



Element API-Software

Element Software

NetApp
July 15, 2026

This PDF was generated from https://docs.netapp.com/de-de/element-software/api/concept_element_api_about_the_api.html on July 15, 2026. Always check docs.netapp.com for the latest.

Inhalt

Element API-Software	1
Erfahren Sie mehr über die Speicherverwaltung mit der Element API.	1
Gemeinsame Objekte	1
Gängige Methoden	1
Account-API-Methoden	1
Administrator-API-Methoden	2
Cluster-API-Methoden	2
API-Methoden zur Clustererstellung	2
Drive-API-Methoden	2
Fibre Channel-API-Methoden	2
Initiator-API-Methoden	2
LDAP-API-Methoden	3
Multi-Faktor-Authentifizierungs-API-Methoden	3
API-Methoden für die Sitzungsauthentifizierung	3
Node-API-Methoden	3
Replizierungs-API-Methoden	3
Sicherheits-API-Methoden	3
SnapMirror API-Methoden	4
Methoden für die Systemkonfiguration-API	4
Mandantenfähige Netzwerk-API-Methoden	4
Volume-API-Methoden	4
API-Methoden für Volume-Zugriffsgruppen	5
Volume Snapshot-API-Methoden	5
API-Methoden für virtuelle Volumes	5
Weitere Informationen	5
Fordern Sie Objektmitglieder an	5
Mitglieder des Antwortobjekts	6
Endpunkte anfordern	7
Cluster-API-Methoden	7
API-Methoden für die Cluster-Erstellung und das Bootstrap	7
API-Methoden pro Node	7
Weitere Informationen	7
API-Authentifizierung	7
Weitere Informationen	8
Asynchrone Methoden	8
Weitere Informationen	8
Merkmale	9
Objektmitglied	9
Anforderungsbeispiel	9

Element API-Software

Erfahren Sie mehr über die Speicherverwaltung mit der Element API.

Die Element-API basiert auf dem JSON-RPC-Protokoll über HTTPS. JSON-RPC ist ein einfaches textbasiertes RPC-Protokoll, das auf dem schlanken JSON-Datenwechselformat basiert. Client-Bibliotheken sind für alle wichtigen Programmiersprachen verfügbar.

API-Anforderungen können über HTTPS-POSTANFORDERUNGEN an den API-Endpunkt gestellt werden. Der Text der POST-Anforderung ist ein JSON-RPC Request-Objekt. Derzeit unterstützt die API keine Batchanforderungen (mehrere Anforderungsobjekte in einem EINZELNEN POST). Beim Senden von API-Anforderungen müssen Sie „Application/json-rpc“ als Inhaltstyp der Anfrage verwenden und sicherstellen, dass der Körper nicht formcodiert ist.



Die Element Web-UI nutzt die in diesem Dokument beschriebenen API-Methoden. Sie können API-Vorgänge in der Benutzeroberfläche überwachen, indem Sie das API-Protokoll aktivieren. Dadurch können Sie die Methoden anzeigen, die an das System ausgegeben werden. Sie können sowohl Anfragen als auch Antworten aktivieren, um zu sehen, wie das System auf die ausgestellten Methoden antwortet.

Sofern nicht anders angegeben, gelten alle Datumstrings in den API-Antworten im UTC+0-Format.



Wenn der Storage-Cluster stark ausgelastet ist oder Sie zahlreiche aufeinander folgende API-Anfragen ohne dazwischenende Verzögerungen senden, schlägt die Methode unter Umständen fehl und gibt den Fehler „xDBVersionMismatch“ zurück. In diesem Fall wiederholen Sie den Methodenaufruf.

Gemeinsame Objekte

Die API der Element Software verwendet JSON-Objekte, um organisierte Datenkonzepte darzustellen. Viele dieser API-Methoden nutzen diese Objekte für die Dateneingabe und -Ausgabe. Dieser Abschnitt dokumentiert diese häufig verwendeten Objekte; Objekte, die nur in einer einzigen Methode verwendet werden, werden mit dieser Methode anstelle von in diesem Abschnitt dokumentiert.

["Lerne gängige Gegenstände kennen"](#)

Gängige Methoden

Häufig verwendete Methoden sind Methoden zum Abrufen von Informationen über das Storage-Cluster, die API selbst oder fortlaufende API-Vorgänge.

["Lernen Sie gängige Methoden kennen"](#)

Account-API-Methoden

Mit Kontomethoden können Sie Konto- und Sicherheitsinformationen hinzufügen, entfernen, anzeigen und ändern.

["Erfahren Sie mehr über die API-Methoden für Konten."](#)

Administrator-API-Methoden

Mithilfe von Administrator-API-Methoden können Storage-Cluster-Administratoren Storage-Cluster-Administratoren erstellen, ändern, anzeigen und entfernen sowie Zugriffsebenen und Berechtigungen für Benutzer mit Zugriff auf ein Storage-Cluster zuweisen.

["Erfahren Sie mehr über die Administrator-API-Methoden."](#)

Cluster-API-Methoden

Mithilfe der Cluster-API-Methoden der Element Software können Sie die Konfiguration und Topologie des Storage-Clusters und der Nodes, die zu einem Storage-Cluster gehören, managen.

Einige Cluster-API-Methoden werden auf Nodes ausgeführt, die Teil eines Clusters sind oder für die Verbindung zu einem Cluster konfiguriert wurden. Sie können einem neuen Cluster oder einem vorhandenen Cluster Nodes hinzufügen. Nodes, die zu einem Cluster hinzugefügt werden können, befinden sich in einem „ausstehend“, was bedeutet, dass sie konfiguriert, jedoch noch nicht dem Cluster hinzugefügt wurden.

["Erfahren Sie mehr über Cluster-API-Methoden."](#)

API-Methoden zur Clustererstellung

Sie können diese API-Methoden verwenden, um ein Storage-Cluster zu erstellen. Alle diese Methoden müssen auf einem einzelnen Node gegen den API-Endpunkt eingesetzt werden.

["Erfahren Sie mehr über die API-Methoden zur Clustererstellung."](#)

Drive-API-Methoden

Mit den Drive-API-Methoden können Laufwerke hinzugefügt und gemanagt werden, die einem Storage-Cluster zur Verfügung stehen. Wenn Sie dem Storage-Cluster einen Storage-Node hinzufügen oder neue Laufwerke in einem vorhandenen Storage-Node installieren, können die Laufwerke dem Storage-Cluster hinzugefügt werden.

["Erfahren Sie mehr über die Drive-API-Methoden."](#)

Fibre Channel-API-Methoden

Fibre Channel-API-Methoden können zum Hinzufügen, Ändern oder Entfernen von Fibre Channel-Node-Mitgliedern eines Storage-Clusters verwendet werden.

["Erfahren Sie mehr über Fibre Channel API-Methoden"](#)

Initiator-API-Methoden

Mithilfe von Initiator-Methoden können Sie iSCSI-Initiator-Objekte hinzufügen, entfernen, anzeigen und ändern, die die Kommunikation zwischen dem Speichersystem und externen Speicher-Clients behandeln.

["Erfahren Sie mehr über die Initiator-API-Methoden."](#)

LDAP-API-Methoden

Sie können das Lightweight Directory Access Protocol (LDAP) verwenden, um den Zugriff auf Element Storage zu authentifizieren. Mit den in diesem Abschnitt beschriebenen LDAP-API-Methoden können Sie den LDAP-Zugriff auf das Storage-Cluster konfigurieren.

["Erfahren Sie mehr über die LDAP-API-Methoden."](#)

Multi-Faktor-Authentifizierungs-API-Methoden

Sie können Multi-Faktor-Authentifizierung (MFA) verwenden, um Benutzersitzungen über einen Drittanbieter-Identitätsanbieter (IdP) über die Security Assertion Markup Language (SAML) zu verwalten.

["Erfahren Sie mehr über API-Methoden zur Multi-Faktor-Authentifizierung."](#)

API-Methoden für die Sitzungsauthentifizierung

Sie können die sitzungsbasierte Authentifizierung verwenden, um Benutzersitzungen zu verwalten.

["Erfahren Sie mehr über die API-Methoden zur Sitzungsauthentifizierung."](#)

Node-API-Methoden

Sie können Node-API-Methoden verwenden, um einzelne Nodes zu konfigurieren. Diese Methoden arbeiten auf einzelnen Nodes, die konfiguriert werden müssen, konfiguriert sind, aber noch nicht an einem Cluster beteiligt sind oder aktiv an einem Cluster teilnehmen. Mithilfe von Node-API-Methoden können Sie Einstellungen für einzelne Nodes und das Cluster-Netzwerk, das zur Kommunikation mit dem Node verwendet wird, anzeigen und ändern. Sie müssen diese Methoden für einzelne Nodes ausführen. Sie können keine API-Methoden pro Node für die Adresse des Clusters ausführen.

["Lernen Sie die Node-API-Methoden kennen."](#)

Replizierungs-API-Methoden

Mit den Replication-API-Methoden können Sie zwei Cluster verbinden, um einen kontinuierlichen Datenschutz (CDP) zu ermöglichen. Wenn Sie zwei Cluster verbinden, können aktive Volumes innerhalb eines Clusters kontinuierlich auf ein zweites Cluster repliziert werden, um eine Datenwiederherstellung bereitzustellen. Durch das Pairing von Volumes zur Replikation können Sie Ihre Daten vor Ereignissen schützen, die den Zugriff auf diese Dateien möglicherweise nicht ermöglichen.

["Erfahren Sie mehr über die Replikations-API-Methoden."](#)

Sicherheits-API-Methoden

Sie können Element Software in externe, sicherheitsbezogene Services wie einen externen Verschlüsselungsmanagementserver integrieren. Mit diesen sicherheitsbezogenen Methoden können Sie Sicherheitsfunktionen für Komponenten wie externes Verschlüsselungsmanagement für die Verschlüsselung im Ruhezustand konfigurieren.

["Erfahren Sie mehr über Sicherheits-API-Methoden."](#)

SnapMirror API-Methoden

Die SnapMirror API-Methoden werden von der Element Web-Benutzeroberfläche zum Management von Snapshots verwendet, die mit Remote-ONTAP-Systemen gespiegelt wurden. Diese Methoden sind nur für die Verwendung durch Element Web UI gedacht. Wenn Sie API-Zugriff auf die SnapMirror-Funktion benötigen, verwenden Sie die ONTAP-APIs. Beispiele für Anfragen und Rückgabeverfahren werden nicht für SnapMirror API-Methoden zur Verfügung gestellt.

["Erfahren Sie mehr über die SnapMirror API-Methoden."](#)

Methoden für die Systemkonfiguration-API

Mit Systemkonfigurations-API-Methoden können Sie Konfigurationswerte abrufen und festlegen, die für alle Knoten im Cluster gelten.

["Erfahren Sie mehr über die API-Methoden zur Systemkonfiguration."](#)

Mandantenfähige Netzwerk-API-Methoden

Das mandantenfähige Netzwerk in Element Storage-Clustern ermöglicht den Datenverkehr zwischen mehreren Clients, die sich in separaten logischen Netzwerken befinden, ohne Layer-3-Routing mit einem Element Storage-Cluster verbunden werden.

Verbindungen zum Storage-Cluster sind im Netzwerk-Stack durch VLAN-Tagging getrennt.

Voraussetzungen für die Einrichtung eines mandantenfähigen virtuellen Netzwerks

- Sie müssen den Block der Client-Netzwerk-IP-Adressen identifiziert haben, die den virtuellen Netzwerken auf den Storage-Nodes zugewiesen werden sollen.
- Sie müssen eine SVIP-Adresse (Client Storage Network IP) für den gesamten Storage-Datenverkehr als Endpunkt angegeben haben.

Reihenfolge der Vorgänge virtueller Netzwerke

1. Verwenden Sie die AddVirtualNetwork-Methode, um die IP-Adressen, die Sie eingeben, in Massen bereitzustellen.

Nachdem Sie ein virtuelles Netzwerk hinzugefügt haben, führt der Cluster automatisch die folgenden Schritte aus:

- Jeder Storage-Node erstellt eine virtuelle Netzwerkschnittstelle.
 - Jedem Speicherknoten wird eine VLAN-Adresse zugewiesen, die über das virtuelle SVIP weitergeleitet werden kann.
 - Bei einem Neubooten eines Node bleiben VLAN-IP-Adressen auf jedem Node erhalten.
2. Wenn die virtuelle Netzwerkschnittstelle und die VLAN-Adressen zugewiesen wurden, können Sie dem virtuellen SVIP Client-Netzwerkverkehr zuweisen.

["Erfahren Sie mehr über Multitenant-Netzwerk-API-Methoden"](#)

Volume-API-Methoden

Mit Element Software für die Volume-API-Methoden können Sie Volumes managen, die sich auf einem

Storage-Node befinden. Mit diesen Methoden können Sie Volumes erstellen, ändern, klonen und löschen. Sie können auch Volume-API-Methoden verwenden, um Datenmessungen für ein Volume zu erfassen und anzuzeigen.

["Erfahren Sie mehr über die Volume-API-Methoden."](#)

API-Methoden für Volume-Zugriffsgruppen

Mit Methoden für Volume-Zugriffsgruppen können Sie Volume-Zugriffsgruppen hinzufügen, entfernen, anzeigen und ändern. Dabei handelt es sich um Sammlungen von Volumes, auf die Benutzer über iSCSI- oder Fibre-Channel-Initiatoren zugreifen können.

["Erfahren Sie mehr über die API-Methoden für Volumenzugriffsgruppen."](#)

Volume Snapshot-API-Methoden

Mit Element Software Volume Snapshot-API-Methoden können Sie Volume-Snapshots verwalten. Mithilfe der API-Methoden für den Volume-Snapshot können Volume-Snapshots erstellt, geändert, geklont und gelöscht werden.

["Erfahren Sie mehr über die API-Methoden für Volume-Snapshots."](#)

API-Methoden für virtuelle Volumes

Mit Element Software können Sie Virtual Volume API-Methoden (VVols) managen. Vorhandene VVols können mit diesen API-Methoden angezeigt werden sowie Storage Container für virtuelle Volumes erstellen, ändern und löschen. Obwohl Sie diese Methoden nicht zum Betrieb auf normalen Volumes verwenden können, können Sie die normalen Volume-API-Methoden verwenden, um Informationen über VVols aufzulisten.

["Erfahren Sie mehr über die API-Methoden für virtuelle Volumes."](#)

Weitere Informationen

- ["Dokumentation von SolidFire und Element Software"](#)
- ["Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"](#)

Fordern Sie Objektmitglieder an

Jede Element Software-API-Anforderung besitzt die folgenden grundlegenden Komponenten:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Methode	Name der anzurufenden Methode.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Parameter	Objekt, das die Parameter für die aufgerufene Methode enthält. Benannte Parameter sind erforderlich. Positionsparameter (als Array übergeben) sind nicht zulässig.	JSON-Objekt	{}	Nein
id	Die Kennung, die für die Antwort der Anforderung verwendet wurde, wurde im Ergebnis zurückgegeben.	Zeichenfolge oder Ganzzahl	{}	Nein

Mitglieder des Antwortobjekts

Jeder Element Software-API-Antwortkörper hat die folgenden grundlegenden Bestandteile:

Name	Beschreibung	Typ
Ergebnis	Das von der Methode zurückgegebene Objekt. Das System gibt ein Objekt mit benannten Mitgliedern zurück, die dem dokumentierten Rückgabewert der Methode entsprechen. Dieses Mitglied ist nicht vorhanden, wenn ein Fehler aufgetreten ist.	JSON-Objekt
Fehler	Das Objekt wird bei Auftreten eines Fehlers zurückgegeben. Dieses Mitglied ist nur vorhanden, wenn ein Fehler aufgetreten ist.	Objekt
id	Eine Kennung, die der Anforderung der Antwort entspricht, wie in der Anforderung angegeben.	Zeichenfolge oder Ganzzahl
UnusedParameter	Eine Warnmeldung, dass mindestens ein falscher Parameter an die API-Methode übergeben wurde und nicht verwendet wurde.	Objekt

Endpunkte anfordern

Die API verwendet drei Typen von Anforderungsendpunkten (Storage-Cluster, Storage-Cluster-Erstellung und pro Node). Sie sollten immer den neuesten Endpunkt verwenden, der von Ihrer Version der Element Software unterstützt wird.

Die drei Anforderungsendpunkte in der API sind wie folgt gekennzeichnet:

Cluster-API-Methoden

Der HTTPS-Endpunkt für Storage-Cluster-weite API-Anforderungen ist `https://<mvip>/json-rpc/<api-version>`, Wo:

- `<mvip>` Ist die Management-virtuelle IP-Adresse für das Storage-Cluster.
- `<api-version>` Ist die Version der API, die Sie verwenden.

API-Methoden für die Cluster-Erstellung und das Bootstrap

Der HTTPS-Endpunkt zum Erstellen eines Storage-Clusters und zum Zugriff auf Bootstrap-API-Anforderungen ist `https://<nodeIP>/json-rpc/<api-version>`, Wo:

- `<nodeIP>` Die IP-Adresse des Node, den Sie dem Cluster hinzufügen.
- `<api-version>` Ist die Version der API, die Sie verwenden.

API-Methoden pro Node

Der HTTPS-Endpunkt für individuelle API-Anforderungen an den Storage-Node ist `https://<nodeIP>:442/json-rpc/<api-version>`, Wo:

- `<nodeIP>` Ist die Management-IP-Adresse des Storage-Node; 442 ist der Port, auf dem der HTTPS-Server ausgeführt wird.
- `<api-version>` Ist die Version der API, die Sie verwenden.

Weitere Informationen

- ["Dokumentation von SolidFire und Element Software"](#)
- ["Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"](#)

API-Authentifizierung

Sie können sich beim Verwenden der API mit dem System authentifizieren, indem Sie eine HTTP Basic-Authentifizierungskopfzeile mit allen API-Anforderungen verwenden. Wenn Sie keine Authentifizierungsinformationen angeben, weist das System die nicht authentifizierte Anfrage mit einer HTTP 401-Antwort zurück. Das System unterstützt die HTTP Basic-Authentifizierung über TLS.

Verwenden Sie das Cluster-Administratorkonto für die API-Authentifizierung.

Weitere Informationen

- ["Dokumentation von SolidFire und Element Software"](#)
- ["Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"](#)

Asynchrone Methoden

Einige API-Methoden sind asynchron. Dies bedeutet, dass der von ihnen vorführen Vorgang möglicherweise nicht abgeschlossen ist, wenn die Methode zurückkehrt. Asynchrone Methoden geben ein Handle zurück, das Sie abfragen können, um den Status des Vorgangs anzuzeigen. Statusinformationen für einige Vorgänge können einen prozentualen Anteil der Fertigstellung enthalten.

Wenn Sie einen asynchronen Vorgang abfragen, kann dessen Ergebnis einer der folgenden Typen sein:

- `DriveAdd`: Das System fügt dem Cluster ein Laufwerk hinzu.
- `BulkVolume`: Das System führt einen Kopiervorgang zwischen Volumes durch, z. B. eine Sicherung oder Wiederherstellung.
- `Clone`: Das System kloniert ein Volumen.
- `DriveRemoval`: Das System kopiert Daten von einem Laufwerk in Vorbereitung, um es aus dem Cluster zu entfernen.
- `RtFiPendingNode`: Das System installiert kompatible Software auf einem Knoten, bevor sie dem Cluster hinzugefügt wird.

Beachten Sie die folgenden Punkte, wenn Sie asynchrone Methoden verwenden oder den Status eines laufenden asynchronen Vorgangs erhalten:

- Asynchrone Methoden sind in der Dokumentation der einzelnen Methoden angegeben.
- Asynchrone Methoden geben eine „`Async`“ zurück, ein Griff, der durch die emittierenden API-Methode bekannt ist. Mit dem Handle können Sie den Status oder das Ergebnis des asynchronen Vorgangs abfragen.
- Sie können das Ergebnis einzelner asynchroner Methoden mit der `GetAsyncResult`-Methode abrufen. Wenn Sie `GetAsyncResult` verwenden, um einen abgeschlossenen Vorgang abzufragen, gibt das System das Ergebnis zurück und reinigt das Ergebnis automatisch vom System. Wenn Sie `GetAsyncResult` verwenden, um eine unvollständige Operation abzufragen, gibt das System das Ergebnis zurück, löscht es aber nicht.
- Sie können den Status und die Ergebnisse aller ausgeführten oder abgeschlossenen asynchronen Methoden mit der `ListAsyncResults`-Methode abrufen. In diesem Fall löscht das System die Ergebnisse für abgeschlossene Vorgänge nicht.

Weitere Informationen

- ["Dokumentation von SolidFire und Element Software"](#)
- ["Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"](#)

Merkmale

Viele API-Anfragen und -Antworten verwenden Objekte sowie einfache Typen. Objekte sind eine Sammlung von Schlüsselwert-Paaren, wobei der Wert ein einfacher Typ oder möglicherweise ein anderes Objekt ist. Attribute sind benutzerdefinierte Name-Wert-Paare, die vom Benutzer in JSON-Objekten festgelegt werden können. Mithilfe einiger Methoden können Sie beim Erstellen oder Ändern von Objekten Attribute hinzufügen.

Für codierte Attributobjekte gibt es eine Begrenzung von 1000 Byte.

Objektmitglied

Dieses Objekt enthält das folgende Mitglied:

Name	Beschreibung	Typ
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt

Anforderungsbeispiel

Das folgende Anforderungsbeispiel verwendet die AddClusterAdmin-Methode:

```
{
  "method": "AddClusterAdmin",
  "params": {
    "username": "joeadmin",
    "password": "68!5Aru268)$",
    "access": [
      "volume",
      "reporting"
    ],
    "attributes": {
      "name1": "value1",
      "name2": "value2",
      "name3": "value3"
    }
  }
}
```

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.