



# Managen von S3-Zugriffsschlüsseln

## StorageGRID

NetApp  
March 12, 2025

# Inhalt

- Managen von S3-Zugriffsschlüsseln ..... 1
  - Managen von S3-Zugriffsschlüsseln ..... 1
  - Erstellen Ihrer eigenen S3-Zugriffsschlüssel ..... 1
  - Die S3-Zugriffsschlüssel anzeigen ..... 2
  - Löschen Ihrer eigenen S3-Zugriffsschlüssel ..... 3
  - Erstellen Sie die S3-Zugriffstasten eines anderen Benutzers ..... 4
  - Zeigen Sie die S3-Zugriffstasten eines anderen Benutzers an ..... 5
  - Löschen Sie die S3-Zugriffstasten eines anderen Benutzers ..... 6

# Managen von S3-Zugriffsschlüsseln

## Managen von S3-Zugriffsschlüsseln

Jeder Benutzer eines S3-Mandantenkontos muss über einen Zugriffsschlüssel verfügen, um Objekte im StorageGRID System zu speichern und abzurufen. Ein Zugriffsschlüssel besteht aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel.

S3-Zugriffsschlüssel können wie folgt gemanagt werden:

- Benutzer, die die Berechtigung **Manage your own S3 credentials** besitzen, können ihre eigenen S3-Zugriffsschlüssel erstellen oder entfernen.
- Benutzer mit der Berechtigung **Root-Zugriff** können die Zugriffsschlüssel für das S3-Root-Konto und alle anderen Benutzer verwalten. Root-Zugriffsschlüssel bieten vollständigen Zugriff auf alle Buckets und Objekte für Mandanten, sofern nicht ausdrücklich von einer Bucket-Richtlinie deaktiviert wurde.

StorageGRID unterstützt die Authentifizierung nach Signature Version 2 und Signature Version 4. Der Zugriff auf übergreifende Konten ist nur zulässig, wenn diese durch eine Bucket-Richtlinie ausdrücklich aktiviert wurde.

## Erstellen Ihrer eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel erstellen. Sie benötigen einen Zugriffsschlüssel für den Zugriff auf Ihre Buckets und Objekte.

### Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören zu einer Benutzergruppe mit dem "[Managen Sie Ihre eigenen S3-Anmeldedaten oder Root-Zugriffsberechtigungen](#)".

### Über diese Aufgabe

Sie können einen oder mehrere S3-Zugriffsschlüssel erstellen und managen, mit denen Sie Buckets für Ihr Mandantenkonto erstellen und verwalten können. Nachdem Sie einen neuen Zugriffsschlüssel erstellt haben, aktualisieren Sie die Anwendung mit Ihrer neuen Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel. Aus Sicherheitsgründen sollten Sie nicht mehr Schlüssel erstellen, als Sie benötigen, und die Schlüssel löschen, die Sie nicht verwenden. Wenn Sie nur einen Schlüssel haben und demnächst ablaufen, erstellen Sie einen neuen Schlüssel, bevor der alte Schlüssel abläuft, und löschen Sie dann den alten Schlüssel.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder keinen Ablauf haben. Beachten Sie die folgenden Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für Ihre Schlüssel fest, um den Zugriff auf einen bestimmten Zeitraum zu beschränken. Durch die Einrichtung einer kurzen Ablaufzeit kann Ihr Risiko verringert werden, wenn Ihre Zugriffsschlüssel-ID und Ihr geheimer Zugriffsschlüssel versehentlich ausgesetzt sind. Abgelaufene Schlüssel werden automatisch entfernt.
- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie nicht regelmäßig neue Schlüssel erstellen müssen, müssen Sie keine Ablaufzeit für Ihre Schlüssel festlegen. Wenn Sie sich zu einem späteren Zeitpunkt für die Erstellung neuer Schlüssel entscheiden, löschen Sie die alten Schlüssel manuell.



Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und teilen Sie sie niemals mit anderen Benutzern.

## Schritte

1. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.

Die Seite Meine Zugriffsschlüssel wird angezeigt und enthält alle vorhandenen Zugriffsschlüssel.

2. Wählen Sie **Schlüssel erstellen**.
3. Führen Sie einen der folgenden Schritte aus:
  - Wählen Sie **Verfallszeit nicht festlegen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)
  - Wählen Sie **Verfallszeit festlegen**, und legen Sie das Ablaufdatum und die Uhrzeit fest.



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Verfallszeit kann mindestens eine Minute von der aktuellen Zeit entfernt sein.

4. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld Zugriffsschlüssel herunterladen wird angezeigt, in dem Ihre Zugriffsschlüssel-ID und Ihr geheimer Zugriffsschlüssel aufgeführt sind.

5. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.



Schließen Sie dieses Dialogfeld erst, wenn Sie diese Informationen kopiert oder heruntergeladen haben. Sie können keine Schlüssel kopieren oder herunterladen, nachdem das Dialogfeld geschlossen wurde.

6. Wählen Sie **Fertig**.

Die neue Taste wird auf der Seite eigene Zugriffsschlüssel angezeigt.

7. Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie optional die Tenant Management API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quellraster manuell auf den Mandanten im Zielraster zu klonen. Siehe "[Klonen von S3-Zugriffsschlüsseln mithilfe der API](#)".

## Die S3-Zugriffsschlüssel anzeigen

Wenn Sie einen S3-Mandanten verwenden und über den verfügen "[Entsprechende Berechtigung](#)", können Sie eine Liste Ihrer S3-Zugriffsschlüssel anzeigen. Sie können die Liste nach Ablauf der Zeit sortieren, sodass Sie feststellen können, welche Schlüssel bald ablaufen. Nach Bedarf können "[Erstellen Sie neue Schlüssel](#)" oder "[Schlüssel löschen](#)" die Sie nicht mehr verwenden.



Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und teilen Sie sie niemals mit anderen Benutzern.

### Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören zu einer Benutzergruppe, die über die eigenen S3-Anmeldeinformationen verwalten "[Berechtigung](#)" verfügt.

### Schritte

1. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.
2. Sortieren Sie auf der Seite Meine Zugriffsschlüssel alle vorhandenen Zugriffsschlüssel nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
3. Erstellen Sie nach Bedarf neue Schlüssel oder löschen Sie alle Schlüssel, die Sie nicht mehr verwenden.

Wenn Sie neue Schlüssel erstellen, bevor die vorhandenen Schlüssel ablaufen, können Sie mit der Verwendung der neuen Schlüssel beginnen, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

## Löschen Ihrer eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel löschen. Nach dem Löschen eines Zugriffsschlüssels kann dieser nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

### Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Management Ihrer eigenen S3-Berechtigungenachweise](#)".



Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und teilen Sie sie niemals mit anderen Benutzern.

### Schritte

1. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.
2. Aktivieren Sie auf der Seite Meine Zugriffsschlüssel das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie entfernen möchten.
3. Wählen Sie \* Taste löschen\*.
4. Wählen Sie im Bestätigungsdialogfeld **Delete key**.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt.

## Erstellen Sie die S3-Zugriffstasten eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie S3-Zugriffsschlüssel für andere Benutzer erstellen, beispielsweise Applikationen, die Zugriff auf Buckets und Objekte benötigen.

### Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören zu einer Benutzergruppe mit dem "[Root-Zugriffsberechtigung](#)".

### Über diese Aufgabe

Sie können einen oder mehrere S3-Zugriffsschlüssel für andere Benutzer erstellen und managen, damit sie Buckets für ihr Mandantenkonto erstellen und verwalten können. Nachdem Sie einen neuen Zugriffsschlüssel erstellt haben, aktualisieren Sie die Anwendung mit der neuen Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel. Erstellen Sie aus Sicherheitsgründen nicht mehr Schlüssel als der Benutzer benötigt, und löschen Sie die Schlüssel, die nicht verwendet werden. Wenn Sie nur einen Schlüssel haben und demnächst ablaufen, erstellen Sie einen neuen Schlüssel, bevor der alte Schlüssel abläuft, und löschen Sie dann den alten Schlüssel.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder keinen Ablauf haben. Beachten Sie die folgenden Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für die Schlüssel fest, um den Zugriff des Benutzers auf einen bestimmten Zeitraum zu beschränken. Durch das Festlegen einer kurzen Ablaufzeit kann das Risiko verringert werden, wenn die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel versehentlich ausgesetzt sind. Abgelaufene Schlüssel werden automatisch entfernt.
- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie keine periodischen neuen Schlüssel erstellen müssen, müssen Sie keine Ablaufzeit für die Schlüssel festlegen. Wenn Sie sich zu einem späteren Zeitpunkt für die Erstellung neuer Schlüssel entscheiden, löschen Sie die alten Schlüssel manuell.



Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals anderen Benutzern zur Verfügung.

### Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.
2. Wählen Sie den Benutzer aus, dessen S3-Zugriffsschlüssel Sie managen möchten.

Die Seite mit den Benutzerdetails wird angezeigt.

3. Wählen Sie **Zugriffstasten**, und wählen Sie dann **Schlüssel erstellen**.
4. Führen Sie einen der folgenden Schritte aus:
  - Wählen Sie **Keine Ablaufzeit einstellen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)

- Wählen Sie **Verfallszeit festlegen**, und legen Sie das Ablaufdatum und die Uhrzeit fest.



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Verfallszeit kann mindestens eine Minute von der aktuellen Zeit entfernt sein.

#### 5. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld Zugriffsschlüssel herunterladen wird angezeigt, in dem die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel aufgeführt sind.

6. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.



Schließen Sie dieses Dialogfeld erst, wenn Sie diese Informationen kopiert oder heruntergeladen haben. Sie können keine Schlüssel kopieren oder herunterladen, nachdem das Dialogfeld geschlossen wurde.

#### 7. Wählen Sie **Fertig**.

Der neue Schlüssel wird auf der Registerkarte Zugriffsschlüssel der Seite mit den Benutzerdetails angezeigt.

8. Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie optional die Tenant Management API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quellraster manuell auf den Mandanten im Zielraster zu klonen. Siehe "[Klonen von S3-Zugriffsschlüsseln mithilfe der API](#)".

## Zeigen Sie die S3-Zugriffstasten eines anderen Benutzers an

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers anzeigen. Sie können die Liste nach Ablauf der Zeit sortieren, sodass Sie feststellen können, welche Schlüssel bald ablaufen. Nach Bedarf können Sie neue Schlüssel erstellen und Schlüssel löschen, die nicht mehr verwendet werden.

### Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Root-Zugriffsberechtigung](#)".



Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals anderen Benutzern zur Verfügung.

### Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.

2. Wählen Sie auf der Seite Benutzer den Benutzer aus, dessen S3-Zugriffsschlüssel Sie anzeigen möchten.
3. Wählen Sie auf der Seite mit den Benutzerdetails **Zugriffstasten** aus.
4. Sortieren Sie die Tasten nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
5. Erstellen Sie bei Bedarf neue Schlüssel und löschen Sie manuell die nicht mehr verwendeten Schlüssel.

Wenn Sie neue Schlüssel erstellen, bevor die vorhandenen Schlüssel ablaufen, kann der Benutzer mit der Verwendung der neuen Schlüssel beginnen, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

#### Verwandte Informationen

- ["Erstellen von S3-Zugriffsschlüsseln eines anderen Benutzers"](#)
- ["Löschen Sie die S3-Zugriffsschlüssel eines anderen Benutzers"](#)

## Löschen Sie die S3-Zugriffstasten eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers löschen. Nach dem Löschen eines Zugriffsschlüssels kann dieser nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

#### Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die ["Root-Zugriffsberechtigung"](#).



Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals anderen Benutzern zur Verfügung.

#### Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.
2. Wählen Sie auf der Seite Benutzer den Benutzer aus, dessen S3-Zugriffsschlüssel Sie verwalten möchten.
3. Wählen Sie auf der Seite mit den Benutzerdetails **Zugriffsschlüssel** aus, und aktivieren Sie dann das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie löschen möchten.
4. Wählen Sie **Aktionen > Ausgewählte Taste löschen**.
5. Wählen Sie im Bestätigungsdiaologfeld **Delete key**.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt.



## Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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.