Die FPolicy Konfiguration erstellen

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nas-audit/create-fpolicy-external-engine-task.html on November 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

Die FPolicy Konfiguration erstellen . . . 1
- ONTAP FPolicy externe Engines erstellen . . . 1
- ONTAP FPolicy-Ereignisse erstellen . . . 2
  - Das FPolicy Ereignis erstellen . . . 2
  - Die FPolicy Access Denied-Ereignisse erstellen . . . 3
- ONTAP FPolicy persistente Speicher erstellen . . . 3
  - Persistenten Speicher erstellen (ONTAP 9.15.1 oder höher) . . . 3
  - Erstellen eines persistenten Speichers (ONTAP 9.14.1) . . . 4
- ONTAP FPolicy-Richtlinien erstellen . . . 5
- ONTAP FPolicy-Bereiche erstellen . . . 7
- ONTAP FPolicy Richtlinien aktivieren . . . 8

Die FPolicy Konfiguration erstellen

ONTAP FPolicy externe Engines erstellen

Sie müssen eine externe Engine erstellen, um mit der Erstellung einer FPolicy-Konfiguration zu beginnen. Die externe Engine definiert, wie FPolicy Verbindungen zu externen FPolicy-Servern herstellt und verwaltet. Wenn Ihre Konfiguration die interne ONTAP Engine (die native externe Engine) für einfaches Dateiblockieren verwendet, ist keine separate FPolicy externe Engine zu konfigurieren und dieser Schritt ist nicht erforderlich.

Bevor Sie beginnen

Das "externe Engine" Arbeitsblatt sollte ausgefüllt werden.

Über diese Aufgabe

Wenn die externe Engine in einer MetroCluster Konfiguration verwendet wird, sollten die IP-Adressen der FPolicy-Server am Quellstandort als primäre Server angegeben werden. Die IP-Adressen der FPolicy-Server am Zielstandort sollten als sekundäre Server angegeben werden.

Schritte

1. Die externe FPolicy Engine wird mit dem `vserver fpolicy policy external-engine create` Befehl erstellt.

   Der folgende Befehl erstellt eine externe Engine auf der Storage Virtual Machine (SVM) vs1.example.com. Für die externe Kommunikation mit dem FPolicy Server ist keine Authentifizierung erforderlich.

   ```
   vserver fpolicy policy external-engine create -vserver vs1.example.com -engine
   -name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option no-
   auth
   ```

2. Die Konfiguration der externen FPolicy Engine kann mithilfe des `vserver fpolicy policy external-engine show` Befehls überprüft werden.

   Der folgende Befehl zeigt Informationen über alle auf SVM vs1.example.com konfigurierten externen Engines an:

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                Primary         Secondary
   External
   Vserver             Engine   Servers         Servers        Port Engine
   Type
   ----------------    ---------- --------------- ----------- ------
   -----------
   vs1.example.com     engine1  10.1.1.2,       -              6789
   synchronous
                                10.1.1.3
   ```

Der folgende Befehl zeigt detaillierte Informationen über die externe Engine mit dem Namen “engine1” auf SVM vs1.example.com an:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
-name engine1
```

```
                            Vserver: vs1.example.com
                             Engine: engine1
              Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
       Port Number of FPolicy Service: 6789
            Secondary FPolicy Servers: -
                 External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
               Certificate Authority: -
```

ONTAP FPolicy-Ereignisse erstellen

Im Rahmen der Erstellung einer FPolicy Richtlinienkonfiguration ist ein FPolicy Ereignis zu erstellen. Das Ereignis wird mit der FPolicy Richtlinie verknüpft, wenn diese erstellt wird. Ein Ereignis legt fest, welches Protokoll überwacht wird und welche Dateizugriffsereignisse überwacht und gefiltert werden.

Bevor Sie beginnen

Das FPolicy-Ereignis sollte abgeschlossen werden "Arbeitsblatt".

Das FPolicy Ereignis erstellen

1. Das FPolicy Ereignis wird mit dem `vserver fpolicy policy event create` Befehl erstellt.

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. Die FPolicy Ereigniskonfiguration kann mit dem `vserver fpolicy policy event show` Befehl überprüft werden.

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                    Event               File                      Is Volume
   Vserver          Name      Protocols Operations    Filters     Operation
   ---------------  --------- --------- ------------- ---------
   ------------
   vs1.example.com  event1    cifs      open, close,  -           false
                                        read, write
   ```

Die FPolicy Access Denied-Ereignisse erstellen

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen über fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen erhalten. Diese Benachrichtigungen sind wertvoll für Sicherheit, Ransomware-Schutz und Governance.

1. Das FPolicy Ereignis wird mit dem `vserver fpolicy policy event create` Befehl erstellt.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

ONTAP FPolicy persistente Speicher erstellen

Persistente Speicher können die Client-E/A-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu reduzieren. Ab ONTAP 9.14.1 ermöglicht FPolicy die Einrichtung von "persistente Speicher" zum Erfassen von Dateizugriffsereignissen für asynchrone, nicht obligatorische Richtlinien in der SVM. Synchrone (obligatorische oder nicht obligatorische) und asynchron obligatorische Konfigurationen werden nicht unterstützt.

Ab ONTAP 9.15.1 ist die Konfiguration des persistenten Speichers mit FPolicy vereinfacht. Der `persistent-store create` Befehl automatisiert die Volume-Erstellung für die SVM und konfiguriert das Volume für den persistenten Store.

Es gibt zwei Möglichkeiten, einen persistenten Speicher zu erstellen, abhängig von der ONTAP-Version:

- ONTAP 9.15.1 oder höher: Beim Erstellen des persistenten Speichers erstellt und konfiguriert ONTAP automatisch gleichzeitig dessen Volume. Dies vereinfacht die FPolicy Persistent Store Konfiguration und implementiert alle Best Practices.
- ONTAP 9.14.1: Manuelles Erstellen und Konfigurieren eines Volumes und anschließendes Erstellen eines persistenten Speichers für das neu erstellte Volume.

Auf jeder SVM kann nur ein persistenter Speicher eingerichtet werden. Dieser einzelne persistente Speicher muss für alle FPolicy Konfigurationen auf dieser SVM verwendet werden, selbst wenn die Richtlinien von verschiedenen Partnern stammen.

Persistenten Speicher erstellen (ONTAP 9.15.1 oder höher)

Ab ONTAP 9.15.1 kann der `fpolicy persistent-store create` Befehl verwendet werden, um den FPolicy persistenten Store mit Inline-Volume-Erstellung und -Konfiguration zu erstellen. ONTAP blockiert automatisch den Volume-Zugriff über externe Benutzerprotokolle (CIFS/NFS).

Bevor Sie beginnen

- Die SVM, in der der persistente Speicher erstellt werden soll, muss mindestens ein Aggregat haben.
- Sie sollten Zugriff auf die für die SVM verfügbaren Aggregate und ausreichende Berechtigungen zum Erstellen von Volumes haben.

Schritte

1. Der persistente Speicher wird erstellt, wobei das Volume automatisch erstellt und konfiguriert wird:

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
```

```
<name> -volume <volume_name> -size <size> -autosize-mode
<off|grow|grow_shrink>
```

- Der `vserver` Parameter ist der Name der SVM.
- Der `persistent-store` Parameter ist der Name des persistenten Speichers.
- Der `volume` Parameter ist der Name des persistenten Speichervolumes.

> Wenn Sie ein vorhandenes, leeres Volume verwenden möchten, verwenden Sie den `volume show` Befehl, um es zu finden und im Volume-Parameter anzugeben.

- Der `size`Parameter basiert auf der Zeitdauer, für die die Ereignisse gespeichert werden sollen, die nicht an den externen Server (Partneranwendung) übermittelt werden.

  Wenn beispielsweise Ereignisse der letzten 30 Minuten in einem Cluster mit einer Kapazität von 30.000 Benachrichtigungen pro Sekunde erhalten bleiben sollen:

  Erforderliche Volume-Größe = 30000 x 30 x 60 x 0,6 KB (durchschnittliche Größe eines Benachrichtigungsdatensatzes) = 32400000 KB = ~32 GB

  Um die ungefähre Benachrichtigungsrate zu ermitteln, können Sie entweder Ihre FPolicy Partneranwendung kontaktieren oder den FPolicy Zähler verwenden `requests_dispatched_rate`.

> Wenn Sie ein vorhandenes Volume verwenden, ist der Größenparameter optional. Wenn Sie einen Wert für den Größenparameter angeben, wird das Volume mit der von Ihnen angegebenen Größe geändert.

- Der `autosize-mode`Parameter gibt den Modus für die automatische Größenanpassung des Volumes an. Die unterstützten Modi für die automatische Größenanpassung sind:
  - Aus - Das Volumen wächst oder schrumpft nicht in der Größe in Abhängigkeit vom genutzten Speicherplatz.
  - wachsen - Das Volumen wird automatisch vergrößert, wenn der belegte Speicherplatz im Volumen über dem Wachstumsschwellenwert liegt.
  - grow_shrink - Das Volumen vergrößert oder verkleinert sich in Abhängigkeit vom genutzten Speicherplatz.

2. Die FPolicy Richtlinie wird erstellt und der Name des persistenten Speichers zu dieser Richtlinie hinzugefügt. Weitere Informationen finden sich unter "Die FPolicy Richtlinie erstellen".

Erstellen eines persistenten Speichers (ONTAP 9.14.1)

Sie können ein Volume erstellen und anschließend einen persistenten Speicher einrichten, der dieses Volume nutzt. Anschließend kann der Zugriff externer Benutzerprotokolle (CIFS/NFS) auf das neu erstellte Volume gesperrt werden.

Schritte

1. Ein leeres Volume auf der SVM erstellen, das für den persistenten Speicher bereitgestellt werden kann:

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
-snapshot-policy <none>
```

Es wird erwartet, dass ein Administratorbenutzer mit ausreichenden RBAC-Berechtigungen (zum Erstellen eines Volumes) ein Volume (mittels des CLI-Befehls volume oder der REST-API) in der gewünschten Größe erstellt und den Namen dieses Volumes als `-volume` im CLI-Befehl persistent store create oder in der REST-API angibt.

- Der `vserver` Parameter ist der Name der SVM.
- Der `volume` Parameter ist der Name des persistenten Speichervolumes.
- Der `state`Parameter sollte auf „online“ eingestellt werden, damit das Volume verfügbar ist.
- Der `policy` Parameter wird auf die FPolicy Service-Richtlinie gesetzt, sofern bereits eine konfiguriert ist. Falls nicht, kann die `volume modify` Richtlinie später mit dem Befehl hinzugefügt werden.
- Der `unix-permissions` Parameter ist optional.
- Der `size`Parameter basiert auf der Zeitdauer, für die die Ereignisse gespeichert werden sollen, die nicht an den externen Server (Partneranwendung) übermittelt werden.

  Wenn beispielsweise Ereignisse der letzten 30 Minuten in einem Cluster mit einer Kapazität von 30.000 Benachrichtigungen pro Sekunde erhalten bleiben sollen:

  Erforderliche Volume-Größe = 30000 x 30 x 60 x 0,6 KB (durchschnittliche Größe eines Benachrichtigungsdatensatzes) = 32400000 KB = ~32 GB

Um die ungefähre Benachrichtigungsrate zu ermitteln, können Sie entweder Ihre FPolicy Partneranwendung kontaktieren oder den FPolicy Zähler verwenden `requests_dispatched_rate`.

- Der Aggregatparameter wird für FlexVol Volumes benötigt, ansonsten ist er nicht erforderlich.
- Der `snapshot-policy` Parameter muss auf „none“ gesetzt werden. Dadurch ist sichergestellt, dass keine versehentliche Wiederherstellung des Snapshots erfolgt, die zum Verlust aktueller Ereignisse führen und eine mögliche doppelte Ereignisverarbeitung verhindern könnte.

  Wenn ein vorhandenes, leeres Volume verwendet werden soll, kann der `volume show` Befehl genutzt werden, um es zu finden, und der `volume modify` Befehl, um die erforderlichen Änderungen vorzunehmen. Es ist sicherzustellen, dass Richtlinie, Größe und `snapshot-policy` Parameter für den persistenten Speicher korrekt eingestellt sind.

2. Den persistenten Speicher erstellen:

   ```
   vserver fpolicy persistent store create -vserver <SVM> -persistent-store
   <PS_name> -volume <volume>
   ```

   - Der `vserver` Parameter ist der Name der SVM.
   - Der `persistent-store` Parameter ist der Name des persistenten Speichers.
   - Der `volume` Parameter ist der Name des persistenten Speichervolumes.
3. Die FPolicy Richtlinie wird erstellt und der Name des persistenten Speichers zu dieser Richtlinie hinzugefügt. Weitere Informationen finden sich unter "Die FPolicy Richtlinie erstellen".

ONTAP FPolicy-Richtlinien erstellen

Beim Erstellen der FPolicy Richtlinie wird eine externe Engine und ein oder mehrere Ereignisse mit der Richtlinie verknüpft. Die Richtlinie gibt außerdem an, ob eine

obligatorische Überprüfung erforderlich ist, ob die FPolicy Server privilegierten Zugriff auf Daten auf der Storage Virtual Machine (SVM) haben und ob Passthrough-Read für Offline-Dateien aktiviert ist.

Bevor Sie beginnen

- Das FPolicy Richtlinienarbeitsblatt sollte ausgefüllt werden.
- Wenn die Richtlinie so konfiguriert wird, dass FPolicy Server verwendet werden, muss die externe Engine vorhanden sein.
- Mindestens ein FPolicy-Ereignis, das mit der FPolicy-Richtlinie verknüpft werden soll, muss vorhanden sein.
- Wenn Sie den privilegierten Datenzugriff konfigurieren möchten, muss auf der SVM ein SMB-Server vorhanden sein.
- Um einen persistenten Speicher für eine Richtlinie zu konfigurieren, muss der Engine-Typ **async** sein und die Richtlinie muss **non-mandatory** sein.

  Weitere Informationen finden sich unter "Persistente Speicher erstellen".

- Ab ONTAP 9.20.1 unterstützen FPolicy-Richtlinien S3-Ereignisse, allerdings mit einigen Einschränkungen. FPolicy-Richtlinien mit S3-Ereignissen können Folgendes nicht verwenden:
  - Externe Engine mit aktivierter Ausfallsicherheit
  - Externe Engine mit SSL (Server-Authentifizierung oder gegenseitige Authentifizierung)
  - Externe Engine mit XML-Format
  - Pflichtmodus (-is-mandatory true)
  - Nativ-Engine
  - Persistenter Speicher
  - Privilegierter Zugriff / Passthrough-Lesezugriff
  - Synchrone externe Engine

Schritte

1. Die FPolicy Richtlinie erstellen:

   ```
   vserver fpolicy policy create -vserver <vserver_name> -policy-name
   <policy_name> -engine <engine_name> -events <event_name>[,event_name2,…] [-
   persistent-store <PS_name>] [-is-mandatory {true|false}] [-allow-privileged-
   access {yes|no}] [-privileged-user-name <domain\\user_name>] [-is-passthrough-
   read-enabled {true|false}]
   ```

   - Sie können der FPolicy Policy ein oder mehrere durch Kommas getrennte Ereignisse hinzufügen.
   - Standardmäßig ist die obligatorische Überprüfung aktiviert.
   - Wenn privilegierter Zugriff durch Setzen des `-allow-privileged-access` Parameters auf `yes` erlaubt werden soll, muss auch ein privilegierter Benutzername für den privilegierten Zugriff konfiguriert werden.
   - Wenn passthrough-read durch Setzen des `-is-passthrough-read-enabled` Parameters auf `true` konfiguriert werden soll, muss auch der privilegierte Datenzugriff konfiguriert werden.

     Der folgende Befehl erstellt eine Richtlinie mit dem Namen `policy1`, der das Ereignis mit dem Namen

`event1` und die externe Engine mit dem Namen `engine1` zugeordnet sind. Diese Richtlinie verwendet Standardwerte in der Richtlinienkonfiguration: `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

Der folgende Befehl erstellt eine Richtlinie mit dem Namen `policy2`, der das Ereignis mit dem Namen `event2` und die externe Engine mit dem Namen `engine2` zugeordnet sind. Diese Richtlinie ist so konfiguriert, dass privilegierter Zugriff mit dem angegebenen Benutzernamen verwendet wird. Passthrough-Read ist aktiviert:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
-events event2 -engine engine2 -allow-privileged-access yes -privileged-user
-name example\archive_acct -is-passthrough-read-enabled true
```

Der folgende Befehl erstellt eine Richtlinie mit dem Namen `native1`, der das Ereignis `event3` zugeordnet ist. Diese Richtlinie verwendet die native Engine und verwendet Standardwerte in der Richtlinienkonfiguration:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. Die FPolicy Richtlinienkonfiguration kann mit dem `vserver fpolicy policy show` Befehl überprüft werden.

   Der folgende Befehl zeigt Informationen zu den drei konfigurierten FPolicy Richtlinien an, einschließlich der folgenden Informationen:

   - Die mit der Richtlinie verbundene SVM
   - Die externe Engine, die mit der Richtlinie verknüpft ist
   - Die mit der Richtlinie verbundenen Ereignisse
   - Ob eine obligatorische Überprüfung erforderlich ist
   - Ob ein privilegierter Zugriff erforderlich ist `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                       Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

ONTAP FPolicy-Bereiche erstellen

Nach dem Erstellen der FPolicy Richtlinie ist ein FPolicy Bereich zu erstellen. Beim Erstellen des Bereichs wird dieser mit einer FPolicy Richtlinie verknüpft. Ein Bereich definiert die Grenzen, auf die die FPolicy Richtlinie angewendet wird. Bereiche können Dateien basierend auf Freigaben, Exportrichtlinien, Volumes und Dateierweiterungen ein- oder ausschließen.

Ab ONTAP 9.20.1 unterstützt FPolicy die S3-Überwachung. Der Geltungsbereich von S3 FPolicy kann mithilfe dieser Parameter auf bestimmte NAS-Buckets beschränkt werden:

- `-nas-buckets-to-include`
- `-nas-buckets-to-exclude`

Bevor Sie beginnen

Das FPolicy Scope-Arbeitsblatt muss ausgefüllt werden. Die FPolicy Richtlinie muss mit einer zugehörigen externen Engine vorhanden sein (falls die Richtlinie für die Verwendung externer FPolicy Server konfiguriert ist) und mindestens ein zugehöriges FPolicy Ereignis aufweisen.

Schritte

1. Der FPolicy-Bereich wird mithilfe des `vserver fpolicy policy scope create` Befehls erstellt.

   ```
   vserver fpolicy policy scope create -vserver vs1.example.com -policy-name
   policy1 -volumes-to-include datavol1,datavol2
   ```

2. Die FPolicy Bereichskonfiguration kann mit dem `vserver fpolicy policy scope show` Befehl überprüft werden.

   ```
   vserver fpolicy policy scope show -vserver vs1.example.com -instance
   ```

   ```
                       Vserver: vs1.example.com
                        Policy: policy1
             Shares to Include: -
             Shares to Exclude: -
            Volumes to Include: datavol1, datavol2
            Volumes to Exclude: -
   Export Policies to Include: -
   Export Policies to Exclude: -
   File Extensions to Include: -
   File Extensions to Exclude: -
   ```

ONTAP FPolicy Richtlinien aktivieren

Nachdem die Konfiguration einer FPolicy Richtlinie abgeschlossen ist, wird die FPolicy Richtlinie aktiviert. Durch das Aktivieren der Richtlinie werden deren Priorität festgelegt und die Überwachung des Dateizugriffs für die Richtlinie gestartet.

Bevor Sie beginnen

Die FPolicy Richtlinie muss mit einer zugehörigen externen Engine vorhanden sein (falls die Richtlinie für die Verwendung externer FPolicy Server konfiguriert ist) und mindestens ein zugehöriges FPolicy Ereignis aufweisen. Der Gültigkeitsbereich der FPolicy Richtlinie muss vorhanden sein und der FPolicy Richtlinie zugewiesen werden.

Über diese Aufgabe

Die Priorität wird verwendet, wenn mehrere Richtlinien auf der Storage Virtual Machine (SVM) aktiviert sind und mehr als eine Richtlinie dasselbe Dateizugriff-Ereignis abonniert hat. Richtlinien, die die native Engine-

Konfiguration verwenden, haben eine höhere Priorität als Richtlinien für jede andere Engine, unabhängig von der ihnen bei der Aktivierung der Richtlinie zugewiesenen Sequenznummer.

Auf der Admin-SVM kann keine Richtlinie aktiviert werden.

Schritte

1. Die FPolicy Richtlinie wird mit dem `vserver fpolicy enable`Konfigurationsbefehl aktiviert.

   ```
   vserver fpolicy enable -vserver vs1.example.com -policy-name policy1 -sequence
   -number 1
   ```

2. Es kann mit dem `vserver fpolicy show` Befehl überprüft werden, ob die FPolicy Richtlinie aktiviert ist.

   ```
   vserver fpolicy show -vserver vs1.example.com
   ```

   ```
                                    Sequence
   Vserver          Policy Name       Number  Status   Engine
   ---------------  ----------------- --------  -------- ---------
   vs1.example.com  policy1                 1  on       engine1
   ```

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 IRGENDEINER 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.