참조하십시오
Trident

NetApp
February 02, 2026

목차

참조하십시오

Trident 포트

Trident가 통신에 사용하는 포트에 대해 자세히 알아보십시오.

Trident 포트

Trident Kubernetes 내부 통신에 다음 포트를 사용합니다.

포트	목적
8443	백채널 HTTPS
8001입니다	Prometheus 메트릭 엔드포인트
8000	Trident REST 서버
17546	Trident 디포드에 사용되는 활성/준비 프로브 포트

을 사용하여 설치하는 동안 활성/준비 프로브 포트를 변경할 수 있습니다 `--probe-port` 깃발. 이 포트가 작업자 노드의 다른 프로세스에서 사용되지 않도록 하는 것이 중요합니다.

Trident REST API

Trident REST API와 상호 작용하는 가장 쉬운 방법이지만 "tridentctl 명령 및 옵션"원하는 경우 REST 끝점을 직접 사용할 수 있습니다.

REST API 사용 시기

REST API는 Kubernetes가 아닌 다른 구축 환경에서 Trident를 독립 실행형 바이너리로 사용하는 고급 설치에 유용합니다.

보안을 강화하기 위해 Trident는 `REST API` Pod 내부에서 실행될 때 기본적으로 localhost로 제한됩니다. 이 동작을 변경하려면 해당 POD 구성에서 Trident의 `-address` 인수를 설정해야 합니다.

REST API 사용

이러한 API가 호출되는 방법의 예를 보려면 DEBUG(`-d`) 플래그를 전달합니다. 자세한 내용은 을 "tridentctl을 사용하여 Trident를 관리합니다"참조하십시오.

API는 다음과 같이 작동합니다.

가져오기

`GET <trident-address>/trident/v1/<object-type>`

해당 형식의 모든 개체를 나열합니다.

GET <trident-address>/trident/v1/<object-type>/<object-name>

명명된 개체의 세부 정보를 가져옵니다.

게시

POST <trident-address>/trident/v1/<object-type>

지정된 형식의 개체를 만듭니다.

- 생성할 개체의 JSON 구성이 필요합니다. 각 개체 유형의 사양은 을 "tridentctl을 사용하여 Trident를 관리합니다"참조하십시오.
- 개체가 이미 있는 경우 동작이 달라집니다. backends는 기존 개체를 업데이트하지만 다른 모든 개체 형식은 작업에 실패합니다.

삭제

DELETE <trident-address>/trident/v1/<object-type>/<object-name>

명명된 리소스를 삭제합니다.

백엔드 또는 스토리지 클래스와 연결된 볼륨은 계속 존재하므로 별도로 삭제해야 합니다. 자세한 내용은 을 "tridentctl을 사용하여 Trident를 관리합니다"참조하십시오.

명령줄 옵션

Trident는 Trident 오케스트레이터를 위한 몇 가지 명령줄 옵션을 제공합니다. 이러한 옵션을 사용하여 배포를 수정할 수 있습니다.

로깅

-debug

디버깅 출력을 활성화합니다.

-loglevel <level>

로깅 수준(debug, info, warn, error, fatal)을 설정합니다. 기본적으로 info(정보) 가 사용됩니다.

쿠버네티스

-k8s_pod

이 옵션 또는 을 사용합니다 `-k8s_api_server` Kubernetes 지원을 사용하도록 설정하십시오. 이 설정을 사용하면 Trident에서 포함된 POD의 Kubernetes 서비스 계정 자격 증명을 사용하여 API 서버에 연락합니다. Trident가 서비스 계정이 활성화된 Kubernetes 클러스터에서 POD로 실행되는 경우에만 작동합니다.

-k8s_api_server <insecure-address:insecure-port>

Kubernetes 지원을 활성화하려면 이 옵션 또는 `-k8s_pod` 을 사용합니다. Trident가 지정된 경우 제공된 비보안 주소 및 포트를 사용하여 Kubernetes API 서버에 연결합니다. 따라서 Trident는 Pod 외부에 배포할 수 있지만 API 서버에 대한 안전하지 않은 연결만 지원합니다. 안전하게 연결하려면 옵션을 사용하여 Trident를 Pod에 `-k8s_pod` 배포합니다.

Docker 를 참조하십시오

-volume_driver <name>

Docker 플러그인을 등록할 때 사용되는 드라이버 이름입니다. 기본값은 입니다 `netapp`.

-driver_port <port-number>

UNIX 도메인 소켓이 아닌 이 포트에서 수신 대기합니다.

-config <file>

필수 요소로서 백엔드 구성 파일에 대한 이 경로를 지정해야 합니다.

휴식

-address <ip-or-host>

Trident의 REST 서버가 수신해야 하는 주소를 지정합니다. 기본값은 localhost입니다. localhost에서 듣거나 Kubernetes Pod에서 실행 중인 경우, REST 인터페이스는 Pod 외부에서 직접 액세스할 수 없습니다. 사용 `-address ""` REST 인터페이스를 POD IP 주소에서 액세스할 수 있도록 합니다.

Trident REST 인터페이스는 127.0.0.1(IPv4의 경우) 또는 [::1](IPv6의 경우)에서만 수신 및 서비스하도록 구성할 수 있습니다.

-port <port-number>

Trident의 REST 서버가 수신해야 하는 포트를 지정합니다. 기본값은 8000입니다.

-rest

REST 인터페이스를 활성화합니다. 기본값은 true 입니다.

Kubernetes 및 Trident 오브젝트

REST API를 사용하여 리소스 객체를 읽고 쓰면서 Kubernetes 및 Trident와 상호 작용할 수 있습니다. Kubernetes 및 Trident, Trident 및 스토리지와 Kubernetes 및 스토리지 간의 관계를 결정하는 몇 가지 리소스 개체가 있습니다. 이러한 오브젝트 중 일부는 Kubernetes를 통해 관리되며 나머지는 Trident를 통해 관리됩니다.

개체가 서로 어떻게 상호 작용합니까?

오브젝트, 목표 및 상호 작용 방식을 이해하는 가장 쉬운 방법은 Kubernetes 사용자의 스토리지에 대한 단일 요청을 따르는 것입니다.

1. 사용자가 이전에 관리자가 구성한 Kubernetes의 torageClass에서 특정 크기의 새 PersistentVolume을 요청하는 PersistentVolumeClaim을 만듭니다.
2. Kubernetes의 torageClass는 Trident를 프로비저닝자로 식별하고 Trident에 요청된 클래스에 대한 볼륨 프로비저닝 방법을 알려주는 매개 변수를 포함합니다.
3. Trident는 클래스에 대한 볼륨을 프로비저닝하는 데 사용할 수 있는 일치하는 'backends'와 'toragePools'를 식별하는 이름과 동일한 이름의 자체 'torageClass'를 찾습니다.
4. Trident는 일치하는 백엔드에 스토리지를 프로비저닝하고 Kubernetes의 "PersistentVolume"과

"PersistentVolume"과 실제 스토리지 간의 관계를 유지하는 Trident의 볼륨을 찾고, 마운트하고, 처리하는 방법을 Kubernetes의 "PersistentVolume"과 두 개의 객체를 만듭니다.

5. Kubernetes는 PersistentVolumeClaim을 새로운 PersistentVolume에 바인딩합니다. PersistentVolumeClaim이 실행되는 모든 호스트에서 PersistentVolume이 마운트되는 "PersistentVolumeClaim"이 포함된 POD
6. 사용자가 Trident를 가리키는 VolumeSnapshotClass를 사용하여 기존 PVC의 VolumeSnapshot을 생성합니다.
7. Trident는 PVC와 연결된 볼륨을 식별하고 백엔드에 볼륨의 스냅샷을 생성합니다. 또한 스냅샷을 식별하는 방법을 Kubernetes에 지시하는 'VolumeSnapshotContent'도 생성합니다.
8. 사용자는 'VolumeSnapshot'을 소스로 사용하여 'PersistentVolumeClaim'을 생성할 수 있습니다.
9. Trident는 필요한 스냅샷을 식별하고 "PersistentVolume"과 "Volume"을 생성하는 것과 동일한 단계를 수행합니다.

Kubernetes 객체에 대한 자세한 내용은 를 읽는 것이 좋습니다 "영구 볼륨" 섹션을 참조하십시오.

쿠버네티스 `PersistentVolumeClaim` 오브젝트

Kubernetes "PersistentVolumeClaim" 개체는 Kubernetes 클러스터 사용자가 만든 스토리지 요청입니다.

Trident는 표준 사양 외에도 사용자가 백엔드 구성에서 설정한 기본값을 무효화하려는 경우 다음 볼륨별 주석을 지정할 수 있도록 합니다.

주석	볼륨 옵션	지원되는 드라이버
trident.netapp.io/fileSystem	파일 시스템	ONTAP-SAN, solidfire-SAN, ONTAP-SAN - 경제성
trident.netapp.io/cloneFromPVC	CloneSourceVolume	ontap-nas, ontap-san, solidfire-san, azure-netapp-files, ontap-san-economy
trident.netapp.io/splitOnClone	SplitOnClone 을 참조하십시오	ONTAP-NAS, ONTAP-SAN
trident.netapp.io/protocol	프로토콜	모두
trident.netapp.io/exportPolicy	내보내기 정책	ONTAP-NAS, ONTAP-NAS-이코노미, ONTAP-NAS-Flexgroup
trident.netapp.io/snapshotPolicy	스냅샷 정책	ONTAP-NAS, ONTAP-NAS-이코노미, ONTAP-NAS-Flexgroup, ONTAP-SAN
trident.netapp.io/snapshotReserve	snapshotReserve	온탑나스, 온탑나스플렉스그룹, 온탑산
trident.netapp.io/snapshotDirectory	스냅샷 디렉토리	ONTAP-NAS, ONTAP-NAS-이코노미, ONTAP-NAS-Flexgroup
trident.netapp.io/unixPermissions	unixPermissions	ONTAP-NAS, ONTAP-NAS-이코노미, ONTAP-NAS-Flexgroup
trident.netapp.io/blockSize	블록 크기	solidfire-SAN
트라이던트.넷앱.io/스킵리커버리큐	skipRecoveryQueue	온탑-나스, 온탑-나스-이코노미, 온탑-나스-플렉스그룹, 온탑-샌, 온탑-샌-이코노미

생성된 PV에 'Delete' Reclaim 정책이 있는 경우, Trident는 PV가 해제될 때(즉, 사용자가 PVC를 삭제할 때) PV와 보조 볼륨을 모두 삭제합니다. 삭제 작업이 실패할 경우 Trident는 PV를 해당 상태로 표시하고 성공할 때까지 또는 PV를

수동으로 삭제할 때까지 주기적으로 작업을 다시 시도합니다. PV에서 'Retain' 정책을 사용할 경우 Trident는 이를 무시하고 관리자가 Kubernetes 및 백엔드에서 이를 정리하여 제거하기 전에 볼륨을 백업 또는 검사할 수 있다고 가정합니다. PV를 삭제해도 Trident에서 백업 볼륨을 삭제하지 않습니다. REST API('tridentctl')를 사용하여 제거해야 합니다.

Trident는 CSI 사양을 사용하여 볼륨 스냅샷 생성을 지원합니다. 볼륨 스냅샷을 생성하고 이를 데이터 소스로 사용하여 기존 PVC를 복제할 수 있습니다. 이렇게 하면 PVS의 시점 복제본을 스냅샷 형태로 Kubernetes에 표시할 수 있습니다. 그런 다음 스냅샷을 사용하여 새 PVS를 생성할 수 있습니다. 이 기능이 어떻게 동작하는지 알아보려면 "주문형 볼륨 스냅샷"를 살펴보십시오.

Trident는 도 제공합니다 `cloneFromPVC` 및 `splitOnClone` 클론 생성을 위한 주석. CSI 구현을 사용하지 않고도 이러한 주석을 사용하여 PVC를 복제할 수 있습니다.

예를 들어 이미 mysql이라는 PVC가 있는 사용자는 trident.netapp.io/cloneFromPVC: mysql 같은 주석을 사용해 mysqlclone이라는 새로운 PVC를 만들 수 있습니다. 이 주석을 설정하면 Trident가 볼륨을 처음부터 프로비저닝하는 대신 MySQL PVC에 해당하는 볼륨을 클론합니다.

다음 사항을 고려하십시오.

- NetApp은 유휴 볼륨을 클론 복제할 것을 권장합니다.
- PVC와 그 클론은 동일한 Kubernetes 네임스페이스에서 동일한 스토리지 클래스를 가져야 합니다.
- ONTAP-NAS와 ONTAP-SAN 드라이버를 함께 사용하면 trident.netapp.io/splitOnClone` 과 함께 PVC 주석 trident.netapp.io/cloneFromPVC` 을 설정하는 것이 바람직할 수 있습니다. Trident는 trident.netapp.io/splitOnClone` 를 true로 설정하면 상위 볼륨에서 복제된 볼륨을 분할하여 복제된 볼륨의 수명 주기를 부모 볼륨에서 완전히 분리하여 스토리지 효율성을 잃게 됩니다. trident.netapp.io/splitOnClone` 를 설정하지 않거나 "false"로 설정하지 않으면 상위 볼륨과 클론 볼륨 간의 종속성을 생성하여 클론이 먼저 삭제되지 않으면 상위 볼륨을 삭제할 수 없게 되어 백엔드에서 공간 소비가 줄어듭니다. 클론을 분할하는 것이 올바른 시나리오는 빈 데이터베이스 볼륨을 복제하여 볼륨과 해당 클론이 크게 달라질 것으로 예상되며 ONTAP에서 제공하는 스토리지 효율성의 이점을 얻지 못하는 경우입니다.

를 클릭합니다 `sample-input` 디렉토리에는 Trident와 함께 사용할 PVC 정의의 예가 포함되어 있습니다. 을 참조하십시오 Trident 볼륨과 관련된 매개 변수 및 설정에 대한 자세한 설명을 확인하십시오.

쿠버네티스 `PersistentVolume` 오브젝트

Kubernetes "PersistentVolume" 개체는 Kubernetes 클러스터에서 사용할 수 있는 스토리지 부분을 나타냅니다. 사용 포드와 독립적인 라이프 사이클이 있습니다.

Trident는 "PersistentVolume" 개체를 만들고 프로비저닝하는 볼륨을 기준으로 Kubernetes 클러스터에 자동으로 등록합니다. 스스로 관리할 수 없습니다.

Trident 기반의 'torageClass'를 참조하는 PVC를 생성하면 Trident는 해당 스토리지 클래스를 사용하여 새 볼륨을 프로비저닝하고 해당 볼륨에 대한 새 PV를 등록합니다. 프로비저닝 볼륨과 해당 PV를 구성할 때 Trident는 다음 규칙을 따릅니다.

- Trident는 Kubernetes의 PV 이름과 스토리지 프로비저닝에 사용되는 내부 이름을 생성합니다. 두 경우 모두 이름은 해당 범위에서 고유합니다.
- 볼륨의 크기는 플랫폼에 따라 가장 가까운 할당 가능한 수량으로 반올림될 수 있지만 PVC에서 요청된 크기와 최대한 가깝게 일치합니다.

쿠버네티스 `StorageClass` 오브젝트

Kubernetes의 torageClass 객체는 속성 세트를 사용하여 스토리지를 프로비저닝하기 위해 PersistentVolumeClaims의 이름으로 지정됩니다. 스토리지 클래스 자체는 사용할 구축 소유자를 식별하고 프로비저닝이 이해할 수 있는 조건으로 해당 자산 세트를 정의합니다.

관리자가 만들고 관리해야 하는 두 가지 기본 개체 중 하나입니다. 다른 하나는 Trident 백엔드 객체입니다.

Trident를 사용하는 Kubernetes의 torageClass 개체는 다음과 같습니다.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: <Name>
provisioner: csi.trident.netapp.io
mountOptions: <Mount Options>
parameters: <Trident Parameters>
allowVolumeExpansion: true
volumeBindingMode: Immediate
```

이러한 매개 변수는 Trident에만 해당되며 Trident에 클래스에 볼륨을 프로비저닝하는 방법을 알려줍니다.

스토리지 클래스 매개 변수는 다음과 같습니다.

속성	유형	필수 요소입니다	설명
속성	[string] 문자열을 매핑합니다	아니요	아래의 특성 섹션을 참조하십시오
스토리지 풀	Map [string] StringList 입니다	아니요	내의 스토리지 풀 목록에 백엔드 이름 매핑
추가 StoragePools	Map [string] StringList 입니다	아니요	내의 스토리지 풀 목록에 백엔드 이름 매핑
excludeStoragePools를 참조하십시오	Map [string] StringList 입니다	아니요	내의 스토리지 풀 목록에 백엔드 이름 매핑

스토리지 속성 및 가능한 값은 스토리지 풀 선택 특성 및 Kubernetes 속성으로 분류할 수 있습니다.

스토리지 풀 선택 특성입니다

이러한 매개 변수는 지정된 유형의 볼륨을 프로비저닝하는 데 사용해야 하는 Trident 관리 스토리지 풀을 결정합니다.

속성	유형	값	제공합니다	요청하십시오	에 의해 지원됩니다
미디어 [1]	문자열	HDD, 하이브리드, SSD	풀에는 이 유형의 미디어가 포함되어 있으며, 하이브리드는 둘 모두를 의미합니다	지정된 미디어 유형입니다	ONTAP-NAS, ONTAP-NAS-이코노미, ONTAP-NAS-Flexgroup, ONTAP-SAN, solidfire-SAN
프로비저닝 유형	문자열	얇고 두껍습니다	풀은 이 프로비저닝 방법을 지원합니다	프로비저닝 방법이 지정되었습니다	Thick: All ONTAP; Thin: All ONTAP & solidfire-SAN
백엔드 유형	문자열	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, azure-netapp-files, ontap-san-economy	풀이 이 백엔드 유형에 속합니다	백엔드가 지정되었습니다	모든 드라이버
스냅샷 수	불입니다	참, 거짓	풀은 스냅샷이 있는 볼륨을 지원합니다	스냅샷이 활성화된 볼륨	온탑나스, 온탑씨, 솔리드파이어씨
복제	불입니다	참, 거짓	풀은 볼륨 클론을 지원합니다	클론이 활성화된 볼륨	온탑나스, 온탑씨, 솔리드파이어씨
암호화	불입니다	참, 거짓	풀은 암호화된 볼륨을 지원합니다	암호화가 활성화된 볼륨입니다	ONTAP-NAS, ONTAP-NAS-이코노미, ONTAP-NAS-Flexgroups, ONTAP-SAN
IOPS	내부	양의 정수입니다	풀은 이 범위에서 IOPS를 보장할 수 있습니다	볼륨은 이러한 IOPS를 보장합니다	solidfire-SAN

[1]: ONTAP Select 시스템에서 지원되지 않습니다

대부분의 경우 요청된 값이 프로비저닝에 직접적인 영향을 미치며, 예를 들어 일반 프로비저닝을 요청하면 볼륨이 걸쭉하게 프로비저닝됩니다. 하지만 Element 스토리지 풀은 제공된 IOPS 최소 및 최대값을 사용하여 요청된 값이 아닌 QoS 값을 설정합니다. 이 경우 요청된 값은 스토리지 풀을 선택하는 데만 사용됩니다.

이상적으로는 '속성'을 단독으로 사용하여 특정 클래스의 요구 사항을 충족하는 데 필요한 스토리지의 품질을 모델링할 수 있습니다. Trident는 사용자가 지정한 '속성'의 _ALL_과 일치하는 스토리지 풀을 자동으로 검색하여 선택합니다.

클래스에 맞는 풀을 자동으로 선택하기 위해 속성(attributes)을 사용할 수 없는 경우, 'toragePools' 및 'additionalStoragePools' 매개 변수를 사용하여 풀을 더 세분화하거나 특정 풀 세트를 선택할 수도 있습니다.

'toragePools' 매개 변수를 사용하면 지정된 'attributes'와 일치하는 풀 세트를 추가로 제한할 수 있습니다. 즉, Trident는 프로비저닝에서 'attributes'와 'toragePools' 매개 변수로 식별되는 풀의 교집합을 사용합니다. 매개 변수만 사용하거나 둘 다 함께 사용할 수 있습니다.

"additionalStoragePools" 매개 변수를 사용하면 "attributes" 및 "toragePools" 매개 변수로 선택한 풀에 관계없이 Trident에서 프로비저닝에 사용하는 풀 집합을 확장할 수 있습니다.

'excludeStoragePools' 매개 변수를 사용하여 Trident에서 프로비저닝을 위해 사용하는 풀 집합을 필터링할 수 있습니다. 이 매개 변수를 사용하면 일치하는 풀이 모두 제거됩니다.

'toragePools' 및 'additionalStoragePools' 매개 변수에서 각 항목은 '<backend>:<storagePoolList>' 형식을 사용합니다. 여기서 '<storagePoolList>'는 지정된 백엔드에 대한 쉼표로 구분된 스토리지 풀 목록입니다. 예를 들어, additionalStoragePools 값은 ontapnas_192.168.1.100:aggr1,aggr2;solidfire_192.168.1.101:bronze처럼 보일 수 있습니다. 이러한 목록에는 백엔드 및 목록 값 모두에 대한 regex 값이 적용됩니다. tridentctl 백엔드 가져오기 를 사용하여 백엔드와 해당 풀의 목록을 가져올 수 있습니다.

Kubernetes 특성

이러한 특성은 동적 프로비저닝 중 Trident가 스토리지 풀/백엔드를 선택하는 데 아무런 영향을 주지 않습니다. 대신 이러한 특성은 Kubernetes 영구 볼륨에서 지원하는 매개 변수만 제공합니다. 작업자 노드는 파일 시스템 생성 작업을 담당하며 xfsprogs와 같은 파일 시스템 유틸리티가 필요할 수 있습니다.

속성	유형	값	설명	관련 드라이버	**Kubernetes** 버전
fsType입니다	문자열	ext4, ext3, xfs	블록 볼륨의 파일 시스템 유형입니다	solidfire-SAN, ONTAP-NAS, ONTAP-NAS-이코노미, ONTAP-NAS-Flexgroup, ONTAP-SAN, ONTAP-SAN - 경제성	모두
allowVolumeExpansion	부울	참, 거짓	PVC 크기 증가에 대한 지원을 활성화 또는 비활성화합니다	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economy, solidfire-san, azure-netapp-files	1.11+
볼륨BindingMode를 선택합니다	문자열	Immediate, WaitForFirstConsumer입니다	볼륨 바인딩 및 동적 프로비저닝이 수행될 시기를 선택합니다	모두	1.19-1.26

- 를 클릭합니다 `fsType` 매개 변수는 SAN LUN에 대해 원하는 파일 시스템 유형을 제어하는 데 사용됩니다. 또한 Kubernetes는 의 존재 여부를 사용합니다 `fsType` 파일 시스템이 있음을 나타내는 스토리지 클래스에 있습니다. 볼륨 소유권은 를 사용하여 제어할 수 있습니다 `fsGroup` POD의 보안 컨텍스트는 에만 해당됩니다 `fsType` 가 설정됩니다. 을 참조하십시오 "Kubernetes: Pod 또는 컨테이너의 보안 컨텍스트를 구성합니다" 를 사용하여 볼륨 소유권을 설정하는 방법에 대한 개요를 보려면 를 참조하십시오 `fsGroup` 상황. Kubernetes가 에 적용됩니다 `fsGroup` 다음 경우에만 값:

  - 스토리지 클래스에 fsType이 설정되어 있습니다.
  - PVC 액세스 모드는 RWO입니다.

  NFS 스토리지 드라이버의 경우 파일 시스템이 NFS 내보내기의 일부로 이미 존재합니다. fsGroup을 사용하려면 스토리지 클래스가 여전히 fsType을 지정해야 합니다. NFS 또는 null이 아닌 값으로 설정할 수 있습니다.

- 을 참조하십시오 "볼륨 확장" 볼륨 확장에 대한 자세한 내용은 를 참조하십시오.
- Trident 설치 프로그램 번들에는 'Sample-input/storage-class- *.YAML'의 Trident와 함께 사용할 수 있는 여러 가지 스토리지 클래스 정의가 포함되어 있습니다. Kubernetes 스토리지 클래스를 삭제하면 해당 Trident 스토리지 클래지도 삭제됩니다.

쿠버네티스 `VolumeSnapshotClass` 오브젝트

쿠버네티스 VolumeSnapshotClass 객체는 'torageClaes'와 유사합니다. 이 기능을 사용하면 여러 스토리지 클래스를 정의할 수 있으며, 스냅샷을 필요한 스냅샷 클래스와 연결하기 위해 볼륨 스냅숏에서 참조할 수 있습니다. 각 볼륨 스냅샷은 단일 볼륨 스냅샷 클래스와 연결됩니다.

스냅샷을 생성하려면 관리자가 VolumeSnapshotClass를 정의해야 합니다. 볼륨 스냅샷 클래스는 다음과 같은 정의로 생성됩니다.

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: csi-snapclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

driver는 CSI-snapclass 클래스의 볼륨 스냅샷을 요청하는 Kubernetes를 Trident에서 처리하도록 지정합니다. "eletionPolicy"는 스냅샷을 삭제할 때 수행할 작업을 지정합니다. "eletionPolicy"를 "Delete"로 설정하면 스냅샷이 삭제될 때 스토리지 클러스터의 기본 스냅샷과 볼륨 스냅샷 객체가 제거됩니다. 또는 '유지'로 설정하면 VolumeSnapshotContent와 물리적 스냅샷이 보존됩니다.

쿠버네티스 `VolumeSnapshot` 오브젝트

Kubernetes 'VolumeSnapshot' 개체는 볼륨의 스냅샷을 생성하는 요청입니다. PVC는 사용자가 볼륨에 대해 요청하는 것처럼 볼륨 스냅샷은 사용자가 기존 PVC의 스냅샷을 생성하도록 요청하는 것입니다.

볼륨 스냅샷 요청이 들어오면 Trident는 백엔드의 볼륨에 대한 스냅샷 생성을 자동으로 관리하고 고유한 'VolumeSnapshotContent' 객체를 생성하여 스냅샷을 표시합니다. 기존 PVC에서 스냅샷을 생성하고 새 PVC를 생성할 때 스냅샷을 DataSource로 사용할 수 있습니다.

VolumeSnapshot의 수명 주기는 소스 PVC와 무관합니다. 즉, 소스 PVC가 삭제된 후에도 스냅샷은 유지됩니다. 연관된 스냅샷이 있는 PVC를 삭제할 때 Trident는 이 PVC에 대한 백업 볼륨을 * Deleting * 상태로 표시하지만 완전히 제거하지는 않습니다. 연결된 모든 스냅샷이 삭제되면 볼륨이 제거됩니다.

쿠버네티스 `VolumeSnapshotContent` 오브젝트

Kubernetes의 'VolumeSnapshotContent' 객체는 이미 프로비저닝된 볼륨에서 생성된 스냅샷을 나타냅니다. 이 스냅샷은 "PersistentVolume"과 유사하며 스토리지 클러스터에서 프로비저닝된 스냅샷을 나타냅니다. 스냅샷이 생성될 때 PersistentVolumeClaim 및 PersistentVolume 개체와 마찬가지로 VolumeSnapshotContent 개체는 스냅샷 생성을 요청한 VolumeSnapshot 객체에 대한 일대일 매핑을 유지합니다.

VolumeSnapshotContent 객체에는 스냅샷 스냅샷(스냅샷 핸들 등)을 고유하게 식별하는 세부 정보가 포함되어 있습니다. 이 나프산Handle은 PV의 이름과 VolumeSnapshotContent 객체의 이름을 조합한 독특한 것이다.

스냅샷 요청이 들어오면 Trident가 백엔드에 스냅샷을 생성합니다. 스냅샷이 생성된 후 Trident는 'VolumeSnapshotContent' 객체를 구성하여 해당 스냅샷을 Kubernetes API에 노출합니다.

일반적으로 오브젝트를 관리할 필요가 `VolumeSnapshotContent` 없습니다. Trident 외부에서 만들려는 경우는 "볼륨 스냅샷을 가져옵니다"예외입니다.

Kubernetes `VolumeGroupSnapshotClass` 오브젝트

Kubernetes `VolumeGroupSnapshotClass` 오브젝트는 과 `VolumeSnapshotClass`유사합니다. 이러한 스냅샷은 여러 스토리지 클래스를 정의하는 데 도움이 되며, 볼륨 그룹 스냅샷에서 참조되어 스냅샷을 필요한 스냅샷 클래스와 연결합니다. 각 볼륨 그룹 스냅샷은 단일 볼륨 그룹 스냅샷 클래스와 연결됩니다.

에이 `VolumeGroupSnapshotClass` 스냅샷 그룹을 생성하려면 관리자가 정의해야 합니다. 볼륨 그룹 스냅샷 클래스는 다음 정의를 사용하여 생성됩니다.

```
apiVersion: groupsnapshot.storage.k8s.io/v1beta1
kind: VolumeGroupSnapshotClass
metadata:
  name: csi-group-snap-class
  annotations:
    kubernetes.io/description: "Trident group snapshot class"
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

는 Trident에서 처리합니다. `deletionPolicy` 그룹 스냅샷을 삭제해야 할 때 수행할 작업을 지정합니다 . `deletionPolicy` 로 설정됩니다 `Delete` 스냅샷이 삭제되면 볼륨 그룹 스냅샷 개체와 스토리지 클러스터의 기본 스냅샷도 제거됩니다. 또는 로 설정하면 `Retain` `VolumeGroupSnapshotContent` 및 물리적 스냅샷이 보존됩니다.

Kubernetes `VolumeGroupSnapshot` 오브젝트

쿠버네티스 `VolumeGroupSnapshot` 객체는 여러 볼륨의 스냅샷을 생성하라는 요청입니다. PVC가 사용자가 볼륨에 대해 요청한 것을 나타내는 것처럼, 볼륨 그룹 스냅샷은 사용자가 기존 PVC의 스냅샷을 생성하라는 요청입니다.

볼륨 그룹 스냅샷 요청이 들어오면 Trident는 백엔드의 볼륨에 대한 그룹 스냅샷 생성을 자동으로 관리하고 고유한 스냅샷을 생성하여 스냅샷을 노출합니다. `VolumeGroupSnapshotContent` 물체. 기존 PVC에서 스냅샷을 생성하고 새 PVC를 생성할 때 스냅샷을 DataSource로 사용할 수 있습니다.

> VolumeGroupSnapshot의 수명 주기는 소스 PVC와 무관합니다. 즉, 소스 PVC가 삭제된 후에도 스냅샷은 유지됩니다. 연관된 스냅샷이 있는 PVC를 삭제할 때 Trident는 이 PVC에 대한 백업 볼륨을 * Deleting * 상태로 표시하지만 완전히 제거하지는 않습니다. 연결된 모든 스냅샷이 삭제되면 볼륨 그룹 스냅샷도 제거됩니다.

Kubernetes `VolumeGroupSnapshotContent` 오브젝트

쿠버네티스 `VolumeGroupSnapshotContent` 개체는 이미 프로비저닝된 볼륨에서 가져온 그룹 스냅샷을 나타냅니다. 이 스냅샷은 A와 유사하며 `PersistentVolume` 스토리지 클러스터에서 프로비저닝된 스냅샷을 나타냅니다. 및 `PersistentVolume` 객체와 마찬가지로 `PersistentVolumeClaim` 스냅샷이 생성될 때 `VolumeSnapshotContent` 객체는 스냅샷 생성을 요청한 객체에 대한 일대일 매핑을 `VolumeSnapshot` 유지합니다.

그만큼 `VolumeGroupSnapshotContent` 개체에는 스냅샷 그룹을 식별하는 세부 정보(예: `volumeGroupSnapshotHandle` 그리고 개별 볼륨 스냅샷이 스토리지 시스템에 존재합니다.

스냅샷 요청이 들어오면 Trident는 백엔드에 볼륨 그룹 스냅샷을 생성합니다. 볼륨 그룹 스냅샷이 생성된 후 Trident는 `VolumeGroupSnapshotContent` 객체를 생성하여 Kubernetes API에 스냅샷을 노출합니다.

쿠버네티스 `CustomResourceDefinition` 오브젝트

Kubernetes 사용자 지정 리소스는 관리자가 정의하며 비슷한 객체를 그룹화하는 데 사용되는 Kubernetes API의 엔드포인트입니다. Kubernetes에서는 오브젝트 컬렉션을 저장하기 위한 사용자 지정 리소스의 생성을 지원합니다. kubeck Get CRD를 실행하여 이러한 리소스 정의를 얻을 수 있습니다.

사용자 정의 리소스 정의(CRD) 및 관련 오브젝트 메타데이터는 Kubernetes에서 메타데이터 저장소에 저장됩니다. 따라서 Trident를 위한 별도의 저장소가 필요하지 않습니다.

Trident에서는 오브젝트를 사용하여 `CustomResourceDefinition` Trident 백 엔드, Trident 스토리지 클래스 및 Trident 볼륨과 같은 Trident 오브젝트의 ID를 유지합니다. 이러한 오브젝트는 Trident에서 관리합니다. 또한 CSI 볼륨 스냅샷 프레임워크는 볼륨 스냅샷을 정의하는 데 필요한 일부 CRD를 소개합니다.

CRD는 Kubernetes를 구성하는 것입니다. 위에 정의된 리소스의 객체는 Trident에 의해 생성됩니다. 간단히 예로, 'tridentctl'을 사용하여 백엔드를 생성할 때 해당하는 'tridentbackends' CRD 객체는 Kubernetes에서 사용할 수 있도록 생성됩니다.

다음은 Trident의 CRD에 대해 고려해야 할 몇 가지 사항입니다.

- Trident가 설치되면 일련의 CRD가 생성되어 다른 리소스 유형과 마찬가지로 사용할 수 있습니다.
- 를 사용하여 Trident를 제거하는 경우 `tridentctl uninstall` Command, Trident Pod가 삭제되지만 생성된 CRD는 정리되지 않습니다. 을 참조하십시오 "Trident를 제거합니다" Trident를 완전히 제거하고 처음부터 다시 구성할 수 있는 방법을 이해합니다.

Trident 개체 `StorageClass`

Trident가 Kubernetes에 맞는 스토리지 클래스를 생성합니다 `StorageClass` 지정하는 개체입니다 `csi.trident.netapp.io` 그들의 공급자 분야. 스토리지 클래스 이름이 Kubernetes의 클래스 이름과 일치합니다

`StorageClass` 나타내는 개체입니다.

> Kubernetes를 사용하면 Trident를 프로비저닝한 Kubernetes의 torageClass가 등록되면 이러한 객체가 자동으로 생성됩니다.

스토리지 클래스는 볼륨에 대한 일련의 요구 사항으로 구성됩니다. Trident는 이러한 요구 사항을 각 스토리지 풀에 있는 속성과 일치시킵니다. 일치하는 경우 해당 스토리지 풀이 해당 스토리지 클래스를 사용하여 볼륨을 프로비저닝할 수 있는 유효한 타겟입니다.

REST API를 사용하여 스토리지 클래스를 직접 정의하는 스토리지 클래스 구성을 생성할 수 있습니다. 그러나 Kubernetes 구축의 경우 새로운 Kubernetes의 torageClass 오브젝트를 등록할 때 이러한 객체가 생성되기를 기대합니다.

Trident 백엔드 객체

백엔드는 Trident가 볼륨을 프로비저닝하는 스토리지 공급자를 나타냅니다. 단일 Trident 인스턴스가 원하는 수의 백엔드를 관리할 수 있습니다.

> 이것은 직접 만들고 관리하는 두 가지 개체 유형 중 하나입니다. 다른 하나는 Kubernetes의 torageClass 오브젝트입니다.

이러한 개체를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 "백엔드 구성 중".

Trident 개체 `StoragePool`

스토리지 풀은 각 백엔드에서 프로비저닝에 사용할 수 있는 고유한 위치를 나타냅니다. ONTAP 의 경우 이는 SVM의 집계에 해당합니다. NetApp HCI/ SolidFire 의 경우 이는 관리자가 지정한 QoS 대역에 해당합니다. 각 스토리지 풀에는 성능 특성과 데이터 보호 특성을 정의하는 일련의 고유한 스토리지 속성이 있습니다.

다른 오브젝트와 달리 스토리지 풀 후보 는 항상 자동으로 검색되고 관리됩니다.

Trident 개체 `Volume`

볼륨은 프로비저닝의 기본 단위로, NFS 공유, iSCSI 및 FC LUN 등의 백엔드 엔드포인트를 구성합니다. Kubernetes에서 이러한 항목은 에 직접 `PersistentVolumes` 대응합니다. 볼륨을 생성할 때 볼륨의 용량을 할당할 수 있는 위치와 크기를 결정하는 스토리지 클래스가 있는지 확인합니다.

> - Kubernetes에서 이러한 오브젝트는 자동으로 관리됩니다. 프로비저닝 Trident를 보려면 해당 Trident를 확인하십시오.
> - 연결된 스냅샷이 있는 PV를 삭제하면 해당 Trident 볼륨이 * Deleting * 상태로 업데이트됩니다. Trident 볼륨을 삭제하려면 볼륨의 스냅샷을 제거해야 합니다.

볼륨 구성은 프로비저닝된 볼륨에 있어야 하는 속성을 정의합니다.

속성	유형	필수 요소입니다	설명
버전	문자열	아니요	Trident API 버전("1")
이름	문자열	예	생성할 볼륨의 이름입니다

속성	유형	필수 요소입니다	설명
storageClass 를 선택합니다	문자열	예	볼륨을 프로비저닝할 때 사용할 스토리지 클래스입니다
크기	문자열	예	용량 할당할 볼륨의 크기(바이트)입니다
프로토콜	문자열	아니요	사용할 프로토콜 유형;"파일" 또는 "블록"
내부 이름	문자열	아니요	스토리지 시스템에 있는 객체의 이름으로, Trident에서 생성
CloneSourceVolume	문자열	아니요	ONTAP(NAS, SAN) 및 SolidFire - *: 복제할 볼륨의 이름입니다
SplitOnClone 을 참조하십시오	문자열	아니요	ONTAP(NAS, SAN): 상위 클론에서 클론을 분할합니다
스냅샷 정책	문자열	아니요	ONTAP - *: 사용할 스냅샷 정책
snapshotReserve	문자열	아니요	ONTAP - *: 스냅숏용으로 예약된 볼륨의 비율입니다
내보내기 정책	문자열	아니요	ONTAP-NAS *: 사용할 엑스포트 정책
스냅샷 디렉토리	불입니다	아니요	ONTAP-NAS *: 스냅샷 디렉토리가 표시되는지 여부를 나타냅니다
unixPermissions	문자열	아니요	ONTAP-NAS *: 초기 UNIX 권한
블록 크기	문자열	아니요	SolidFire - *: 블록/섹터 크기
파일 시스템	문자열	아니요	파일 시스템 유형입니다
skipRecoveryQueue	문자열	아니요	볼륨을 삭제하는 동안 저장소의 복구 대기열을 우회하고 볼륨을 즉시 삭제합니다.

Trident는 볼륨을 생성할 때 'internalName'을 생성합니다. 이 단계는 두 단계로 구성됩니다. 먼저, 저장소 접두사(기본 "트리덴트" 또는 백엔드 구성의 접두사)를 볼륨 이름에 추가하여 "<prefix>-<volume-name>" 형식의 이름을 만듭니다. 그런 다음 백엔드에서 허용되지 않는 문자를 대체하여 이름을 삭제하는 작업을 진행합니다. ONTAP 백엔드의 경우 하이픈을 밑줄로 바꿉니다. 따라서 내부 이름은 "<prefix>_<volume-name>"이 됩니다. 요소 백엔드의 경우 밑줄을 하이픈으로 바꿉니다.

볼륨 구성을 사용하여 REST API를 사용하여 볼륨을 직접 프로비저닝할 수 있지만 Kubernetes 배포에서는 대부분의 사용자가 표준 Kubernetes "PersistentVolumeClaim" 방법을 사용할 것으로 예상됩니다. Trident는 프로비저닝 프로세스의 일부로 이 볼륨 개체를 자동으로 만듭니다.

Trident 개체 `Snapshot`

스냅샷은 볼륨의 시점 복제본으로, 새 볼륨을 용량 할당하거나 복구 상태를 복구하는 데 사용할 수 있습니다. Kubernetes에서는 이러한 객체가 'VolumeSnapshotContent' 객체와 직접 일치합니다. 각 스냅샷은 스냅샷에 대한 데이터의 소스인 볼륨에 연결됩니다.

각 '스냅샷' 개체에는 아래 나열된 속성이 포함됩니다.

속성	유형	필수 요소입니다	설명
버전	문자열	예	Trident API 버전("1")
이름	문자열	예	Trident 스냅샷 개체의 이름입니다
내부 이름	문자열	예	스토리지 시스템의 Trident 스냅샷 개체의 이름입니다
볼륨 이름	문자열	예	스냅샷이 생성된 영구 볼륨의 이름입니다
볼륨 국제 이름	문자열	예	스토리지 시스템에서 연결된 Trident 볼륨 개체의 이름입니다

Kubernetes에서 이러한 오브젝트는 자동으로 관리됩니다. 프로비저닝 Trident를 보려면 해당 Trident를 확인하십시오.

Kubernetes 'VolumeSnapshot' 객체 요청이 생성되면 Trident는 백업 스토리지 시스템에 스냅샷 객체를 생성하여 작동합니다. 이 스냅샷 개체의 인터날Name은 볼륨 스냅샷 개체의 UID(예: 스냅샷-e8d8a0ca-9826-11e9-9807 -525400f3f660)와 접두사 스냅샷-UID를 결합하여 생성됩니다. 볼륨 이름 과 볼륨 InternalName 은 백업 볼륨의 세부 정보를 가져오는 방식으로 채워집니다.

Trident 개체입니다 `ResourceQuota`

Trident deamonset은 `system-node-critical` Trident가 정상적인 노드 종료 중에 볼륨을 식별 및 정리하고 Trident demonset Pod가 리소스 압력이 높은 클러스터에서 낮은 우선 순위로 워크로드를 사전 지정할 수 있도록 하기 위해 Kubernetes에서 사용 가능한 가장 높은 우선 순위 클래스인 우선 순위 클래스를 사용합니다.

이를 위해 Trident는 객체를 사용하여 `ResourceQuota` Trident 데몬 세트의 "시스템 노드 중요" 우선 순위 클래스가 충족되도록 합니다. 배포 및 demonset 생성 전에 Trident는 객체를 찾고 `ResourceQuota` 발견되지 않은 경우 이를 적용합니다.

기본 리소스 할당량 및 우선순위 클래스에 대한 더 많은 제어가 필요한 경우 'CUSTOM.YAML'을 생성하거나 제어 차트를 사용하여 'ResourceQuota' 객체를 구성할 수 있습니다.

다음은 Trident 데모의 우선 순위를 지정하는 'ResourceQuota' 개체의 예입니다.

```
apiVersion: <version>
kind: ResourceQuota
metadata:
  name: trident-csi
  labels:
    app: node.csi.trident.netapp.io
spec:
  scopeSelector:
    matchExpressions:
      - operator: In
        scopeName: PriorityClass
        values:
          - system-node-critical
```

리소스 할당량에 대한 자세한 내용은 을 참조하십시오 "Kubernetes: 리소스 할당량".

정리 `ResourceQuota` 설치에 실패한 경우

드문 경우지만 ResourceQuota 객체를 만든 후 설치가 실패하는 경우 먼저 시도해 보십시오 "제거 중" 그런 다음 다시 설치합니다.

이 기능이 작동하지 않으면 수동으로 ResourceQuota 객체를 제거합니다.

제거 `ResourceQuota`

리소스 할당을 직접 제어하려는 경우 다음 명령을 사용하여 Trident 개체를 제거할 수 `ResourceQuota` 있습니다.

```
kubectl delete quota trident-csi -n trident
```

POD 보안 표준(PSS) 및 보안 컨텍스트 제약(SCC)

Kubernetes Pod 보안 표준(PSS) 및 Pod 보안 정책(PSP)에서 사용 권한 수준을 정의하고 Pod의 동작을 제한합니다. OpenShift Security Context Constraints(SCC)도 OpenShift Kubernetes Engine에 특정한 POD 제한을 정의합니다. 이러한 사용자 지정 기능을 제공하기 위해 Trident는 설치 중에 특정 권한을 활성화합니다. 다음 섹션에서는 Trident에서 설정한 사용 권한에 대해 자세히 설명합니다.

PSS는 Pod 보안 정책(PSP)을 대체합니다. PSP는 Kubernetes v1.21에서 사용되지 않으며 v1.25에서 제거됩니다. 자세한 내용은 을 참조하십시오 "Kubernetes: 보안".

필요한 Kubernetes 보안 컨텍스트 및 관련 필드

권한	설명
특별 권한	CSI를 사용하려면 마운트 지점이 양방향이어야 합니다. 즉, Trident 노드 포드가 권한이 있는 컨테이너를 실행해야 합니다. 자세한 내용은 을 참조하십시오 "Kubernetes: 마운트 전파".
호스트 네트워킹	iSCSI 데몬에 필요합니다. iscsiadm은 iSCSI 마운트를 관리하고 호스트 네트워킹을 사용하여 iSCSI 데몬과 통신합니다.
호스트 IPC	NFS는 IPC(프로세스 간 통신)를 사용하여 NFSD와 통신합니다.
호스트 PID	NFS를 시작하기 위해 `rpc-statd` 필요합니다. Trident는 NFS 볼륨을 마운트하기 전에 호스트 프로세스를 쿼리하여 가 실행 중인지 여부를 `rpc-statd` 확인합니다.
제공합니다	'SYS_ADMIN' 기능은 권한 있는 컨테이너의 기본 기능의 일부로 제공됩니다. 예를 들어, Docker는 권한이 있는 컨테이너인 'CapPrm:0000003fffffffff'CapEff:0000003fffffffff'에 대해 이러한 기능을 설정합니다
Seccomp	Seccomp 프로필은 권한이 있는 컨테이너에서 항상 "제한 없음"이므로 Trident에서 활성화할 수 없습니다.
SELinux	OpenShift에서는 권한이 있는 컨테이너가 `spc_t` ("상위 권한 있는 컨테이너") 도메인에서 실행되고 권한이 없는 컨테이너는 `container_t` 도메인에서 실행됩니다. `containerd`가 설치되어 있으면 `container-selinux` 모든 컨테이너가 도메인에서 실행되어 `spc_t` SELinux가 효과적으로 비활성화됩니다. 따라서 Trident는 컨테이너에 추가되지 `seLinuxOptions` 않습니다.
DAC	권한이 있는 컨테이너는 루트로 실행되어야 합니다. 권한이 없는 컨테이너는 root로 실행되어 CSI에 필요한 UNIX 소켓에 액세스합니다.

POD 보안 표준(PSS)

라벨	설명	기본값
pod-security.Kubernetes.io/force 포드-security.Kubernetes.io/force -version을 적용합니다	Trident 컨트롤러와 노드를 설치 네임스페이스에 받아들일 수 있습니다. 네임스페이스 레이블을 변경하지 마십시오.	최근 실시한 PSS의 최신 버전이나 PSS의 최고 버전 >

네임스페이스 레이블을 변경하면 포드가 예약되지 않고 "오류 생성:..." 또는 "경고: 트리덴트 - CSI -..." 가 발생할 수 있습니다. 이 경우 특권 네임스페이스 레이블이 변경되었는지 확인합니다. 있는 경우 Trident를 다시 설치합니다.

PSP(POD 보안 정책)

필드에 입력합니다	설명	기본값
'allowPrivilegeegeEscalation'	권한 있는 컨테이너는 권한 에스컬레이션을 허용해야 합니다.	"참"입니다
'allowedCSIDrivers'입니다	Trident는 인라인 CSI 임시 볼륨을 사용하지 않습니다.	비어 있습니다
'allowedCapabilities'	권한이 없는 Trident 컨테이너는 기본 세트보다 더 많은 기능을 필요로 하지 않으며 권한이 있는 컨테이너에 모든 가능한 기능이 부여됩니다.	비어 있습니다
'allowedFlexVolumes'	Trident는 을 사용하지 않습니다 "FlexVolume 드라이버"따라서 허용된 볼륨 목록에 포함되지 않습니다.	비어 있습니다
'allowedHostPaths'	Trident 노드 포드는 노드의 루트 파일 시스템을 마운트하므로 이 목록을 설정하는 데는 아무런 이점이 없습니다.	비어 있습니다
'allowedProcMountTypes'	Trident는 'ProcMountTypes'를 사용하지 않습니다.	비어 있습니다
'allowedUnsafeSysctls'	Trident는 안전하지 않은 '스컬'을 필요로 하지 않습니다.	비어 있습니다
"기본 추가 기능"을 참조하십시오	권한이 있는 컨테이너에 기능을 추가할 필요가 없습니다.	비어 있습니다
월권 AllowPrivilegeEscalation	권한 에스컬레이션을 허용하는 작업은 각 Trident 포드에서 처리됩니다.	거짓입니다
'바이디니데시스틀스'	'스매스들'은 허용되지 않습니다.	비어 있습니다
'fsGroup'입니다	Trident 컨테이너가 루트로 실행됩니다.	러아사니
호스티IPC	NFS 볼륨을 마운트하려면 호스트 IPC가 nfsd와 통신해야 합니다	"참"입니다
호스트 네트워크	iscsiadm을 사용하려면 호스트 네트워크가 iSCSI 데몬과 통신해야 합니다.	"참"입니다
'hostPID'	노드에서 RPC-statd가 실행되고 있는지 확인하려면 호스트 PID가 필요합니다.	"참"입니다
호스트 포트	Trident는 호스트 포트를 사용하지 않습니다.	비어 있습니다
특권	Trident 노드 포드는 볼륨을 마운트하려면 권한이 있는 컨테이너를 실행해야 합니다.	"참"입니다
"RootFilesystem"을 선택합니다	Trident 노드 포드는 노드 파일 시스템에 써야 합니다.	거짓입니다

필드에 입력합니다	설명	기본값
레퀴레드드롭카포비스	Trident 노드 포드는 권한이 있는 컨테이너를 실행하고 기능을 삭제할 수 없습니다.	"없음"
루아그룹	Trident 컨테이너가 루트로 실행됩니다.	러아사니
'runAsUser’입니다	Trident 컨테이너가 루트로 실행됩니다.	루아안니
'런타임 클래스'	트라이던트(Trident)는 RuntimeClasses를 사용하지 않습니다.	비어 있습니다
'e linux'	Trident는 현재 컨테이너 실행 시간과 Kubernetes 배포판이 SELinux를 처리하는 방식에 차이가 있으므로 'eLinuxOptions’를 설정하지 않습니다.	비어 있습니다
업플레탈그룹	Trident 컨테이너가 루트로 실행됩니다.	러아사니
'볼륨'	Trident Pod에는 이러한 볼륨 플러그인이 필요합니다.	대스트패스, 투상도, 최고가

SCC(Security Context Constraints)

라벨	설명	기본값
'allowHostDirVolumePlugin’을 선택합니다	Trident 노드 포드는 노드의 루트 파일 시스템을 마운트합니다.	"참"입니다
'allowHostIPC’입니다	NFS 볼륨을 마운트하려면 호스트 IPC가 nfsd와 통신해야 합니다.	"참"입니다
'allowHostNetwork’입니다	iscsiadm을 사용하려면 호스트 네트워크가 iSCSI 데몬과 통신해야 합니다.	"참"입니다
'allowHostPID'	노드에서 RPC-statd가 실행되고 있는지 확인하려면 호스트 PID가 필요합니다.	"참"입니다
'allowHostPorts’입니다	Trident는 호스트 포트를 사용하지 않습니다.	거짓입니다
'allowPrivilegeegeEscalation'	권한 있는 컨테이너는 권한 에스컬레이션을 허용해야 합니다.	"참"입니다
'allowPrivilegedContainer'	Trident 노드 포드는 볼륨을 마운트하려면 권한이 있는 컨테이너를 실행해야 합니다.	"참"입니다
'allowedUnsafeSysctls'	Trident는 안전하지 않은 '스컬’을 필요로 하지 않습니다.	"없음"

라벨	설명	기본값
'allowedCapabilities'	권한이 없는 Trident 컨테이너는 기본 세트보다 더 많은 기능을 필요로 하지 않으며 권한이 있는 컨테이너에 모든 가능한 기능이 부여됩니다.	비어 있습니다
"기본 추가 기능"을 참조하십시오	권한이 있는 컨테이너에 기능을 추가할 필요가 없습니다.	비어 있습니다
'fsGroup'입니다	Trident 컨테이너가 루트로 실행됩니다.	러아사니
그룹	이 SCC는 Trident에만 해당되며 사용자에게 바인딩됩니다.	비어 있습니다
"RootFilesystem"을 선택합니다	Trident 노드 포드는 노드 파일 시스템에 써야 합니다.	거짓입니다
레퀴레드드롭카포비스	Trident 노드 포드는 권한이 있는 컨테이너를 실행하고 기능을 삭제할 수 없습니다.	"없음"
'runAsUser'입니다	Trident 컨테이너가 루트로 실행됩니다.	러아사니
새리눅스컨텍스트	Trident는 현재 컨테이너 실행 시간과 Kubernetes 배포판이 SELinux를 처리하는 방식에 차이가 있으므로 'eLinuxOptions'를 설정하지 않습니다.	비어 있습니다
'eccompProfiles	특권 컨테이너는 항상 "비제한" 상태로 실행됩니다.	비어 있습니다
업플레탈그룹	Trident 컨테이너가 루트로 실행됩니다.	러아사니
'사용자'	이 SCC를 Trident 네임스페이스의 Trident 사용자에게 바인딩하기 위해 하나의 항목이 제공됩니다.	해당 없음
'볼륨'	Trident Pod에는 이러한 볼륨 플러그인이 필요합니다.	hostPath, downwardAPI, 투영, emptyDir