Die FPolicy Ereigniskonfiguration planen

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nas-audit/plan-fpolicy-event-config-concept.html on November 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

Die FPolicy Ereigniskonfiguration planen . . . 1
- Informationen zur ONTAP FPolicy Ereigniskonfiguration . . . 1
  - Was es bedeutet, ein FPolicy Ereignis zu erstellen . . . 1
  - Was die FPolicy Ereigniskonfiguration enthält . . . 1
- Unterstützte FPolicy Dateioperationen und Filter für SMB in ONTAP . . . 5
- Unterstützte FPolicy Dateioperationen und Filter für NFSv3 in ONTAP . . . 6
- Unterstützte FPolicy Dateioperationen und Filter für NFSv4 in ONTAP . . . 7
- Unterstützte Dateioperationen- und Filterkombinationen, die ONTAP FPolicy für S3 überwacht . . . 9
  - Filterbeschreibungen . . . 9
  - Zusätzliche Überlegungen zu S3 FPolicy Ereignissen . . . 10
- ONTAP FPolicy Ereigniskonfigurationsarbeitsblatt . . . 10

Die FPolicy Ereigniskonfiguration planen

Informationen zur ONTAP FPolicy Ereigniskonfiguration

Bevor Sie FPolicy-Ereignisse konfigurieren, ist es wichtig zu verstehen, was es bedeutet, ein FPolicy-Ereignis zu erstellen. Es sollte festgelegt werden, welche Protokolle das Ereignis überwachen soll, welche Ereignisse überwacht werden und welche Ereignisfilter verwendet werden. Diese Informationen unterstützen die Planung der gewünschten Werte.

Was es bedeutet, ein FPolicy Ereignis zu erstellen

Das Erstellen eines FPolicy-Ereignisses bedeutet, Informationen zu definieren, die der FPolicy-Prozess benötigt, um zu bestimmen, welche Dateizugriffsvorgänge überwacht werden sollen und welche Benachrichtigungen über die überwachten Ereignisse an den externen FPolicy-Server gesendet werden sollen. Die FPolicy-Ereigniskonfiguration definiert die folgenden Konfigurationsinformationen:

- Name der Storage Virtual Machine (SVM)
- Veranstaltungsname
- Zu überwachende Protokolle

  FPolicy kann Dateizugriffsvorgänge über SMB, NFSv3, NFSv4, NFSv4.1 (ab ONTAP 9.15.1) und S3 (ab ONTAP 9.20.1) überwachen.

- Welche Dateivorgänge überwacht werden sollen

  Nicht alle Dateivorgänge sind für jedes Protokoll gültig.

- Welche Dateifilter konfiguriert werden sollten

  Nur bestimmte Kombinationen von Dateivorgängen und Filtern sind gültig. Jedes Protokoll hat seine eigene Menge an unterstützten Kombinationen.

- Ob die Ein- und Aushängevorgänge von Datenträgern überwacht werden

> Es besteht eine Abhängigkeit zwischen drei der Parameter (`-protocol`, `-file-operations`, `-filters`). Die folgenden Kombinationen sind für die drei Parameter gültig:
>
> - Sie können die `-protocol` und `-file-operations` Parameter angeben.
> - Sie können alle drei Parameter angeben.
> - Es kann keiner der Parameter angegeben werden.

Was die FPolicy Ereigniskonfiguration enthält

Die folgende Liste der verfügbaren FPolicy Ereigniskonfigurationsparameter kann bei der Planung der Konfiguration unterstützen:

Art der Information	Option

SVM Gibt den SVM Namen an, der mit diesem FPolicy Ereignis verknüpft werden soll. Jede FPolicy Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienbereich und die Richtlinie, die zusammen eine FPolicy Richtlinienkonfiguration bilden, müssen alle derselben SVM zugeordnet sein.	`-vserver vserver_name`
Ereignisname Gibt den Namen an, der dem FPolicy-Ereignis zugewiesen werden soll. Beim Erstellen der FPolicy Richtlinie wird das FPolicy Ereignis der Richtlinie anhand des Ereignisnamens zugeordnet. Der Name darf maximal 256 Zeichen lang sein. Der Name darf maximal 200 Zeichen lang sein, wenn das Ereignis in einer MetroCluster oder SVM-Notfallwiederherstellungskonfiguration konfiguriert wird. Der Name kann jede beliebige Kombination der folgenden ASCII-Zeichen enthalten: • `a`durch `z` • `A`durch `Z` • `0`durch `9` • "`_`", “-”, and “.”	`-event-name event_name`
Protokoll Gibt an, welches Protokoll für das FPolicy-Ereignis konfiguriert werden soll. Die Liste für `-protocol` kann einen der folgenden Werte enthalten: • `cifs` • `nfsv3` • `nfsv4` • `nfsv4.1` (beginnend mit ONTAP 9.15.1) • `s3`(ab ONTAP 9.20.1) Wenn `-protocol` angegeben wird, muss ein gültiger Wert im `-file-operations` Parameter angegeben werden. Mit Änderungen an der Protokollversion können sich die gültigen Werte ändern.	`-protocol protocol`

Dateioperationen Gibt die Liste der Dateivorgänge für das FPolicy Ereignis an. Das Ereignis prüft die in dieser Liste aufgeführten Operationen aller Clientanfragen, die das im `-protocol` Parameter angegebene Protokoll verwenden. Eine oder mehrere Dateioperationen können als kommagetrennte Liste aufgeführt werden. Die Liste für `-file -operations` kann einen oder mehrere der folgenden Werte enthalten: • `close` für Dateischließungsvorgänge • `create` für Dateierstellungsvorgänge • `create-dir` für Verzeichniserstellungsoperationen • `delete` für Dateilöschvorgänge • `delete_dir` für Verzeichnislöschvorgänge • `getattr` für Attributabrufoperationen • `link` für Link-Operationen • `lookup` für Suchvorgänge • `object_create` für S3-Dateioperationen • `object_delete` für S3-Dateioperationen • `object_tag` für S3-Dateivorgänge • `open` für Dateiöffnungsvorgänge • `read` für Dateileseoperationen • `write` für Dateischreibvorgänge • `rename` für Dateiumbenennungsvorgänge • `rename_dir` für Verzeichnisumbenennungsvorgänge • `setattr` für Set-Attribut-Operationen • `symlink` für Symbol-Link-Operationen Wenn `-file-operations` angegeben wird, muss im `-protocol` Parameter ein gültiges Protokoll angegeben werden.	`-file-operations file_operations,...`

Filter Gibt die Liste der Filter für eine bestimmte Dateioperation für das angegebene Protokoll an. Die Werte im `-filters` Parameter werden verwendet, um Clientanfragen zu filtern. Die Liste kann einen oder mehrere der folgenden enthalten: Wenn Sie den `-filters` Parameter angeben, müssen Sie auch gültige Werte für die `-file-operations` und `-protocol` Parameter angeben. • `close-with-modification`Option zum Filtern der Client-Anfrage zum Schließen mit Änderung. • `close-without-modification`Option zum Filtern der Client-Anfrage zum Schließen ohne Änderung. • `first-read`Option zum Filtern der Client-Anfrage für den ersten Lesevorgang. • `first-write` Option zum Filtern der Clientanfrage für den ersten Schreibvorgang. • `monitor-ads`Option zum Filtern der Clientanfrage nach alternativem Datenstrom. • `object-create-with-put` Option zum Filtern von S3-Objekten. • `object-create-with-copy` Option zum Filtern von S3-Objekten. • `object-create-with-complete-mpu` Option zum Filtern von S3-Objekten. • `exclude-multi-delete` Option zum Filtern von S3-Objekten. • `object-tag-put` Option zum Filtern von S3-Objekten. • `object-tag-delete` Option zum Filtern von S3-Objekten. • `offline-bit`Option zum Filtern der Clientanfrage nach gesetztem Offline-Bit. Durch das Setzen dieses Filters erhält der FPolicy Server nur dann eine Benachrichtigung, wenn auf Offline-Dateien zugegriffen wird. • `open-with-delete-intent`Option zum Filtern der Client-Anfrage für das Öffnen mit Löschabsicht. Durch Aktivieren dieses Filters erhält der FPolicy-Server nur dann eine Benachrichtigung, wenn versucht wird, eine Datei mit der Absicht zu öffnen, sie zu löschen. Dies wird von Dateisystemen verwendet, wenn das `FILE_DELETE_ON_CLOSE` Flag angegeben ist. • `open-with-write-intent`Option zum Filtern von Client-Requests zum Öffnen mit Schreibabsicht. Durch die Einstellung dieses Filters erhält der FPolicy Server nur dann eine Benachrichtigung, wenn versucht wird, eine Datei mit der Absicht	`-filters filter, ...`

Ist ein Volume-Vorgang erforderlich? Gibt an, ob die Überwachung von Volume-Mount- und Unmount-Vorgängen erforderlich ist. Der Standardwert ist `false`.	`-volume-operation {true`

`false}`
 	
`-filters filter, ...`
	FPolicy-Zugriff verweigert Benachrichtigungen
	
	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. Benachrichtigungen werden für fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen generiert, darunter:
	
	• Fehler aufgrund von NTFS-Berechtigungen.
	• Fehler aufgrund von Unix-Modusbits.
	• Fehler aufgrund von NFSv4 ACLs.

`-monitor-fileop-failure {true`	`false}`

Unterstützte FPolicy Dateioperationen und Filter für SMB in ONTAP

Bei der Konfiguration Ihres FPolicy-Ereignisses ist zu beachten, dass nur bestimmte Kombinationen von Dateioperationen und Filtern für die Überwachung von SMB-Dateizugriffsvorgängen unterstützt werden.

Die Liste der unterstützten Dateioperationen- und Filterkombinationen für die FPolicy Überwachung von SMB-Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
schließen	monitor-ads, offline-bit, close-with-modification, close-without-modification, close-with-read, exclude-directory
erstellen	monitor-ads, offline-bit
Verzeichnis erstellen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
löschen	monitor-ads, offline-bit

Verzeichnis löschen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
getattr	offline-Bit, exclude-dir
offen	monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
lesen	monitor-ads, offline-bit, first-read
schreiben	monitor-ads, offline-bit, first-write, write-with-size-change
umbenennen	monitor-ads, offline-bit
Verzeichnis umbenennen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
setattr	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen über fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen erhalten. Die Liste der unterstützten Kombinationen aus verweigerten Dateizugriffsvorgängen und Filtern für die FPolicy Überwachung von SMB Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Datei-Zugriffsverweigerungsoperation	Unterstützte Filter
offen	NA

Unterstützte FPolicy Dateioperationen und Filter für NFSv3 in ONTAP

Bei der Konfiguration Ihres FPolicy Ereignisses ist zu beachten, dass für die Überwachung von NFSv3-Dateizugriffsvorgängen nur bestimmte Kombinationen von Dateivorgängen und Filtern unterstützt werden.

Die Liste der unterstützten Dateioperationen- und Filterkombinationen für die FPolicy Überwachung von NFSv3-Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
erstellen	Offline Bit
Verzeichnis erstellen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
löschen	Offline Bit
Verzeichnis löschen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
Link	Offline Bit
Nachschlagen	offline-Bit, exclude-dir
lesen	Offline-Bit, First-Read
schreiben	offline-bit, First-Write, Write-with-Size-Change

umbenennen	Offline Bit
Verzeichnis umbenennen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
Symlink	Offline Bit

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen über fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen erhalten. Die Liste der unterstützten Kombinationen aus verweigertem Dateizugriff und Filter für die FPolicy Überwachung von NFSv3 Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Datei-Zugriffsverweigerungsoperation	Unterstützte Filter
Zugriff	NA
erstellen	NA
Verzeichnis erstellen	NA
löschen	NA
Verzeichnis löschen	NA
Link	NA
lesen	NA
umbenennen	NA
Verzeichnis umbenennen	NA
setattr	NA
schreiben	NA

Unterstützte FPolicy Dateioperationen und Filter für NFSv4 in ONTAP

Bei der Konfiguration Ihres FPolicy Ereignisses ist zu beachten, dass für die Überwachung von NFSv4-Dateizugriffsvorgängen nur bestimmte Kombinationen von Dateivorgängen und Filtern unterstützt werden.

Ab ONTAP 9.15.1 unterstützt FPolicy das NFSv4.1 Protokoll.

Ab ONTAP 9.19.1 können Administratoren die Verfügbarkeit von NFSv4.2 auf SVM-Ebene steuern, indem sie das Protokoll für einzelne Storage-VMs entweder über System Manager, die CLI oder REST API aktivieren oder deaktivieren.

Ab ONTAP 9.20.1 unterstützt FPolicy die Überwachung von NFSv4.2-Dateizugriffsereignissen, einschließlich neuer Dateivorgänge für Schreibvorgänge mit erweiterten Attributen (xattr) und Sicherheitslabelfiltern für Labeled NFS-Aktivitäten. Weitere Informationen zu "NFS für ONTAP SVMs aktivieren oder deaktivieren".

Sicherheitslabel-Filter (`setattr_with_security_label_change` und

`getattr_with_security_label_read`) erfordern, dass NFSv4.2-Sicherheitslabels (Labeled NFS) auf der SVM aktiviert sind. Weitere Informationen zu "Aktivierung von NFSv4.2 Sicherheitskennzeichnungen". `getxattr` und `listxattrs` sind schreibgeschützte Operationen und werden nicht von FPolicy überwacht.

Die Liste der unterstützten Dateioperations- und Filterkombinationen für die FPolicy-Überwachung von Dateizugriffsereignissen in NFSv4, NFSv4.1 oder NFSv4.2 ist in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
schließen	Offline-Bit, exclude-directory
erstellen	Offline Bit
Verzeichnis erstellen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
löschen	Offline Bit
Verzeichnis löschen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
getattr	offline-bit, exclude-directory getattr_with_security_label_read (Ab ONTAP 9.20.1 ist dieser Filter verfügbar, Labeled NFS ist erforderlich)
Link	Offline Bit
Nachschlagen	Offline-Bit, exclude-directory
offen	Offline-Bit, exclude-directory
lesen	Offline-Bit, First-Read
schreiben	offline-bit, First-Write, Write-with-Size-Change
umbenennen	Offline Bit
Verzeichnis umbenennen	Aktuell wird für diese Dateioperation kein Filter unterstützt.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory setattr_with_security_label_change (ab ONTAP 9.20.1 unterstützt ONTAP diesen Filter; Voraussetzung ist Labeled NFS)
setxattr	Ab ONTAP 9.20.1 wird dieser Dateivorgang unterstützt und erfordert Labeled NFS. Derzeit wird für diesen Dateivorgang kein Filter unterstützt.
removexattr	Ab ONTAP 9.20.1 wird dieser Dateivorgang unterstützt und erfordert Labeled NFS. Derzeit wird für diesen Dateivorgang kein Filter unterstützt.
Symlink	Offline Bit

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen über fehlgeschlagene Dateivorgänge aufgrund fehlender Berechtigungen erhalten. Die Liste der unterstützten Kombinationen aus Zugriffsverweigerung bei Dateivorgängen und Filtern für die FPolicy-Überwachung von Dateizugriffsereignissen in NFSv4, NFSv4.1 oder NFSv4.2 ist in der folgenden Tabelle aufgeführt:

Unterstützte Datei-Zugriffsverweigerungsoperation	Unterstützte Filter
Zugriff	k. A.
erstellen	k. A.

Verzeichnis erstellen	k. A.
löschen	k. A.
Verzeichnis löschen	k. A.
Link	k. A.
offen	k. A.
lesen	k. A.
umbenennen	k. A.
Verzeichnis umbenennen	k. A.
setattr	k. A.
schreiben	k. A.

Unterstützte Dateioperationen- und Filterkombinationen, die ONTAP FPolicy für S3 überwacht

Bei der Konfiguration Ihres FPolicy-Ereignisses ist zu beachten, dass für die Überwachung von S3-Objektzugriffsvorgängen nur bestimmte Kombinationen von Dateivorgängen und Filtern unterstützt werden.

Ab ONTAP 9.20.1 unterstützt FPolicy Benachrichtigungen für S3-Objektereignisse auf NAS-Buckets. S3 FPolicy arbeitet ausschließlich im asynchronen, nicht obligatorischen Modus.

Die Liste der unterstützten Dateivorgänge und Filterkombinationen für die FPolicy Überwachung von S3-Objektzugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
object_create	object-create-with-put, object-create-with-copy, object-create-with-complete-mpu
object_delete	exclude-multi-delete
object_tag	object-tag-put, object-tag-delete

Filterbeschreibungen

Die folgende Liste beschreibt jeden S3 FPolicy-Filter:

- object-create-with-put: Überwachung von Objekterstellungsvorgängen, die mithilfe einer PUT-Anfrage durchgeführt werden.
- object-create-with-copy: Überwachung von Objekterstellungsvorgängen, die mit einer COPY-Anforderung durchgeführt werden.
- object-create-with-complete-mpu: Überwachung von Objekterstellungsvorgängen, die durch das Abschließen eines Multipart-Uploads ausgeführt werden.
- Mehrfachlöschung ausschließen: Benachrichtigungen für Objekte, die im Rahmen einer Mehrfachlöschungsanforderung gelöscht wurden, werden ausgeschlossen. Wenn dieser Filter aktiviert ist, generiert FPolicy nur Benachrichtigungen für Löschvorgänge einzelner Objekte.
- object-tag-put: Überwachung von Vorgängen, die ein Objekt-Tag hinzufügen oder ändern.

- object-tag-delete: Überwachung von Vorgängen, die ein Objekt-Tag entfernen.

Zusätzliche Überlegungen zu S3 FPolicy Ereignissen

- Nur erfolgreiche, clientgesteuerte S3-Operationen generieren FPolicy-Benachrichtigungen. Intern generierte Operationen (wie z. B. Objektablauf oder Snapshot-Wiederherstellung) und fehlgeschlagene Operationen generieren keine Benachrichtigungen.
- GET-Operationen (Lesen) werden für die S3 FPolicy Überwachung nicht unterstützt.
- Eine Mehrfachlöschanforderung kann bis zu 1.000 Objekte löschen. FPolicy generiert für jedes erfolgreich gelöschte Objekt eine Benachrichtigung. Jede Benachrichtigung innerhalb derselben Mehrfachlöschanforderung verwendet dieselbe FPolicy Anforderungs-ID und S3 Anforderungs-ID zur Korrelation.
- Benachrichtigungen über verweigerten Zugriff werden für S3-Ereignisse nicht unterstützt.

ONTAP FPolicy Ereigniskonfigurationsarbeitsblatt

Sie können dieses Arbeitsblatt verwenden, um die Werte zu erfassen, die Sie während des FPolicy Ereignis-Konfigurationsprozesses benötigen. Wenn ein Parameterwert erforderlich ist, muss vor der Konfiguration des FPolicy Ereignisses festgelegt werden, welcher Wert für diese Parameter zu verwenden ist.

Es empfiehlt sich, festzuhalten, ob jede Parametereinstellung in die FPolicy Ereigniskonfiguration aufgenommen werden soll, und anschließend den Wert der Parameter zu notieren, die aufgenommen werden sollen.

Art der Information	Erforderlich	Enthalten	Ihre Werte
Name der Storage Virtual Machine (SVM)	Ja	Ja	
Veranstaltungsname	Ja	Ja	
Protokoll	Nein		
Dateivorgänge	Nein		
Filter	Nein		
Volume-Betrieb	Nein		
Zugriffsverweigerungsereignisse + (Unterstützung ab ONTAP 9.13)	Nein		

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.