



Trident Protect를 설치합니다

Trident

NetApp
September 26, 2025

목차

Trident Protect를 설치합니다	1
Trident 보호 요구 사항	1
Trident는 Kubernetes 클러스터 호환성을 보호합니다	1
Trident는 스토리지 백엔드 호환성을 보호합니다	1
NAS 경제 볼륨에 대한 요구 사항	2
KubeVirt VM으로 데이터 보호	2
SnapMirror 복제에 대한 요구 사항	3
Trident Protect를 설치하고 구성합니다	4
Trident Protect를 설치합니다	4
Trident Protect 컨테이너 리소스 제한을 지정합니다	8
Trident Protect CLI 플러그인을 설치합니다	9
Trident Protect CLI 플러그인을 설치합니다	9
Trident CLI 플러그인 도움말을 봅니다	11
명령 자동 완성 활성화	11

Trident Protect를 설치합니다

Trident 보호 요구 사항

운영 환경, 애플리케이션 클러스터, 애플리케이션 및 라이선스의 준비 상태를 확인하는 것으로 시작하십시오. Trident Protect를 배포 및 운영하기 위해 사용자 환경이 이러한 요구 사항을 충족하는지 확인합니다.

Trident는 Kubernetes 클러스터 호환성을 보호합니다

Trident Protect는 다음과 같은 완전관리형 및 자가 관리형 Kubernetes 오퍼링과 호환됩니다.

- Amazon Elastic Kubernetes Service(EKS)
- Google Kubernetes Engine(GKE)
- Microsoft Azure Kubernetes Service(AKS)
- Red Hat OpenShift
- 수세 목장
- VMware Tanzu 포트폴리오
- 업스트림 Kubernetes



Trident Protect를 설치하는 클러스터가 실행 중인 스냅샷 컨트롤러와 관련 CRD로 구성되어 있는지 확인합니다. 스냅샷 컨트롤러를 설치하려면 을 ["참조하십시오"](#)참조하십시오.

Trident는 스토리지 백엔드 호환성을 보호합니다

Trident Protect는 다음 스토리지 백엔드를 지원합니다.

- NetApp ONTAP용 Amazon FSx
- Cloud Volumes ONTAP
- ONTAP 스토리지 어레이
- Google Cloud NetApp 볼륨
- Azure NetApp Files

스토리지 백엔드가 다음 요구 사항을 충족하는지 확인합니다.

- 클러스터에 연결된 NetApp 스토리지가 Astra Trident 24.02 이상을 사용하는지 확인합니다(Trident 24.10 권장).
 - Astra Trident가 24.06.1 이전 버전이고 NetApp SnapMirror 재해 복구 기능을 사용하려면 Astra Control Provisioner를 수동으로 활성화해야 합니다.
- 최신 Astra Control Provisioner(Astra Trident 24.06.1 기준으로 기본적으로 설치 및 활성화됨)가 있는지 확인합니다.
- NetApp ONTAP 스토리지 백엔드가 있는지 확인합니다.
- 백업을 저장할 오브젝트 스토리지 버킷을 구성했는지 확인합니다.

- 응용 프로그램 또는 응용 프로그램 데이터 관리 작업에 사용할 응용 프로그램 네임스페이스를 만듭니다. Trident Protect는 이러한 네임스페이스를 자동으로 만들지 않습니다. 사용자 지정 리소스에 존재하지 않는 네임스페이스를 지정하면 작업이 실패합니다.

NAS 경제 볼륨에 대한 요구 사항

Trident Protect는 NAS 경제 볼륨에 대한 백업 및 복원 작업을 지원합니다. 현재 NAS 경제 볼륨으로의 스냅샷, 클론, SnapMirror 복제는 지원되지 않습니다. Trident Protect와 함께 사용할 각 NAS 경제 볼륨에 대해 스냅샷 디렉토리를 활성화해야 합니다.



일부 애플리케이션은 스냅샷 디렉토리를 사용하는 볼륨과 호환되지 않습니다. 이러한 애플리케이션의 경우 ONTAP 스토리지 시스템에서 다음 명령을 실행하여 스냅샷 디렉토리를 숨겨야 합니다.

```
nfs modify -vserver <svm> -v3-hide-snapshot enabled
```

각 NAS 경제 볼륨에 대해 다음 명령을 실행하여 스냅샷 디렉토리를 설정할 수 있으며, 변경할 볼륨의 UUID로 바꿀 수 <volume-UUID> 있습니다.

```
tridentctl update volume <volume-UUID> --snapshot-dir=true --pool-level=true -n trident
```



Trident 백엔드 구성 옵션을 `true` 설정하면 기본적으로 새 볼륨에 대해 스냅샷 디렉토리를 설정할 수 `snapshotDir` 있습니다. 기존 볼륨은 영향을 받지 않습니다.

KubeVirt VM으로 데이터 보호

KubeVirt VM에서 실행 중인 애플리케이션을 보호할 때 Trident Protect 24.10 및 24.10.1 이상의 동작이 다릅니다. 두 버전의 경우 모두 데이터 보호 작업 중에 파일 시스템 고정 및 고정 해제를 설정하거나 해제할 수 있습니다.



모든 Trident Protect 버전에 대해 OpenShift 환경에서 자동 고정 기능을 활성화 또는 비활성화하려면 애플리케이션 네임스페이스에 권한 있는 권한을 부여해야 할 수 있습니다. 예를 들면 다음과 같습니다.

```
oc adm policy add-scc-to-user privileged -z default -n <application-namespace>
```

Trident Protect 24.10

Trident Protect 24.10은 데이터 보호 작업 중에 KubeVirt VM 파일 시스템의 일관된 상태를 자동으로 보장하지 않습니다. Trident Protect 24.10을 사용하여 KubeVirt VM 데이터를 보호하려면 데이터 보호 작업 전에 파일 시스템에 대해 고정/고정 해제 기능을 수동으로 활성화해야 합니다. 이렇게 하면 파일 시스템이 정합성 보장 상태가 됩니다.

를 사용하여 데이터 보호 작업 중에 VM 파일 시스템의 고정 및 고정 해제를 관리하도록 Trident Protect 24.10을 구성한 후 다음 명령을 사용하여 관리할 수 "가상화 구성" 있습니다.

```
kubectl set env deployment/trident-protect-controller-manager
NEPTUNE_VM_FREEZE=true -n trident-protect
```

Trident Protect 24.10.1 이상

Trident Protect 24.10.1부터 Trident Protect는 데이터 보호 작업 중에 KubeVirt 파일 시스템이 자동으로 작동 중지되고 작동 중지되지 않습니다. 다음 명령을 사용하여 이 자동 동작을 비활성화할 수도 있습니다.

```
kubectl set env deployment/trident-protect-controller-manager
NEPTUNE_VM_FREEZE=false -n trident-protect
```

SnapMirror 복제에 대한 요구 사항

NetApp SnapMirror는 다음 ONTAP 솔루션에 대해 Trident Protect와 함께 사용할 수 있습니다.

- NetApp ASA
- NetApp AFF
- NetApp FAS
- NetApp ONTAP Select를 참조하십시오
- NetApp Cloud Volumes ONTAP를 참조하십시오
- NetApp ONTAP용 Amazon FSx

SnapMirror 복제를 위한 ONTAP 클러스터 요구 사항

SnapMirror 복제를 사용하려는 경우 ONTAP 클러스터가 다음 요구 사항을 충족하는지 확인하십시오.

- * Astra Control Provisioner 또는 Trident *: Astra Control Provisioner 또는 Trident는 ONTAP를 백엔드로 활용하는 소스 및 대상 Kubernetes 클러스터 모두에 존재해야 합니다. Trident Protect는 다음 드라이버를 통해 지원되는 스토리지 클래스를 사용하여 NetApp SnapMirror 기술을 통한 복제를 지원합니다.
 - ontap-nas
 - ontap-san
- * 라이선스 *: 소스 및 대상 ONTAP 클러스터 모두에서 데이터 보호 번들을 사용하는 ONTAP SnapMirror 비동기 라이선스를 활성화해야 합니다. 자세한 내용은 ["ONTAP의 SnapMirror 라이선스 개요"](#) 참조하십시오.

SnapMirror 복제에 대한 피어링 고려 사항

스토리지 백엔드 피어링을 사용하려는 경우 환경이 다음 요구 사항을 충족하는지 확인하십시오.

- * 클러스터 및 SVM *: ONTAP 스토리지 백엔드를 피어링해야 합니다. 자세한 내용은 ["클러스터 및 SVM 피어링 개요"](#) 참조하십시오.



두 ONTAP 클러스터 간의 복제 관계에 사용되는 SVM 이름이 고유한지 확인합니다.

- * Astra Control Provisioner 또는 Trident 및 SVM *: 피어링된 원격 SVM을 대상 클러스터의 Astra Control Provisioner 또는 Trident에서 사용할 수 있어야 합니다.

- * 관리되는 백엔드 *: 복제 관계를 만들려면 Trident Protect에서 ONTAP 스토리지 백엔드를 추가 및 관리해야 합니다.
- * over TCP *: Trident Protect는 NVMe over TCP 프로토콜을 사용하는 스토리지 백엔드에 대해 NetApp SnapMirror 복제를 지원하지 않습니다.

SnapMirror 복제를 위한 Trident/ONTAP 구성

Trident Protect를 사용하려면 소스 및 대상 클러스터 모두에 대해 복제를 지원하는 스토리지 백엔드를 하나 이상 구성해야 합니다. 소스 및 대상 클러스터가 동일한 경우 대상 애플리케이션은 최상의 복원력을 위해 소스 애플리케이션과 다른 스토리지 백엔드를 사용해야 합니다.

Trident Protect를 설치하고 구성합니다

사용 중인 환경이 Trident Protect 요구 사항을 충족하는 경우 다음 단계에 따라 클러스터에 Trident Protect를 설치할 수 있습니다. NetApp에서 Trident Protect를 얻거나 개인 레지스트리에서 설치할 수 있습니다. 클러스터가 인터넷에 액세스할 수 없는 경우 개인 레지스트리에서 설치하는 것이 유용합니다.



기본적으로 Trident Protect는 클러스터 및 관리형 애플리케이션에 대한 로그, 메트릭, 토폴로지 정보 등 파트너가 개설했을 수 있는 모든 NetApp 지원 사례에 도움이 되는 지원 정보를 수집합니다. Trident Protect는 이러한 지원 번들을 일일 일정에 따라 NetApp로 전송합니다. Trident Protect를 설치할 때 선택적으로 이 지원 번들 컬렉션을 비활성화할 수 있습니다. 언제든지 수동으로 수행할 수 ["지원 번들을 생성합니다"](#) 있습니다.

Trident Protect를 설치합니다

NetApp에서 Trident Protect를 설치합니다

단계

1. Trident Helm 저장소 추가:

```
helm repo add netapp-trident-protect  
https://netapp.github.io/trident-protect-helm-chart
```

2. Trident Protect CRD를 설치합니다.

```
helm install trident-protect-crds netapp-trident-protect/trident-  
protect-crds --version 100.2410.1 --create-namespace --namespace  
trident-protect
```

3. Helm을 사용하여 다음 명령 중 하나를 사용하여 Trident Protect를 설치합니다. 클러스터에 할당되고 클러스터의 백업 및 스냅샷을 식별하는 데 사용되는 클러스터 이름으로 바꿉니다 <name_of_cluster>.

- Trident Protect를 정상적으로 설치합니다.

```
helm install trident-protect netapp-trident-protect/trident-  
protect --set clusterName=<name_of_cluster> --version 100.2410.1  
--create-namespace --namespace trident-protect
```

- Trident Protect를 설치하고 예약된 일일 Trident Protect AutoSupport 지원 번들 업로드를 비활성화합니다.

```
helm install trident-protect netapp-trident-protect/trident-  
protect --set autoSupport.enabled=false --set  
clusterName=<name_of_cluster> --version 100.2410.1 --create  
-namespace --namespace trident-protect
```

개인 레지스트리로부터 Trident Protect를 설치합니다

Kubernetes 클러스터가 인터넷에 액세스할 수 없는 경우 개인 이미지 레지스트리에서 Trident Protect를 설치할 수 있습니다. 이 예제에서는 대괄호 안의 값을 사용자 환경의 정보로 바꿉니다.

단계

1. 다음 이미지를 로컬 컴퓨터로 가져와서 태그를 업데이트한 다음 개인 레지스트리에 푸시합니다.

```
netapp/controller:24.10.1
netapp/restic:24.10.1
netapp/kopia:24.10.1
netapp/trident-autosupport:24.10.0
netapp/execheek:24.10.1
netapp/resourcebackup:24.10.1
netapp/resourcerestore:24.10.1
netapp/resourcedelete:24.10.1
bitnami/kubectl:1.30.2
kubebuilder/kube-rbac-proxy:v0.16.0
```

예를 들면 다음과 같습니다.

```
docker pull netapp/controller:24.10.1
```

```
docker tag netapp/controller:24.10.1 <private-registry-
url>/controller:24.10.1
```

```
docker push <private-registry-url>/controller:24.10.1
```

2. Trident Protect 시스템 네임스페이스를 생성합니다.

```
kubectl create ns trident-protect
```

3. 레지스트리에 로그인합니다.

```
helm registry login <private-registry-url> -u <account-id> -p <api-
token>
```

4. 개인 레지스트리 인증에 사용할 풀 암호를 만듭니다.

```
kubectl create secret docker-registry regcred --docker
-username=<registry-username> --docker-password=<api-token> -n
trident-protect --docker-server=<private-registry-url>
```

5. Trident Helm 저장소 추가:

```
helm repo add netapp-trident-protect
https://netapp.github.io/trident-protect-helm-chart
```

6. 라는 이름의 파일을 `protectValues.yaml` 만듭니다. Trident Protect에 다음 설정이 포함되어 있는지 확인합니다.

```
---
image:
  registry: <private-registry-url>
imagePullSecrets:
  - name: regcred
controller:
  image:
    registry: <private-registry-url>
rbacProxy:
  image:
    registry: <private-registry-url>
crCleanup:
  imagePullSecrets:
    - name: regcred
webhooksCleanup:
  imagePullSecrets:
    - name: regcred
```

7. Trident Protect CRD를 설치합니다.

```
helm install trident-protect-crds netapp-trident-protect/trident-protect-crds --version 100.2410.1 --create-namespace --namespace trident-protect
```

8. Helm을 사용하여 다음 명령 중 하나를 사용하여 Trident Protect를 설치합니다. 클러스터에 할당되고 클러스터의 백업 및 스냅샷을 식별하는 데 사용되는 클러스터 이름으로 바꿉니다 `<name_of_cluster>`.

- Trident Protect를 정상적으로 설치합니다.

```
helm install trident-protect netapp-trident-protect/trident-protect --set clusterName=<name_of_cluster> --version 100.2410.1 --create-namespace --namespace trident-protect -f protectValues.yaml
```

- Trident Protect를 설치하고 예약된 일일 Trident Protect AutoSupport 지원 번들 업로드를 비활성화합니다.

```
helm install trident-protect netapp-trident-protect/trident-protect --set autoSupport.enabled=false --set clusterName=<name_of_cluster> --version 100.2410.1 --create --namespace --namespace trident-protect -f protectValues.yaml
```

Trident Protect 컨테이너 리소스 제한을 지정합니다

Trident Protect를 설치한 후 구성 파일을 사용하여 Trident Protect 컨테이너에 대한 리소스 제한을 지정할 수 있습니다. 리소스 제한을 설정하면 Trident Protect 작업에서 사용되는 클러스터 리소스의 양을 제어할 수 있습니다.

단계

1. 라는 이름의 파일을 resourceLimits.yaml 만듭니다.
2. 환경 요구 사항에 따라 Trident Protect 컨테이너에 대한 리소스 제한 옵션을 파일에 채웁니다.

다음 예제 구성 파일은 사용 가능한 설정을 보여 주며 각 리소스 제한에 대한 기본 values를 포함합니다.

```
---
jobResources:
  defaults:
    limits:
      cpu: 8000m
      memory: 10000Mi
      ephemeralStorage: ""
    requests:
      cpu: 100m
      memory: 100Mi
      ephemeralStorage: ""
  resticVolumeBackup:
    limits:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
    requests:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
  resticVolumeRestore:
    limits:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
    requests:
      cpu: ""
```

```

    memory: ""
    ephemeralStorage: ""
kopiaVolumeBackup:
  limits:
    cpu: ""
    memory: ""
    ephemeralStorage: ""
  requests:
    cpu: ""
    memory: ""
    ephemeralStorage: ""
kopiaVolumeRestore:
  limits:
    cpu: ""
    memory: ""
    ephemeralStorage: ""
  requests:
    cpu: ""
    memory: ""
    ephemeralStorage: ""

```

3. 파일의 값을 적용합니다 resourceLimits.yaml.

```

helm upgrade trident-protect -n trident-protect -f <resourceLimits.yaml>
--reuse-values

```

Trident Protect CLI 플러그인을 설치합니다

Trident 유틸리티의 확장인 Trident Protect 명령줄 플러그인을 사용하여 Trident CRS(사용자 지정 리소스)를 만들고 상호 작용할 수 있습니다 tridentctl.

Trident Protect CLI 플러그인을 설치합니다

명령줄 유틸리티를 사용하기 전에 클러스터에 액세스하는 데 사용하는 시스템에 설치해야 합니다. 컴퓨터에서 x64 또는 ARM CPU를 사용하는지 여부에 따라 다음 단계를 수행합니다.

Linux AMD64 CPU용 플러그인을 다운로드합니다

단계

1. Trident Protect CLI 플러그인 다운로드:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-protect-linux-amd64
```

Linux ARM64 CPU용 플러그인을 다운로드합니다

단계

1. Trident Protect CLI 플러그인 다운로드:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-protect-linux-arm64
```

Mac AMD64 CPU용 플러그인을 다운로드합니다

단계

1. Trident Protect CLI 플러그인 다운로드:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-protect-macos-amd64
```

Mac ARM64 CPU용 플러그인을 다운로드합니다

단계

1. Trident Protect CLI 플러그인 다운로드:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-protect-macos-arm64
```

1. 플러그인 바이너리에 대한 실행 권한 활성화:

```
chmod +x tridentctl-protect
```

2. PATH 변수에 정의된 위치에 플러그인 바이너리를 복사합니다. 예를 /usr/bin 들어, 또는 /usr/local/bin (Elevated Privileges가 필요할 수 있음):

```
cp ./tridentctl-protect /usr/local/bin/
```

3. 선택적으로 플러그인 바이너리를 홈 디렉토리의 위치로 복사할 수 있습니다. 이 경우 위치가 PATH 변수의 일부인지 확인하는 것이 좋습니다.

```
cp ./tridentctl-protect ~/bin/
```



PATH 변수의 위치에 플러그인을 복사하면 또는 `tridentctl protect` 임의의 위치에서 플러그인을 사용할 수 `tridentctl-protect` 있습니다.

Trident CLI 플러그인 도움말을 봅니다

내장 플러그인 도움말 기능을 사용하여 플러그인 기능에 대한 자세한 도움말을 얻을 수 있습니다.

단계

1. 도움말 기능을 사용하여 사용 지침을 봅니다.

```
tridentctl-protect help
```

명령 자동 완성 활성화

Trident Protect CLI 플러그인을 설치한 후 특정 명령에 대해 자동 완성 기능을 활성화할 수 있습니다.

Bash 셸에 대해 자동 완성 기능을 활성화합니다

단계

1. 완료 스크립트 다운로드:

```
curl -L -O https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-completion.bash
```

2. 스크립트를 포함할 홈 디렉토리에 새 디렉토리를 만듭니다.

```
mkdir -p ~/.bash/completions
```

3. 다운로드한 스크립트를 디렉터리로 이동합니다 ~/.bash/completions.

```
mv tridentctl-completion.bash ~/.bash/completions/
```

4. 홈 디렉토리의 파일에 다음 줄을 추가합니다 ~/.bashrc.

```
source ~/.bash/completions/tridentctl-completion.bash
```

Z 셸에 대한 자동 완성 기능을 활성화합니다

단계

1. 완료 스크립트 다운로드:

```
curl -L -O https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-completion.zsh
```

2. 스크립트를 포함할 홈 디렉토리에 새 디렉토리를 만듭니다.

```
mkdir -p ~/.zsh/completions
```

3. 다운로드한 스크립트를 디렉터리로 이동합니다 ~/.zsh/completions.

```
mv tridentctl-completion.zsh ~/.zsh/completions/
```

4. 홈 디렉토리의 파일에 다음 줄을 추가합니다 ~/.zprofile.

```
source ~/.zsh/completions/tridentctl-completion.zsh
```

결과

다음 셸 로그인 시 tridentctl-protect 플러그인으로 명령 자동 완성 기능을 사용할 수 있습니다.

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.