



Installieren Sie Trident Protect

Trident

NetApp
February 05, 2026

This PDF was generated from <https://docs.netapp.com/de-de/trident-2410/trident-protect/trident-protect-requirements.html> on February 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

Installieren Sie Trident Protect	1
Anforderungen von Trident Protect	1
Trident Protect Kubernetes-Clusterkompatibilität	1
Kompatibilität des Trident Protect-Speicher-Backends	1
Anforderungen für nas-Economy-Volumen	2
Datensicherung mit KubeVirt VMs	2
Anforderungen für die SnapMirror-Replizierung	3
Trident Protect installieren und konfigurieren	4
Installieren Sie Trident Protect	4
Legen Sie die Ressourcenbeschränkungen für Trident Protect-Container fest.	8
Installieren Sie das Trident Protect CLI-Plugin	9
Installieren Sie das Trident Protect CLI-Plugin	9
Trident CLI Plug-in-Hilfe ansehen	11
Aktivieren Sie die automatische Vervollständigung von Befehlen	11

Installieren Sie Trident Protect

Anforderungen von Trident Protect

Beginnen Sie mit der Überprüfung der Einsatzbereitschaft Ihrer Betriebsumgebung, Anwendungscluster, Anwendungen und Lizenzen. Stellen Sie sicher, dass Ihre Umgebung diese Anforderungen erfüllt, um Trident Protect bereitstellen und betreiben zu können.

Trident Protect Kubernetes-Clusterkompatibilität

Trident Protect ist mit einer Vielzahl von vollständig verwalteten und selbstverwalteten Kubernetes-Angeboten kompatibel, darunter:

- Amazon Elastic Kubernetes Service (EKS)
- Google Kubernetes Engine (GKE)
- Microsoft Azure Kubernetes Service (AKS)
- Red hat OpenShift
- SUSE Rancher
- VMware Tanzu Portfolio
- Vorgelagerte Kubernetes-Systeme



Stellen Sie sicher, dass der Cluster, auf dem Sie Trident Protect installieren, mit einem laufenden Snapshot-Controller und den zugehörigen CRDs konfiguriert ist. Informationen zur Installation eines Snapshot-Controllers finden Sie unter ["Diese Anweisungen"](#).

Kompatibilität des Trident Protect-Speicher-Backends

Trident Protect unterstützt die folgenden Speichersysteme:

- Amazon FSX für NetApp ONTAP
- Cloud Volumes ONTAP
- ONTAP Storage-Arrays
- Google Cloud NetApp Volumes
- Azure NetApp Dateien

Stellen Sie sicher, dass Ihr Storage-Back-End die folgenden Anforderungen erfüllt:

- Vergewissern Sie sich, dass mit dem Cluster verbundener NetApp-Storage Astra Trident 24.02 oder neuer verwendet (Trident 24.10 wird empfohlen).
 - Wenn Astra Trident älter als die Version 24.06.1 ist und Sie die Disaster-Recovery-Funktion von NetApp SnapMirror nutzen möchten, müssen Sie die Astra Control Provisioner manuell aktivieren.
- Stellen Sie sicher, dass Sie über die neueste Astra Control Provisioner-Version verfügen (standardmäßig installiert und aktiviert ab Astra Trident 24.06.1).
- Stellen Sie sicher, dass Sie über ein NetApp ONTAP Storage-Back-End verfügen.

- Stellen Sie sicher, dass Sie einen Objekt-Storage-Bucket zum Speichern von Backups konfiguriert haben.
- Erstellen Sie alle Anwendungs-Namespace, die Sie für Anwendungen oder Anwendungsdatenverwaltungsvorgänge verwenden möchten. Trident Protect erstellt diese Namespaces nicht für Sie; wenn Sie in einer benutzerdefinierten Ressource einen nicht existierenden Namespace angeben, schlägt der Vorgang fehl.

Anforderungen für nas-Economy-Volumen

Trident Protect unterstützt Backup- und Wiederherstellungsvorgänge auf nas-economy-Volumes. Snapshots, Klone und die SnapMirror Replikation auf nas-economy-Volumes werden derzeit nicht unterstützt. Sie müssen für jedes NAS-Economy-Volume, das Sie mit Trident Protect verwenden möchten, ein Snapshot-Verzeichnis aktivieren.



Einige Anwendungen sind nicht mit Volumes kompatibel, die ein Snapshot-Verzeichnis verwenden. Für diese Anwendungen müssen Sie das Snapshot-Verzeichnis ausblenden, indem Sie den folgenden Befehl auf dem ONTAP-Speichersystem ausführen:

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

Sie können das Snapshot-Verzeichnis aktivieren, indem Sie den folgenden Befehl für jedes nas-Economy-Volume ausführen und durch die UUID des Volumes ersetzen <volume-UUID>, das Sie ändern möchten:

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



Sie können Snapshot-Verzeichnisse standardmäßig für neue Volumes aktivieren, indem Sie die Trident-Backend-Konfigurationsoption auf true setzen snapshotDir. Vorhandene Volumes werden nicht beeinträchtigt.

Datensicherung mit KubeVirt VMs

Trident Protect 24.10 und 24.10.1 sowie neuere Versionen verhalten sich unterschiedlich, wenn Sie Anwendungen schützen, die auf KubeVirt VMs ausgeführt werden. Bei beiden Versionen können Sie das Einfrieren und Auftauen des Dateisystems während Datensicherungsvorgängen aktivieren oder deaktivieren.



Bei allen Trident Protect-Versionen müssen Sie möglicherweise dem Anwendungs-Namespace privilegierte Berechtigungen erteilen, um die automatische Einfrierfunktion in OpenShift-Umgebungen zu aktivieren oder zu deaktivieren. Beispiel:

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

Trident Protect 24.10

Trident Protect 24.10 gewährleistet nicht automatisch einen konsistenten Zustand der KubeVirt VM-Dateisysteme während Datensicherungsvorgängen. Wenn Sie Ihre KubeVirt VM-Daten mit Trident Protect 24.10 schützen möchten, müssen Sie die Freeze/Unfreeze-Funktionalität für die Dateisysteme vor dem

Datensicherungsvorgang manuell aktivieren. Dadurch wird sichergestellt, dass sich die Dateisysteme in einem konsistenten Zustand befinden.

Sie können Trident Protect 24.10 so konfigurieren, dass das Einfrieren und Auftauen des VM-Dateisystems während Datensicherungsvorgängen verwaltet wird, indem "[Konfiguration der Virtualisierung](#)" und anschließend mit folgendem Befehl:

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

Trident Protect 24.10.1 und neuer

Ab Trident Protect 24.10.1 friert Trident Protect KubeVirt-Dateisysteme während Datensicherungsoperationen automatisch ein und taut sie wieder auf. Optional können Sie dieses automatische Verhalten mit dem folgenden Befehl deaktivieren:

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

Anforderungen für die SnapMirror-Replizierung

NetApp SnapMirror ist für die Verwendung mit Trident Protect für die folgenden ONTAP Lösungen verfügbar:

- NetApp ASA
- NetApp AFF
- NetApp FAS
- NetApp ONTAP Select
- NetApp Cloud Volumes ONTAP
- Amazon FSX für NetApp ONTAP

ONTAP-Cluster-Anforderungen für die SnapMirror-Replizierung

Stellen Sie sicher, dass Ihr ONTAP Cluster die folgenden Anforderungen erfüllt, wenn Sie SnapMirror Replizierung nutzen möchten:

- *** Astra Control Provisioner oder Trident***: Astra Control Provisioner oder Trident muss sowohl auf dem Quell- als auch auf dem Ziel-Kubernetes-Cluster vorhanden sein, die ONTAP als Backend verwenden. Trident Protect unterstützt die Replikation mit der NetApp SnapMirror Technologie unter Verwendung von Speicherklassen, die von den folgenden Treibern unterstützt werden:
 - ontap-nas
 - ontap-san
- **Lizenzen**: Asynchrone Lizenzen von ONTAP SnapMirror, die das Datensicherungspaket verwenden, müssen sowohl auf den Quell- als auch auf den Ziel-ONTAP-Clustern aktiviert sein. Weitere Informationen finden Sie unter "[Übersicht über die SnapMirror Lizenzierung in ONTAP](#)".

Peering-Überlegungen für die SnapMirror-Replizierung

Stellen Sie sicher, dass Ihre Umgebung die folgenden Anforderungen erfüllt, wenn Sie Storage-Back-End-Peering verwenden möchten:

- **Cluster und SVM:** Die ONTAP Speicher-Back-Ends müssen aktiviert werden. Weitere Informationen finden Sie unter ["Übersicht über Cluster- und SVM-Peering"](#).



Vergewissern Sie sich, dass die in der Replizierungsbeziehung zwischen zwei ONTAP-Clustern verwendeten SVM-Namen eindeutig sind.

- **Astra Control Provisioner oder Trident und SVM:** Die Remote-SVMs müssen für die Astra Control Bereitstellung oder die Trident im Ziel-Cluster verfügbar sein.
- **Verwaltete Backends:** Sie müssen ONTAP -Speicher-Backends in Trident Protect hinzufügen und verwalten, um eine Replikationsbeziehung herzustellen.
- **NVMe über TCP:** Trident Protect unterstützt keine NetApp SnapMirror Replikation für Speicher-Backends, die das NVMe-over-TCP-Protokoll verwenden.

Trident/ONTAP-Konfiguration für SnapMirror-Replikation

Trident Protect erfordert, dass Sie mindestens ein Storage-Backend konfigurieren, das die Replikation sowohl für den Quell- als auch für den Zielcluster unterstützt. Wenn Quell- und Zielcluster identisch sind, sollte die Zielanwendung für eine optimale Ausfallsicherheit ein anderes Speichersystem als die Quellanwendung verwenden.

Trident Protect installieren und konfigurieren

Wenn Ihre Umgebung die Anforderungen für Trident Protect erfüllt, können Sie die folgenden Schritte befolgen, um Trident Protect auf Ihrem Cluster zu installieren. Sie können Trident Protect von NetApp beziehen oder es aus Ihrer eigenen privaten Registry installieren. Die Installation aus einer privaten Registry ist hilfreich, wenn Ihr Cluster keinen Internetzugang hat.



Standardmäßig erfasst Trident Protect Supportinformationen, die bei der Bearbeitung von NetApp Supportfällen hilfreich sind, darunter Protokolle, Metriken und Topologieinformationen zu Clustern und verwalteten Anwendungen. Trident Protect sendet diese Support-Pakete täglich an NetApp. Sie können diese Support-Bundle-Sammlung optional deaktivieren, wenn Sie Trident Protect installieren. Sie können manuell ["Generieren Sie ein Support-Bundle"](#) jederzeit.

Installieren Sie Trident Protect

Installieren Sie Trident Protect von NetApp

Schritte

1. Trident Helm Repository hinzufügen:

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

2. Installieren Sie die Trident Protect CRDs:

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

3. Verwenden Sie Helm, um Trident Protect mit einem der folgenden Befehle zu installieren. Ersetzen `<name_of_cluster>` mit einem Clusternamen, der dem Cluster zugewiesen wird und zur Identifizierung der Backups und Snapshots des Clusters verwendet wird:

- Installieren Sie Trident Protect wie gewohnt:

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

- Installieren Sie Trident Protect und deaktivieren Sie die geplanten täglichen Uploads des Trident Protect AutoSupport Supportpakets:

```
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
```

Installieren Sie Trident Protect aus einer privaten Registry.

Sie können Trident Protect aus einer privaten Image-Registry installieren, wenn Ihr Kubernetes-Cluster keinen Zugriff auf das Internet hat. Ersetzen Sie in diesen Beispielen die Werte in Klammern durch Informationen aus Ihrer Umgebung:

Schritte

1. Ziehen Sie die folgenden Bilder auf Ihren lokalen Computer, aktualisieren Sie die Tags und schieben Sie sie dann in Ihre private Registrierung:

```
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
```

Beispiel:

```
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. Erstellen Sie den Trident Protect-Systemnamensraum:

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

3. Melden Sie sich bei der Registrierung an:

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

4. Erstellen Sie einen Pull-Schlüssel, der für die Authentifizierung der privaten Registrierung verwendet werden soll:

```
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 Repository hinzufügen:


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

6. Erstellen Sie eine Datei mit dem Namen `protectValues.yaml`. Stellen Sie sicher, dass es die folgenden Trident Protect-Einstellungen enthält:

```
---  
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. Installieren Sie die Trident Protect CRDs:

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

8. Verwenden Sie Helm, um Trident Protect mit einem der folgenden Befehle zu installieren. Ersetzen `<name_of_cluster>` mit einem Clusternamen, der dem Cluster zugewiesen wird und zur Identifizierung der Backups und Snapshots des Clusters verwendet wird:

- Installieren Sie Trident Protect wie gewohnt:

```
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
```

- Installieren Sie Trident Protect und deaktivieren Sie die geplanten täglichen Uploads des Trident Protect AutoSupport Supportpakets:

```
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
```

Legen Sie die Ressourcenbeschränkungen für Trident Protect-Container fest.

Sie können nach der Installation von Trident Protect eine Konfigurationsdatei verwenden, um Ressourcenlimits für Trident Protect-Container festzulegen. Durch das Festlegen von Ressourcenlimits können Sie steuern, wie viele der Clusterressourcen von Trident Protect-Operationen verbraucht werden.

Schritte

1. Erstellen Sie eine Datei mit dem Namen `resourceLimits.yaml`.
2. Füllen Sie die Datei mit Ressourcenlimitierungsoptionen für Trident Protect-Container entsprechend den Anforderungen Ihrer Umgebung.

Die folgende Beispielkonfigurationsdatei zeigt die verfügbaren Einstellungen und enthält die Standardvaules für jedes Ressourcenlimit:

```
---
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. Anwenden der Werte aus der `resourceLimits.yaml` Datei:

```

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

```

Installieren Sie das Trident Protect CLI-Plugin.

Sie können das Trident Protect-Befehlszeilen-Plugin verwenden, das eine Erweiterung von Trident ist. `tridentctl` Hilfsprogramm zum Erstellen und Interagieren mit benutzerdefinierten Ressourcen (CRs) von Trident Protect.

Installieren Sie das Trident Protect CLI-Plugin.

Bevor Sie das Befehlszeilendienstprogramm verwenden, müssen Sie es auf dem Computer installieren, mit dem Sie auf das Cluster zugreifen. Befolgen Sie diese Schritte, je nachdem, ob Ihr Computer eine x64- oder ARM-CPU verwendet.

Download Plugin für Linux AMD64 CPUs

Schritte

1. Laden Sie das Trident Protect CLI-Plugin herunter:

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

Download Plugin für Linux ARM64 CPUs

Schritte

1. Laden Sie das Trident Protect CLI-Plugin herunter:

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

Download Plugin für Mac AMD64 CPUs

Schritte

1. Laden Sie das Trident Protect CLI-Plugin herunter:

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

Download Plugin für Mac ARM64 CPUs

Schritte

1. Laden Sie das Trident Protect CLI-Plugin herunter:

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

1. Ausführungsberechtigungen für die Plug-in-Binärdatei aktivieren:

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

2. Kopieren Sie die Plugin-Binärdatei an einen Speicherort, der in Ihrer PFADVARIABLE definiert ist. Beispiel /usr/bin: Oder /usr/local/bin (Sie benötigen möglicherweise erhöhte Privileges):

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

3. Optional können Sie die Plugin-Binärdatei an einen Speicherort in Ihrem Home-Verzeichnis kopieren. In diesem Fall wird empfohlen, sicherzustellen, dass der Speicherort Teil Ihrer PFADVARIABLE ist:

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



Das Kopieren des Plugins an einen Ort in Ihrer PFADVARIABLE ermöglicht es Ihnen, das Plugin durch Eingabe oder `tridentctl protect` von einem beliebigen Ort zu verwenden `tridentctl-protect`.

Trident CLI Plug-in-Hilfe ansehen

Sie können die integrierten Plug-in-Hilfefunktionen nutzen, um detaillierte Hilfe zu den Funktionen des Plug-ins zu erhalten:

Schritte

1. Verwenden Sie die Hilfefunktion, um die Verwendungshilfe anzuzeigen:

```
tridentctl-protect help
```

Aktivieren Sie die automatische Vervollständigung von Befehlen

Nach der Installation des Trident Protect CLI-Plugins können Sie die automatische Vervollständigung für bestimmte Befehle aktivieren.

Aktivieren Sie die automatische Vervollständigung für die Bash-Shell

Schritte

1. Download des Abschlussskripts:

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

2. Erstellen Sie ein neues Verzeichnis in Ihrem Home-Verzeichnis, um das Skript zu enthalten:

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

3. Das heruntergeladene Skript in das Verzeichnis verschieben ~/.bash/completions:

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

4. Fügen Sie der Datei im Home-Verzeichnis folgende Zeile hinzu ~/.bashrc:

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

Aktivieren Sie die automatische Vervollständigung für die Z-Shell

Schritte

1. Download des Abschlussskripts:

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

2. Erstellen Sie ein neues Verzeichnis in Ihrem Home-Verzeichnis, um das Skript zu enthalten:

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

3. Das heruntergeladene Skript in das Verzeichnis verschieben ~/.zsh/completions:

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

4. Fügen Sie der Datei im Home-Verzeichnis folgende Zeile hinzu ~/.zprofile:

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

Ergebnis

Bei Ihrer nächsten Shell-Anmeldung können Sie den Befehl Auto-Vervollständigung mit dem tridentctl-Protect-Plugin verwenden.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.