



FlexCache-Dualität

ONTAP 9

NetApp
February 05, 2026

Inhalt

- FlexCache-Dualität 1
 - Häufig gestellte Fragen zur FlexCache-Dualität 1
 - Häufig gestellte Fragen 1
 - S3-Zugriff auf NAS-FlexCache-Volumes aktivieren 2
 - Voraussetzungen 2
 - Schritt 1: Zertifikate erstellen und signieren 2
 - Schritt 2: Konfigurieren Sie den S3-Server 6
 - Schritt 3: Client einrichten 8

FlexCache-Dualität

Häufig gestellte Fragen zur FlexCache-Dualität

Diese FAQ beantwortet häufig gestellte Fragen zur FlexCache-Dualität, die in ONTAP 9.18.1 eingeführt wurde.

Häufig gestellte Fragen

Was ist „Dualität“?

Dualität ermöglicht den einheitlichen Zugriff auf dieselben Daten sowohl über Datei- (NAS) als auch Objekt- (S3) Protokolle. Eingeführt in ONTAP 9.12.1 ohne FlexCache-Unterstützung, wurde Dualität in ONTAP 9.18.1 auf FlexCache-Volumes erweitert, sodass der S3-Protokollzugriff auf NAS-Dateien möglich ist, die in einem FlexCache-Volume zwischengespeichert sind.

Welche S3-Operationen werden für einen FlexCache S3-Bucket unterstützt?

S3-Operationen, die auf Standard-S3-NAS-Buckets unterstützt werden, sind auch auf FlexCache S3-NAS-Buckets verfügbar, mit Ausnahme der `COPY` Operation. Eine aktuelle Liste der nicht unterstützten Operationen für einen Standard-S3-NAS-Bucket finden Sie unter ["Interoperabilitätsdokumentation"](#).

Kann ich FlexCache im Write-Back-Modus mit FlexCache-Dualität verwenden?

Nein. Wenn ein FlexCache S3-NAS-Bucket auf einem FlexCache Volume erstellt wird, **muss** sich das FlexCache Volume im Write-Around-Modus befinden. Wenn Sie versuchen, einen FlexCache S3-NAS-Bucket auf einem FlexCache Volume im Write-Back-Modus zu erstellen, schlägt der Vorgang fehl.

Ich kann einen meiner Cluster aufgrund von Hardwarebeschränkungen nicht auf ONTAP 9.18.1 aktualisieren. Funktioniert die Dualität in meinem Cluster weiterhin, wenn nur der Cache-Cluster mit ONTAP 9.18.1 läuft?

Nein. Sowohl der Cache-Cluster als auch der Ursprungscluster müssen mindestens die effektive Clusterversion 9.18.1 aufweisen. Wenn Sie versuchen, einen FlexCache S3-NAS-Bucket auf einem Cache-Cluster zu erstellen, der mit einem Ursprungscluster verbunden ist, auf dem eine ONTAP Version vor 9.18.1 ausgeführt wird, schlägt der Vorgang fehl.

Ich habe eine MetroCluster-Konfiguration. Kann ich die FlexCache-Dualität nutzen?

Nein. FlexCache-Dualität wird in MetroCluster-Konfigurationen nicht unterstützt.

Kann ich den S3-Zugriff auf Dateien in einem FlexCache S3 NAS-Bucket überwachen?

Die S3-Überwachung wird durch die NAS-Überwachungsfunktionalität bereitgestellt, die FlexCache-Volumes verwenden. Weitere Informationen zur NAS-Überwachung von FlexCache-Volumes finden Sie unter ["Erfahren Sie mehr über FlexCache-Auditing"](#).

Was sollte ich erwarten, wenn das Cache-Cluster vom Origin-Cluster getrennt wird?

S3-Anfragen an einen FlexCache S3-NAS-Bucket schlagen mit einem `503 Service Unavailable` Fehler fehl, wenn der Cache-Cluster vom Ursprungscluster getrennt ist.

Kann ich mehrteilige S3-Operationen mit FlexCache Dualität verwenden?

Damit S3-Multipart-Operationen funktionieren, muss das Feld „granulare Daten“ des zugrunde liegenden FlexCache-Volumes auf „erweitert“ gesetzt sein. Dieses Feld wird auf den Wert gesetzt, der für das Ursprungsvolume festgelegt ist.

Unterstützt die Dualität von FlexCache HTTP- und HTTPS-Zugriff?

Ja. Standardmäßig ist HTTPS erforderlich. Sie können den S3-Dienst so konfigurieren, dass HTTP-Zugriff zugelassen wird, falls erforderlich.

S3-Zugriff auf NAS-FlexCache-Volumes aktivieren

Ab ONTAP 9.18.1 können Sie den S3-Zugriff auf NAS-FlexCache-Volumes aktivieren, auch als „Dualität“ bezeichnet. Dadurch können Clients auf Daten, die in einem FlexCache-Volume gespeichert sind, zusätzlich zu den herkömmlichen NAS-Protokollen wie NFS und SMB auch über das S3-Protokoll zugreifen. Sie können die folgenden Informationen verwenden, um die FlexCache-Dualität einzurichten.

Voraussetzungen

Bevor Sie beginnen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Stellen Sie sicher, dass das S3-Protokoll und die gewünschten NAS-Protokolle (NFS, SMB oder beide) auf der SVM lizenziert und konfiguriert sind.
- Überprüfen Sie, ob DNS und alle anderen erforderlichen Dienste konfiguriert sind.
- Cluster und SVM Peered
- FlexCache Volume erstellen
- Data-lif erstellt



Eine ausführlichere Dokumentation zur FlexCache-Dualität finden Sie unter ["ONTAP S3 Multiprotokollunterstützung"](#).

Schritt 1: Zertifikate erstellen und signieren

Um den S3-Zugriff auf ein FlexCache-Volume zu aktivieren, müssen Sie Zertifikate für die SVM installieren, die das FlexCache-Volume hostet. In diesem Beispiel werden selbstsignierte Zertifikate verwendet, aber in einer Produktionsumgebung sollten Sie Zertifikate verwenden, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert sind.

1. Erstellen einer SVM-Root-CA:

```
security certificate create -vserver <svm> -type root-ca -common-name  
<arbitrary_name>
```

2. Generieren Sie eine Zertifikatsignierungsanforderung:

```
security certificate generate-csr -common-name <dns_name_of_data_lif>  
-dns-name <dns_name_of_data_lif> -ipaddr <data_lif_ip>
```

Beispielausgabe:

```

-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwHzEdMBsGA1UEAxMUy2FjaGUxZy1kYXRhLm5hcy5sYWwgEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk07508Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa5OxbAEal5o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIws5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----

```

Beispiel für einen privaten Schlüssel:

```

-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBywggSiAgEAAoIBAQCusJk07508Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgwBtx1K4IlrCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7o1Z9zEI
...
rXGEdDaqp7jQGNXUGlxbO3zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHly9ph7w
dJfFCshsPalMuAp2OuKIANa9l6fT9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxm19jHT5Qql0DaZVUmMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----

```



Bewahren Sie eine Kopie Ihrer Zertifikatsanforderung und Ihres privaten Schlüssels für zukünftige Referenz auf.

3. Signieren Sie das Zertifikat:

Das root-ca ist diejenige, die Sie in [Erstellen Sie eine SVM-Root-CA](#) erstellt haben.

```

certificate sign -ca <svm_root_ca> -ca-serial <svm_root_ca_sn> -expire
-days 364 -format PEM -vserver <svm>

```

4. Fügen Sie die in [Generieren Sie eine Zertifikatsignierungsanforderung](#) generierte Zertifikatsignierungsanforderung (CSR) ein.

Beispiel:

```

-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwHzEdMBsGA1UEAxMUy2FjaGUxZy1kYXRhLm5hcy5sYWlwgGEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk075O8Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa5OxbAEa15o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIwS5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----

```

Dadurch wird ein signiertes Zertifikat auf der Konsole ausgegeben, ähnlich wie im folgenden Beispiel.

Beispiel für ein signiertes Zertifikat:

```

-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMwYy2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU0WhcNMjYxMTIwMjIxNTU0WjAfMR0wGwYDVRQDEExRjYWN0ZTFnLWRhdGEu
...
qS7zhj3ikWE3Gp9s+QijKWXx/0HDD1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EC1Uw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhSl8TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztkivf
J0eoluDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----

```

5. Kopieren Sie das Zertifikat für den nächsten Schritt.

6. Installieren Sie das Serverzertifikat auf der SVM:

```

certificate install -type server -vserver <svm> -cert-name flexcache-
duality

```

7. Fügen Sie das signierte Zertifikat von [Signieren Sie das Zertifikat](#) ein.

Beispiel:

```

Please enter Certificate: Press <Enter> [twice] when done
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMwY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMakGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU4WhcNMjYxMTIwMjIxNTU4WjAfMR0wGwYDVQQDEXRjYWNoZTFnLWRhdGEu
bmFzLmxhYjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK6wmTTvk7xS
...
qS7zhj3ikWE3Gp9s+QijKWXx/0Hdd1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EC1Uw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhSl8TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztktivf
J0eoluDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----

```

8. Fügen Sie den privaten Schlüssel, der in [Generieren Sie eine Zertifikatsignierungsanforderung](#) generiert wurde, ein.

Beispiel:

```

Please enter Private Key: Press <Enter> [twice] when done
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBywggSiAgEAAoIBAQCusJk07508Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgwBtx1K4IlrCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7olZ9zeI
W/gaEIajgpXIwGNWZ+weKQK+yoolxC+gy4IUE7WvnEUiezaIdoqzyPhYq5GC4XWf
0johpQugOPe0/w2nVFRWJoFQp3ZP3NZAXc8H0qkRB6SjaM243XV2jnuEzX2joXvT
wHHH+IBAQ2JDs7s1TY0I20e49J2Fx2+HvUxDx4BHao7CCHA1+MnmEl+9E38wTaEk
NLsU724ZAgMBAAECggEABHUy06wxcIk5h03S9Ik1FDZV3JWzsu5gGdLSQOHRd5W+
...
rXGEddaq7jQGNXUGlxb03zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHLY9ph7w
dJfFCshsPalMuAp2OuKIANa916fT9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxml9jHT5Qql0DaZVUmMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----

```

9. Geben Sie die Zertifikate der Zertifizierungsstellen (CA) ein, die die Zertifikatskette des Serverzertifikats bilden.

Dies beginnt mit dem ausstellenden CA-Zertifikat des Serverzertifikats und kann bis zum Root-CA-Zertifikat reichen.

```
Do you want to continue entering root and/or intermediate certificates
{y|n}: n
```

You should keep a copy of the private key and the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

```
CA: cache-164g-svm-root-ca
serial: 187A256E0BF90CFA
```

10. Ermitteln Sie den öffentlichen Schlüssel für die SVM-Root-CA:

```
security certificate show -vserver <svm> -common-name <root_ca_cn> -ca
<root_ca_cn> -type root-ca -instance
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIDgTCCAmmgAwIBAgIIGHokTnbsHKEwDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMwY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMakGA1UEBhMCVVMwHhcNMjUxMTIx
MjE1NTIzWhcNMjUxMTIxMjE1NTIzWjAuMR8wHQYDVQQDExZjYWNoZS0xNjRnLXN2
bS1yb290LWNhMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
```

```
...
```

```
DoOL7vZFFt44xd+rp0DwafhSnLH5HNhdIAfa2JvZW+eJ7rgevH9wmOzyclvaihl3
Ewtb6cz1a/mtESSYRNBMgkIGM/SFCy5v1ROZXCzF96XPbYQN4cW0AYI3AHYBZP0A
HlNzDR8iml4k9IuKf6BHLFA+VwLTJJZKrdf5Jvjgh0trGAbQGI/Hp2Bjuiopkui+
n4aa5Rz0JFQopqQddAYnMuvqc10CyNn7S0vF/XLd3fJaprh8kQ==
```

```
-----END CERTIFICATE-----
```



Dies ist erforderlich, um den Client so zu konfigurieren, dass er den von der SVM-Root-CA signierten Zertifikaten vertraut. Der öffentliche Schlüssel wird in der Konsole ausgegeben. Kopieren und speichern Sie den öffentlichen Schlüssel. Die Werte in diesem Befehl sind die gleichen wie die, die Sie in [Erstellen Sie eine SVM-Root-CA](#) eingegeben haben.

Schritt 2: Konfigurieren Sie den S3-Server

1. S3-Protokollzugriff aktivieren:

```
vserver show -vserver <svm> -fields allowed-protocols
```



S3 ist auf SVM-Ebene standardmäßig zulässig.

2. Eine vorhandene Richtlinie klonen:


```
network interface service-policy clone -vserver <svm> -policy default-  
data-files -target-vserver <svm> -target-policy <any_name>
```

3. Fügen Sie S3 zur geklonten Richtlinie hinzu:

```
network interface service-policy add-service -vserver <svm> -policy  
<any_name> -service data-s3-server
```

4. Fügen Sie die neue Richtlinie der Daten-LIF hinzu:

```
network interface modify -vserver <svm> -lif <data_lif> -service-policy  
duality
```



Die Änderung der Dienstrichtlinie eines bestehenden LIF kann zu Störungen führen. Dazu muss das LIF heruntergefahren und anschließend mit einem Listener für den neuen Dienst neu gestartet werden. TCP sich davon zwar schnell erholen, dennoch sollten mögliche Auswirkungen beachtet werden.

5. Erstellen Sie den S3-Objektspeicherserver auf der SVM:

```
vserver object-store-server create -vserver <svm> -object-store-server  
<dns_name_of_data_lif> -certificate-name flexcache-duality
```

6. S3-Funktionalität auf dem FlexCache-Volume aktivieren:

Die flexcache config Option `-is-s3-enabled` muss auf `true` gesetzt werden, bevor Sie einen Bucket erstellen können. Sie müssen außerdem die Option `-is-writeback-enabled` auf `false` setzen.

Der folgende Befehl ändert eine bestehende FlexCache:

```
flexcache config modify -vserver <svm> -volume <fcache_vol> -is  
-writeback-enabled false -is-s3-enabled true
```

7. Erstellen Sie einen S3-Bucket:

```
vserver object-store-server bucket create -vserver <svm> -bucket  
<bucket_name> -type nas -nas-path <flexcache_junction_path>
```

8. Erstellen Sie eine Bucket-Richtlinie:

```
vserver object-store-server bucket policy add-statement -vserver <svm>
-bucket <bucket_name> -effect allow
```

9. Erstellen Sie einen S3-Benutzer:

```
vserver object-store-server user create -user <user> -comment ""
```

Beispielausgabe:

```
Vserver: <svm>>
  User: <user>>
Access Key: WCOT7...Y7D6U
Secret Key: 6l43s...pd__P
  Warning: The secret key won't be displayed again. Save this key for
future use.
```

10. Schlüssel für den Root-Benutzer neu generieren:

```
vserver object-store-server user regenerate-keys -vserver <svm> -user
root
```

Beispielausgabe:

```
Vserver: <svm>>
  User: root
Access Key: US791...2F1RB
Secret Key: tgYmn...8_3o2
  Warning: The secret key won't be displayed again. Save this key for
future use.
```

Schritt 3: Client einrichten

Es gibt viele S3-Clients. Ein guter Ausgangspunkt ist die AWS CLI. Weitere Informationen finden Sie unter ["Installation der AWS CLI"](#).

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.