



S3-Zugriffsschlüssel verwalten

StorageGRID software

NetApp

October 21, 2025

Inhalt

- S3-Zugriffsschlüssel verwalten. 1
 - S3-Zugriffsschlüssel verwalten. 1
 - Erstellen Sie Ihre eigenen S3-Zugriffsschlüssel. 1
 - Zeigen Sie Ihre S3-Zugriffsschlüssel an 2
 - Löschen Sie Ihre eigenen S3-Zugriffsschlüssel 3
 - Erstellen Sie die S3-Zugriffsschlüssel eines anderen Benutzers. 4
 - Anzeigen der S3-Zugriffsschlüssel eines anderen Benutzers 5
 - Löschen Sie die S3-Zugriffsschlüssel eines anderen Benutzers 6

S3-Zugriffsschlüssel verwalten

S3-Zugriffsschlüssel verwalten

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 verwaltet werden:

- Benutzer mit der Berechtigung **Eigene S3-Anmeldeinformationen verwalten** 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 dem Mandanten vollständigen Zugriff auf alle Buckets und Objekte, sofern dies nicht ausdrücklich durch eine Bucket-Richtlinie deaktiviert wird.

StorageGRID unterstützt die Authentifizierung mit Signature Version 2 und Signature Version 4. Der kontoübergreifende Zugriff ist nicht zulässig, es sei denn, er wird ausdrücklich durch eine Bucket-Richtlinie aktiviert.

Erstellen Sie Ihre eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechende Berechtigung verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel erstellen. Sie benötigen einen Zugriffsschlüssel, um auf Ihre Buckets und Objekte zugreifen zu können.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Sie gehören einer Benutzergruppe an, die über die ["Verwalten Sie Ihre eigenen S3-Anmeldeinformationen oder Root-Zugriffsberechtigungen"](#) .

Informationen zu diesem Vorgang

Sie können einen oder mehrere S3-Zugriffsschlüssel erstellen, 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 Ihrem geheimen Zugriffsschlüssel. Erstellen Sie aus Sicherheitsgründen nicht mehr Schlüssel als nötig und löschen Sie die Schlüssel, die Sie nicht verwenden. Wenn Sie nur einen Schlüssel haben und dieser bald abläuft, erstellen Sie einen neuen Schlüssel, bevor der alte abläuft, und löschen Sie dann den alten.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder nicht ablaufen. Befolgen Sie diese Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für Ihre Schlüssel fest, um Ihren Zugriff auf einen bestimmten Zeitraum zu beschränken. Durch das Festlegen einer kurzen Ablaufzeit können Sie Ihr Risiko verringern, wenn Ihre Zugriffsschlüssel-ID und Ihr geheimer Zugriffsschlüssel versehentlich offengelegt werden. Abgelaufene Schlüssel werden automatisch entfernt.
- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie nicht regelmäßig neue Schlüssel erstellen müssen, müssen Sie für Ihre Schlüssel keine Ablaufzeit festlegen. Wenn Sie sich später entscheiden, neue Schlüssel zu erstellen, löschen Sie die alten Schlüssel manuell.



Auf die zu Ihrem Konto gehörenden S3-Buckets und -Objekte kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für Ihr Konto im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

1. Wählen Sie **SPEICHER (S3) > Meine Zugriffsschlüssel**.

Die Seite „Meine Zugriffsschlüssel“ wird angezeigt und listet alle vorhandenen Zugriffsschlüssel auf.

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



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Ablaufzeit kann mindestens eine Minute nach der aktuellen Zeit liegen.

4. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld „Zugriffsschlüssel herunterladen“ wird angezeigt und listet Ihre Zugriffsschlüssel-ID und Ihren geheimen Zugriffsschlüssel auf.

5. Kopieren Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel 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 nicht, bis Sie diese Informationen kopiert oder heruntergeladen haben. Sie können keine Schlüssel kopieren oder herunterladen, nachdem das Dialogfeld geschlossen wurde.

6. Wählen Sie **Fertig**.

Der neue Schlüssel wird auf der Seite „Meine Zugriffsschlüssel“ aufgeführt.

7. Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie optional die Mandantenverwaltungs-API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quell-Grid manuell auf den Mandanten im Ziel-Grid zu klonen. Sehen ["Klonen Sie S3-Zugriffsschlüssel mithilfe der API"](#).

Zeigen Sie Ihre S3-Zugriffsschlüssel an

Wenn Sie einen S3-Tenant verwenden und über die ["entsprechende Erlaubnis"](#) können Sie eine Liste Ihrer S3-Zugriffsschlüssel anzeigen. Sie können die Liste nach Ablaufzeit sortieren, um festzustellen, welche Schlüssel bald ablaufen. Bei Bedarf können Sie ["neue Schlüssel erstellen"](#) oder ["Schlüssel löschen"](#) die Sie nicht mehr verwenden.



Auf die zu Ihrem Konto gehörenden S3-Buckets und -Objekte kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für Ihr Konto im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und geben Sie sie niemals an andere Benutzer weiter.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **SPEICHER (S3) > Meine Zugriffsschlüssel**.
2. Sortieren Sie auf der Seite „Meine Zugriffsschlüssel“ alle vorhandenen Zugriffsschlüssel nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
3. Erstellen Sie bei 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 die neuen Schlüssel verwenden, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

Löschen Sie Ihre eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechende Berechtigung verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel löschen. Nachdem ein Zugriffsschlüssel gelöscht wurde, kann er nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Sie haben die ["Verwalten Sie Ihre eigenen S3-Anmeldeinformationen"](#) .



Auf die zu Ihrem Konto gehörenden S3-Buckets und -Objekte kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für Ihr Konto im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

1. Wählen Sie **SPEICHER (S3) > Meine Zugriffsschlüssel**.
2. Aktivieren Sie auf der Seite „Meine Zugriffsschlüssel“ das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie entfernen möchten.
3. Wählen Sie **Löschtaste**.
4. Wählen Sie im Bestätigungsdialogfeld **Schlüssel löschen** aus.

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

Erstellen Sie die S3-Zugriffsschlüssel eines anderen Benutzers

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem ["unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über die ["Root-Zugriffsberechtigung"](#).

Informationen zu diesem Vorgang

Sie können einen oder mehrere S3-Zugriffsschlüssel für andere Benutzer erstellen, damit diese 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 dieser bald abläuft, erstellen Sie einen neuen Schlüssel, bevor der alte abläuft, und löschen Sie dann den alten.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder nicht ablaufen. Befolgen Sie diese Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für die Schlüssel fest, um den Zugriff des Benutzers auf einen bestimmten Zeitraum zu beschränken. Durch Festlegen einer kurzen Ablaufzeit können Sie das Risiko verringern, wenn die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel versehentlich offengelegt werden. Abgelaufene Schlüssel werden automatisch entfernt.
- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie nicht regelmäßig neue Schlüssel erstellen müssen, müssen Sie für die Schlüssel keine Ablaufzeit festlegen. Wenn Sie sich später entscheiden, neue Schlüssel zu erstellen, löschen Sie die alten Schlüssel manuell.



Auf die S3-Buckets und -Objekte eines Benutzers kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für diesen Benutzer im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

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

Die Benutzerdetailseite wird angezeigt.

3. Wählen Sie **Zugriffsschlüssel** und dann **Schlüssel erstellen**.
4. Führen Sie einen der folgenden Schritte aus:
 - Wählen Sie **Keine Ablaufzeit festlegen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)
 - Wählen Sie **Ablaufzeit festlegen** und legen Sie das Ablaufdatum und die Ablaufzeit fest.



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Ablaufzeit kann mindestens eine Minute nach der aktuellen Zeit liegen.

5. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld „Zugriffsschlüssel herunterladen“ wird angezeigt und listet die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel auf.

6. Kopieren Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel 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 nicht, bis 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 Benutzerdetailseite aufgeführt.

8. Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie optional die Mandantenverwaltungs-API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quell-Grid manuell auf den Mandanten im Ziel-Grid zu klonen. Sehen ["Klonen Sie S3-Zugriffsschlüssel mithilfe der API"](#).

Anzeigen der S3-Zugriffsschlüssel eines anderen Benutzers

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 Ablaufzeit sortieren, um festzustellen, welche Schlüssel bald ablaufen. Bei Bedarf können Sie neue Schlüssel erstellen und nicht mehr verwendete Schlüssel löschen.

Bevor Sie beginnen

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



Auf die S3-Buckets und -Objekte eines Benutzers kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für diesen Benutzer im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals an andere Benutzer weiter.

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 „Benutzerdetails“ **Zugriffsschlüssel** aus.
4. Sortieren Sie die Schlüssel nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
5. Erstellen Sie bei Bedarf neue Schlüssel und löschen Sie nicht mehr verwendete Schlüssel manuell.

Wenn Sie neue Schlüssel erstellen, bevor die vorhandenen Schlüssel ablaufen, kann der Benutzer die

neuen Schlüssel verwenden, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

Ähnliche Informationen

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

Löschen Sie die S3-Zugriffsschlüssel eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers löschen.

Nachdem ein Zugriffsschlüssel gelöscht wurde, kann er nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

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



Auf die S3-Buckets und -Objekte eines Benutzers kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für diesen Benutzer im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals an andere Benutzer weiter.

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 „Benutzerdetails“ **Zugriffsschlüssel** aus und aktivieren Sie dann das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie löschen möchten.
4. Wählen Sie **Aktionen > Ausgewählten Schlüssel löschen**.
5. Wählen Sie im Bestätigungsdialogfeld **Schlüssel löschen** aus.

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 Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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