



## 配置和管理后端 Astra Trident

NetApp  
April 18, 2024

# 目录

配置和管理后端 .....	1
配置后端 .....	1
Azure NetApp Files .....	1
为Google Cloud后端配置Cloud Volumes Service .....	16
配置 NetApp HCI 或 SolidFire 后端 .....	31
ONTAP SAN 驱动程序 .....	37
ONTAP NAS 驱动程序 .....	59
适用于 NetApp ONTAP 的 Amazon FSX .....	86
使用 kubectl 创建后端 .....	101
管理后端 .....	107

# 配置和管理后端

## 配置后端

后端定义了 Astra Trident 与存储系统之间的关系。它告诉 Astra Trident 如何与该存储系统进行通信，以及 Astra Trident 如何从该存储系统配置卷。

Astra Trident会自动从后端提供符合存储类定义的要求的存储池。了解如何为存储系统配置后端。

- ["配置 Azure NetApp Files 后端"](#)
- ["配置适用于 Google 云平台的 Cloud Volumes Service 后端"](#)
- ["配置 NetApp HCI 或 SolidFire 后端"](#)
- ["使用 ONTAP 或 Cloud Volumes ONTAP NAS 驱动程序配置后端"](#)
- ["使用 ONTAP 或 Cloud Volumes ONTAP SAN 驱动程序配置后端"](#)
- ["将 Astra Trident 与适用于 NetApp ONTAP 的 Amazon FSX 结合使用"](#)

## Azure NetApp Files

### 配置 Azure NetApp Files 后端

您可以将Azure NetApp Files配置为Astra三端。您可以使用Azure NetApp Files后端连接NFS和SMB卷。Asta Trident还支持使用托管身份为Azure Kubnetes Services (AKS)集群管理凭据。

#### Azure NetApp Files驱动程序详细信息

Asta三端磁盘提供了以下Azure NetApp Files存储驱动程序、用于与集群进行通信。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
azure-netapp-files	NFS SMB	文件系统	Rwo、ROX、rwx、RWOP	nfs， smb

#### 注意事项

- Azure NetApp Files 服务不支持小于100 GB的卷。如果请求的卷较小、Asta三端技术支持会自动创建100-GiB卷。
- Astra Trident仅支持将SMB卷挂载到Windows节点上运行的Pod。

#### AKS的受管身份

Asta三项功能支持 ["受管身份"](#) 适用于Azure Kubnetes Services集群。要利用受管身份提供的简化凭据管理、您必须：

- 使用AKS部署的Kubernetes集群
- 在AKS Kubernetes集群上配置的受管身份
- 已安装Asta三项功能、其中包括 `cloudProvider` 以指定 "Azure"。

### Trident 运算符

要使用三端运算符安装Astra三端、请编辑 `tridentorchestrator_cr.yaml` 设置 `cloudProvider` to "Azure"。例如：

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "Azure"
```

### 掌舵

以下示例将安装Asta三项功能集 `cloudProvider` 使用环境变量将其添加到Azure \$CP：

```
helm install trident trident-operator-100.2402.0.tgz --create
--namespace --namespace <trident-namespace> --set cloudProvider=$CP
```

### `tridentctl`

以下示例将安装Asta Dent并设置 `cloudProvider` 标记为 Azure：

```
tridentctl install --cloud-provider="Azure" -n trident
```

## 适用于AKS的云身份

通过云身份、Kubnetes Pod可以通过作为工作负载身份进行身份验证来访问Azure资源、而不是提供明确的Azure凭据。

要在Azure中利用云身份、您必须：

- 使用AKS部署的Kubernetes集群
- 在AKS Kubelnetes集群上配置的工作负载身份和oidc-Issuer
- 已安装Asta三项功能、其中包括 `cloudProvider` 以指定 "Azure" 和 `cloudIdentity` 指定工作负载标识

## Trident 运算符

要使用三端运算符安装Astra三端、请编辑 `tridentorchestrator_cr.yaml` 设置 `cloudProvider` to "Azure" 并设置 `cloudIdentity` to `azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`。

例如：

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "Azure"
  *cloudIdentity: 'azure.workload.identity/client-id: xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx' *
```

## 掌舵

使用以下环境变量设置\*云提供程序(CP)\*和\*云身份(CI)\*标志的值：

```
export CP="Azure"
export CI="azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx"
```

以下示例将安装Astra Dent和Sets `cloudProvider` 使用环境变量将其添加到Azure `$CP` 并设置 `cloudIdentity` 使用环境变量 `$CI`：

```
helm install trident trident-operator-100.2402.0.tgz --set
cloudProvider=$CP --set cloudIdentity=$CI
```

## <code>tridentctl</code>

使用以下环境变量设置\*云提供程序\*和\*云身份\*标志的值：

```
export CP="Azure"
export CI="azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx"
```

以下示例将安装Astra Dent并设置 `cloud-provider` 标记为 `$CP`，和 `cloud-identity` to `$CI`：

```
tridentctl install --cloud-provider=$CP --cloud-identity="$CI" -n
trident
```

## 准备配置Azure NetApp Files 后端

在配置Azure NetApp Files 后端之前、您需要确保满足以下要求。

### NFS和SMB卷的前提条件

如果您是首次使用Azure NetApp Files 或在新位置使用、则需要进行一些初始配置来设置Azure NetApp Files 并创建NFS卷。请参见 ["Azure：设置Azure NetApp Files 并创建NFS卷"](#)。

配置和使用 ["Azure NetApp Files"](#) 后端，您需要满足以下要求：



- subscriptionID, tenantID, clientID, location, 和 clientSecret 在AKS集群上使用受管身份时为可选。
- tenantID, clientID, 和 clientSecret 在AKS集群上使用云标识时可选。

- 一个容量池。请参见 ["Microsoft：为Azure NetApp Files 创建容量池"](#)。
- 委派给Azure NetApp Files 的子网。请参见 ["Microsoft：将子网委派给Azure NetApp Files"](#)。
- subscriptionID 来自启用了 Azure NetApp Files 的 Azure 订阅。
- tenantID, clientID, 和 clientSecret 从 ["应用程序注册"](#) 在 Azure Active Directory 中，具有足够的 Azure NetApp Files 服务权限。应用程序注册应使用以下任一项：
  - 所有者或贡献者角色 ["由Azure预定义"](#)。
  - 答 ["自定义贡献者角色"](#) 订阅级别 (assignableScopes)、并具有以下权限、这些权限仅限于Astra Trident所需的权限。创建自定义角色后、["使用Azure门户分配角色"](#)。

```

{
  "id": "/subscriptions/<subscription-id>/providers/Microsoft.Authorization/roleDefinitions/<role-definition-id>",
  "properties": {
    "roleName": "custom-role-with-limited-perms",
    "description": "custom role providing limited permissions",
    "assignableScopes": [
      "/subscriptions/<subscription-id>"
    ],
    "permissions": [
      {
        "actions": [

"Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/MountTargets/read",

          "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/read",

```

```

"Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/write",

"Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/delete",

        "Microsoft.Features/features/read",
        "Microsoft.Features/operations/read",
        "Microsoft.Features/providers/features/read",

"Microsoft.Features/providers/features/register/action",

"Microsoft.Features/providers/features/unregister/action",

"Microsoft.Features/subscriptionFeatureRegistrations/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
}
}

```

- Azure location 至少包含一个 ["委派子网"](#)。自Trident 22.01日开始 location 参数是后端配置文件顶层的必填字段。在虚拟池中指定的位置值将被忽略。
- 以使用 Cloud Identity 请获取 `client ID` 从A ["用户分配的托管身份"](#) 并在中指定此ID  
 azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx。

## SMB卷的其他要求

要创建SMB卷、您必须具有：

- 已配置Active Directory并连接到Azure NetApp Files。请参见 ["Microsoft：创建和管理Azure NetApp Files的Active Directory连接"](#)。
- 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 2019的Windows工作节点。Astra Trident仅支持将SMB卷挂载到Windows节点上运行的Pod。
- 至少一个包含Active Directory凭据的Astra Trident密钥、以便Azure NetApp Files 可以向Active Directory进行身份验证。以生成密钥 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。



# Azure NetApp Files 后端配置选项和示例

了解适用于Azure NetApp Files的NFS和SMB后端配置选项并查看配置示例。

## 后端配置选项

Asta三端存储使用您的后端配置(子网、虚拟网络、服务级别和位置)在请求位置可用的容量池上创建Azure NetApp Files卷、并与请求的服务级别和子网匹配。



Astra Trident 不支持手动 QoS 容量池。

Azure NetApp Files后端提供了这些配置选项。

参数	Description	Default
ve版本		始终为 1
storageDriverName	存储驱动程序的名称	"Azure-netapp-files"
backendName	自定义名称或存储后端	驱动程序名称 + "_" + 随机字符
ssubscriptionID。	Azure 订阅中的订阅 ID  如果在AKS集群上启用了受管标识、则为可选。	
租户 ID。	应用程序注册中的租户 ID  如果在AKS集群上使用托管身份或云身份、则可选。	
客户端 ID。	应用程序注册中的客户端 ID  如果在AKS集群上使用托管身份或云身份、则可选。	
clientSecret。	应用程序注册中的客户端密钥  如果在AKS集群上使用托管身份或云身份、则可选。	
s服务级别	s标准，高级或超级之一	""（随机）
位置	要创建新卷的 Azure 位置的名称  如果在AKS集群上启用了受管标识、则为可选。	
resourceGroups	用于筛选已发现资源的资源组列表	[]（无筛选器）
netappAccounts	用于筛选已发现资源的 NetApp 帐户列表	[]（无筛选器）
容量池	用于筛选已发现资源的容量池列表	[]（无筛选器，随机）
virtualNetwork	具有委派子网的虚拟网络的名称	""

参数	Description	Default
ssubnet	委派给 Microsoft.Netapp/volumes 的子网的名称	""
网络功能	一个卷的一组vNet功能可能是 Basic 或 Standard。网络功能并非在所有地区都可用、可能需要在订阅中启用。指定 networkFeatures 如果未启用此功能、则会导致卷配置失败。	""
nfsMountOptions	精细控制 NFS 挂载选项。SMB卷已忽略。要使用NFS 4.1挂载卷、请包括 nfsvers=4 在逗号分隔的挂载选项列表中选择NFS v4.1。存储类定义中设置的挂载选项会覆盖后端配置中设置的挂载选项。	"nfsvers=3"
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）
debugTraceFlags	故障排除时要使用的调试标志。示例，` \ { "api" : false , "method" : true , "discovery" : true } `。除非您正在进行故障排除并需要详细的日志转储，否则请勿使用此功能。	空
nasType	配置NFS或SMB卷创建。选项包括 nfs, smb 或为空。默认情况下、将设置为空会将NFS卷设置为空。	nfs



有关网络功能的详细信息、请参见 ["配置Azure NetApp Files 卷的网络功能"](#)。

#### 所需权限和资源

如果在创建PVC时收到"No Capacity Pools"(未找到容量池)错误、则您的应用程序注册可能没有关联的所需权限和资源(子网、虚拟网络、容量池)。如果启用了调试、则Astra Trident将记录创建后端时发现的Azure资源。验证是否正在使用适当的角色。

的值 resourceGroups, netappAccounts, capacityPools, virtualNetwork, 和 subnet 可以使用短名称或完全限定名称来指定。在大多数情况下、建议使用完全限定名称、因为短名称可以与多个同名资源匹配。

。 resourceGroups, netappAccounts, 和 capacityPools 值是指筛选器、用于将发现的一组资源限制为此存储后端可用的资源、并且可以以任意组合方式指定。完全限定名称采用以下格式：

Type	格式。
Resource group	< 资源组 >
NetApp 帐户	< 资源组 >/< NetApp 帐户 >
容量池	< 资源组 >/< NetApp 帐户 >/< 容量池 >

Type	格式。
虚拟网络	< 资源组 >/< 虚拟网络 >
Subnet	< 资源组 >/< 虚拟网络 >/< 子网 >

## 卷配置

您可以通过在配置文件的特殊部分中指定以下选项来控制默认卷配置。请参见 [\[示例配置\]](#) 了解详细信息。

参数	Description	Default
exportRule	新卷的导出规则。 exportRule 必须是以CIDR表示法表示的任意IPv4地址或IPv4子网组合的逗号分隔列表。SMB卷已忽略。	"0.0.0.0/0"
snapshotDir	控制 .snapshot 目录的可见性	false
s大小	新卷的默认大小	"100 克 "
unixPermissions	新卷的UNIX权限(4个八进制数字)。SMB卷已忽略。	""（预览功能，需要在订阅中列入白名单）

## 示例配置

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。

## 最低配置

这是绝对的最低后端配置。使用此配置、Asta三端存储可以发现已配置位置委派给Azure NetApp Files的所有NetApp帐户、容量池和子网、并随机将新卷放置在其中一个池和子网上。因为 nasType 省略 nfs 默认情况下适用、后端将为NFS卷配置。

当您刚刚开始使用Azure NetApp Files并尝试某些操作时、此配置是理想的选择、但实际上、您需要为所配置的卷提供额外的范围界定。

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
```

## AKS的受管身份

此后端配置会出现异常 subscriptionID, tenantID, clientID, 和 clientSecret, 在使用受管身份时是可选的。

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  capacityPools: ["ultra-pool"]
  resourceGroups: ["aks-ami-eastus-rg"]
  netappAccounts: ["smb-na"]
  virtualNetwork: eastus-prod-vnet
  subnet: eastus-anf-subnet
```

## 适用于AKS的云身份

此后端配置会出现异常 tenantID, clientID, 和 clientSecret, 在使用云标识时是可选的。

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  capacityPools: ["ultra-pool"]
  resourceGroups: ["aks-ami-eastus-rg"]
  netappAccounts: ["smb-na"]
  virtualNetwork: eastus-prod-vnet
  subnet: eastus-anf-subnet
  location: eastus
  subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
```

此后端配置会将卷放置在Azure中 `eastus` 位置 `Ultra` 容量池。Asta三端存储自动发现该位置委派给Azure NetApp Files的所有子网、并随机在其中一个子网上放置一个新卷。

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
- application-group-1/account-1/ultra-1
- application-group-1/account-1/ultra-2
```

此后端配置进一步将卷放置范围缩小为一个子网，并修改了某些卷配置默认值。

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
- application-group-1/account-1/ultra-1
- application-group-1/account-1/ultra-2
virtualNetwork: my-virtual-network
subnet: my-subnet
networkFeatures: Standard
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 500Gi
defaults:
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  snapshotDir: 'true'
  size: 200Gi
  unixPermissions: '0777'
```

## 虚拟池配置

此后端配置可在一个文件中定义多个存储池。如果您有多个容量池支持不同的服务级别，并且您希望在 Kubernetes 中创建表示这些服务级别的存储类，则此功能非常有用。虚拟池标签用于根据区分池 performance。

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
resourceGroups:
- application-group-1
networkFeatures: Basic
nfsMountOptions: vers=3,proto=tcp,timeo=600
labels:
  cloud: azure
storage:
- labels:
    performance: gold
    serviceLevel: Ultra
    capacityPools:
    - ultra-1
    - ultra-2
    networkFeatures: Standard
- labels:
    performance: silver
    serviceLevel: Premium
    capacityPools:
    - premium-1
- labels:
    performance: bronze
    serviceLevel: Standard
    capacityPools:
    - standard-1
    - standard-2
```

## 存储类定义

以下内容 StorageClass 定义是指上述存储池。

使用的示例定义 `parameter.selector` 字段

使用 `parameter.selector` 您可以为每个指定 `StorageClass` 用于托管卷的虚拟池。卷将在选定池中定义各个方面。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: bronze
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze"
allowVolumeExpansion: true
```

### **SMB**卷的示例定义

使用 `nasType`, `node-stage-secret-name`, 和 `node-stage-secret-namespace`、您可以指定SMB卷并提供所需的Active Directory凭据。



## 默认命名空间上的基本配置

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
```

## 每个命名空间使用不同的密钥

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

## 每个卷使用不同的密钥

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: ${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```



nasType: smb 支持SMB卷的池的筛选器。nasType: nfs 或 nasType: null NFS池的筛选器。

## 创建后端

创建后端配置文件后，运行以下命令：

```
tridentctl create backend -f <backend-file>
```

如果后端创建失败，则后端配置出现问题。您可以运行以下命令来查看日志以确定发生原因：

```
tridentctl logs
```

确定并更正配置文件中的问题后，您可以再次运行 create 命令。

## 为Google Cloud后端配置Cloud Volumes Service

了解如何使用提供的示例配置将适用于Google Cloud的NetApp Cloud Volumes Service 配置为Astra Trident安装的后端。

### Google Cloud驱动程序详细信息

Astra三项功能提供 gcp-cvs 与集群通信的驱动程序。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
GCP-CVS	NFS	文件系统	Rwo、ROX、rwx、RWOP	nfs

### 了解适用于Google Cloud的Cloud Volumes Service 的Astra Trident支持

Astra Trident可以在两个卷中创建Cloud Volumes Service 卷之一 **"服务类型"**：

- **CVS-Performance**：默认的Astra Trident服务类型。这种性能优化的服务类型最适合重视性能的生产工作负载。CVS-Performance服务类型是一种硬件选项、支持的卷大小至少为100 GiB。您可以选择一个 **"三个服务级别"**：
  - standard
  - premium
  - extreme
- **\* CVS\***：CVS服务类型提供高区域可用性、性能级别限制为中等。CVS服务类型是一个软件选项、可使用存储池支持小至1 GiB的卷。存储池最多可包含50个卷、其中所有卷都共享池的容量和性能。您可以选择一个 **"两个服务级别"**：
  - standardsw

## 您需要的内容

以配置和使用 "适用于 Google Cloud 的 Cloud Volumes Service" 后端，您需要满足以下要求：

- 配置了NetApp Cloud Volumes Service 的Google Cloud帐户
- Google Cloud 帐户的项目编号
- 具有 `netappcloudvolumes.admin` 角色的 Google Cloud 服务帐户
- Cloud Volumes Service 帐户的API密钥文件

## 后端配置选项

每个后端都会在一个 Google Cloud 区域中配置卷。要在其他区域创建卷，您可以定义其他后端。

参数	Description	Default
ve版本		始终为 1
storageDriverName	存储驱动程序的名称	"GCP-CVS"
backendName	自定义名称或存储后端	驱动程序名称 + "_" + API 密钥的一部分
s存储类	用于指定CVS服务类型的可选参数。使用 ... software 选择CVS服务类型。否则、Astra Trident将 采用CVS-Performance服务类型 (hardware) 。	
storagePools	仅限CVS服务类型。用于指定用于创建卷的存储池的可 选参数。	
projectNumber	Google Cloud 帐户项目编号。此值可在Google Cloud 门户主页上找到。	
hostProjectNumber	如果使用共享VPC网络、则为必需项。在此情景中、 projectNumber 是服务项目、和 hostProjectNumber 是主机项目。	
区域	Astra Trident创建Cloud Volumes Service 卷的Google 云区域。创建跨区域Kubernetes集群时、在中创建的 卷 apiRegion 可用于在多个Google Cloud地区的节点 上计划的工作负载。跨区域流量会产生额外成本。	
apiKey	Google Cloud服务帐户的API密钥 netappcloudvolumes.admin 角色。它包括 Google Cloud 服务帐户专用密钥文件的 JSON 格式的 内容（逐字复制到后端配置文件）。	
代理 URL	代理服务器需要连接到CVS帐户时的代理URL。代理服 务器可以是 HTTP 代理，也可以是 HTTPS 代理。对于 HTTPS 代理，将跳过证书验证，以允许在代理服务器 中使用自签名证书。不支持启用了身份验证的代理服务 器。	
nfsMountOptions	精细控制 NFS 挂载选项。	"nfsvers=3"

参数	Description	Default
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）
s服务级别	新卷的CVS-Performance或CVS服务级别。CVS-Performance值为 standard, premium`或`extreme。CVS值为 standardsw 或 zoneredundantstandardsw。	CVS-Performance默认值为"standard"。CVS默认值为"standardsw"。
网络	用于Cloud Volumes Service 卷的Google云网络。	default
debugTraceFlags	故障排除时要使用的调试标志。示例、 \\{"api":false, "method":true}。除非您正在进行故障排除并需要详细的日志转储，否则请勿使用此功能。	空
allowedTopologies	要启用跨区域访问、请定义StorageClass allowedTopologies 必须包括所有地区。例如： - key: topology.kubernetes.io/region values: - us-east1 - europe-west1	

## 卷配置选项

您可以在中控制默认卷配置 defaults 部分。

参数	Description	Default
exportRule	新卷的导出规则。必须是以 CIDR 表示法表示的任意 IPv4 地址或 IPv4 子网组合的逗号分隔列表。	"0.0.0.0/0
snapshotDir	访问`.snapshot`目录	false
sSnapshot 预留	为快照预留的卷百分比	""（接受 CVS 默认值为 0）
s大小	新卷的大小。CVS性能最小值为100 GiB。CVS最小值为1 GiB。	CVS-Performance服务类型默认为"100GiB"。CVS服务类型未设置默认值、但至少需要1 GiB。

## CVS-Performance服务类型示例

以下示例提供了CVS-Performance服务类型的示例配置。

```
---
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
apiRegion: us-west2
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qP8B4Kws8zX5ojY9m
    XsYg6gyxy4zq7OlwWgLwGa==
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@my-gcp-
    project.iam.gserviceaccount.com
  client_id: '123456789012345678901'
  auth_uri: https://accounts.google.com/o/oauth2/auth
```

```
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
```

### 示例2：服务级别配置

此示例说明了后端配置选项、包括服务级别和卷默认值。

[illegible]

```
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
proxyURL: http://proxy-server-hostname/
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 10Ti
serviceLevel: premium
defaults:
  snapshotDir: 'true'
  snapshotReserve: '5'
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  size: 5Ti
```





```

-----END PRIVATE KEY-----
client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
client_id: '123456789012345678901'
auth_uri: https://accounts.google.com/o/oauth2/auth
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
nfsMountOptions: vers=3,proto=tcp,timeo=600
defaults:
  snapshotReserve: '5'
  exportRule: 0.0.0.0/0
labels:
  cloud: gcp
region: us-west2
storage:
- labels:
  performance: extreme
  protection: extra
  serviceLevel: extreme
  defaults:
    snapshotDir: 'true'
    snapshotReserve: '10'
    exportRule: 10.0.0.0/24
- labels:
  performance: extreme
  protection: standard
  serviceLevel: extreme
- labels:
  performance: premium
  protection: extra
  serviceLevel: premium
  defaults:
    snapshotDir: 'true'
    snapshotReserve: '10'
- labels:
  performance: premium
  protection: standard
  serviceLevel: premium
- labels:
  performance: standard
  serviceLevel: standard

```

## 存储类定义

以下StorageClass定义适用于虚拟池配置示例。使用 `parameters.selector`、您可以为每个StorageClass指定用于托管卷的虚拟池。卷将在选定池中定义各个方面。

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-extra-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=extreme; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-standard-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium-extra-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-standard
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=standard"

```

```
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extra-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=extra"
allowVolumeExpansion: true
```

- 第一个StorageClass (cvs-extreme-extra-protection)映射到第一个虚拟池。这是唯一一个可提供极高性能且 Snapshot 预留为 10% 的池。
- 最后一个StorageClass (cvs-extra-protection)调用提供10%快照预留的任何存储池。Astra Trident决定选择哪个虚拟池、并确保满足快照预留要求。

## CVS服务类型示例

以下示例提供了CVS服务类型的示例配置。

[illegible]

```
auth_uri: https://accounts.google.com/o/oauth2/auth
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
serviceLevel: standardsw
```

## 示例2：存储池配置

此示例后端配置使用 `storagePools` 配置存储池。

```
---
version: 1
storageDriverName: gcp-cvs
backendName: gcp-std-so-with-pool
projectNumber: '531265380079'
apiRegion: europe-west1
apiKey:
  type: service_account
  project_id: cloud-native-data
  private_key_id: "<id_value>"
  private_key: |-
    -----BEGIN PRIVATE KEY-----
    MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQDaT+Oui9FBAw19
    L1AGEkrYU5xd9K5NlO5jMkIFND5wCD+Nv+jd1GvtFRLaLK5RvXyF5wzvztmODNS+
    qtScpQ+5cFpQkuGtv9U9+N6qtuVYYO3b504Kp5CtqVPJCgMJaK2j8pZTIqUiMum/
    5/Y9oTbZrjAHSMgJm2nHzFq2X0rqVMAHghI6ATm4DOuWx8XGWKTGIPlc0qPqJlqS
    LLaWOH4VIZQZCAyW5IU9p9CAmwqHgdG0uhFNfCgMmED6PBUvVLsLvcq86X+QSWR9k
    ETqElj/sGCenPF7ti1DhGBFafd9hPnxg9PZY29ArEZwY9G/ZjZQX7WPgs0VvxiNR
    DxZRC3GXAgMBAAECggEACn5c59bG/qnVEVI1CwMAa1M5M2z09JFh1L1ljKwntNPj
    Vilw2eTW2+UE7HbJru/S7KQgA5Dnn9kvCraEahPRuddUMrD0vG4kTl/IODV6uFuk
    Y0sZfbqd4jMUQ21smvGsqFzwloYWS5qzO1W83ivXH/HW/iqkmY2eW+EPRS/hwSSu
    SscR+SojI7PB0BWSJhlV4yqYf3vcD/D95e12CVHfRCkL85DKumeZ+yHENpiXGZAE
    t8xSs4a50OPm6NHhevCw2a/UQ95/foXNUR450HtbjieJo5o+FF6EYZQGfU2ZHZO8
    37FBKuaJkdGW5xqaI9TL7aqkGkFMF4F2qvOZM+vy8QKBgQD4oVuOkJD1hkTHP86W
    esFlw1kpWyJR9ZA7LI0g/rVpslnX+XdDq0WQf4umDLNau5hYEH9LU6ZSGs1Xk3/B
    NHwR6OXFuqEKNiu83d0zSlHhTy7PZpOZdj5a/vVvQfPDMz7OvsqLRd7YCAbdzuQ0
    +Ahq0Ztwvg0HQ64hdW0ukpYRRwKBgQDgyHj98oqswoYuIa+pPlyS0pPwLmjwKyNm
    /HayzCp+Qjiyy7Tzg8AUqlH1Ou83XbV428jvg7kDhO7PCCKFq+mMmfqHmTpb0Maq
    KpKnZg4ipsqPlyHNNEoRmcailXbwIhCLewMqMrggUiLOmCw4PscL5nK+4GKu2XE1
    jLqjWAZFMQKBgFhkQ9XXRAJ1kR3XpGHOgn890pZOkCVSrqu6aUef/5KY1Fct8ew
    F/+aIXM2iQSVmWQYOvVCnhuY/F2GfAQ7d0om3decuwIOCX/xy7PjHMkLXa2uaZs4
    WR17sLduj62RqXRLX0c0QkwBiNFyHbRcpdkZJQujbYMhBa+7j7SxT4BtAoGAWMWT
    UucocRXZm/pdvz9wteNH3YDwnJLMxm1KC06qMXbBoYrliY4sm3ywJWMC+iCd/H8A
    Gecxd/xVu5mA2L2N3KMq18Zhz8Th0G5DwKyDRJgOQ0Q46yuNXOoYEjlo4Wjyk8Me
    +t1Q8iK98E0UmZnhTgfSpSNElbz2AqnzQ3MN9uECgYAqdvdpVnKGfvdT2ZDjyMoJ
    E89UIC41WjjJGmHsd8W65+3X0RwMzKMT6aZc5tK9J5dHvmWIETnbM+lTImdBbFga
    NWOC6f3r2xbGXHhaWSl+nobpTuvlo56ZRJVvVk7lFMsiddzMuHH8pxfgNJemwA4P
    ThDHCEjv035NNV6KyoO0tA==
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@cloud-native-
  data.iam.gserviceaccount.com
  client_id: '107071413297115343396'
```



```

auth_uri: https://accounts.google.com/o/oauth2/auth
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40cloud-native-data.iam.gserviceaccount.com
storageClass: software
zone: europe-west1-b
network: default
storagePools:
- 1bc7f380-3314-6005-45e9-c7dc8c2d7509
serviceLevel: Standardsw

```

## 下一步是什么？

创建后端配置文件后，运行以下命令：

```
tridentctl create backend -f <backend-file>
```

如果后端创建失败，则后端配置出现问题。您可以运行以下命令来查看日志以确定发生原因：

```
tridentctl logs
```

确定并更正配置文件中的问题后，您可以再次运行 `create` 命令。

## 配置 NetApp HCI 或 SolidFire 后端

了解如何在Asta Trident安装中创建和使用Element后端。

### Element驱动程序详细信息

Asta三项功能提供 `solidfire-san` 用于与集群通信的存储驱动程序。支持的访问模式包括：  
*ReadWriteOnce(RWO)*、*ReadOnlyMany(ROX)*、*ReadWriteMany(rwx)*、*ReadWriteOncePod(RWOP)*。

。 `solidfire-san` 存储驱动程序支持 `_file_` 和 `_block_` 卷模式。。 `Filesystem volumemode`、Astra Trident 会创建卷并创建文件系统。文件系统类型由 `StorageClass` 指定。

驱动程序	协议	卷模式	支持的访问模式	支持的文件系统
<code>solidfire-san</code>	iSCSI	块	Rwo、ROX、rwx、RWOP	无文件系统。原始块设备。

驱动程序	协议	卷模式	支持的访问模式	支持的文件系统
solidfire-san	iSCSI	文件系统	Rwo、RWO1.	xfss , ext3 , ext4

## 开始之前

在创建Element后端之前、您需要满足以下要求。

- 运行 Element 软件的受支持存储系统。
- NetApp HCI/SolidFire 集群管理员或租户用户的凭据，可用于管理卷。
- 所有 Kubernetes 工作节点都应安装适当的 iSCSI 工具。请参见 ["工作节点准备信息"](#)。

## 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	始终为 "solidfire-san"
backendName	自定义名称或存储后端	SolidFire + 存储（iSCSI）IP 地址
端点	使用租户凭据的 SolidFire 集群的 MVIP	
sVIP	存储（iSCSI）IP 地址和端口	
标签	要应用于卷的一组任意 JSON 格式的标签。	"
租户名称	要使用的租户名称（如果未找到，则创建）	
InitiatorIFace	将 iSCSI 流量限制为特定主机接口	default
UseCHAP	使用CHAP对iSCSI进行身份验证。Asta三端到子使用CHAP。	true
访问组	要使用的访问组 ID 列表	查找名为 "trident " 的访问组的 ID
类型	QoS 规范	
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）
debugTraceFlags	故障排除时要使用的调试标志。示例 { "api" : false , "method " : true }	空



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。

## 示例1：的后端配置 solidfire-san 具有三种卷类型的驱动程序

此示例显示了一个后端文件，该文件使用 CHAP 身份验证并使用特定 QoS 保证对三种卷类型进行建模。然后，您很可能会使用 IOPS storage class 参数定义存储类以使用其中的每种类型。

```
---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
SVIP: "<svip>:3260"
TenantName: "<tenant>"
labels:
  k8scluster: dev1
  backend: dev1-element-cluster
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000
```

## 示例2：的后端和存储类配置 solidfire-san 具有虚拟池的驱动程序

此示例显示了使用虚拟池配置的后端定义文件以及引用这些池的StorageClasses。

在配置时、Astra Trident会将存储池上的标签复制到后端存储LUN。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。

在下面所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、这些存储池设置了 type 在Silver。虚拟池在中进行定义 storage 部分。在此示例中、某些存储池会设置自己的类型、而某些存储池会覆盖上面设置的默认值。

```
---
version: 1
storageDriverName: solidfire-san
```

```
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
SVIP: "<svip>:3260"
TenantName: "<tenant>"
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000
type: Silver
labels:
  store: solidfire
  k8scluster: dev-1-cluster
region: us-east-1
storage:
- labels:
    performance: gold
    cost: '4'
    zone: us-east-1a
    type: Gold
- labels:
    performance: silver
    cost: '3'
    zone: us-east-1b
    type: Silver
- labels:
    performance: bronze
    cost: '2'
    zone: us-east-1c
    type: Bronze
- labels:
    performance: silver
    cost: '1'
    zone: us-east-1d
```

以下StorageClass定义引用了上述虚拟池。使用 `parameters.selector` 字段中、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 (`solidfire-gold-four`)将映射到第一个虚拟池。这是唯一一个可通过提供金牌性能的池 Volume Type QoS 金牌。最后一个StorageClass (`solidfire-silver`)调用提供银牌性能的任何存储池。Astra Trident将决定选择哪个虚拟池、并确保满足存储要求。

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-gold-four
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold; cost=4"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-three
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=3"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-bronze-two
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze; cost=2"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-one
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=1"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
  fsType: "ext4"

```

了解更多信息

- ["卷访问组"](#)

## ONTAP SAN 驱动程序

### ONTAP SAN驱动程序概述

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

### ONTAP SAN驱动程序详细信息

Asta三端存储提供了以下SAN存储驱动程序、用于与ONTAP集群进行通信。支持的访问模式包括：  
*ReadWriteOnce(RWO)*、*ReadOnlyMany(ROX)*、*ReadWriteMany(rwx)*、*ReadWriteOncePod(RWOP)*。



如果您使用Astra Control进行保护、恢复和移动、请阅读 [Astra Control驱动程序兼容性](#)。

驱动程序	协议	卷模式	支持的访问模式	支持的文件系统
ontap-san	iSCSI	块	Rwo、ROX、rwx、RWOP	无文件系统；原始块设备
ontap-san	iSCSI	文件系统	Rwo、RW01.  Rox和rwx在文件系统卷模式下不可用。	xfs ， ext3 ， ext4
ontap-san	NVMe/TCP  请参见 <a href="#">NVMe/TCP 的其他注意 事项。</a>	块	Rwo、ROX、rwx、RWOP	无文件系统；原始块设备
ontap-san	NVMe/TCP  请参见 <a href="#">NVMe/TCP 的其他注意 事项。</a>	文件系统	Rwo、RW01.  Rox和rwx在文件系统卷模式下不可用。	xfs ， ext3 ， ext4
ontap-san-economy.	iSCSI	块	Rwo、ROX、rwx、RWOP	无文件系统；原始块设备
ontap-san-economy.	iSCSI	文件系统	Rwo、RW01.  Rox和rwx在文件系统卷模式下不可用。	xfs ， ext3 ， ext4

## Astra Control驱动程序兼容性

Astra Control可为使用创建的卷提供无缝保护、灾难恢复和移动性(在Kubernetes集群之间移动卷) `ontap-nas` , `ontap-nas-flexgroup`, 和 `ontap-san` 驱动程序。请参见 ["Astra Control复制前提条件"](#) 了解详细信息。



- 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。

## 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。

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

## NVMe/TCP的其他注意事项

Asta三端存储器支持使用的非易失性内存快速(NVMe)协议 `ontap-san` 驱动程序包括：

- IPv6
- NVMe卷的快照和克隆
- 调整NVMe卷大小
- 导入在Asta Trident外部创建的NVMe卷、以便Asta Trident可以管理其生命周期
- NVMe本机多路径
- 正常或非正常关闭K8s节点(24.02)

Astra三项技术不支持：

- DH-HMAC-CHAP、由NVMe本机提供支持
- 设备映射程序(Device mapper、DM)多路径
- 进行了加密

## 准备使用ONTAP SAN驱动程序配置后端

了解使用ONTAP SAN驱动程序配置ONTAP后端的要求和身份验证选项。



## 要求

对于所有 ONTAP 后端，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，您可以配置使用 `ontap-san` 驱动程序的 `san-dev` 类和使用 `ontap-san-economy-one` 的 `san-default` 类。

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

## 对 ONTAP 后端进行身份验证

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）。

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

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：

## YAML

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: password
```

## JSON

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

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

启用基于证书的身份验证

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

- `clientCertificate`：客户端证书的 Base64 编码值。
- `clientPrivateKey`：关联私钥的 Base64 编码值。
- `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=admin"
```

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

```
security certificate install -type server -cert-name <trusted-ca-cert-name> -vserver <vserver-name>
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca <cert-authority>
```

3. 在 ONTAP 集群上安装客户端证书和密钥（从步骤 1 开始）。

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

4. 确认 ONTAP 安全登录角色支持 cert 身份验证方法。

```
security login create -user-or-group-name admin -application ontapi -authentication-method cert
security login create -user-or-group-name admin -application http -authentication-method cert
```

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

```
curl -X POST -Lk https://<ONTAP-Management-LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key --cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp xmlns="http://www.netapp.com/filer/admin" version="1.21" vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. 使用 Base64 对证书，密钥和可信 CA 证书进行编码。

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

7. 使用从上一部获得的值创建后端。

```
cat cert-backend.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "trustedCACertificate": "QNFinfO...SiqOyN",
  "storagePrefix": "myPrefix_"
}

tridentctl create backend -f cert-backend.json -n trident
+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                UUID                |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |         0 |
+-----+-----+-----+-----+
+-----+-----+
```

#### 更新身份验证方法或轮换凭据

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

```
cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "password",
  "storagePrefix": "myPrefix_"
}

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

+-----+-----+-----+
+-----+-----+
| NAME | STORAGE DRIVER | UUID |
STATE | VOLUMES |
+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online | 9 |
+-----+-----+-----+
+-----+-----+
```



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

更新后端不会中断对已创建卷的访问，也不会影响在之后建立的卷连接。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。

#### 使用双向 **CHAP** 对连接进行身份验证

Astra Trident 可以使用双向 CHAP 对 iSCSI 会话进行身份验证 `ontap-san` 和 `ontap-san-economy` 驱动程序。这需要启用 `useCHAP` 选项。设置为 `true` 中，A 作用 是将 SVM 的默认启动程序安全性配置为双向 CHAP，并设置后端文件中的用户名和密钥。NetApp 建议使用双向 CHAP 对连接进行身份验证。请参见以下配置示例：

```

---
version: 1
storageDriverName: ontap-san
backendName: ontap_san_chap
managementLIF: 192.168.0.135
svm: ontap_iscsi_svm
useCHAP: true
username: vsadmin
password: password
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz

```



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

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

#### 工作原理

通过将 `useCHAP` 设置为 `true`，存储管理员指示 Astra Trident 在存储后端配置 CHAP。其中包括：

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

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

#### 轮换凭据并更新后端

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



更新后端的 CHAP 密码时，必须使用 `tridentctl` 来更新后端。请勿通过 CLI/ONTAP UI 更新存储集群上的凭据，因为 Astra Trident 将无法选取这些更改。

```
cat backend-san.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap_san_chap",
  "managementLIF": "192.168.0.135",
  "svm": "ontap_iscsi_svm",
  "useCHAP": true,
  "username": "vsadmin",
  "password": "password",
  "chapInitiatorSecret": "cl9qxUpDaTeD",
  "chapTargetInitiatorSecret": "rqxigXgkeUpDaTeD",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
}

./tridentctl update backend ontap_san_chap -f backend-san.json -n trident
+-----+-----+-----+-----+
+-----+-----+
| NAME | STORAGE DRIVER | UUID |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| ontap_san_chap | ontap-san | aa458f3b-ad2d-4378-8a33-1a472ffbeb5c |
online | 7 |
+-----+-----+-----+-----+
+-----+-----+
```

现有连接将不受影响；如果凭据由 SVM 上的 Astra Trident 更新，则这些连接将继续保持活动状态。新连接将使用更新后的凭据，现有连接将继续保持活动状态。断开并重新连接旧的 PV 将导致它们使用更新后的凭据。

### ONTAP SAN配置选项和示例

了解如何在Astra三端安装中创建和使用ONTAP SAN驱动程序。本节提供了将后端映射到StorageClasses的后端配置示例和详细信息。

#### 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
storageDrive rName	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	<p>集群或SVM管理LIF的IP地址。</p> <p>可以指定完全限定域名(FQDN)。</p> <p>如果使用IPv6标志安装了Asta三元组、则可以设置为使用IPv6地址。IPv6地址必须使用方括号进行定义、例如 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。</p> <p>有关无缝MetroCluster切换、请参见 <a href="#">MetroCluster示例</a>。</p>	"10.0.0.1", "2001: 1234 : abcd :: fefe]
dataLIF	<p>协议 LIF 的 IP 地址。</p> <p>请勿为iSCSI指定。Astra Trident使用 "<a href="#">ONTAP 选择性LUN映射</a>" 发现建立多路径会话所需的iSCSI LIF。如果出现、则会生成警告 dataLIF 已明确定义。</p> <p>*对于MetroCluster省略。*请参见 <a href="#">MetroCluster示例</a>。</p>	由SVM派生
sVM	<p>要使用的 Storage Virtual Machine</p> <p>*对于MetroCluster省略。*请参见 <a href="#">MetroCluster示例</a>。</p>	如果指定了 SVM managementLIF，则派生
使用 CHAP	使用CHAP对iSCSI的ONTAP SAN驱动程序进行身份验证[布尔值]。设置为 true 让Astra Trident为后端给定的SVM配置并使用双向CHAP作为默认身份验证。请参见 " <a href="#">准备使用ONTAP SAN驱动程序配置后端</a> " 了解详细信息。	false
chapInitiatorSecret	CHAP 启动程序密钥。如果为 useCHAP=true，则为必需项	""
标签	要应用于卷的一组任意 JSON 格式的标签	""
chapTargetInitiatorSecret	CHAP 目标启动程序密钥。如果为 useCHAP=true，则为必需项	""
chapUsername	入站用户名。如果为 useCHAP=true，则为必需项	""
chapTargetUsername	目标用户名。如果为 useCHAP=true，则为必需项	""
客户端证书	客户端证书的 Base64 编码值。用于基于证书的身份验证	""
clientPrivateKey	客户端专用密钥的 Base64 编码值。用于基于证书的身份验证	""



参数	Description	Default
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	与ONTAP 集群通信所需的用户名。用于基于凭据的身份验证。	""
密码	与ONTAP 集群通信所需的密码。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
s存储前缀	在 SVM 中配置新卷时使用的前缀。无法稍后修改。要更新此参数、您需要创建一个新的后端。	trident
limitAggregateUsage	如果使用量超过此百分比，则配置失败。如果您使用适用于NetApp ONTAP 后端的Amazon FSX、请勿指定 limitAggregateUsage。提供的 fsxadmin 和 vsadmin 请勿包含检索聚合使用情况所需的权限、并使用Astra Trident对其进行限制。	""（默认情况下不强制实施）
limitVolumeSize	如果请求的卷大小超过此值、则配置失败。此外、还会限制它为qtree和LUN管理的卷的最大大小。	""(默认情况下不强制实施)
lunsPerFlexvol	每个 FlexVol 的最大 LUN 数，必须在 50 ， 200 范围内	100
debugTraceFlags	故障排除时要使用的调试标志。例如、 {"api": false、"METHO": true}  除非正在进行故障排除并需要详细的日志转储、否则请勿使用。	null
useREST	用于使用 ONTAP REST API 的布尔参数。* 技术预览*  useREST 作为一个*技术预览版提供、建议用于测试环境、而不是生产工作负载。设置为 true、Astra Trident将使用ONTAP REST API与后端进行通信。此功能需要使用ONTAP 9.11.1及更高版本。此外、使用的ONTAP 登录角色必须有权访问 ontap 应用程序。这一点可通过预定义来满足 vsadmin 和 cluster-admin 角色。  useREST MetroCluster 不支持。  useREST 完全符合NVMe/TCP要求。	false
sanType	使用选择 iscsi 对于iSCSI或 nvme 适用于NVMe/TCP。	iscsi 如果为空

## 用于配置卷的后端配置选项

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

参数	Description	Default
spaceAllocation	LUN 的空间分配	"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。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。	""
adaptiveQosPolicy	要为创建的卷分配的自适应 QoS 策略组。选择每个存储池 / 后端的 qosPolicy 或 adaptiveQosPolicy 之一	""
sSnapshot 预留	为快照预留的卷百分比	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Astra Trident中配置的任何卷都将启用NAE。有关详细信息、请参见： <a href="#">"Astra Trident如何与NVE和NAE配合使用"</a> 。	false
luksEncryption	启用LUKS加密。请参见 <a href="#">"使用Linux统一密钥设置(LUKS)"</a> 。  NVMe/TCP不支持使用此类数据加密。	""
securityStyle	新卷的安全模式	unix
分层策略	使用"无"的层策略	对于ONTAP 9.5 SVM-DR之前的配置、为"仅快照"

#### 卷配置示例

下面是一个定义了默认值的示例：

```

---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: trident_svm
username: admin
password: <password>
labels:
  k8scluster: dev2
  backend: dev2-sanbackend
storagePrefix: alternate-trident
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: standard
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'

```



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

对于定义 snapshotReserve 的后端，Astra Trident 将按如下方式计算卷的大小：

$$\text{Total volume size} = [(\text{PVC requested size}) / (1 - (\text{snapshotReserve percentage} / 100))] * 1.1$$

1.1 是 Astra Trident 向 FlexVol 额外添加 10% 以容纳 LUN 元数据。对于 snapshotReserve = 5%，PVC 请求 = 5GiB，卷总大小为 5.79GiB，可用大小为 5.5GiB。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_e42ec6fe_3baa_4af6_996d_134adbbb8e6d	online	RW	5.79GB	5.50GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

3 entries were displayed.

目前，调整大小是对现有卷使用新计算的唯一方法。

## 最低配置示例

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



如果您将Amazon FSx on NetApp ONTAP与Asta Dent结合使用、则建议您为指定DNS名称、而不是IP地址。

### ONTAP SAN示例

这是使用的基本配置 `ontap-san` 驱动程序。

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
username: vsadmin
password: <password>
```

### ONTAP SAN经济性示例

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

## 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-san
managementLIF: 192.168.1.66
username: vsadmin
password: password
```

## 基于证书的身份验证示例

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

```
---
version: 1
storageDriverName: ontap-san
backendName: DefaultSANBackend
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

## 双向CHAP示例

这些示例使用创建后端 `useCHAP` 设置为 `true`。

### ONTAP SAN CHAP示例

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
```

### ONTAP SAN经济性CHAP示例

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
```

## NVMe/TCP示例

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

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

## 虚拟池后端示例

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

A作用 是在"Comments"字段中设置配置标签。注释在FlexVol 上设置。在配置时、Astra 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-san
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: 'false'
  encryption: 'false'
  qosPolicy: standard
labels:
  store: san_store
  kubernetes-cluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  protection: gold
  creditpoints: '40000'
  zone: us_east_1a
  defaults:
    spaceAllocation: 'true'
    encryption: 'true'
    adaptiveQosPolicy: adaptive-extreme
- labels:
  protection: silver
  creditpoints: '20000'
  zone: us_east_1b
  defaults:
    spaceAllocation: 'false'
    encryption: 'true'
    qosPolicy: premium
- labels:
  protection: bronze
  creditpoints: '5000'
  zone: us_east_1c
  defaults:
    spaceAllocation: 'true'
    encryption: 'false'

```

```

---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: 'false'
  encryption: 'false'
labels:
  store: san_economy_store
region: us_east_1
storage:
- labels:
  app: oracledb
  cost: '30'
  zone: us_east_1a
  defaults:
    spaceAllocation: 'true'
    encryption: 'true'
- labels:
  app: postgresdb
  cost: '20'
  zone: us_east_1b
  defaults:
    spaceAllocation: 'false'
    encryption: 'true'
- labels:
  app: mysqldb
  cost: '10'
  zone: us_east_1c
  defaults:
    spaceAllocation: 'true'
    encryption: 'false'
- labels:
  department: legal
  creditpoints: '5000'

```

```
zone: us_east_1c
defaults:
  spaceAllocation: 'true'
  encryption: 'false'
```

## NVMe/TCP示例

```
---
version: 1
storageDriverName: ontap-san
sanType: nvme
managementLIF: 10.0.0.1
svm: nvme_svm
username: vsadmin
password: <password>
useREST: true
defaults:
  spaceAllocation: 'false'
  encryption: 'true'
storage:
- labels:
  app: testApp
  cost: '20'
  defaults:
    spaceAllocation: 'false'
    encryption: 'false'
```

## 将后端映射到 **StorageClasses**

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

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

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

- 。 protection-not-gold StorageClass将映射到中的第二个和第三个虚拟池 ontap-san 后端。只有这些池提供的保护级别不是gold。

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

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

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

- 。 protection-silver-creditpoints-20k StorageClass将映射到中的第二个虚拟池 ontap-san 后端。这是唯一提供银牌保护和20000个信用点的池。

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"

```

- 。 creditpoints-5k StorageClass将映射到中的第三个虚拟池 ontap-san 中的后端和第四个虚拟池 ontap-san-economy 后端。这是唯一一款信用点数为5000的池产品。

```

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

```

- 。 my-test-app-sc StorageClass将映射到 testAPP 中的虚拟池 ontap-san 驱动程序 sanType: nvme。这是唯一的池产品 testApp。

```

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

```

Astra Trident将决定选择哪个虚拟池、并确保满足存储要求。

## 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

Asta三端存储提供了以下NAS存储驱动程序、用于与ONTAP集群进行通信。支持的访问模式包括：  
： *ReadWriteOnce(RWO)*、 *ReadOnlyMany(ROX)*、 *ReadWriteMany(rwx)*、 *ReadWriteOncePod(RWOP)*。



如果您使用Astra Control进行保护、恢复和移动、请阅读 [Astra Control驱动程序兼容性](#)。

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、RWO P	""、 nfs， smb
ontap-nas-economy.	NFS SMB	文件系统	Rwo、ROX、rwx、RWO P	""、 nfs， smb
ontap-nas-flexgroup	NFS SMB	文件系统	Rwo、ROX、rwx、RWO P	""、 nfs， smb

Astra Control驱动程序兼容性

Astra Control可为使用创建的卷提供无缝保护、灾难恢复和移动性(在Kubernetes集群之间移动卷) `ontap-nas`， `ontap-nas-flexgroup`， 和 `ontap-san` 驱动程序。请参见 ["Astra Control复制前提条件"](#) 了解详细信息。



- 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。

用户权限

Astra Trident应以ONTAP 或SVM管理员身份运行、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应使用集群以ONTAP 或SVM管理员身份运行 `fsxadmin` 用户或 `vsadmin` SVM用户或具有相同角色的其他名称的用户。。 `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。

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。

### 要求

- 对于所有 ONTAP 后端，Astra Trident 需要至少为 SVM 分配一个聚合。
- 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：
- Astra Trident仅支持将SMB卷挂载到Windows节点上运行的Pod。请参见 [准备配置SMB卷](#) 了解详细信息。

### 对ONTAP后端进行身份验证

Astra 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：此模式要求在后端安装证书、才能使Astra Trident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

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：

## YAML

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

## JSON

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

请注意，后端定义是凭据以纯文本格式存储的唯一位置。创建后端后，用户名 / 密码将使用 Base64 进行编码并存储为 Kubernetes 密钥。创建 / 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                      |
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。

Asta三叉式存储提供了动态管理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。



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
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、为Astra三端存储专用SVM。

以下是使用上述示例对此功能的工作原理进行的说明：

- `autosExportPolicy` 设置为 `true`。这表示 Astra Trident 将为 `svm1` SVM 创建导出策略，并使用 `autosExportCIDRS` 地址块处理规则的添加和删除。例如，UUID 为 `403b5326-8482-40db-96d0-d83fb3f4daec` 且 `autosExportPolicy` 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。
- `autosExportCIDR` 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 `autosExportCIDRS` 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 `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 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: ""
    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
```

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、请使用更新后端 `tridentctl update backend` 将确保 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、后端上的卷在重新挂载时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 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。

## 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。



要创建、您必须在 SVM 上同时配置 NFS 和 SMB/CCIFS 协议 `ontap-nas-economy` 适用于内部 ONTAP 的 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。

## 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 2019的Windows工作节点。Astra Trident仅支持将SMB卷挂载到Windows节点上运行的Pod。
- 至少一个包含Active Directory凭据的Astra Trident密钥。以生成密钥 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Astra三端存储为您创建一个共享。



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 vserver_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Asta三端到功能创建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 <b>ntfs</b> 或 <b>mixed</b> 用于 <b>SMB</b> 卷。	ntfs 或 mixed 对于SMB卷
unixPermissions	新卷的模式。对于SMB卷、必须留空。	""

## ONTAP NAS配置选项和示例

了解如何创建ONTAP NAS驱动程序并将其用于Astra三端安装。本节提供了将后端映射到StorageClasses的后端配置示例和详细信息。

### 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经济"、"ONTAP NAS灵活组"、"ONTAP SAN "、"ONTAP SAN经济"
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)。  如果使用IPv6标志安装了Asta三元组、则可以设置为使用IPv6地址。IPv6地址必须使用方括号进行定义、例如 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。  有关无缝MetroCluster切换、请参见 <a href="#">MetroCluster示例</a> 。	"10.0.0.1 "， "2001： 1234： abcd：：： fefe]"

参数	Description	Default
dataLIF	<p>协议 LIF 的 IP 地址。</p> <p>建议指定 dataLIF。如果未提供此参数、则Astra Trident会从SVM提取数据LIF。您可以指定用于NFS挂载操作的完全限定域名(FQDN)、从而可以创建循环DNS、以便在多个数据LIF之间实现负载平衡。</p> <p>可以在初始设置后更改。请参见 。</p> <p>如果使用IPv6标志安装了Astra三元组、则可以设置为使用IPv6地址。IPv6地址必须使用方括号进行定义、例如 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]。</p> <p>*对于MetroCluster省略。*请参见 <a href="#">MetroCluster示例</a>。</p>	指定的地址或派生自SVM (如果未指定)(不建议)
sVM	<p>要使用的 Storage Virtual Machine</p> <p>*对于MetroCluster省略。*请参见 <a href="#">MetroCluster示例</a>。</p>	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、Astra Trident可以自动管理导出策略。	false
autosExportCIDR	<p>用于筛选Kubbernetes节点IP的CIDR列表 autoExportPolicy 已启用。</p> <p>使用 autoExportPolicy 和 autoExportCIDRs 选项、Astra Trident可以自动管理导出策略。</p>	["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	
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	"三级联"
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。此外、还会限制它为qtree和LUN以及管理的卷的最大大小 qtreesPerFlexvol 选项用于自定义每个FlexVol 的最大qtree数。	""(默认情况下不强制实施)



参数	Description	Default
lunsPerFlexvol	每个 FlexVol 的最大 LUN 数，必须在 50 ， 200 范围内	"100"
debugTraceFlags	故障排除时要使用的调试标志。例如、 {"api": false、"METHO": true}  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卷创建。选项包括 nfs， smb 或为空。默认情况下、将设置为空会将NFS卷设置为空。	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、但如果在存储类中未指定挂载选项、则Astra 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Astra 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Astra三端到功能创建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	用于使用 ONTAP REST API 的布尔参数。* 技术预览 * useREST 作为一个*技术预览版提供、建议用于测试环境、而不是生产工作负载。设置为 true、Astra Trident将使用ONTAP REST API与后端进行通信。此功能需要使用ONTAP 9.11.1及更高版本。此外、使用的ONTAP 登录角色必须有权访问 ontap 应用程序。这一点可通过预定义来满足 vsadmin 和 cluster-admin 角色。 useREST MetroCluster 不支持。	false

## 用于配置卷的后端配置选项

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

参数	Description	Default
spaceAllocation	LUN 的空间分配	"正确"
s页面预留	空间预留模式；"无"(精简)或"卷"(厚)	"无"

参数	Description	Default
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Astra Trident中配置的任何卷都将启用NAE。有关详细信息、请参见： <a href="#">"Astra Trident如何与NVE和NAE配合使用"</a> 。	false
分层策略	使用"无"的层策略	对于ONTAP 9.5 SVM-DR之前的配置、为"仅快照"
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	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。



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。

#### 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'

```

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：

```

Total volume size = (PVC requested size) / (1 - (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` 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 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。此操作对于也是如此 ontap-nas-economy 和 ontap-nas-flexgroup 驱动程序。

```
---
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_
```

## 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。

A作用 是在"Comments"字段中设置配置标签。在FlexVol上为设置了注释 ontap-nas 或FlexGroup ontap-nas-flexgroup。在配置时、Astra 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"

```

Astra 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数据LIF、方法是运行以下命令、为新的后端JSON文件提供更新的数据LIF。

```

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、则必须关闭所有对应Pod、然后将其恢复到、新数据LIF才能生效。

## 适用于 NetApp ONTAP 的 Amazon FSX

将 **Astra Trident** 与适用于 **NetApp ONTAP** 的 **Amazon FSX** 结合使用

"适用于 NetApp ONTAP 的 Amazon FSX" 是一种完全托管的AWS服务、可使客户启动和运行由NetApp ONTAP 存储操作系统提供支持的文件系统。借助适用于ONTAP 的FSx、您可以利用您熟悉的NetApp功能、性能和管理功能、同时利用在AWS上存储数据的简便性、灵活性、安全性和可扩展性。FSX for ONTAP 支持ONTAP 文件系统功能和管理API。

### 概述

文件系统是 Amazon FSX 中的主要资源，类似于内部部署的 ONTAP 集群。在每个 SVM 中，您可以创建一个或多个卷，这些卷是将文件和文件夹存储在文件系统中的数据容器。借助适用于 NetApp ONTAP 的 Amazon FSX，Data ONTAP 将作为云中的托管文件系统提供。新的文件系统类型称为 \* NetApp ONTAP \*。

通过将 Astra Trident 与适用于 NetApp ONTAP 的 Amazon FSx 结合使用，您可以确保在 Amazon Elastic Kubernetes Service （EKS）中运行的 Kubernetes 集群可以配置由 ONTAP 备份的块和文件永久性卷。

### 注意事项

- SMB卷：
  - SMB卷支持使用 `ontap-nas` 仅限驱动程序。
  - Astra Trident EKS加载项不支持SMB卷。
  - Astra Trident仅支持将SMB卷挂载到Windows节点上运行的Pod。
- 在Astra Trident 24.02之前的版本中、在启用了自动备份的Amazon FSx文件系统上创建的卷无法被Trident删除。要在Astra三端到高24.02或更高版本中阻止此问题描述、请指定 `fsxFilesystemID`、`AWS apiRegion`、`AWS apiKey``和`AWS `secretKey` 在AWS FSx for ONTAP的后端配置文件中。



如果要为Astra Trident指定IAM角色、则可以省略指定 `apiRegion`，`apiKey`，和 `secretKey` 将字段显式添加到Astra三端。有关详细信息，请参见 ["适用于ONTAP 的FSX配置选项和示例"](#)。

### FSx for ONTAP驱动程序详细信息

您可以使用以下驱动程序将Astra Trident与适用于NetApp ONTAP 的Amazon FSx集成：

- `ontap-san`：配置的每个 PV 都是其自己的 Amazon FSX for NetApp ONTAP 卷中的一个 LUN。
- `ontap-san-economy`：为 NetApp ONTAP 卷配置的每个 PV 都是一个 LUN，每个 Amazon FSX 具有可配置的 LUN 数量。
- `ONONTAP NAS`：配置的每个 PV 都是适用于 NetApp ONTAP 的完整 Amazon FSX 卷。
- `ontap-nas-economy.`：配置的每个 PV 都是一个 `qtree`，对于 NetApp ONTAP 卷，每个 Amazon FSx 的 `qtree` 数量是可配置的。



- `ontap-nas-flexgroup`：配置的每个 PV 都是适用于 NetApp ONTAP FlexGroup 卷的完整 Amazon FSX 。

有关驱动程序详细信息、请参见 "[NAS驱动程序](#)" 和 "[SAN驱动程序](#)"。

## 身份验证

Astra Trident提供两种身份验证模式。

- 基于证书：Astra Trident 将使用 SVM 上安装的证书与 FSX 文件系统上的 SVM 进行通信。
- 基于凭据：您可以使用文件系统的 `fsxadmin` 用户或为 SVM 配置的 `vsadmin` 用户。



Astra Trident应作为运行 `vsadmin` SVM用户或具有相同角色的其他名称的用户。适用于NetApp ONTAP 的Amazon FSX具有 `fsxadmin` 有限更换ONTAP 的用户 `admin` 集群用户。我们强烈建议使用 `vsadmin` 使用Astra Trident。

您可以更新后端以在基于凭据的方法和基于证书的方法之间移动。但是、如果您尝试提供\*凭据和证书\*、则后端创建将失败。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。

有关启用身份验证的详细信息、请参阅适用于您的驱动程序类型的身份验证：

- "[ONTAP NAS身份验证](#)"
- "[ONTAP SAN身份验证](#)"

## 适用于EKS的云身份

通过云身份、Kubernetes Pod可以通过作为AWS IAM角色进行身份验证来访问AWS资源、而不是提供显式AWS凭据。

要在AWS中利用云身份、您必须：

- 使用EKS部署的Kubernetes集群
- 已安装Astra三项功能、其中包括 `cloudProvider` 指定 "AWS" 和 `cloudIdentity` 指定AWS IAM角色。

## Trident 运算符

要使用三端运算符安装Astra三端、请编辑 `tridentorchestrator_cr.yaml` 设置 `cloudProvider` to "AWS" 并设置 `cloudIdentity` 分配给AWS IAM角色。

例如：

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "AWS"
  cloudIdentity: "'eks.amazonaws.com/role-arn:
arn:aws:iam::123456:role/astratrident-role'"
```

## 掌舵

使用以下环境变量设置\*云提供程序\*和\*云身份\*标志的值：

```
export CP="AWS"
export CI="'eks.amazonaws.com/role-arn:
arn:aws:iam::123456:role/astratrident-role'"
```

以下示例将安装Astra Dent和Sets `cloudProvider` to AWS 使用环境变量 `$CP` 并使用环境变量设置"云标识" `$CI`：

```
helm install trident trident-operator-100.2402.0.tgz --set
cloudProvider=$CP --set cloudIdentity=$CI
```

## <code>tridentctl</code>

使用以下环境变量设置\*云提供程序\*和\*云身份\*标志的值：

```
export CP="AWS"
export CI="'eks.amazonaws.com/role-arn:
arn:aws:iam::123456:role/astratrident-role'"
```

以下示例将安装Astra Dent并设置 `cloud-provider` 标记为 `$CP`，和 `cloud-identity` to `$CI`：

```
tridentctl install --cloud-provider=$CP --cloud-identity="$CI" -n
trident
```

了解更多信息

- ["Amazon FSX for NetApp ONTAP 文档"](#)
- ["有关适用于 NetApp ONTAP 的 Amazon FSX 的博客文章"](#)

## 集成适用于NetApp ONTAP 的Amazon FSX

您可以将适用于NetApp ONTAP 的Amazon FSX文件系统与Astra Trident集成、以确保在Amazon Elastic Kubernetes Service (EKS)中运行的Kubernetes集群可以配置由ONTAP提供支持的块和文件永久性卷。

### 要求

此外 ["Astra Trident 要求"](#)要将适用于ONTAP 的FSx与Astra Trident集成、您需要：

- 已安装 `kubectl` 的现有 Amazon EKS 集群或自管理 Kubernetes 集群。
- 可从集群的工作节点访问的现有Amazon FSx for NetApp ONTAP文件系统和Storage Virtual Machine (SVM)。
- 为准备工作的工作节点 ["NFS或iSCSI"](#)。



确保按照Amazon Linux和Ubuntu所需的节点准备步骤进行操作 ["Amazon Machine 映像"](#) (AMIS)，具体取决于您的 EKS AMI 类型。

- Astra Trident仅支持将SMB卷挂载到Windows节点上运行的Pod。请参见 [准备配置SMB卷](#) 了解详细信息。

## ONTAP SAN和NAS驱动程序集成



如果要为SMB卷配置、则必须读取 [准备配置SMB卷](#) 创建后端之前。

### 步骤

1. 使用其中一种部署Astra Trident ["部署方法"](#)。
2. 收集SVM管理LIF DNS名称。例如、使用AWS命令行界面查找 `DNSName` 下的条目 `Endpoints → Management` 运行以下命令后：

```
aws fsx describe-storage-virtual-machines --region <file system region>
```

3. 创建和安装证书 ["NAS后端身份验证"](#) 或 ["SAN后端身份验证"](#)。



您可以从可以访问文件系统的任何位置使用 SSH 登录到文件系统（例如，安装证书）。使用 `fsxadmin` 用户，创建文件系统时配置的密码以及 `AWS FSx describe` 文件系统 中的管理 DNS 名称。

4. 使用您的证书和管理 LIF 的 DNS 名称创建后端文件，如以下示例所示：

## YAML

```
version: 1
storageDriverName: ontap-san
backendName: customBackendName
managementLIF: svm-XXXXXXXXXXXXXXXXXXXX.fs-XXXXXXXXXXXXXXXXXXXX.fsx.us-
east-2.aws.internal
svm: svm01
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

## JSON

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "customBackendName",
  "managementLIF": "svm-XXXXXXXXXXXXXXXXXXXX.fs-
XXXXXXXXXXXXXXXXXXXX.fsx.us-east-2.aws.internal",
  "svm": "svm01",
  "clientCertificate": "ZXR0ZXJwYXB...ICMgJ3BhcGVyc2",
  "clientPrivateKey": "vciwKIyAgZG...0cnksIGRlc2NyaX",
  "trustedCACertificate": "zcyBbaG...b3Igb3duIGNsYXNz"
}
```

或者、您也可以使用存储在AWS机密管理器中的SVM凭据(用户名和密码)创建后端文件、如以下示例所示：

## YAML

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
    fsxFileSystemID: fs-xxxxxxxxxx
  managementLIF:
  credentials:
    name: "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name"
    type: awsarn
```

## JSON

```
{
  "apiVersion": "trident.netapp.io/v1",
  "kind": "TridentBackendConfig",
  "metadata": {
    "name": "backend-tbc-ontap-nas"
  },
  "spec": {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "tbc-ontap-nas",
    "svm": "svm-name",
    "aws": {
      "fsxFileSystemID": "fs-xxxxxxxxxx"
    },
    "managementLIF": null,
    "credentials": {
      "name": "arn:aws:secretsmanager:us-west-
2:xxxxxxx:secret:secret-name",
      "type": "awsarn"
    }
  }
}
```

有关创建后端的信息，请参见以下链接：

- ["使用 ONTAP NAS 驱动程序配置后端"](#)
- ["使用 ONTAP SAN 驱动程序配置后端"](#)

## 准备配置SMB卷

您可以使用配置SMB卷 `ontap-nas` 驱动程序。完成前 [ONTAP SAN和NAS驱动程序集成](#) 完成以下步骤。

### 开始之前

才能使用配置SMB卷 `ontap-nas` 驱动程序、则必须满足以下条件。

- 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 2019的Windows工作节点。Astra Trident仅支持将SMB卷挂载到Windows节点上运行的Pod。
- 至少一个包含Active Directory凭据的Astra Trident密钥。以生成密钥 `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. 创建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 vserver_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、或者允许Asta三端到功能创建SMB共享的名称。  对于Amazon FSx for ONTAP后端、此参数是必需的。	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 <b>ntfs</b> 或 <b>mixed</b> 用于 <b>SMB</b> 卷。	ntfs 或 mixed 对于SMB卷
unixPermissions	新卷的模式。对于SMB卷、必须留空。	""

## 适用于ONTAP 的FSX配置选项和示例

了解适用于ONTAP 的Amazon FSX的后端配置选项。本节提供了后端配置示例。

### 后端配置选项

有关后端配置选项，请参见下表：

参数	Description	示例
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  可以指定完全限定域名(FQDN)。  如果使用IPv6标志安装了Asta三元组、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]。	"10.0.0.1", "2001 : 1234 : abcd : : : fefe]"

参数	Description	示例
dataLIF	<p>协议 LIF 的 IP 地址。</p> <p><b>* ONTAP NAS驱动程序*：</b>建议指定dataLIF。如果未提供此参数、则Astra Trident会从SVM提取数据LIF。您可以指定用于NFS挂载操作的完全限定域名(FQDN)、从而可以创建循环DNS、以便在多个数据LIF之间实现负载平衡。可以在初始设置后更改。请参见。</p> <p><b>* ONTAP SAN驱动程序*：</b>不为iSCSI指定。Astra Trident使用ONTAP 选择性LUN映射来发现建立多路径会话所需的iSCSI LIF。如果明确定义了dataLIF、则会生成警告。</p> <p>如果使用IPv6标志安装了Asta三元组、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]。</p>	
autosExportPolicy	启用自动创建和更新导出策略[布尔值]。使用 autoExportPolicy 和 autoExportCIDRs 选项、Astra Trident可以自动管理导出策略。	false
autosExportCIDR	<p>用于筛选Kubbernetes节点IP的CIDR列表 autoExportPolicy 已启用。</p> <p>使用 autoExportPolicy 和 autoExportCIDRs 选项、Astra Trident可以自动管理导出策略。</p>	"["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	用于连接到集群或SVM的用户名。用于基于凭据的身份验证。例如、vsadmin。	
密码	用于连接到集群或SVM的密码。用于基于凭据的身份验证。	



参数	Description	示例
sVM	要使用的 Storage Virtual Machine	如果指定SVM管理LIF则派生。
s存储前缀	在 SVM 中配置新卷时使用的前缀。创建后无法修改。要更新此参数、您需要创建一个新的后端。	trident
limitAggregateUsage	*请勿为适用于NetApp ONTAP的Amazon FSX指定。*提供的fsxadmin和vsadmin请勿包含检索聚合使用情况所需的权限、并使用Astra Trident对其进行限制。	请勿使用。
limitVolumeSize	如果请求的卷大小超过此值、则配置失败。此外、还会限制它为qtree和LUN以及管理的卷的最大大小qtreesPerFlexvol 选项用于自定义每个FlexVol 的最大qtree数。	"（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。仅限SAN。	100
debugTraceFlags	故障排除时要使用的调试标志。例如、{"api": false、"method " : true} 不使用debugTraceFlags 除非您正在进行故障排除并需要详细的日志转储。	空
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、但如果在存储类中未指定挂载选项、则Astra 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Astra Trident不会在关联的永久性卷上设置任何挂载选项。	""
nasType	配置NFS或SMB卷创建。选项包括nfs、smb`或为空。*必须设置为`smb 对于SMB卷。*如果设置为空、则默认为NFS卷。	nfs
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、或者允许Astra三端到功能创建SMB共享的名称。  对于Amazon FSx for ONTAP后端、此参数是必需的。	smb-share

参数	Description	示例
useREST	用于使用 ONTAP REST API 的布尔参数。 * 技术预览 * useREST 作为一个*技术预览版提供、建议用于测试环境、而不是生产工作负载。设置为 true、Astra Trident将使用ONTAP REST API与后端进行通信。此功能需要使用ONTAP 9.11.1及更高版本。此外、使用的ONTAP 登录角色必须有权访问 ontap 应用程序。这一点可通过预定义来满足 vsadmin 和 cluster-admin 角色。	false
aws	您可以在AWS FSx for ONTAP的配置文件中指定以下内容： - fsxFilesystemID：指定AWS FSx文件系统的ID。 - apiRegion：AWS API区域名称。 - apikey：AWS API密钥。 - secretKey：AWS机密密钥。	"" "" ""
credentials	指定要存储在AWS机密管理器中的FSx SVM凭据。 - name：密钥的Amazon资源名称(ARN)、其中包含SVM的凭据。 - type：设置为 awsarn。 请参见 <a href="#">"创建AWS机密管理器密钥"</a> 有关详细信息 ...	

更新 dataLIF 初始配置后

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

```
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、则必须关闭所有对应Pod、然后将其恢复到、新数据LIF才能生效。

用于配置卷的后端配置选项

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

参数	Description	Default
spaceAllocation	LUN 的空间分配	true
s页面预留	空间预留模式； " 无 " （精简）或 " 卷 " （厚）	无

参数	Description	Default
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。选择每个存储池或后端的qosPolicy或adaptiveQosPolicy之一。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。	"
adaptiveQosPolicy	要为创建的卷分配的自适应 QoS 策略组。选择每个存储池或后端的qosPolicy或adaptiveQosPolicy之一。不受 ontap-nas-economy.	"
sSnapshot 预留	为快照预留的卷百分比为 "0"	条件 snapshotPolicy 为 none, else "
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Astra Trident中配置的任何卷都将启用NAE。有关详细信息、请参见： <a href="#">"Astra Trident如何与NVE和NAE配合使用"</a> 。	false
luksEncryption	启用LUKS加密。请参见 <a href="#">"使用Linux统一密钥设置(LUKS)"</a> 。仅限SAN。	""
分层策略	要使用的层策略 none	snapshot-only 适用于ONTAP 9.5 SVM-DR之前的配置
unixPermissions	新卷的模式。对于 <b>SMB</b> 卷保留为空。	""
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。

## 示例配置

## 配置SMB卷的存储类

使用 `nasType`, `node-stage-secret-name`, 和 `node-stage-secret-namespace`、您可以指定SMB卷并提供所需的Active Directory凭据。SMB卷支持使用 `ontap-nas` 仅限驱动程序。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: nas-smb-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
```

## 使用密钥管理器配置AWS FSx for ONTAP

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
    fsxFileSystemID: fs-xxxxxxxxxx
  managementLIF:
  credentials:
    name: "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-name"
    type: awsarn
```

## 在EKS集群上配置Asta Trident EKS加载项23.10版

Asta三端存储简化了Kubernetes中适用于NetApp ONTAP存储的Amazon FSx管理、使开发人员和管理员能够专注于应用程序部署。A作用 是通过AWS验证、可与Amazon EKS配合使用。通过EKS加载项、您可以始终确保Amazon EKS集群安全稳定、并减少安装、配置和更新加载项所需的工作量。

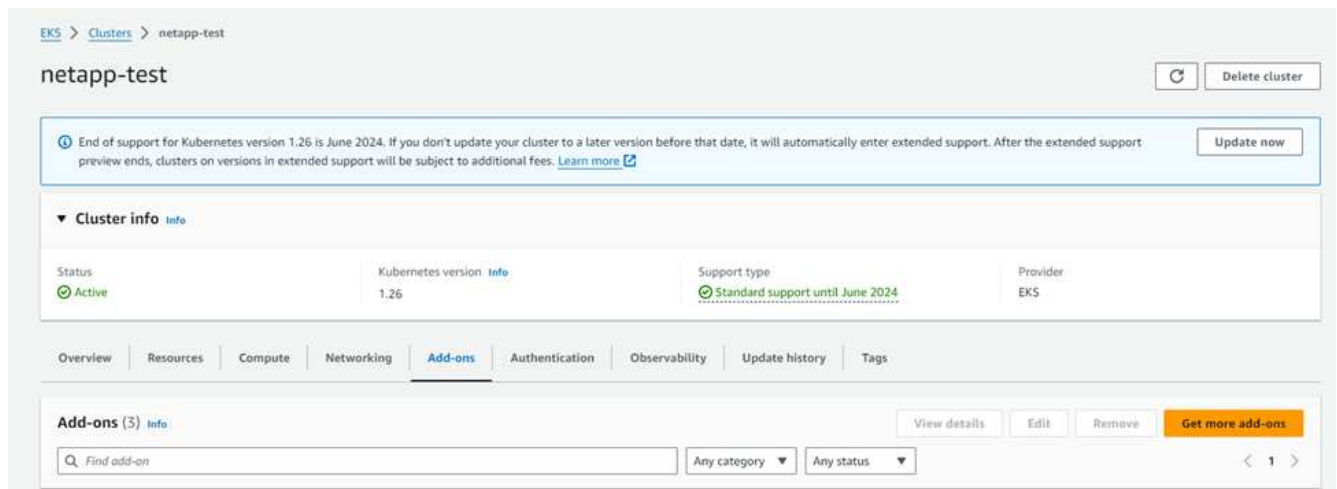
## 前提条件

在配置适用于AWS EKS的Asta TrIDeNT加载项之前、请确保满足以下条件：

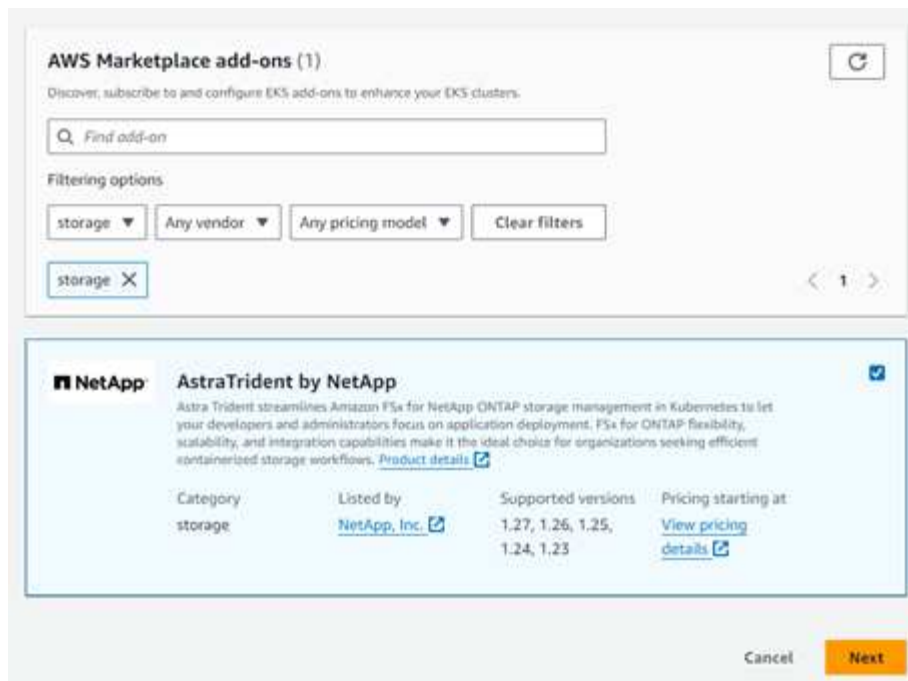
- 具有附加订阅的Amazon EKS集群帐户
- AWS对AWS Marketplace的权限：  
"aws-marketplace:ViewSubscriptions",  
"aws-marketplace:Subscribe",  
"aws-marketplace:Unsubscribe"
- AMI类型：Amazon Linux 2 (AL2\_x86\_64)或Amazon Linux 2 ARM (AL2\_ARM\_64)
- 节点类型：AMD或ARM
- 现有Amazon FSx for NetApp ONTAP文件系统

## 步骤

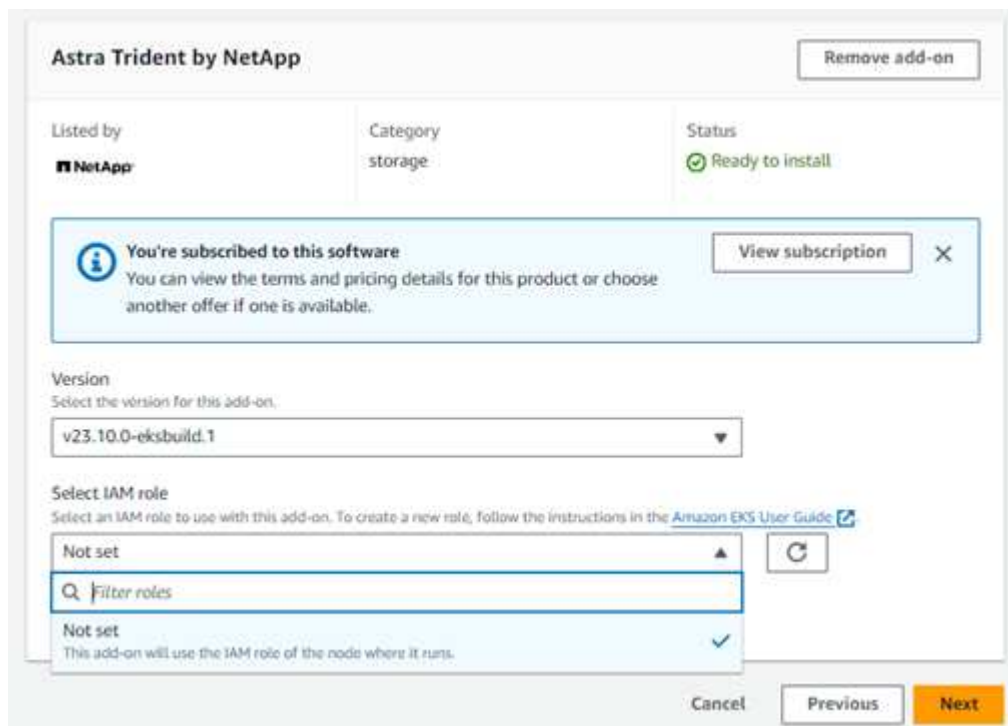
1. 在EKS Kubernetes集群上、导航到\*附加项\*选项卡。



2. 转到\*AWS Marketplace附加项\*并选择\_storage\_类别。



3. 找到\*AstraDent\* by AstraDent\*并选中NetApp插件的复选框。
4. 选择所需的附加软件版本。



5. 选择要从节点继承的IAM角色选项。
6. 根据需要配置任何可选设置，然后选择\*Next\*。

### Review and add

**Step 1: Select add-ons**
Edit

Selected add-ons

Find add-on

Add-on name	Type	Status
netapp_trident-operator	storage	Ready to install

**Step 2: Configure selected add-ons settings**
Edit

Selected add-ons version

Add-on name	Version	IAM role
netapp_trident-operator	v23.10.0-eksbuild.1	Inherit from node

Cancel
Previous
Create

- 选择 \* 创建 \*。
- 验证此加载项的状态是否为 `_Active_`。

Add-ons (1)				
Find add-on				
Any category Any status				
<div> <b>AstraTrident by NetApp</b> </div> <p>Astra Trident is a container storage management solution for Kubernetes that provides a secure and efficient way to manage storage for your applications. It is designed to be easy to install, configure, and manage, and it provides a wide range of features to help you get the most out of your storage. For more information, see the Astra Trident documentation.</p>				
Category	Status	Version	IAM role	Created by
storage	Active	v23.10.0-eksbuild.1	Inherited from node	NetApp, Inc.

使用命令行界面安装/卸载A作用 的三端EKS加载项

使用命令行界面安装Asta Trident EKS加载项：

以下示例命令用于安装Asta Trident EKS加载项：

```
eksctl create addon --cluster K8s-arm --name netapp_trident-operator --version v23.10.0-eksbuild.1
eksctl create addon --cluster K8s-arm --name netapp_trident-operator --version v23.10.0-eksbuild.1 (使用专用版本)
```

使用命令行界面卸载Asta Trident EKS加载项：

以下命令将卸载Asta三端EKS加载项：

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

## 使用 kubectl 创建后端

后端定义了 Astra Trident 与存储系统之间的关系。它告诉 Astra Trident 如何与该存储系统进行通信，以及 Astra Trident 如何从该存储系统配置卷。安装 Astra Trident 后，下一步是创建后端。使用 TridentBackendConfig Custom Resource Definition （CRD），您

可以直接通过 Kubernetes 界面创建和管理 Trident 后端。为此，您可以对 Kubernetes 分发版使用 `kubectl` 或等效的命令行界面工具。

## TridentBackendConfig

`TridentBackendConfig` (`tbc` , `tbconfig` , `tbackendconfig`) 是一个前端命名的 CRD , 可用于使用 `kubectl` 管理 Astra Trident 后端。现在, Kubernetes 和存储管理员可以直接通过 Kubernetes 命令行界面创建和管理后端, 而无需专用命令行实用程序 (`tridentctl`) 。

创建 `TridentBackendConfig` 对象时, 将发生以下情况:

- Astra Trident 会根据您提供的配置自动创建后端。此值在内部表示为 `TridentBackend` (`tbe` , `tridentbackend`) CR 。
- `TridentBackendConfig` 唯一绑定到由 Astra Trident 创建的 `TridentBackend` 。

每个 `TridentBackendConfig` 都与 `TridentBackend` 保持一对一映射。前者是为用户提供的用于设计和配置后端的接口; 后者是 Trident 表示实际后端对象的方式。



`TridentBackend` CRS 由 Astra Trident 自动创建。您 \* 不应 \* 修改它们。如果要更新后端, 请通过修改 `TridentBackendConfig` 对象来执行此操作。

有关 `TridentBackendConfig` CR 的格式, 请参见以下示例:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

您还可以查看中的示例 "[Trident 安装程序](#)" 所需存储平台 / 服务的示例配置目录。

。 `spec` 获取后端特定的配置参数。在此示例中、后端使用 `ontap-san` 存储驱动程序、并使用此处所示的配置参数。有关所需存储驱动程序的配置选项列表、请参阅 "[存储驱动程序的后端配置信息](#)"。

`spec` 部分还包括 `credentials` 和 `deletionPolicy` 字段, 这些字段在 `TridentBackendConfig` CR 中新增:

- `credentials`: 此参数为必填字段, 包含用于向存储系统 / 服务进行身份验证的凭据。此密码设置为用户创建的 Kubernetes Secret。凭据不能以纯文本形式传递, 因此会导致错误。



- `deletionPolicy`：此字段定义删除 `TridentBackendConfig` 时应发生的情况。它可以采用以下两种可能值之一：
  - `delete`：这将同时删除 `TridentBackendConfig` CR 和关联后端。这是默认值。
  - `retain`：删除 `TridentBackendConfig` CR 后，后端定义仍存在，可使用 `tridentctl` 进行管理。将删除策略设置为 `retain` 允许用户降级到早期版本（21.04 之前）并保留创建的后端。创建 `TridentBackendConfig` 后，可以更新此字段的值。



后端名称使用 `sPec.backendName` 设置。如果未指定，则后端的名称将设置为 `TridentBackendConfig` 对象的名称（`metadata.name`）。建议使用 `sPec.backendName` 显式设置后端名称。



使用 `tridentctl` 创建的后端没有关联的 `TridentBackendConfig` 对象。您可以通过创建 `TridentBackendConfig` CR，选择使用 `kubectl` 来管理此类后端。必须注意指定相同的配置参数（例如 `sPec.backendName`，`sPec.storagePrefix`，`sPec.storageDriverName` 等）。Astra Trident 会自动将新创建的 `TridentBackendConfig` 与已有的后端绑定。

## 步骤概述

要使用 `kubectl` 创建新后端，应执行以下操作：

1. 创建 **"Kubernetes 机密"**。此密钥包含 Astra Trident 与存储集群 / 服务通信所需的凭据。
2. 创建 `TridentBackendConfig` 对象。其中包含有关存储集群 / 服务的详细信息，并引用了上一步中创建的密钥。

创建后端后，您可以使用 `kubectl get tbc <tbc-name> -n <trident 命名空间>` 来观察其状态，并收集其他详细信息。

## 第 1 步：创建 Kubernetes 机密

创建一个机密，其中包含后端的访问凭据。这是每个存储服务 / 平台所特有的。以下是一个示例：

```
kubectl -n trident create -f backend-tbc-ontap-san-secret.yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-san-secret
type: Opaque
stringData:
  username: cluster-admin
  password: t@Ax@7q(>
```

下表汇总了每个存储平台的机密中必须包含的字段：

存储平台机密字段问题描述	机密	字段问题描述
Azure NetApp Files	clientId	应用程序注册中的客户端 ID
适用于 GCP 的 Cloud Volumes Service	private_key_id	专用密钥的 ID。具有 CVS 管理员角色的 GCP 服务帐户的 API 密钥的一部分
适用于 GCP 的 Cloud Volumes Service	private_key	专用密钥。具有 CVS 管理员角色的 GCP 服务帐户的 API 密钥的一部分
Element （ NetApp HCI/SolidFire ）	端点	使用租户凭据的 SolidFire 集群的 MVIP
ONTAP	username	用于连接到集群 /SVM 的用户名。用于基于凭据的身份验证
ONTAP	password	连接到集群 /SVM 的密码。用于基于凭据的身份验证
ONTAP	客户端权限密钥	客户端专用密钥的 Base64 编码值。用于基于证书的身份验证
ONTAP	用户名	入站用户名。如果 useCHAP=true，则为必需项。适用于 ontap-san 和 ontap-san-economy。
ONTAP	chapInitiatorSecret	CHAP 启动程序密钥。如果 useCHAP=true，则为必需项。适用于 ontap-san 和 ontap-san-economy。
ONTAP	chapTargetUsername	目标用户名。如果 useCHAP=true，则为必需项。适用于 ontap-san 和 ontap-san-economy。
ONTAP	chapTargetInitiatorSecret	CHAP 目标启动程序密钥。如果 useCHAP=true，则为必需项。适用于 ontap-san 和 ontap-san-economy。

在下一步中创建的 TridentBackendConfig 对象的 spec.credentials 字段将引用此步骤中创建的机密。

## 第2步：创建 TridentBackendConfig CR

现在，您可以创建 TridentBackendConfig CR 了。在此示例中，使用 TridentBackendConfig 对象创建使用`ontap-san`驱动程序的后端，如下所示：

```
kubectl -n trident create -f backend-tbc-ontap-san.yaml
```

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

### 第3步：验证的状态 TridentBackendConfig CR

现在，您已创建 TridentBackendConfig CR，可以验证状态。请参见以下示例：

```
kubectl -n trident get tbc backend-tbc-ontap-san
```

NAME	BACKEND NAME	BACKEND UUID
PHASE STATUS		
backend-tbc-ontap-san	ontap-san-backend	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
Bound	Success	

已成功创建后端并将其绑定到 TridentBackendConfig CR。

阶段可以采用以下值之一：

- Bound：TridentBackendConfig CR与后端关联、后端包含 configRef 设置为 TridentBackendConfig CR的uid。
- Unbound：使用 `` 表示。TridentBackendConfig 对象未绑定到后端。默认情况下，所有新创建的 TridentBackendConfig CRS 均处于此阶段。此阶段发生更改后，它将无法再次还原为 "Unbound（已取消绑定）"。
- Deleting：TridentBackendConfig CR deletionPolicy 已设置为delete。当 TridentBackendConfig CR将被删除、它将过渡到Deleting状态。
  - 如果后端不存在永久性卷请求（PVC），则删除 TridentBackendConfig 将导致 Astra Trident 删除后端以及 TridentBackendConfig CR。
  - 如果后端存在一个或多个 PVC，则会进入删除状态。TridentBackendConfig CR 随后也会进入删除阶段。只有在删除所有 PVC 后，才会删除后端和 TridentBackendConfig。
- Lost：与 TridentBackendConfig CR 关联的后端被意外或故意删除，TridentBackendConfig CR

仍引用已删除的后端。无论 deletionPolicy 值如何，仍可删除 TridentBackendConfig CR。

- Unknown: Astra Trident无法确定与关联的后端的状态或是否存在 TridentBackendConfig CR.例如、如果API服务器未响应或 tridentbackends.trident.netapp.io 缺少CRD。这可能需要干预。

在此阶段，已成功创建后端！此外，还可以处理多个操作，例如 ["后端更新和后端删除"](#)。

## （可选）第 4 步：获取更多详细信息

您可以运行以下命令来获取有关后端的详细信息：

```
kubectl -n trident get tbc backend-tbc-ontap-san -o wide
```

NAME	BACKEND NAME	BACKEND UUID	
PHASE	STATUS	STORAGE DRIVER	DELETION POLICY
backend-tbc-ontap-san	ontap-san-backend	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8	Bound Success ontap-san delete

此外，您还可以获取 YAML/JSON 转储 TridentBackendConfig。

```
kubectl -n trident get tbc backend-tbc-ontap-san -o yaml
```

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  creationTimestamp: "2021-04-21T20:45:11Z"
  finalizers:
    - trident.netapp.io
  generation: 1
  name: backend-tbc-ontap-san
  namespace: trident
  resourceVersion: "947143"
  uid: 35b9d777-109f-43d5-8077-c74a4559d09c
spec:
  backendName: ontap-san-backend
  credentials:
    name: backend-tbc-ontap-san-secret
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  storageDriverName: ontap-san
  svm: trident_svm
  version: 1
status:
  backendInfo:
    backendName: ontap-san-backend
    backendUUID: 8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
  deletionPolicy: delete
  lastOperationStatus: Success
  message: Backend 'ontap-san-backend' created
  phase: Bound

```

backendInfo 包含为响应 TridentBackendConfig CR 而创建的后端的 backendName 和 backendUUID。lastOperationStatus 字段表示 TridentBackendConfig CR 的上次操作状态，该操作可以是用户触发的（例如，用户在 spec 中更改了某个内容），也可以是由 Astra Trident 触发的（例如，在 Astra Trident 重新启动期间）。可以是成功，也可以是失败。phase 表示 TridentBackendConfig CR 与后端之间关系的状态。在上面的示例中，phase 的值为 bound，这意味着 TridentBackendConfig CR 与后端关联。

您可以运行 `kubectl -n trident describe tbc <tbc-cr-name>` 命令来获取事件日志的详细信息。



您不能使用 `tridentctl` 更新或删除包含关联的 TridentBackendConfig 对象的后端。要了解在 `tridentctl` 和 TridentBackendConfig 之间切换所涉及的步骤，[“请参见此处”](#)。

## 管理后端

### 使用 `kubectl` 执行后端管理

了解如何使用 `kubectl` 执行后端管理操作。

## 删除后端

通过删除 `TridentBackendConfig`，您可以指示 Astra Trident 删除 / 保留后端（基于 `deletionPolicy`）。要删除后端，请确保将 `deletionPolicy` 设置为 `delete`。要仅删除 `TridentBackendConfig`，请确保将 `deletionPolicy` 设置为 `Retain`。这样可以确保后端仍然存在，并可使用 `tridentctl` 进行管理。

运行以下命令：

```
kubectl delete tbc <tbc-name> -n trident
```

Astra Trident 不会删除 `TridentBackendConfig` 使用的 Kubernetes 机密。Kubernetes 用户负责清理密钥。删除机密时必须小心。只有在后端未使用机密时，才应将其删除。

## 查看现有后端

运行以下命令：

```
kubectl get tbc -n trident
```

您也可以运行 `tridentctl get backend -n trident` 或 `tridentctl get backend -o YAML -n trident` 来获取存在的所有后端的列表。此列表还将包括使用 `tridentctl` 创建的后端。

## 更新后端

更新后端可能有多种原因：

- 存储系统的凭据已更改。要更新凭据，必须更新 `TridentBackendConfig` 对象中使用的 Kubernetes Secret。Astra Trident 将使用提供的最新凭据自动更新后端。运行以下命令以更新 Kubernetes Secret：

```
kubectl apply -f <updated-secret-file.yaml> -n trident
```

- 需要更新参数（例如所使用的 ONTAP SVM 的名称）。
  - 您可以更新 `TridentBackendConfig` 使用以下命令直接通过 KubeNet 访问对象：

```
kubectl apply -f <updated-backend-file.yaml>
```

- 或者、您也可以对现有进行更改 `TridentBackendConfig` 使用以下命令执行 CR：

```
kubectl edit tbc <tbc-name> -n trident
```



- 如果后端更新失败，则后端仍会保持在其上次已知配置中。您可以通过运行 `kubectl get tbc <tbc-name> -o yaml -n trident` 或 `kubectl describe tbc <tbc-name> -n trident` 来查看日志以确定发生原因。
- 确定并更正配置文件中的问题后，您可以重新运行 `update` 命令。

## 使用 **tridentctl** 执行后端管理

了解如何使用 `tridentctl` 执行后端管理操作。

### 创建后端

创建后 "[后端配置文件](#)"下，运行以下命令：

```
tridentctl create backend -f <backend-file> -n trident
```

如果后端创建失败，则后端配置出现问题。您可以运行以下命令来查看日志以确定发生原因：

```
tridentctl logs -n trident
```

确定并更正配置文件中的问题后，您只需再次运行 `create` 命令即可。

### 删除后端

要从 Astra Trident 中删除后端，请执行以下操作：

1. 检索后端名称：

```
tridentctl get backend -n trident
```

2. 删除后端：

```
tridentctl delete backend <backend-name> -n trident
```



如果 Astra Trident 从此后端配置了仍存在的卷和快照，则删除后端将阻止其配置新卷。后端将继续处于 "删除" 状态，而 Trident 将继续管理这些卷和快照，直到将其删除为止。

### 查看现有后端

要查看 Trident 了解的后端，请执行以下操作：

- 要获取摘要，请运行以下命令：

```
tridentctl get backend -n trident
```

- 要获取所有详细信息，请运行以下命令：

```
tridentctl get backend -o json -n trident
```

## 更新后端

创建新的后端配置文件后，运行以下命令：

```
tridentctl update backend <backend-name> -f <backend-file> -n trident
```

如果后端更新失败，则后端配置出现问题或您尝试的更新无效。您可以运行以下命令来查看日志以确定发生原因：

```
tridentctl logs -n trident
```

确定并更正配置文件中的问题后，您只需再次运行 `update` 命令即可。

## 确定使用后端的存储类

以下是您可以使用问题解答与 JSON 回答的问题的示例，这些问题会 `tridentctl` 后端对象的输出。此操作将使用 `jq` 实用程序，您需要安装该实用程序。

```
tridentctl get backend -o json | jq '[.items[] | {backend: .name, storageClasses: [.storage[].storageClasses]|unique}]'
```

这也适用于使用 `TridentBackendConfig` 创建的后端。

## 在后端管理选项之间移动

了解如何在 Astra Trident 中管理后端。

### 用于管理后端的选项

随附 `TridentBackendConfig` 现在，管理员可以通过两种独特的方式管理后端。这会提出以下问题：

- 使用 `tridentctl` 创建的后端是否可以使用 `TridentBackendConfig` 进行管理？
- 使用 `TridentBackendConfig` 创建的后端是否可以使用 `tridentctl` 进行管理？



## 管理 tridentctl 后端使用 TridentBackendConfig

本节介绍通过创建 TridentBackendConfig 对象直接通过 Kubernetes 界面管理使用 tridentctl 创建的后端所需的步骤。

这适用于以下情形：

- 已有后端、但没有 TridentBackendConfig 因为它们是使用创建的 tridentctl。
- 使用 tridentctl 创建的新后端，而存在其他 TridentBackendConfig 对象。

在这两种情况下，后端仍会存在，其中 Astra Trident 会计划卷并对其进行操作。管理员可以选择以下两种方式之一：

- 继续使用 tridentctl 管理使用它创建的后端。
- 使用 tridentctl 创建的后端绑定到新的 TridentBackendConfig 对象。这样做意味着将使用 kubectl 而不是 tridentctl 来管理后端。

要使用 kubectl 管理已有后端，您需要创建一个绑定到现有后端的 TridentBackendConfig。下面简要介绍了它的工作原理：

1. 创建 Kubernetes 机密。此密钥包含 Astra Trident 与存储集群 / 服务通信所需的凭据。
2. 创建 TridentBackendConfig 对象。其中包含有关存储集群 / 服务的详细信息，并引用了上一步中创建的密钥。必须注意指定相同的配置参数（例如 spec.backendName，spec.storagePrefix，spec.storageDriverName 等）。spec.backendName 必须设置为现有后端的名称。

### 第 0 步：确定后端

以创建 TridentBackendConfig 如果绑定到现有后端、则需要获取后端配置。在此示例中，假设已使用以下 JSON 定义创建了后端：

```
tridentctl get backend ontap-nas-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE  | VOLUMES |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-nas-backend     | ontap-nas      | 52f2eb10-e4c6-4160-99fc-96b3be5ab5d7 |
| online |      25 |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

cat ontap-nas-backend.json

{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.10.10.1",
```

```

"dataLIF": "10.10.10.2",
"backendName": "ontap-nas-backend",
"svm": "trident_svm",
"username": "cluster-admin",
"password": "admin-password",

"defaults": {
  "spaceReserve": "none",
  "encryption": "false"
},
"labels":{"store":"nas_store"},
"region": "us_east_1",
"storage": [
  {
    "labels":{"app":"msoffice", "cost":"100"},
    "zone":"us_east_1a",
    "defaults": {
      "spaceReserve": "volume",
      "encryption": "true",
      "unixPermissions": "0755"
    }
  },
  {
    "labels":{"app":"mysqldb", "cost":"25"},
    "zone":"us_east_1d",
    "defaults": {
      "spaceReserve": "volume",
      "encryption": "false",
      "unixPermissions": "0775"
    }
  }
]
}

```

#### 第 1 步：创建 **Kubernetes** 机密

创建一个包含后端凭据的机密，如以下示例所示：

```
cat tbc-ontap-nas-backend-secret.yaml

apiVersion: v1
kind: Secret
metadata:
  name: ontap-nas-backend-secret
type: Opaque
stringData:
  username: cluster-admin
  password: admin-password

kubectl create -f tbc-ontap-nas-backend-secret.yaml -n trident
secret/backend-tbc-ontap-san-secret created
```

## 第2步：创建 TridentBackendConfig CR

下一步是创建一个 TridentBackendConfig CR，该 CR 将自动绑定到已有的 ontap-nas-backend（如本示例所示）。确保满足以下要求：

- 在 `sPec.backendName` 中定义了相同的后端名称。
- 配置参数与原始后端相同。
- 虚拟池(如果存在)必须与原始后端的顺序相同。
- 凭据通过 Kubernetes Secret 提供，而不是以纯文本形式提供。

在这种情况下，TridentBackendConfig 将如下所示：

```

cat backend-tbc-ontap-nas.yaml
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: tbc-ontap-nas-backend
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.10.10.1
  dataLIF: 10.10.10.2
  backendName: ontap-nas-backend
  svm: trident_svm
  credentials:
    name: mysecret
  defaults:
    spaceReserve: none
    encryption: 'false'
  labels:
    store: nas_store
  region: us_east_1
  storage:
  - labels:
    app: msoffice
    cost: '100'
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: 'true'
      unixPermissions: '0755'
  - labels:
    app: mysqldb
    cost: '25'
    zone: us_east_1d
    defaults:
      spaceReserve: volume
      encryption: 'false'
      unixPermissions: '0775'

kubectl create -f backend-tbc-ontap-nas.yaml -n trident
tridentbackendconfig.trident.netapp.io/tbc-ontap-nas-backend created

```

### 第3步：验证的状态 TridentBackendConfig **CR**

创建 TridentBackendConfig 后，其阶段必须为 bound。它还应反映与现有后端相同的后端名称和 UUID。

```
kubectl get tbc tbc-ontap-nas-backend -n trident
```

NAME	BACKEND NAME	BACKEND UUID
tbc-ontap-nas-backend	ontap-nas-backend	52f2eb10-e4c6-4160-99fc-96b3be5ab5d7
Bound	Success	

#confirm that no new backends were created (i.e., TridentBackendConfig did not end up creating a new backend)

```
tridentctl get backend -n trident
```

NAME	STORAGE DRIVER	UUID
ontap-nas-backend	ontap-nas	52f2eb10-e4c6-4160-99fc-96b3be5ab5d7
online	25	

现在，可以使用 tbc-ontap-nas-backend TridentBackendConfig 对象对后端进行全面管理。

管理 TridentBackendConfig 后端使用 tridentctl

tridentctl 可用于列出使用 TridentBackendConfig 创建的后端。此外，管理员还可以选择通过 tridentctl 来完全管理此类后端，方法是删除 TridentBackendConfig 并确保将 spec.deletionPolicy 设置为 retain。

第 0 步：确定后端

例如，假设使用 TridentBackendConfig 创建了以下后端：

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
```

NAME	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-san	ontap-san-backend	81abcb27-ea63-49bb-b606-0a5315ac5f82

```
tridentctl get backend ontap-san-backend -n trident
```

NAME	STORAGE DRIVER	UUID
ontap-san-backend	ontap-san	81abcb27-ea63-49bb-b606-0a5315ac5f82

从输出中可以看出这一点 TridentBackendConfig 已成功创建并绑定到后端[观察后端的UUID]。

第1步：确认 deletionPolicy 设置为 retain

让我们来看看 deletionPolicy 的价值。需要将此值设置为 retain。这样可以确保删除 TridentBackendConfig CR 时，后端定义仍存在，并可使用 tridentctl 进行管理。

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
```

NAME	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-san	ontap-san-backend	81abcb27-ea63-49bb-b606-0a5315ac5f82

```
# Patch value of deletionPolicy to retain
kubectl patch tbc backend-tbc-ontap-san --type=merge -p
'{"spec":{"deletionPolicy":"retain"}}' -n trident
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-san patched

#Confirm the value of deletionPolicy
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
```

NAME	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-san	ontap-san-backend	81abcb27-ea63-49bb-b606-0a5315ac5f82



请勿继续执行下一步，除非将 deletionPolicy 设置为 retain。

## 第2步：删除 TridentBackendConfig CR

最后一步是删除 TridentBackendConfig CR。确认 deletionPolicy 设置为 retain 后，您可以继续执行删除：

```
kubectl delete tbc backend-tbc-ontap-san -n trident
tridentbackendconfig.trident.netapp.io "backend-tbc-ontap-san" deleted

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |                      UUID                      |
| STATE  | VOLUMES |                      |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-0a5315ac5f82 |
| online |      33 |                      |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

删除 TridentBackendConfig 对象后，Astra Trident 只需删除该对象，而无需实际删除后端本身。

## 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。