百分比, 则配置失败。* 不适用于适用于 ONTAP 的 Amazon FSx *	" (默认情况下不强制实施)
limitVolumeSize	如果请求的卷大小超过此值、则配置失败。	" (默认情况下不强制实施)
lunsPerFlexvol	每个 FlexVol 的最大 LUN 数, 必须在 50 , 200 范围内	100

参数	Description	Default
debugTraceFlags	故障排除时要使用的调试标志。示例 { "api": false , "method " : true }	空
nfsMountOptions	NFS 挂载选项的逗号分隔列表	"
qtreesPerFlexvol	每个 FlexVol 的最大 qtree 数，必须在 50 , 300 范围内	200
useREST	用于使用 ONTAP REST API 的布尔参数。* 技术预览 *	false



useREST 提供了一个 * 技术预览 *，建议用于测试环境，而不是生产工作负载。如果设置为 true，则 Astra Trident 将使用 ONTAP REST API 与后端进行通信。此功能需要使用 ONTAP 9.9 及更高版本。此外，使用的 ONTAP 登录角色必须能够访问 ONTAP 应用程序。这一点可通过预定义的 vsadmin 和 cluster-admin 角色来满足。

要与 ONTAP 集群通信，您应提供身份验证参数。这可以是安全登录的用户名 / 密码，也可以是已安装的证书。



如果您使用适用于 NetApp ONTAP 后端的 Amazon FSX，请勿指定 limitAggregateUsage 参数。Amazon FSX for NetApp ONTAP 提供的 fsxadmin 和 vsadmin 角色不包含检索聚合使用情况并通过 Astra Trident 对其进行限制所需的访问权限。



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。



创建后端时，请记住，创建后无法修改 dataLIF 和 storagePrefix。要更新这些参数，您需要创建一个新的后端。

可以为 managementLIF 选项指定完全限定域名（FQDN）。也可以为 dataLIF 选项指定 FQDN，在这种情况下，FQDN 将用于 NFS 挂载操作。这样，您就可以创建循环 DNS，以便在多个数据 LIF 之间实现负载平衡。

对于所有 ONTAP 驱动程序，也可以将 managementLIF 设置为 IPv6 地址。请务必使用 ` -use-ipv6 ` 标志安装 Astra Trident。必须 m 方括号内的 anagementLIF IPv6 地址。



使用 IPv6 地址时，请确保在方括号内定义 managementLIF 和 dataLIF（如果包含在后端定义中），例如 [28e8 : d9fb : a825 : b7bf : 69a8 : d02f : 9e7b : 3555]。如果未提供 dataLIF，则 Astra Trident 将从 SVM 提取 IPv6 数据 LIF。

使用 autosExportPolicy 和 autosExportCIDR 选项，CSI Trident 可以自动管理导出策略。所有 ontap-nas-* 驱动程序均支持此功能。

对于 ontap-nas-economy 驱动程序，limitVolumeSize 选项还会限制它为 qtree 和 FlexVol 管理的卷的最大大小，而 qtreesPerFlexvol 选项允许自定义每个的最大 qtree 数。

可以使用 nfsMountOptions 参数指定挂载选项。Kubernetes 永久性卷的挂载选项通常在存储类中指定，但如果在存储类中未指定挂载选项，则 Astra Trident 将回退为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 Astra Trident 不会在关联的永久性卷上设置任何挂载选项。



Astra Trident 会在使用 `ontap-NAS` 和 `ontap-nas-flexgroup` 创建的所有卷的 "Comments" 字段中设置配置标签。根据所使用的驱动程序，注释将在 FlexVol (`ontap-NAS`) 或 FlexGroup (`ontap-nas-flexgroup`) 上进行设置。Astra Trident 会在配置存储池时将存储池上的所有标签复制到该存储卷。存储管理员可以为每个存储池定义标签，并对存储池中创建的所有卷进行分组。这样，您就可以根据后端配置中提供的一组可自定义标签来方便地区分卷了。

用于配置卷的后端配置选项

您可以在配置的特殊部分中使用这些选项来控制默认配置每个卷的方式。有关示例，请参见以下配置示例。

参数	Description	Default
<code>spaceAllocation</code>	LUN 的空间分配	true
<code>s页面预留</code>	空间预留模式；"无"（精简）或"卷"（厚）	无
<code>sSnapshot 策略</code>	要使用的 Snapshot 策略	无
<code>qosPolicy</code>	要为创建的卷分配的 QoS 策略组。选择每个存储池 / 后端的 <code>qosPolicy</code> 或 <code>adaptiveQosPolicy</code> 之一	"
<code>adaptiveQosPolicy</code>	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 <code>qosPolicy</code> 或 <code>adaptiveQosPolicy</code> 之一。不受 <code>ontap-nas-economy</code> 。	"
<code>sSnapshot 预留</code>	为快照预留的卷百分比为 "0"	如果 <code>snapshotPolicy</code> 为 "无"，则为 "无"，否则为 ""
<code>splitOnClone</code>	创建克隆时，从其父级拆分该克隆	false
<code>加密</code>	启用 NetApp 卷加密	false
<code>securityStyle</code>	新卷的安全模式	"unix"
<code>分层策略</code>	使用 "无" 的分层策略	适用于 ONTAP 9.5 SVM-DR 之前的配置的 "仅快照"
<code>unixPermissions</code>	新卷的模式	777.
<code>snapshotDir</code>	控制 <code>.snapshot</code> 目录的可见性	false
<code>导出策略</code>	要使用的导出策略	default
<code>securityStyle</code>	新卷的安全模式	"unix"



在 Astra Trident 中使用 QoS 策略组需要 ONTAP 9.8 或更高版本。建议使用非共享 QoS 策略组，并确保策略组分别应用于每个成分卷。共享 QoS 策略组将对所有工作负载的总吞吐量实施上限。

下面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，Astra Trident 现在使用新的计算方法来确保 FlexVol 的大小正确，并使用 snapshotReserve 百分比和 PVC。当用户请求 PVC 时，Astra Trident 会使用新计算创建具有更多空间的原始 FlexVol。此计算可确保用户在 PVC 中收到所请求的可写空间，而不是小于所请求的空间。在 v21.07 之前，如果用户请求 PVC（例如，5GiB），并且 snapshotReserve 为 50%，则只会获得 2.5 GiB 的可写空间。这是因为用户请求的是整个卷，而 snapshotReserve 是其中的一个百分比。在 Trident 21.07 中，用户请求的是可写空间，Astra Trident 将 snapshotReserve number 定义为整个卷的百分比。这不适用于 ontap-nas-economy”。请参见以下示例以了解其工作原理：

计算方法如下：

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

对于 snapshotReserve = 50%，PVC 请求 = 5GiB，卷总大小为 $2/5 = 10\text{GiB}$ ，可用大小为 5GiB，这是用户在 PVC 请求中请求的大小。volume show 命令应显示与以下示例类似的结果：

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.

在升级 Astra Trident 时，先前安装的现有后端将按照上述说明配置卷。对于在升级之前创建的卷，您应调整其卷的大小，以便观察到所做的更改。例如，一个 2 GiB PVC，其 `snapshotReserve=50 earlier` 会导致一个卷提供 1 GiB 的可写空间。例如，将卷大小调整为 3GiB 可为应用程序在一个 6 GiB 卷上提供 3GiB 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` 具有基于证书的身份验证的驱动程序

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）分别填充在 `backend.json` 中，并采用客户端证书，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": "ZXROZXJwYXB...ICMgJ3BhcGVyc2",
  "clientPrivateKey": "vciwKIyAgZG...0cnksIGRlc2NyaX",
  "trustedCACertificate": "zcyBbaG...b3Igb3duIGNsYXNz",
  "storagePrefix": "myPrefix_"
}
```

`ontap-nas` 具有自动导出策略的驱动程序

此示例显示了如何指示 Astra Trident 使用动态导出策略自动创建和管理导出策略。这对于 `ontap-nas-economy` 和 `ontap-nas-flexgroup` 驱动程序也是如此。

```
{
  "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": "secret",
  "nfsMountOptions": "nfsvers=4",
}
```

ontap-nas-flexgroup 驱动程序

```
{
  "version": 1,
  "storageDriverName": "ontap-nas-flexgroup",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "labels": {"k8scluster": "test-cluster-east-1b", "backend": "test1-
ontap-cluster"},
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret",
}
```

ontap-nas 支持IPv6的驱动程序

```
{
  "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": "netapp123"
}
```

```
{
  "version": 1,
  "storageDriverName": "ontap-nas-economy",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret"
}
```

虚拟存储池后端示例

在下面显示的示例后端定义文件中，会为所有存储池设置特定的默认值，例如 `spaceReserve at none`，`spaceAllocation at false` 和 `encryption at false`。虚拟存储池在存储部分中进行定义。

在此示例中，某些存储池会设置自己的 `spaceReserve`，`spaceAllocation` 和 `encryption` 值，而某些池会覆盖上述设置的默认值。

ontap-nas 驱动程序

```
{
  {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "managementLIF": "10.0.0.1",
    "dataLIF": "10.0.0.2",
    "svm": "svm_nfs",
    "username": "admin",
    "password": "secret",
    "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":{"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 驱动程序

```

{
    "version": 1,
    "storageDriverName": "ontap-nas-flexgroup",
    "managementLIF": "10.0.0.1",
    "dataLIF": "10.0.0.2",
    "svm": "svm_nfs",
    "username": "vsadmin",

```

```

"password": "secret",

"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-economy 驱动程序

```
{
  "version": 1,
  "storageDriverName": "ontap-nas-economy",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret",

  "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": {"department": "legal", "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 定义引用了上述虚拟存储池。使用 `parameters.selector` 字段，每个 StorageClass 都会调用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。

- 第一个 StorageClass (`protection-gold`) 将映射到 `ontap-nas-flexgroup` 后端的第一个，第二个虚拟存储池以及 `ontap-san` 后端的第一个虚拟存储池。这是唯一一个提供黄金级保护的池。
- 第二个 StorageClass (`protection-not-gold`) 将映射到 `ontap-nas-flexgroup` 后端的第三个，第四个虚拟存储池以及 `ontap-san` 后端的第二个，第三个虚拟存储池。这些池是唯一提供黄金级以外保护级别的池。
- 第三个 StorageClass (`app-mysqldb`) 将映射到 `ontap-NAS` 后端的第四个虚拟存储池和 `ontap-san-economy-backend` 的第三个虚拟存储池。这些池是唯一为 `mysqldb` 类型的应用程序提供存储池配置的池。
- 第四个存储类 (`protection-silver-creditpoin-20k`) 将映射到 `ontap-nas-flexgroup` 后端的第三个虚拟存储池和 `ontap-san` 后端的第二个虚拟存储池。这些池是唯一以 20000 个信用点提供黄金级保护的池。
- 第五个存储类 (`credits-5k`) 将映射到 `ontap-nas-economy-backend` 中的第二个虚拟存储池和 `ontap-san` 后端的第三个虚拟存储池。这些是唯一一款具有 5000 个信用点的池产品。

Astra Trident 将决定选择哪个虚拟存储池，并确保满足存储要求。

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: netapp.io/trident
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: netapp.io/trident
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: netapp.io/trident
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

版权信息

版权所有 © 2024 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。