



Managen von Cloud Volumes

Cloud Volumes Service

NetApp

October 04, 2023

Inhalt

- Managen von Cloud Volumes 1
 - Erstellen eines Cloud Volume 1
 - Cloud-Volume mounten 7
 - Ändern eines Cloud-Volumes 8
 - Löschen eines Cloud-Volumes 9

Managen von Cloud Volumes

Erstellen eines Cloud Volume

Sie erstellen Cloud Volumes über die NetApp Cloud Orchestrator Website.

Voraussetzungen

Ihre AWS-Umgebung muss bestimmte Anforderungen erfüllen, bevor Sie Ihr erstes Cloud-Volume erstellen können. Für jede AWS Region, in der Cloud-Volumes implementiert werden sollen, sind folgende Eigenschaften erforderlich:

- Virtuelle Private Cloud (VPC)
- Virtual Private Gateway (VGW), das mit Ihrem VPC verbunden ist
- Subnetz für die VPC
- Definierte Routen, die das Netzwerk einschließen, auf dem Cloud Volumes ausgeführt werden
- Optional ein Direct Connect Gateway

Zum Erstellen Ihres ersten Cloud-Volumes in einer Region müssen Sie über die folgenden Informationen verfügen:

- **AWS Konto-ID:** Eine 12-stellige Amazon-Account-ID ohne Striche.
- **Classless Inter-Domain Routing (CIDR) Block:** Ein nicht verwendeter IPv4-CIDR-Block. Das Netzwerkpräfix muss zwischen /16 und /28 liegen und muss auch innerhalb der Bereiche liegen, die für private Netzwerke reserviert sind (RFC 1918). Wählen Sie kein Netzwerk aus, das Ihre VPC-CIDR-Zuweisungen überschneidet.
- Sie müssen die richtige Region ausgewählt haben, in der Sie den Service verwenden möchten. Siehe ["Wählen Sie die Region aus"](#).

Falls Sie die erforderlichen AWS Netzwerkkomponenten nicht konfiguriert haben, finden Sie im ["NetApp Cloud Volumes Service für AWS – Kontoeinrichtung"](#) Leitfaden für weitere Informationen.

Hinweis: Wenn Sie planen, ein SMB-Volume zu erstellen, müssen Sie einen Windows Active Directory-Server zur Verfügung haben, mit dem Sie eine Verbindung herstellen können. Sie geben diese Informationen bei der Erstellung des Volumes ein. Stellen Sie außerdem sicher, dass der Admin-Benutzer in der Lage ist, ein Maschinenkonto im angegebenen Organisationseinheit-Pfad (OU) zu erstellen.

Geben Sie die Volume-Details ein

Füllen Sie die Felder oben auf der Seite „Volume erstellen“ aus, um den Namen, die Größe, das Service Level und mehr des Volumes zu definieren.

1. Nachdem Sie sich beim angemeldet haben ["NetApp Cloud Orchestrator"](#) Site mit der E-Mail-Adresse, die Sie während Ihres Abonnements angegeben haben, und Sie haben ["Die Region ausgewählt"](#) Klicken Sie auf die Schaltfläche **Neues Volume erstellen**.

The screenshot shows the 'Create volume' interface with the following configuration:

- Protocol: NFS
- Name: (empty)
- Region Required: us-east-1
- Timezone: Any
- Volume path Required: lonely-stoic-yonath
- Service level Required: Standard
- Allocated capacity: 1000 GB
- NFS version: NFSv3
- Security style: UNIX
- Tags: (empty)
- Checkbox: Show snapshot directory (read-only)

2. Wählen Sie auf der Seite Create Volume **NFS**, **SMB** oder **Dual-Protocol** als Protokoll für das Volumen, das Sie erstellen möchten.
3. Geben Sie im Feld **Name** den Namen an, den Sie für das Volume verwenden möchten.
4. Wählen Sie im Feld **Region** die Region AWS aus, in der Sie das Volume erstellen möchten. Diese Region muss mit der Region übereinstimmen, die Sie für AWS konfiguriert haben.
5. Wählen Sie im Feld **Zeitzone** Ihre Zeitzone aus.
6. Geben Sie im Feld **Volume PATH** den Pfad an, den Sie verwenden möchten, oder übernehmen Sie den automatisch generierten Pfad.
7. Wählen Sie im Feld **Service Level** das Leistungsniveau für die Lautstärke aus: **Standard**, **Premium** oder **Extreme**.

Siehe "[Auswählen des Service-Levels](#)" Entsprechende Details.

8. Wählen Sie im Feld **zugewiesene Kapazität** die erforderliche Kapazität aus. Beachten Sie, dass die Anzahl der verfügbaren Inodes von der zugewiesenen Kapazität abhängt.

Siehe "[Auswählen der zugewiesenen Kapazität](#)" Entsprechende Details.

9. Wählen Sie im Feld **NFS Version** die Option **NFSv3**, **NFSv4.1** oder **beides** aus, je nach Ihren Anforderungen.
10. Wenn Sie das Dual-Protokoll ausgewählt haben, können Sie den Sicherheitsstil im Feld **Sicherheitsstil** auswählen, indem Sie im Dropdown-Menü **NTFS** oder **UNIX** wählen.

Sicherheitsstile beeinflussen den verwendeten Berechtigungstyp und die Art der Änderung der Berechtigungen.

- UNIX verwendet Bits im NFSv3 Modus, und nur NFS-Clients können Berechtigungen ändern.
- NTFS verwendet NTFS ACLs. Nur SMB-Clients können Berechtigungen ändern.

11. Behalten Sie im Feld **Snapshot-Verzeichnis** den Standardwert bei, in dem Sie das Snapshot-Verzeichnis für dieses Volume anzeigen können, oder deaktivieren Sie das Kästchen, um die Liste der Snapshot-

Kopien auszublenden.

Netzwerkdetails eingeben (einmalige Einstellung pro AWS Region)

Wenn Sie zum ersten Mal in dieser AWS-Region ein Cloud-Volume erstellt haben, wird der Abschnitt **Network** angezeigt, damit Sie Ihr Cloud Volumes-Konto mit Ihrem AWS-Konto verbinden können:

1. Geben Sie im Feld * CIDR (IPv4)* den gewünschten IPv4-Bereich für die Region ein. Das Netzwerkpräfix muss zwischen /16 und /28 liegen. Das Netzwerk muss auch innerhalb der Bereiche liegen, die für private Netzwerke reserviert sind (RFC 1918). Wählen Sie kein Netzwerk aus, das Ihre VPC-CIDR-Zuweisungen überschneidet.
2. Geben Sie im Feld **AWS Account ID** Ihre 12-stellige Amazon-Account-ID ohne Bindestriche ein.

Network

! You do not yet have your Cloud Volumes account connected to your AWS account. To connect these accounts we need your AWS network information. Please enter a valid private network CIDR (RFC1918) with a prefix ranging between /16 and /28 that does not overlap with your existing networks. See the [Cloud Volumes Service for AWS Account Setup document](#) for details.

CIDR (IPv4) Required ? AWS account ID Required

192.168.0.0/28

Regeln für die Exportrichtlinie eingeben (optional)

Wenn Sie NFS oder Dual-Protocol ausgewählt haben, können Sie im Abschnitt **Richtlinie exportieren** eine Exportrichtlinie erstellen, um die Clients zu identifizieren, die auf das Volume zugreifen können:

1. Geben Sie im Feld **zulässige Clients** die zulässigen Clients unter Verwendung einer IP-Adresse oder eines Classless Inter-Domain Routing (CIDR) an.
2. Wählen Sie im Feld **Zugriff** die Option **Lesen & Schreiben** oder **Schreibgeschützt** aus.
3. Wählen Sie im Feld **Protocols** das Protokoll (oder Protokolle, wenn das Volume NFSv3 und NFSv4.1 Zugriff erlaubt) aus, das für den Benutzerzugriff verwendet wird.

Export policy

+ Add export policy rule

Rule index	Allowed clients <small>Required</small>	Access	Protocol/s
Rule-1	0.0.0.0/0	Read & Write Read only	NFSv3 NFSv4.1

i "Allowed clients" will accept a comma separated list of IPs (v4) and/or cidrs. In most cases this is the private IP of your instance/VM. If using public IPs please be aware that they have to be reachable from the volume's network for the export policy to work correctly.

Klicken Sie auf **+ Regel für Exportrichtlinie hinzufügen**, wenn Sie zusätzliche Regeln für die Exportrichtlinie definieren möchten.

Datenverschlüsselung aktivieren (optional)

1. Wenn Sie SMB oder Dual-Protocol ausgewählt haben, können Sie die SMB-Sitzungsverschlüsselung aktivieren, indem Sie das Kontrollkästchen für das Feld **SMB3 Protocol Encryption** aktivieren aktivieren aktivieren aktivieren aktivieren aktivieren aktivieren aktivieren aktivieren.

Hinweis: Aktivieren Sie die Verschlüsselung nicht, wenn SMB 2.1 Clients das Volume mounten müssen.

Integrieren des Volumes in einen Active Directory Server (SMB und Dual Protocol)

Wenn Sie SMB oder Dual-Protocol ausgewählt haben, können Sie wählen, ob das Volume mit einem Windows Active Directory-Server oder einem von AWS verwalteten Microsoft AD im Abschnitt **Active Directory** integriert werden soll.

Wählen Sie im Feld **Verfügbare Einstellungen** einen vorhandenen Active Directory-Server aus oder fügen Sie einen neuen AD-Server hinzu.

So konfigurieren Sie eine Verbindung zu einem neuen AD-Server:

1. Geben Sie im Feld **DNS-Server** die IP-Adresse(n) des/der DNS-Server ein. Verwenden Sie ein Komma, um die IP-Adressen zu trennen, wenn Sie auf mehrere Server verweisen, z. B. 172.31.25.223, 172.31.2.74.
2. Geben Sie im Feld **Domäne** die Domäne für die SMB-Freigabe ein.

Verwenden Sie bei Verwendung von AWS Managed Microsoft AD den Wert aus dem Feld „Directory DNS Name“.

3. Geben Sie im Feld **SMB Server NetBIOS** einen NetBIOS-Namen für den zu erstellenden SMB-Server ein.
4. Geben Sie im Feld **Organisationseinheit** „CN=Computer“ für Verbindungen zu Ihrem eigenen Windows Active Directory-Server ein.

Bei Verwendung von AWS Managed Microsoft AD muss die Organisationseinheit im Format „OU=<NetBIOS_Name>“ eingegeben werden. Beispiel: **OU=AWSmanagedAD**.

Um eine geschachtelte Organisationseinheit zu verwenden, müssen Sie zuerst die OU der niedrigsten Ebene bis zur OU der höchsten Ebene aufrufen. BEISPIEL:
OU=THIRDLEVEL,OU=SECONDLEVEL,OU=FIRLEVEL.

5. Geben Sie im Feld **Benutzername** einen Benutzernamen für Ihren Active Directory-Server ein.


Sie können jeden Benutzernamen verwenden, der zum Erstellen von Computerkonten in der Active Directory-Domäne autorisiert ist, zu der Sie sich dem SMB-Server anschließen.

6. Geben Sie im Feld **Passwort** das Passwort für den von Ihnen angegebenen AD-Benutzernamen ein.

Enable SMB3 Protocol Encryption ?

Active directory

Available settings

 \\cloudvol.NGS-AWS.local


DNS server Required

Domain Required

NetBIOS Required ?

Organizational unit ?

Username Required

Password Required 

Siehe ["Entwerfen einer Standorttopologie für Active Directory Domain Services"](#) Richtlinien zum Design einer optimalen Microsoft AD-Implementierung

Siehe ["Einrichtung des AWS Directory Service mit NetApp Cloud Volumes Service für AWS"](#) Ausführliche Anweisungen zur Verwendung von AWS Managed Microsoft AD finden Sie in diesem Leitfaden.



Sie sollten die Anleitung zu den AWS-Sicherheitseinstellungen befolgen, um die korrekte Integration von Cloud Volumes in Windows Active Directory-Server zu ermöglichen. Siehe ["Einstellungen der AWS Sicherheitsgruppen für Windows AD Server"](#) Finden Sie weitere Informationen.

Hinweis: UNIX-Benutzer, die das Volume mit NFS mounten, werden als Windows-Benutzer "root" für UNIX-Root und "pcuser" für alle anderen Benutzer authentifiziert. Stellen Sie sicher, dass diese Benutzerkonten in Active Directory vorhanden sind, bevor Sie ein Dual-Protokoll-Volume bei der Verwendung von NFS mounten.

Erstellen einer Snapshot-Richtlinie (optional)

Wenn Sie eine Snapshot-Policy für dieses Volume erstellen möchten, geben Sie die Details im Abschnitt **Snapshot-Richtlinie** ein:

1. Wählen Sie die Snapshot-Frequenz aus: **Stündlich**, **täglich**, **wöchentlich** oder **monatlich**.
2. Wählen Sie die Anzahl der zu behenden Snapshots aus.
3. Wählen Sie den Zeitpunkt, zu dem der Snapshot erstellt werden soll.

Snapshot policy ▼

Hourly
 Daily
 Weekly
 Monthly

Snapshots to keep:
 Hour:
 Minute:

Explanation: Will take a snapshot every day at 1:05 AM and keep 7 of the most recent snapshots.

Sie können weitere Snapshot-Richtlinien erstellen, indem Sie die oben beschriebenen Schritte wiederholen oder die Registerkarte Snapshots im linken Navigationsbereich auswählen.

Erstellen Sie das Volume

1. Scrollen Sie nach unten auf der Seite und klicken Sie auf **Lautstärke erstellen**.

Wenn Sie zuvor ein Cloud-Volume in dieser Region erstellt haben, wird das neue Volume auf der Seite Volumes angezeigt.

Wenn dies das erste Cloud-Volume ist, das Sie in dieser AWS-Region erstellt haben und Sie die Netzwerkinformationen im Abschnitt Netzwerk dieser Seite eingegeben haben, wird ein Fortschrittsdialog angezeigt, in dem die nächsten Schritte angezeigt werden, die Sie befolgen müssen, um das Volume mit AWS-Schnittstellen zu verbinden.

Network and volume creation in progress... ✕

Accepting virtual interfaces

1. Open the [AWS DirectConnect Management console](#).
2. Accept the virtual interfaces `NetApp-CloudVolumes-1A` and `NetApp-CloudVolumes-2B`, they should appear momentarily.
3. When accepting the virtual interfaces, make sure to attach them to the VirtualGateway/DirectConnect gateway with the ASN number you provided (64512).
4. Cloud Volumes will then attempt to establish a BGP session with your provided network configuration, this can take up to 10 minutes.
5. On successful completion, your new volume will be created.

2. Akzeptieren Sie die virtuellen Schnittstellen, wie in Abschnitt 6.4 beschrieben "[NetApp Cloud Volumes Service für AWS – Kontoeinrichtung](#)" Begleiten. Sie müssen diese Aufgabe innerhalb von 10 Minuten ausführen, oder das System kann sich abstellen.

Wenn die Schnittstellen nicht innerhalb von 10 Minuten angezeigt werden, kann es ein Konfigurationsproblem geben; in diesem Fall sollten Sie sich an den Support wenden.

Nachdem die Schnittstellen und andere Netzwerkkomponenten erstellt wurden, wird das erstellte Volume auf der Seite Volumes angezeigt, und das Feld Aktionen wird als verfügbar aufgeführt.

<input type="checkbox"/>	Name ↓	Export path/s	Region	Allocated capacity	Created	Actions
<input type="checkbox"/>	Cloud_Volume_013	NFS: 172.16.80.36/jolly-nostalgic-walsh (🔗)	us-east	1 TB	2018-07-20 20:01:16	Available ▼

Nachdem Sie fertig sind

Weiter mit "[Cloud-Volume mounten](#)".

Cloud-Volume mounten

Ein Cloud-Volume kann in Ihre AWS Instanz eingebunden werden. Cloud Volumes unterstützen derzeit NFSv3 und NFSv4.1 für Linux- und UNIX-Clients sowie SMB 2.1, 3.0 und 3.1.1 für Windows-Clients.

Hinweis: Bitte verwenden Sie das hervorgehobene Protokoll/Dialekt, das von Ihrem Kunden unterstützt wird.

Schritte

1. Erhalten Sie Mount-Anweisungen für das von Ihnen erstellte Volumen, indem Sie auf das blaue Fragezeichen (?) klicken. Am Ende des Feldes Exportpfade neben dem Namen des Volumes.

Wenn Sie den Mauszeiger über das Fragezeichen bewegen, wird **Mount-Anweisungen anzeigen** angezeigt.



2. Klicken Sie auf das Fragezeichen, um die Montageanweisungen anzuzeigen.

NFS-Beispiel:

Setting up your instance

1. Open an SSH client and connect to your instance.
2. Install the nfs client on your instance.
 - On Red Hat Enterprise Linux or CentOS Linux instance:


```
sudo yum install -y nfs-utils
```
 - On an Ubuntu or Debian instance:


```
sudo apt-get install nfs-common
```

Mounting your volume

1. Create a new directory on your instance, such as "g":


```
sudo mkdir g
```
2. Mount your NFSv3 volume using the example command below:


```
sudo mount -t nfs -o rw,hard,rsize=65536,wsiz=65536,vers=3,tcp 172.25.0.4:/tender-modest-hofstadter g
```

Note. Please use mount options appropriate for your specific workloads when known.

Die von definierte maximale I/O-Größe `rsiz` Und `wsiz` Optionen sind 1048576, allerdings wird für die meisten Anwendungsfälle der empfohlene Standardwert von 65536 verwendet.

Beachten Sie, dass Linux-Clients standardmäßig NFSv4.1 verwenden, sofern die Version nicht angegeben wird.

SMB-Beispiel:

Mount instructions
✕

Mapping your network drive

1. Click the Start button and then click on Computer.
2. Click Map Network Drive.
3. In the Drive list, click any available drive letter.
4. In the Folder box, type `\\test.cv-pm.local\silly-condescending-mcnulty` . To connect every time you log on to your computer, select the Reconnect at logon check box.
5. Click Finish.

3. Stellen Sie über eine SSH oder RDP-Client eine Verbindung zu Ihrer Amazon Elastic Compute Cloud (EC2) Instanz her, und befolgen Sie dann die Mount-Anweisungen für Ihre Instanz.

Nach Abschluss der Schritte in der Mount-Anleitung haben Sie das Cloud-Volume erfolgreich in die AWS-Instanz eingebunden.

Ändern eines Cloud-Volumes

Sie können vorhandene Volumes ändern, darunter auch die Änderung des Volumes-Namens, der zugewiesenen Kapazität oder des Service-Levels.

Schritte

1. Melden Sie sich bei an ["NetApp Cloud Orchestrator"](#).

2. Klicken Sie auf den Namen des Volumes, das Sie verwalten möchten.

3. Ändern Sie die folgenden Volume-Felder, falls zutreffend:

- Name
- Tags
- Zugewiesene Kapazität
- Service-Level

Eine Änderung des Service-Levels ist nicht mit Unterbrechungen verbunden und hat keine Auswirkung auf den Zugriff auf die Client-Daten.

Beachten Sie, dass die Anzahl der verfügbaren Inodes von der zugewiesenen Kapazität abhängt.

Siehe "[Auswahl des entsprechenden Service Levels und der zugewiesenen Kapazität](#)" Entsprechende Details.

Löschen eines Cloud-Volumes

Sie können ein nicht mehr benötigter Cloud-Volume löschen.

Schritte

1. Heben Sie die Bereitstellung des Volumes von allen Clients ab:
 - Verwenden Sie unter Linux-Clients das `umount` Befehl.
 - Klicken Sie unter Windows-Clients auf **Netzlaufwerk trennen**.
2. Geben Sie auf der Seite Volumes die Volumes an, die Sie löschen möchten, indem Sie die entsprechenden Kontrollkästchen auswählen, auf **Aktionen** klicken und dann in der Dropdown-Liste *Volume/s löschen auswählen.
3. Geben Sie im Bestätigungsdiaologfeld ein `delete` Um zu bestätigen, dass Sie das Volume löschen möchten, und klicken Sie dann auf **Löschen**.

Copyright-Informationen

Copyright © 2023 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.