Audit S3-Ereignisse

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/s3-audit/index.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Audit S3-Ereignisse . . . 1
- Informationen zur Überwachung von ONTAP S3-Ereignissen . . . 1
  - Objektzugriff (Daten) Ereignisse nach Release . . . 1
  - Managementereignisse nach Release . . . 1
  - Garantierte Prüfung . . . 3
  - Platzbedarf für die Prüfung . . . 3
- Planung einer ONTAP S3 Audit-Konfiguration . . . 3
  - Allgemeine Parameter . . . 4
  - Parameter für die Rotation des Revisionsprotokolls . . . 5
- Erstellen und Aktivieren einer ONTAP S3 Überwachungskonfiguration . . . 6
- Buckets für ONTAP S3-Auditing auswählen . . . 8
- Ändern einer ONTAP S3 Überwachungskonfiguration . . . 8
- ONTAP S3-Überwachungskonfigurationen anzeigen . . . 9

Audit S3-Ereignisse

Informationen zur Überwachung von ONTAP S3-Ereignissen

Ab ONTAP 9.10.1 ist die Protokollierung von Daten- und Verwaltungsereignissen in ONTAP S3 Umgebungen möglich. Die S3-Protokollierungsfunktionalität ist mit den bestehenden NAS-Protokollierungsfunktionen vergleichbar, und S3- sowie NAS-Protokollierung können in einem Cluster parallel bestehen.

Wenn Sie eine S3-Überwachungskonfiguration auf einer SVM erstellen und aktivieren, werden S3-Ereignisse in einer Protokolldatei aufgezeichnet. Sie können die folgenden Ereignisse angeben, die protokolliert werden sollen:

Objektzugriff (Daten) Ereignisse nach Release

9.11.1:

- ListBucketVersions
- ListBucket (ListObjects von 9.10.1 wurde in diesen umbenannt)
- ListAllMyBuckets (ListBuckets von 9.10.1 wurde in diesen umbenannt)

9.10.1:

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- ListUploads
- ListParts

Managementereignisse nach Release

9.15.1:

- GetBucketCORS

- PutBucketCORS
- DeleteBucketCORS

9.14.1:

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1:

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1:

- GetBucketPolicy
- CopyObject
- UploadPartCopy
- PutBucketPolicy
- DeleteBucketPolicy

9.11.1:

- GetBucketVersioning
- PutBucketVersioning

9.10.1:

- HeadBucket
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

Das Protokollformat ist JavaScript Object Notation (JSON).

Die kombinierte Obergrenze für S3- und NFS-Revisionsprotokollkonfigurationen beträgt 400 SVMs pro Cluster.

Folgende Lizenz ist erforderlich:

- ONTAP One, ehemals Teil des Core Bundle, für das ONTAP S3 Protokoll und Storage

Weitere Informationen finden sich unter "Wie der ONTAP Revisionsprozess funktioniert".

Garantierte Prüfung

Standardmäßig ist die Überwachung von S3 und NAS gewährleistet. ONTAP garantiert, dass alle prüfbaren Bucket-Zugriffsereignisse protokolliert werden, selbst wenn ein Knoten nicht verfügbar ist. Ein angeforderter Bucket-Vorgang kann erst abgeschlossen werden, wenn der Prüfdatensatz für diesen Vorgang im Staging-Volume auf dem persistenten Speicher gespeichert wurde. Können Prüfdatensätze nicht in den Staging-Dateien gespeichert werden, entweder aufgrund von unzureichendem Speicherplatz oder wegen anderer Probleme, werden Client-Operationen abgelehnt.

Platzbedarf für die Prüfung

Im ONTAP Auditing-System werden Audit-Datensätze zunächst in binären Zwischenspeicherdateien auf den einzelnen Knoten gespeichert. Periodisch werden sie konsolidiert und in benutzerlesbare Ereignisprotokolle umgewandelt, die im Verzeichnis für Revisionsprotokolle des SVM gespeichert werden.

Die Staging-Dateien werden in einem dedizierten Staging-Volume gespeichert, das von ONTAP bei der Erstellung der Revisionsprotokoll-Konfiguration erstellt wird. Pro Aggregat existiert ein Staging-Volume.

In der Audit-Konfiguration ist ausreichend verfügbarer Speicherplatz einzuplanen:

- Für die Staging Volumes in Aggregaten, die geprüfte Buckets enthalten.
- Für das Volume, das das Verzeichnis enthält, in dem konvertierte Ereignisprotokolle gespeichert sind.

Sie können die Anzahl der Ereignisprotokolle und damit den verfügbaren Speicherplatz im Volume mit einer von zwei Methoden beim Erstellen der S3 Auditing-Konfiguration steuern:

- Ein numerischer Grenzwert; der `-rotate-limit` Parameter steuert die Mindestanzahl der zu speichernden Revisionsprotokolldateien.
- Ein Zeitlimit; der `-retention-duration` Parameter steuert die maximale Zeitspanne, für die Dateien aufbewahrt werden können.

Bei beiden Parametern können ältere Revisionsprotokolldateien gelöscht werden, sobald der konfigurierte Wert überschritten ist, um Platz für neuere zu schaffen. Für beide Parameter beträgt der Wert 0, was bedeutet, dass alle Dateien erhalten bleiben müssen. Um ausreichend Speicherplatz sicherzustellen, ist es daher eine bewährte Methode, einen der Parameter auf einen Wert ungleich null zu setzen.

Aufgrund der garantierten Revisionsprotokollierung können keine neuen Revisionsprotokolldaten erstellt werden, wenn der verfügbare Speicherplatz für Revisionsprotokolldaten vor dem Rotationslimit erschöpft ist, was dazu führt, dass Clients nicht auf Daten zugreifen können. Daher sollten der Wert für die Revisionsprotokollierung und der für die Revisionsprotokollierung reservierte Speicherplatz sorgfältig gewählt werden, und auf Warnungen des Revisionsprotokollierungssystems bezüglich des verfügbaren Speicherplatzes ist zu reagieren.

Weitere Informationen finden sich unter "Grundlegende Auditierungskonzepte".

Planung einer ONTAP S3 Audit-Konfiguration

Sie müssen für die S3-Auditing-Konfiguration eine Reihe von Parametern festlegen oder die Standardeinstellungen übernehmen. Insbesondere sollte berücksichtigt werden, welche Parameter für die Protokollrotation dazu beitragen, ausreichend freien Speicherplatz sicherzustellen.

Weitere Informationen zu `vserver object-store-server audit create` finden sich in der "ONTAP-Befehlsreferenz".

Allgemeine Parameter

Beim Erstellen der Audit-Konfiguration müssen zwei obligatorische Parameter angegeben werden. Es gibt außerdem drei optionale Parameter, die angegeben werden können.

Art der Information	Option	Erforderlich
SVM Name Name der SVM, auf der die Revisionsprotokoll-Konfiguration erstellt werden soll. Die SVM muss bereits existieren und für S3 aktiviert sein.	`-vserver` *`svm_name`*	Ja
Protokollzielpfad Gibt an, wo die konvertierten Revisionsprotokolle gespeichert werden. Der Pfad muss auf der SVM bereits vorhanden sein. Der Pfad darf maximal 864 Zeichen lang sein und muss über Lese-/Schreibberechtigung verfügen. Ist der Pfad ungültig, schlägt der Revisionsdatei-Konfigurationsbefehl fehl.	`-destination` *`text`*	Ja
Kategorien von zu prüfenden Ereignissen Die folgenden Ereigniskategorien können im Revisionsprotokoll erfasst werden: • Daten GetObject, PutObject und DeleteObject-Ereignisse • Management PutBucket und DeleteBucket Ereignisse Standardmäßig werden nur Datenereignisse geprüft.	`-events {data|management}, …`	Nein

Sie können einen der folgenden Parameter eingeben, um die Anzahl der Revisionsprotokoll Logdateien zu steuern. Wenn kein Wert eingegeben wird, werden alle Logdateien beibehalten.

Art der Information	Option	Erforderlich
Rotationslimit für Protokolldateien Legt fest, wie viele Revisionsprotokoll-Logdateien aufbewahrt werden, bevor die älteste Logdatei entfernt wird. Bei einem Wert von 5 werden beispielsweise die letzten fünf Logdateien aufbewahrt. Der Wert 0 bedeutet, dass alle Protokolldateien beibehalten werden. Der Standardwert ist 0.	`-rotate-limit` *`integer`*	Nein

Dauerbegrenzung für Protokolldateien Legt fest, wie lange eine Protokolldatei aufbewahrt werden kann, bevor sie gelöscht wird. Wenn ein Wert von 5d0h0m eingegeben wird, werden Protokolle, die älter als 5 Tage sind, gelöscht. Der Wert 0 bedeutet, dass alle Protokolldateien beibehalten werden. Der Standardwert ist 0.	`-retention duration` *`integer_time`*	Nein

Parameter für die Rotation des Revisionsprotokolls

Sie können Revisionsprotokolle basierend auf Größe oder Zeitplan rotieren lassen. Standardmäßig werden Revisionsprotokolle basierend auf Größe rotiert.

Protokolle basierend auf der Protokollgröße rotieren

Wenn Sie die Standardmethode für die Protokollrotation und die Standardprotokollgröße verwenden, ist keine spezifische Konfiguration von Parametern für die Protokollrotation erforderlich. Die Standardprotokollgröße beträgt 100 MB.

Wenn Sie nicht die Standardprotokollgröße verwenden möchten, kann der `-rotate-size` Parameter so konfiguriert werden, dass eine benutzerdefinierte Protokollgröße festgelegt wird.

Wenn Sie die Rotation nur anhand der Loggröße zurücksetzen möchten, verwenden Sie den folgenden Befehl, um den `-rotate-schedule-minute` Parameter zu entfernen:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Protokolle gemäß einem Zeitplan rotieren

Wenn Sie sich dafür entscheiden, die Revisionsprotokolle nach einem Zeitplan zu rotieren, kann die Protokollrotation mithilfe der zeitbasierten Rotationsparameter in beliebiger Kombination geplant werden.

- Bei Verwendung einer zeitbasierten Rotation ist der `-rotate-schedule-minute` Parameter obligatorisch.
- Alle anderen zeitbasierten Rotationsparameter sind optional.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- Der Rotationsplan wird anhand aller zeitbezogenen Werte berechnet. Wenn nur der `-rotate-schedule-minute` Parameter angegeben wird, werden die Revisionsprotokoll-Dateien an allen Wochentagen, zu allen Stunden und in allen Monaten des Jahres entsprechend der angegebenen Minuten rotiert.
- Wenn Sie nur einen oder zwei zeitbasierten Rotationsparameter angeben (zum Beispiel `-rotate-schedule-month` und `-rotate-schedule-minutes`), erfolgt die Rotation der Protokolldateien an allen Wochentagen und zu allen Stunden auf Grundlage der angegebenen Minutenwerte, jedoch nur während der festgelegten Monate.

  Beispielsweise kann festgelegt werden, dass das Revisionsprotokoll in den Monaten Januar, März und

August jeweils montags, mittwochs und samstags um 10:30 Uhr rotiert wird.

- Wenn Sie Werte für sowohl `-rotate-schedule-dayofweek` als auch `-rotate-schedule-day` angeben, werden diese unabhängig voneinander betrachtet.

  Wenn beispielsweise `-rotate-schedule-dayofweek` als Freitag und `-rotate-schedule-day` als 13 angegeben werden, werden die Revisionsprotokolle an jedem Freitag und am 13. Tag des angegebenen Monats rotiert, nicht nur an jedem Freitag, der auf den 13. fällt.

- Wenn Sie die Rotation nur anhand eines Zeitplans zurücksetzen möchten, verwenden Sie den folgenden Befehl, um die `-rotate-size parameter` aufzuheben:

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

Protokolldateien basierend auf ihrer Größe und dem Zeitplan rotieren

Sie können die Rotation der Protokolldateien anhand der Protokolldateigröße und eines Zeitplans steuern, indem sowohl der Parameter -rotate-size als auch die zeitbasierten Rotationsparameter in beliebiger Kombination gesetzt werden. Beispielsweise: Wenn `-rotate-size` auf 10 MB und `-rotate-schedule -minute` auf 15 gesetzt ist, werden die Protokolldateien rotiert, sobald die Protokolldateigröße 10 MB erreicht oder in der 15. Minute jeder Stunde (je nachdem, welches Ereignis zuerst eintritt).

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Erstellen und Aktivieren einer ONTAP S3 Überwachungskonfiguration

Zur Implementierung von S3 Auditing wird zunächst eine persistente Objektspeicher Auditing-Konfiguration auf einer S3-fähigen SVM erstellt und anschließend die Konfiguration aktiviert.

Bevor Sie beginnen

- Sie verfügen über eine S3-fähige SVM.
- Bestätigen Sie, dass ausreichend Speicherplatz für Staging-Volumes in der lokalen Tier vorhanden ist.

Über diese Aufgabe

Für jede SVM, die S3-Buckets enthält, die Sie überwachen möchten, ist eine Überwachungskonfiguration erforderlich. Die S3-Überwachung kann auf neuen oder bestehenden S3-Servern aktiviert werden. Überwachungskonfigurationen bleiben in einer S3-Umgebung erhalten, bis sie mit dem Befehl **vserver object-store-server audit delete** entfernt werden.

Die S3-Audit-Konfiguration gilt für alle Buckets in der SVM, die für die Überwachung ausgewählt werden. Eine SVM mit aktivierter Überwachung kann sowohl überwachte als auch nicht überwachte Buckets enthalten.

Es wird empfohlen, die S3-Überwachung für die automatische Protokollrotation zu konfigurieren, die anhand der Protokollgröße oder eines Zeitplans erfolgt. Wenn die automatische Protokollrotation nicht konfiguriert wird, werden standardmäßig alle Protokolldateien beibehalten. Die S3-Protokolldateien können auch manuell mit dem Befehl **vserver object-store-server audit rotate-log** rotiert werden.

Wenn die SVM eine SVM Disaster Recovery-Quelle ist, kann sich der Zielpfad nicht auf dem Root-Volume befinden.

Schritte

1. Die Überwachungskonfiguration ermöglicht das Rotieren von Überwachungsprotokollen basierend auf der Protokollgröße oder einem Zeitplan.

Wenn Sie die Revisionsprotokolle rotieren möchten…	Eingeben…
Loggröße	`vserver object-store-server audit create -vserver` *svm_name* `-destination` *path* `[[-events] {data|management}, …] {[-rotate-limit` *integer*`] | [-retention-duration [`*integer_d*`][`*integer_h*`][`*integer_m*`][`*integers*`]]} [-rotate-size {`*integer*`[KB|MB|GB|TB|PB]}]`
Ein Zeitplan	`vserver object-store-server audit create -vserver` *svm_name* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *integer*`] | [-retention-duration [`*integerd*`][`*integerh*`] [`*integerm*`][`*integers*`]] } [-rotate-schedule-month` *chron_month*`] [-rotate-schedule-dayofweek` *chron_dayofweek*`] [-rotate-schedule-day` *chron_dayofmonth*`] [-rotate-schedule-hour` *chron_hour*`] -rotate-schedule-minute` *chron_minute* Der `-rotate-schedule-minute`Parameter ist erforderlich, wenn eine zeitbasierte Revisionsprotokollrotation konfiguriert wird.

2. S3-Überwachung aktivieren:

   `vserver object-store-server audit enable -vserver` *svm_name*

Beispiele

Das folgende Beispiel erstellt eine Überwachungskonfiguration, die alle S3-Ereignisse (Standard) mithilfe einer größenbasierten Rotation überwacht. Die Protokolle werden im Verzeichnis /audit_log gespeichert. Die maximale Protokolldateigröße beträgt 200 MB. Die Protokolle werden rotiert, sobald sie 200 MB groß sind.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

Das folgende Beispiel erstellt eine Überwachungskonfiguration, die alle S3-Ereignisse (Standard) mithilfe einer größenbasierten Rotation überwacht. Die maximale Protokolldateigröße beträgt 100 MB (Standard), und die Protokolle werden 5 Tage lang aufbewahrt, bevor sie gelöscht werden.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

Das folgende Beispiel erstellt eine Audit-Konfiguration, die S3-Management-Ereignisse und Ereignisse der zentralen Zugriffsrichtlinien-Staging mithilfe zeitbasierter Rotation auditiert. Die Audit-Protokolle werden monatlich um 12:30 Uhr an allen Wochentagen rotiert. Das Protokoll-Rotationslimit beträgt 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
```

```
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Buckets für ONTAP S3-Auditing auswählen

Es ist anzugeben, welche Buckets in einer Audit-aktivierten SVM überwacht werden.

Bevor Sie beginnen

- Sie haben eine SVM für die S3-Überwachung aktiviert.

Über diese Aufgabe

S3-Audit-Konfigurationen werden pro SVM aktiviert, jedoch müssen Sie in den SVMs die Buckets auswählen, die für das Audit aktiviert sind. Wenn Buckets zur SVM hinzugefügt werden und diese neuen Buckets auditiert werden sollen, müssen sie mit diesem Verfahren ausgewählt werden. Es können auch nicht auditierte Buckets in einer SVM für S3-Auditing aktiviert sein.

Die Überwachungskonfigurationen bleiben für Buckets bestehen, bis sie durch den `vserver object-store-server audit event-selector delete` Befehl entfernt werden.

Schritte

1. Wählen Sie einen Bucket für die S3-Überwachung aus:

```
vserver object-store-server audit event-selector create -vserver
<svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
[[-permission] {allow-only|deny-only|all}]
```

   - `-access`: Gibt die Art des zu überwachenden Ereigniszugriffs an: `read-only`, `write-only` oder `all` (Standardwert ist `all`).
   - `-permission`: Gibt den Typ der zu überwachenden Ereignisberechtigung an: `allow-only`, `deny-only` oder `all` (Standardwert ist `all`).

Beispiel

Das folgende Beispiel erstellt eine Bucket-Audit-Konfiguration, die nur zulässige Ereignisse mit Lesezugriff protokolliert:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

Ändern einer ONTAP S3 Überwachungskonfiguration

Sie können die Revisionsparameter einzelner Buckets oder die Revisionskonfiguration aller zur Revision ausgewählten Buckets im SVM anpassen.

Wenn Sie die Revisionsprotokollkonfiguration für… anpassen möchten	Eingeben…
Einzelne Buckets	`vserver object-store-server audit event-selector modify -vserver` *svm_name* `[-bucket` *bucket_name*`] [`*parameters to modify*`]`
Alle Buckets in der SVM	`vserver object-store-server audit modify -vserver` *svm_name* `[`*parameters to modify*`]`

Beispiele

Das folgende Beispiel ändert eine einzelne Bucket-Audit-Konfiguration, um nur Schreibzugriffsereignisse zu protokollieren:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

Das folgende Beispiel ändert die Revisionsprotokollkonfiguration aller Buckets in der SVM, um die Protokollgrößenbeschränkung auf 10 MB zu ändern und 3 Protokolldateien vor der Rotation aufzubewahren.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

ONTAP S3-Überwachungskonfigurationen anzeigen

Nach Abschluss der Revisionsprotokollkonfiguration kann überprüft werden, ob das Revisionsprotokoll ordnungsgemäß konfiguriert und aktiviert ist. Es lassen sich außerdem Informationen zu allen Objektspeicher-Revisionsprotokollkonfigurationen im Cluster anzeigen.

Über diese Aufgabe

Informationen zu Bucket- und SVM-Audit-Konfigurationen lassen sich anzeigen.

- Buckets: Der `vserver object-store-server audit event-selector show`Befehl kann verwendet werden

  Ohne Angabe von Parametern zeigt der Befehl die folgenden Informationen über Buckets in allen SVMs im Cluster mit Objektspeicher-Audit-Konfigurationen an:

  - SVM-Name
  - Bucket Name
  - Zugriffs- und Berechtigungswerte
- SVMs: Mit dem `vserver object-store-server audit show` Befehl

  Ohne Angabe von Parametern zeigt der Befehl die folgenden Informationen zu allen SVMs im Cluster mit Objektspeicher-Revisionsprotokollkonfigurationen an:

- SVM-Name
- Revisionsstatus
- Zielverzeichnis

Sie können den `-fields` Parameter angeben, um festzulegen, welche Revisionsprotokoll-Konfigurationsinformationen angezeigt werden.

Schritte

Informationen zu S3-Audit-Konfigurationen:

Wenn Sie die Konfiguration für … ändern möchten	Eingeben…
Buckets	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
SVMs	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

Beispiele

Das folgende Beispiel zeigt Informationen für einen einzelnen Bucket:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

Das folgende Beispiel zeigt Informationen für alle Buckets auf einer SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

Das folgende Beispiel zeigt den Namen, den Revisionsprotokollstatus, die Ereignistypen, das Protokollformat und das Zielverzeichnis für alle SVMs.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

Das folgende Beispiel zeigt die SVM-Namen und Details zum Revisionsprotokoll für alle SVMs.

```
cluster1::> vserver object-store-server audit show -log-save-details

                  Rotation                              Rotation
      Vserver     File Size Rotation Schedule           Limit
      ----------- --------- ------------------------- --------
      vs1         100MB     -                         0
```

Das folgende Beispiel zeigt in Listenform alle Revisionsprotokoll-Konfigurationsinformationen zu allen SVMs.

```
cluster1::> vserver object-store-server audit show -instance

                            Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                         Log Format: json
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
                  Log Retention Time: 0s
```

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.