



Client-Autorisierung

ONTAP 9

NetApp
January 08, 2026

Inhalt

- Client-Autorisierung 1
 - Übersicht und Optionen für die ONTAP-Clientautorisierung 1
 - Eigenständige OAuth 2.0-Bereiche in ONTAP 2
 - Format der Bereichszeichenfolge 2
 - Beispiele für den Umfang 3
 - CLI-Verwaltungstool 3
 - OAuth 2.0 externe Rollenzuordnung in ONTAP 4
 - Externe Rollen in einem Zugriffstoken 4
 - Konfiguration 4
 - Wie ONTAP den Client-Zugriff bestimmt 5
 - ONTAP 9.16.1 5
 - ONTAP 9.14.1 7

Client-Autorisierung

Übersicht und Optionen für die ONTAP-Clientautorisierung

Die ONTAP OAuth 2.0 Implementierung ist flexibel und robust und bietet Ihnen die Funktionen, die Sie zur Sicherung Ihrer ONTAP Umgebung benötigen. Es stehen mehrere Konfigurationsoptionen zur Verfügung, die sich gegenseitig ausschließen. Die Autorisierungsentscheidungen basieren letztlich auf den ONTAP-REST-Rollen, die entweder in den OAuth 2.0-Zugriffstoken enthalten sind oder von diesen abgeleitet wurden.



Sie können nur verwenden **"ONTAP REST-Rollen"**, wenn Sie die Autorisierung für OAuth 2.0 konfigurieren. Die früheren herkömmlichen ONTAP Rollen werden nicht unterstützt.

ONTAP wendet je nach Konfiguration die am besten geeignete Autorisierungsoption an. Weitere Informationen dazu, wie ONTAP Client-Zugriffsentscheidungen trifft, finden Sie unter ["Wie ONTAP den Zugriff bestimmt"](#).

OAuth 2.0 eigenständige Oszilloskope

Diese Bereiche enthalten eine oder mehrere benutzerdefinierte REST-Rollen, die jeweils in einer einzigen Zeichenfolge im Zugriffstoken eingekapselt sind. Sie sind unabhängig von den Rollendefinitionen von ONTAP. Sie müssen die Bereichszeichenfolgen auf Ihrem Autorisierungsserver konfigurieren. Weitere Informationen finden Sie unter ["Eigenständige Oszilloskope von OAuth 2.0"](#).

Lokale ONTAP-REST-Rollen

Es kann eine einzelne benannte REST-Rolle verwendet werden, entweder erstellt oder benutzerdefiniert. Die scope Syntax für eine benannte Rolle ist **ontap-role-`<URL-encoded-ONTAP-role-name>`**. Wenn die Rolle ONTAP beispielsweise der scope string ist `admin`, wird dies der Fall sein `ontap-role-admin`.

Benutzer

Der Benutzername im Zugriffstoken, der mit Zugriff auf die Anwendung "http" definiert ist, kann verwendet werden. Anhand der definierten Authentifizierungsmethode wird ein Benutzer in der folgenden Reihenfolge getestet: Passwort, Domäne (Active Directory), nsswitch (LDAP).

Gruppen

Die Autorisierungsserver können so konfiguriert werden, dass sie ONTAP-Gruppen für die Autorisierung verwenden. Wenn die lokalen ONTAP-Definitionen überprüft werden, aber keine Zugriffsentscheidung getroffen werden kann, werden die Active Directory („Domain“)- oder LDAP („nsswitch“)-Gruppen verwendet. Gruppeninformationen können auf zwei Arten angegeben werden:

- OAuth 2.0-Scope-String

Unterstützt vertrauliche Anwendungen, die den Ablauf der Clientanmeldeinformationen verwenden, wenn kein Benutzer mit einer Gruppenmitgliedschaft vorhanden ist. Der Umfang sollte benannt werden **ontap-Group-`<URL-encoded-ONTAP-group-name>`**. Wenn die Gruppe beispielsweise „Entwicklung“ ist, lautet der Scope String „ontap-Group-Development“.

- In der „Gruppe“-Forderung

Dies ist für Zugriffstoken vorgesehen, die von ADFS unter Verwendung des Ablaufs Resource Owner (Password Grant) ausgegeben werden.

Sehen ["Arbeiten mit OAuth 2.0- oder SAML-IdP-Gruppen in ONTAP"](#) für weitere Informationen.

Eigenständige OAuth 2.0-Bereiche in ONTAP

In sich geschlossene Bereiche sind Strings, die im Zugriffstoken enthalten sind. Jede dieser Rollen ist vollständig definiert und beinhaltet alles, was ONTAP für eine Zugriffsentscheidung benötigt. Der Umfang unterscheidet sich von jeder der REST-Rollen, die in ONTAP selbst definiert sind.

Format der Bereichszeichenfolge

Auf einer Basisebene wird der Umfang als zusammenhängende Zeichenfolge dargestellt und besteht aus sechs durch Doppelpunkte getrennten Werten. Die im Scope String verwendeten Parameter werden im Folgenden beschrieben.

ONTAP-Literal

Der Umfang muss mit dem Literalwert `ontap` in Kleinbuchstaben beginnen. Der ONTAP-spezifische Umfang wird angegeben.

Cluster

Dies definiert, auf welchen ONTAP Cluster sich der Umfang bezieht. Die Werte können Folgendes umfassen:

- Cluster-UUID

Identifiziert ein einzelnes Cluster.

- Sternchen (*)

Gibt an, dass der Umfang auf alle Cluster angewendet wird.

Sie können den ONTAP-CLI-Befehl verwenden `cluster identity show`, um die UUID Ihres Clusters anzuzeigen. Falls nicht angegeben, gilt der Umfang für alle Cluster. Erfahren Sie mehr über `cluster identity show` in der ["ONTAP-Befehlsreferenz"](#).

Rolle

Der Name der im eigenständigen Bereich enthaltenen REST-Rolle. Dieser Wert wird von ONTAP nicht untersucht oder auf vorhandene REST-Rollen abgestimmt, die für ONTAP definiert sind. Der Name wird für die Protokollierung verwendet.

Zugangsstufe

Dieser Wert gibt die Zugriffsebene an, die auf die Clientanwendung angewendet wird, wenn der API-Endpunkt im Umfang verwendet wird. Es gibt sechs mögliche Werte, wie in der Tabelle unten beschrieben.

Zugangsstufe	Beschreibung
Keine	Verweigert allen Zugriff auf den angegebenen Endpunkt.
readonly	Nur Lesezugriff mit GET ist möglich.

Zugangsstufe	Beschreibung
Read_create	Ermöglicht den Lesezugriff sowie die Erstellung neuer Ressourceninstanzen über POST.
Lesen_ändern	Ermöglicht den Lesezugriff sowie die Möglichkeit, vorhandene Ressourcen mithilfe von PATCHES zu aktualisieren.
Lesen_create_modify	Ermöglicht alle Zugriffe außer Löschen. Zu den zulässigen Operationen gehören GET (read), POST (create) und PATCH (Update).
Alle	Ermöglicht vollständigen Zugriff.

SVM

Der Name der SVM innerhalb des Clusters, für den der Umfang gilt. Verwenden Sie den *-Wert (Sternchen), um alle SVMs anzuzeigen.



Diese Funktion wird von ONTAP 9.14.1 nicht vollständig unterstützt. Sie können den SVM-Parameter ignorieren und ein Sternchen als Platzhalter verwenden. Überprüfen Sie die ["Versionshinweise zu ONTAP"](#), um auf zukünftigen SVM-Support zu prüfen.

REST-API-URI

Der vollständige oder teilweise Pfad zu einer Ressource oder einem Satz zugehöriger Ressourcen. Der String muss mit beginnen `/api`. Wenn Sie keinen Wert angeben, gilt der Umfang für alle API-Endpunkte im ONTAP-Cluster.

Beispiele für den Umfang

Im Folgenden werden einige Beispiele für eigenständige Oszilloskope vorgestellt.

ontap*:joes-role:read_create_modify:*/API/Cluster

Bietet dem Benutzer, dem diese Rolle zugewiesen `/cluster` ist, den Zugriff auf den Endpunkt zu lesen, zu erstellen und zu ändern.

CLI-Verwaltungstool

Um die Verwaltung der eigenständigen Bereiche einfacher und weniger fehleranfällig `security oauth2 scope` zu machen, bietet ONTAP den CLI-Befehl, um auf der Grundlage Ihrer Eingabeparameter Scope Strings zu generieren.

Der Befehl `security oauth2 scope` hat zwei Anwendungsfälle basierend auf Ihrer Eingabe:

- CLI-Parameter für den Umfang einer Zeichenfolge

Mit dieser Version des Befehls können Sie auf Grundlage der Eingabeparameter eine Bereichszeichenfolge generieren.

- Scope-String zu CLI-Parametern

Sie können diese Version des Befehls verwenden, um die Befehlsparameter basierend auf der Zeichenfolge für den Eingabebereich zu generieren.

Beispiel

Im folgenden Beispiel wird eine Scope-String mit der Ausgabe generiert, die nach dem unten stehenden Befehlsbeispiel enthalten ist. Die Definition gilt für alle Cluster.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api /api/cluster
```

```
ontap:*:joes-role:readonly:*/api/cluster
```

Erfahren Sie mehr über `security oauth2 scope` in der ["ONTAP-Befehlsreferenz"](#).

OAuth 2.0 externe Rollenzuordnung in ONTAP

Eine externe Rolle wird bei einem Identifizieren-Anbieter definiert, der für die Verwendung durch ONTAP konfiguriert ist. Sie können Zuordnungsbeziehungen zwischen diesen externen Rollen und den ONTAP Rollen mit der ONTAP CLI erstellen und verwalten.



Sie können auch die externe Rollenzuordnungsfunktion mit der ONTAP REST-API konfigurieren. Erfahren Sie mehr in der ["Dokumentation zur ONTAP Automatisierung"](#).

Externe Rollen in einem Zugriffstoken

Hier ist ein Fragment eines JSON-Zugriffstoken, der zwei externe Rollen enthält.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Konfiguration

Sie können die externe Rollenzuordnungsfunktion über die ONTAP-Befehlszeilenschnittstelle verwalten.

Erstellen

Mit dem Befehl können Sie eine Rollenzuordnungsconfiguration definieren `security login external-role-mapping create`. Sie müssen auf der ONTAP **admin** Berechtigungsebene sein, um diesen Befehl sowie die damit verbundenen Optionen ausgeben zu können.

Parameter

Die Parameter, die zum Erstellen einer Gruppenzuordnung verwendet werden, werden im Folgenden beschrieben.

Parameter	Beschreibung
external-role	Der Name der Rolle, die beim externen Identitätsanbieter definiert wurde.
provider	Der Name des Identitätsanbieters. Dies sollte die Kennung für das System sein.
ontap-role	Gibt die vorhandene ONTAP-Rolle an, der die externe Rolle zugeordnet ist.

Beispiel

```
security login external-role-mapping create -external-role "Global Administrator" -provider entra -ontap-role admin
```

Erfahren Sie mehr über `security login external-role-mapping create` in der ["ONTAP-Befehlsreferenz"](#).

Zusätzliche CLI-Vorgänge

Der Befehl unterstützt mehrere zusätzliche Vorgänge, darunter:

- Anzeigen
- Ändern
- Löschen

Verwandte Informationen

- ["ONTAP-Befehlsreferenz"](#)

Wie ONTAP den Client-Zugriff bestimmt

Um OAuth 2.0 richtig zu entwickeln und zu implementieren, müssen Sie verstehen, wie Ihre Autorisierungskonfiguration von ONTAP verwendet wird, um Zugriffsentscheidungen für die Clients zu treffen. Die wichtigsten Schritte zur Bestimmung des Zugriffs sind unten auf der Grundlage der ONTAP Version dargestellt.



Es gab keine signifikanten Updates für OAuth 2.0 mit ONTAP 9.15.1. Wenn Sie Version 9.15.1 verwenden, lesen Sie die Beschreibung für ONTAP 9.14.1.

Verwandte Informationen

- ["In ONTAP unterstützte Funktionen von OAuth 2.0"](#)

ONTAP 9.16.1

ONTAP 9.16.1 erweitert die Standard-OAuth 2.0-Unterstützung um Microsoft-Entra-ID-spezifische Erweiterungen für native Entra-ID-Gruppen sowie externe Rollenzuordnung.

Bestimmen Sie den Client-Zugriff für ONTAP 9.16.1

Schritt 1: Eigenständige Bereiche

Wenn das Zugriffstoken eigenständige Bereiche enthält, untersucht ONTAP diese Bereiche zuerst. Wenn keine eigenständigen Bereiche vorhanden sind, mit Schritt 2 fortfahren.

Wenn ein oder mehrere eigenständige Bereiche vorhanden sind, wendet ONTAP jeden Bereich an, bis eine explizite **ALLOW**- oder **DENY**-Entscheidung getroffen werden kann. Wenn eine explizite Entscheidung getroffen wird, endet die Verarbeitung.

Wenn ONTAP keine explizite Zugriffsentscheidung treffen kann, fahren Sie mit Schritt 2 fort.

Schritt 2: Überprüfen Sie die lokale Rollenmarkierung

ONTAP überprüft den booleschen Parameter `use-local-roles-if-present`. Der Wert dieses Flags wird für jeden Autorisierungsserver, der für ONTAP definiert ist, separat festgelegt.

- Wenn der Wert lautet, `true` fahren Sie mit Schritt 3 fort.
- Wenn der Wert `false` verarbeitet wird, endet und der Zugriff verweigert wird.

Schritt 3: Benannte ONTAP REST-Rolle

Wenn das Zugriffstoken eine benannte REST-Rolle im Feld `scope` oder `scp` als Antrag enthält `scope`, verwendet ONTAP diese Rolle, um die Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine benannte REST-Rolle vorhanden ist oder die Rolle nicht gefunden wurde, fahren Sie mit Schritt 4 fort.

Schritt 4: Benutzer

Extrahieren Sie den Benutzernamen aus dem Zugriffstoken und versuchen Sie, ihn mit Benutzern zu vergleichen, die Zugriff auf die Anwendung „http“ haben. Die Benutzer werden anhand der Authentifizierungsmethode in der folgenden Reihenfolge untersucht:

- Passwort
- Domäne (Active Directory)
- Nsswitch (LDAP)

Wenn ein übereinstimmender Benutzer gefunden wird, verwendet ONTAP die für den Benutzer definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn ein Benutzer nicht stimmt oder kein Benutzername im Zugriffstoken vorhanden ist, fahren Sie mit Schritt 5 fort.

Schritt 5: Gruppen

Wenn eine oder mehrere Gruppen enthalten sind, wird das Format überprüft. Wenn die Gruppen als UUIDs dargestellt werden, wird eine interne Gruppenzuordnungstabelle durchsucht. Bei einer Gruppenübereinstimmung und einer zugehörigen Rolle verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW**- oder **DENY**-Entscheidung, und die Verarbeitung wird beendet. Weitere Informationen finden Sie unter ["Arbeiten mit OAuth 2.0- oder SAML-IdP-Gruppen in ONTAP"](#).

Wenn Gruppen als Namen dargestellt und mit Domain- oder nsswitch-Autorisierung konfiguriert werden,

versucht ONTAP, sie einer Active Directory- bzw. LDAP-Gruppe zuzuordnen. Wenn eine Gruppenübereinstimme vorhanden ist, verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine Gruppenübereinstimme vorhanden ist oder keine Gruppe im Zugriffstoken vorhanden ist, wird der Zugriff verweigert und die Verarbeitung wird beendet.

ONTAP 9.14.1

Die Unterstützung von OAuth 2.0 wird mit ONTAP 9.14.1 auf Basis der Standard-OAuth 2.0-Funktionen eingeführt.

Bestimmen Sie den Client-Zugriff für ONTAP 9.14.1

Schritt 1: Eigenständige Bereiche

Wenn das Zugriffstoken eigenständige Bereiche enthält, untersucht ONTAP diese Bereiche zuerst. Wenn keine eigenständigen Bereiche vorhanden sind, mit Schritt 2 fortfahren.

Wenn ein oder mehrere eigenständige Bereiche vorhanden sind, wendet ONTAP jeden Bereich an, bis eine explizite **ALLOW**- oder **DENY**-Entscheidung getroffen werden kann. Wenn eine explizite Entscheidung getroffen wird, endet die Verarbeitung.

Wenn ONTAP keine explizite Zugriffsentscheidung treffen kann, fahren Sie mit Schritt 2 fort.

Schritt 2: Überprüfen Sie die lokale Rollenmarkierung

ONTAP überprüft den booleschen Parameter `use-local-roles-if-present`. Der Wert dieses Flags wird für jeden Autorisierungsserver, der für ONTAP definiert ist, separat festgelegt.

- Wenn der Wert lautet, `true` fahren Sie mit Schritt 3 fort.
- Wenn der Wert `false` verarbeitet wird, endet und der Zugriff verweigert wird.

Schritt 3: Benannte ONTAP REST-Rolle

Wenn das Zugriffstoken eine benannte REST-Rolle im Feld oder `scp` enthält `scope`, verwendet ONTAP die Rolle, um die Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine benannte REST-Rolle vorhanden ist oder die Rolle nicht gefunden wurde, fahren Sie mit Schritt 4 fort.

Schritt 4: Benutzer

Extrahieren Sie den Benutzernamen aus dem Zugriffstoken und versuchen Sie, ihn mit Benutzern zu vergleichen, die Zugriff auf die Anwendung „http“ haben. Die Benutzer werden anhand der Authentifizierungsmethode in der folgenden Reihenfolge untersucht:

- Passwort
- Domäne (Active Directory)
- Nsswitch (LDAP)

Wenn ein übereinstimmender Benutzer gefunden wird, verwendet ONTAP die für den Benutzer definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn ein Benutzer nicht stimmt oder kein Benutzername im Zugriffstoken vorhanden ist, fahren Sie mit Schritt 5 fort.

Schritt 5: Gruppen

Wenn eine oder mehrere Gruppen eingeschlossen und mit einer Domain- oder nsswitch-Autorisierung konfiguriert sind, versucht ONTAP, sie einer Active Directory- bzw. LDAP-Gruppe zuzuordnen.

Wenn eine Gruppenübereinstimmung vorhanden ist, verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine Gruppenübereinstimmung vorhanden ist oder keine Gruppe im Zugriffstoken vorhanden ist,

wird der Zugriff verweigert und die Verarbeitung wird beendet.

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 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.