



Zertifikate verwalten

ONTAP Mediator

NetApp
October 19, 2026

Inhalt

Zertifikate verwalten	1
Erneutes Generieren eines temporären selbstsignierten Zertifikats für den ONTAP Mediator Host	1
Ersetzen der selbstsignierten Zertifikate von ONTAP Mediator durch vertrauenswürdige Zertifikate von Drittanbietern	2
Schritt 1: Ein Zertifikat von einem Drittanbieter beziehen, der ein CA-Zertifikat ausstellt.....	3
Schritt 2: Ein Serverzertifikat wird durch Signierung mit einer Drittanbieter-CA-Zertifizierung generiert. . .	5
Schritt 3: Neues Drittanbieter-CA-Zertifikat und Serverzertifikat in der ONTAP Mediator Konfiguration ersetzen	7
Schritt 4: Optional kann ein anderer Pfad oder Name für Ihre Drittanbieterzertifikate verwendet werden.	10
Fehlerbehebung bei ONTAP Mediator Problemen im Zusammenhang mit Zertifikaten	17
Zertifikatsablauf überprüfen	17
X509v3-Erweiterungen in der CA-Zertifizierung überprüfen	17
X509v3-Erweiterungen im Serverzertifikat und Subject Alt Names überprüfen.	19
Es wird überprüft, ob ein privater Schlüssel zu einem Zertifikat passt.	21
Es sollte überprüft werden, ob ein Serverzertifikat von einem bestimmten CA-Zertifikat erstellt wurde.. .	22

Zertifikate verwalten

Erneutes Generieren eines temporären selbstsignierten Zertifikats für den ONTAP Mediator Host

Wenn eine Änderung des Hostnamens oder der IP-Adresse das vorhandene Zertifikat ungültig macht, wird für den aktuellen Host ein temporäres, selbstsigniertes Zertifikat neu generiert.



Dieses Verfahren wird nur auf Systemen unterstützt, auf denen ONTAP Mediator 1.7 oder höher ausgeführt wird.

Über diese Aufgabe

- Diese Aufgabe ist auf dem Linux-Host auszuführen, auf dem ONTAP Mediator installiert wurde.
- Diese Aufgabe kann nur durchgeführt werden, wenn die generierten selbstsignierten Zertifikate aufgrund von Änderungen des Hostnamens oder der IP-Adresse des Hosts nach der Installation von ONTAP Mediator veraltet sind.
- Nachdem das temporäre selbstsignierte Zertifikat durch ein vertrauenswürdigen Zertifikat eines Drittanbieters ersetzt wurde, wird diese Aufgabe *nicht* verwendet, um ein Zertifikat erneut zu generieren. Das Fehlen eines selbstsignierten Zertifikats führt dazu, dass dieses Verfahren fehlschlägt.

Schritt

Um ein neues temporäres selbstsigniertes Zertifikat für den aktuellen Host zu generieren, ist folgender Schritt erforderlich:

1. ONTAP Mediator neu starten:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
```

```
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

Ersetzen der selbstsignierten Zertifikate von ONTAP Mediator durch vertrauenswürdige Zertifikate von Drittanbietern

Sofern Ihre Umgebung dies zulässt, sollten selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate ersetzt werden, die von einer Zertifizierungsstelle ausgestellt wurden.

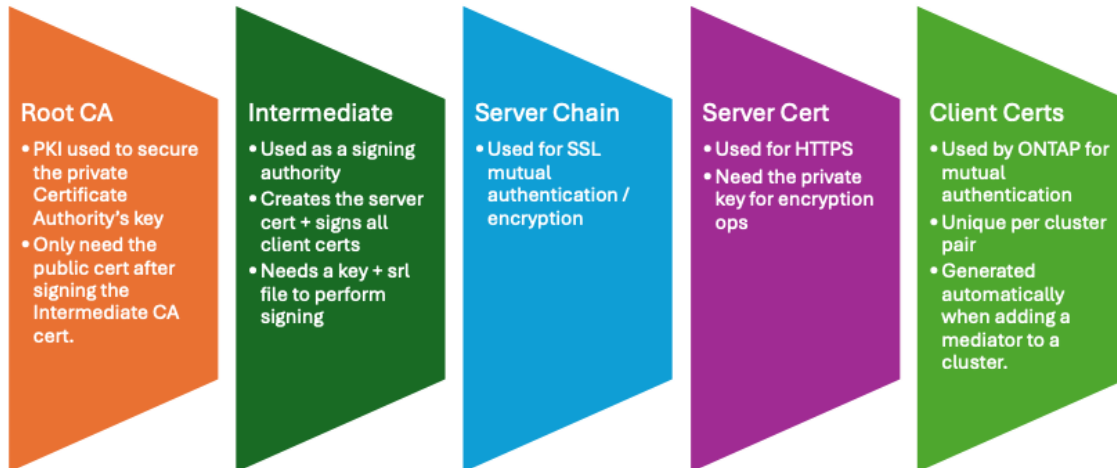


- Zertifikate von Drittanbietern werden erst ab ONTAP 9.16.1 und in einigen früheren ONTAP Patch-Releases unterstützt. Weitere Informationen unter ["NetApp Bugs Online Bug-ID CONTAP-243278"](#).
- Zertifikate von Drittanbietern werden nur auf Systemen unterstützt, auf denen ONTAP Mediator 1.7 oder höher ausgeführt wird.

Über diese Aufgabe

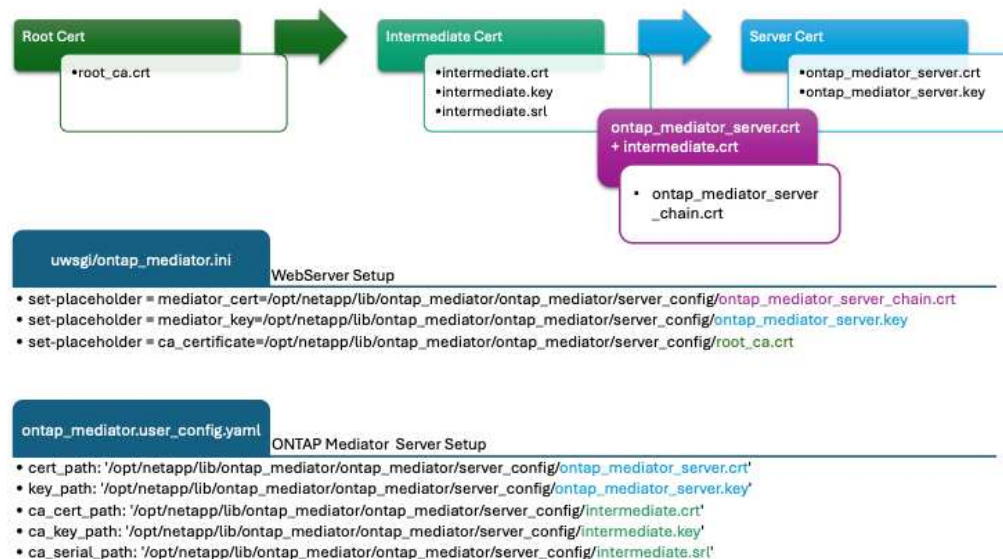
- Diese Aufgabe ist auf dem Linux-Host auszuführen, auf dem ONTAP Mediator installiert wurde.
- Diese Aufgabe können Sie durchführen, wenn die generierten selbstsignierten Zertifikate durch Zertifikate einer vertrauenswürdigen untergeordneten Zertifizierungsstelle (CA) ersetzt werden müssen. Hierfür sollte Zugriff auf eine vertrauenswürdige Public-Key-Infrastruktur (PKI) bestehen.
- Die folgende Abbildung zeigt die Zwecke der einzelnen ONTAP Mediator Zertifikate.

ONTAP Mediator Certificate Purposes



- Das folgende Bild zeigt die Konfiguration für die Webserver-Einrichtung und die ONTAP Mediator-Einrichtung.

ONTAP Mediator Certificates



Schritt 1: Ein Zertifikat von einem Drittanbieter beziehen, der ein CA-Zertifikat ausstellt.

Ein Zertifikat kann von einer PKI-Zertifizierungsstelle mit folgendem Verfahren bezogen werden.

Das folgende Beispiel veranschaulicht den Austausch der selbstsignierten Zertifikatsakteure durch die Zertifikatsakteure von Drittanbietern, die sich unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/` befinden.



Das Beispiel veranschaulicht die notwendigen Kriterien für die für ONTAP Mediator erforderlichen Zertifikate. Die Zertifikate können von einer PKI-Zertifizierungsstelle auf eine von diesem Verfahren abweichende Weise bezogen werden. Das Verfahren kann entsprechend den geschäftlichen Anforderungen angepasst werden.

ONTAP Mediator 1.9 und höher

1. Ein privater Schlüssel `intermediate.key` und eine Konfigurationsdatei `openssl_ca.cnf` werden erstellt, die von der PKI-Behörde zur Erstellung eines Zertifikats verwendet werden.

- a. Den privaten Schlüssel `intermediate.key` generieren:

Beispiel

```
openssl genrsa -aes256 -out intermediate.key 4096
```

- b. Die Konfigurationsdatei `openssl_ca.cnf` (zu finden unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definiert die Eigenschaften, die das generierte Zertifikat haben muss.

2. Den privaten Schlüssel und die Konfigurationsdatei verwenden, um eine Zertifikatsignierungsanforderung zu erstellen `intermediate.csr`:

Beispiel:

```
openssl req -key <private_key_name>.key -new -out  
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@mediator_host server_config]# openssl req -key  
intermediate.key -new -config openssl_ca.cnf -out intermediate.csr  
Enter pass phrase for intermediate.key:  
[root@mediator_host server_config]# cat intermediate.csr  
-----BEGIN CERTIFICATE REQUEST-----  
<certificate_value>  
-----END CERTIFICATE REQUEST-----
```

3. Die Zertifikatsignierungsanforderung `intermediate.csr` wird zur Signierung an eine PKI-Zertifizierungsstelle gesendet.

Die PKI-Zertifizierungsstelle prüft die Anfrage und signiert die `.csr`, wodurch das Zertifikat `intermediate.crt` generiert wird. Zusätzlich muss das `root_ca.crt` Zertifikat, das das `intermediate.crt` Zertifikat von der PKI-Zertifizierungsstelle signiert hat, beschafft werden.



Für SnapMirror active sync Cluster und MetroCluster IP Konfigurationen, die ONTAP Mediator mit HTTPS verwenden, müssen Sie die `intermediate.crt` und `root_ca.crt` Zertifikate zu einem ONTAP Cluster hinzufügen. Informationen finden Sie unter ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#) und ["Den ONTAP Mediator für eine MetroCluster IP-Konfiguration konfigurieren"](#).

ONTAP Mediator 1.8 und früher

1. Ein privater Schlüssel `ca.key` und eine Konfigurationsdatei `openssl_ca.cnf` werden erstellt, die von der PKI-Behörde zur Erstellung eines Zertifikats verwendet werden.
 - a. Den privaten Schlüssel `ca.key` generieren:

Beispiel:

```
openssl genrsa -aes256 -out ca.key 4096
```

- b. Die Konfigurationsdatei `openssl_ca.cnf` (zu finden unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definiert die Eigenschaften, die das generierte Zertifikat haben muss.
2. Den privaten Schlüssel und die Konfigurationsdatei verwenden, um eine Zertifikatsignierungsanforderung zu erstellen `ca.csr`:

Beispiel:

```
openssl req -key <private_key_name>.key -new -out  
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@mediator_host server_config]# openssl req -key ca.key -new  
-config openssl_ca.cnf -out ca.csr  
Enter pass phrase for ca.key:  
[root@mediator_host server_config]# cat ca.csr  
-----BEGIN CERTIFICATE REQUEST-----  
<certificate_value>  
-----END CERTIFICATE REQUEST-----
```

3. Die Zertifikatsignierungsanforderung `ca.csr` wird zur Signierung an eine PKI-Zertifizierungsstelle gesendet.

Die PKI-Zertifizierungsstelle prüft die Anfrage und signiert die `.csr`, wodurch das Zertifikat `ca.crt` generiert wird. Zusätzlich muss das `root_ca.crt` Zertifikat, das das `ca.crt` Zertifikat von der PKI-Zertifizierungsstelle signiert hat, beschafft werden.



Für SnapMirror active sync Cluster müssen die `ca.crt` und `root_ca.crt` Zertifikate zu einem ONTAP Cluster hinzugefügt werden. Weitere Informationen enthält ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#).

Schritt 2: Ein Serverzertifikat wird durch Signierung mit einer Drittanbieter-CA-Zertifizierung generiert

ONTAP Mediator 1.9 und höher

Ein Serverzertifikat muss vom privaten Schlüssel `intermediate.key` und dem Drittanbieterzertifikat `intermediate.crt` signiert sein. Zusätzlich enthält die Konfigurationsdatei `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` bestimmte Attribute, die die für von OpenSSL ausgestellte Serverzertifikate erforderlichen Eigenschaften festlegen.

Die folgenden Befehle können ein Serverzertifikat generieren.

Schritte

1. Um eine Serverzertifikatsignierungsanforderung (CSR) zu generieren, wird folgender Befehl aus dem `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner ausgeführt:

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey  
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out  
ontap_mediator_server.csr
```

2. Um ein Serverzertifikat aus dem CSR zu generieren, wird folgender Befehl aus dem `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner ausgeführt:



Diese Dateien wurden von einer PKI-Zertifizierungsstelle bezogen. Wenn ein anderer Zertifikatsname verwendet wird, `intermediate.crt` und `intermediate.key` durch die entsprechenden Dateinamen ersetzen.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA  
intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095  
-req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- Die `-CAcreateserial` Option wird verwendet, um die `intermediate.srl` Dateien zu generieren.

ONTAP Mediator 1.8 und früher

Ein Serverzertifikat muss vom privaten Schlüssel `ca.key` und dem Drittanbieterzertifikat `ca.crt` signiert sein. Zusätzlich enthält die Konfigurationsdatei

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` bestimmte Attribute, die die für von OpenSSL ausgestellte Serverzertifikate erforderlichen Eigenschaften festlegen.

Die folgenden Befehle können ein Serverzertifikat generieren.

Schritte

1. Um eine Serverzertifikatsignierungsanforderung (CSR) zu generieren, wird folgender Befehl aus dem `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner ausgeführt:

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey  
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out  
ontap_mediator_server.csr
```

2. Um ein Serverzertifikat aus dem CSR zu generieren, wird folgender Befehl aus dem `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner ausgeführt:



Diese Dateien wurden von einer PKI-Zertifizierungsstelle bezogen. Wenn ein anderer Zertifikatsname verwendet wird, `ca.crt` und `ca.key` durch die entsprechenden Dateinamen ersetzen.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt  
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in  
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- Die `-CAcreateserial` Option wird verwendet, um die `ca.srl` Dateien zu generieren.

Schritt 3: Neues Drittanbieter-CA-Zertifikat und Serverzertifikat in der ONTAP Mediator Konfiguration ersetzen

ONTAP Mediator 1.10 und höher

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` bereitgestellt. Die Datei enthält die folgenden Attribute:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` und `key_path` sind Serverzertifikatvariablen.
- `ca_cert_path`, `ca_key_path` und `ca_serial_path` sind CA-Zertifikatsvariablen.

Schritte

1. Alle `intermediate.*` Dateien durch die Zertifikate von Drittanbietern ersetzen.
2. Eine Zertifikatskette aus den `intermediate.crt`- und `ontap_mediator_server.crt`-Zertifikaten erstellen:

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. Die `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` Datei wird aktualisiert.

Aktualisieren Sie die Werte von `ssl_keyfile`, `ssl_certfile` und `ssl_ca_certs`:

```
ssl_keyfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
```

```
ssl_certfile:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_  
server_chain.crt
```

```
ssl_ca_certs:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der `ssl_keyfile`-Wert ist der Schlüsselpfad in der `ontap_mediator_server.crt`-Datei, was `ontap_mediator_server.key` ist.
 - Der `ssl_certfile`-Wert ist der Pfad der `ontap_mediator_server_chain.crt`-Datei.
 - Der `ssl_ca_certs`-Wert ist der Pfad der `root_ca.crt`-Datei.
4. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:
- Linux Gruppeninhaber: `netapp:netapp`
 - Linux-Berechtigungen: `600`
5. ONTAP Mediator neu starten:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 und 1.9

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` bereitgestellt. Die Datei enthält die folgenden Attribute:

```
cert_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi  
ator_server.crt'  
key_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi  
ator_server.key'  
ca_cert_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.crt'  
ca_key_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.key'  
ca_serial_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.srl'
```

- `cert_path` und `key_path` sind Serverzertifikatsvariablen.
- `ca_cert_path`, `ca_key_path` und `ca_serial_path` sind CA-Zertifikatsvariablen.

Schritte

1. Alle `intermediate.*` Dateien durch die Zertifikate von Drittanbietern ersetzen.

2. Eine Zertifikatskette aus den `intermediate.crt`- und `ontap_mediator_server.crt`-Zertifikaten erstellen:

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. Die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei wird aktualisiert.

Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key` und `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt
```

```
set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key
```

```
set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der ``mediator_cert`` Wert ist der Pfad der ``ontap_mediator_server_chain.crt`` Datei.
 - Der `mediator_key` value ist der Schlüsselpfad in der `ontap_mediator_server.crt`-Datei, der `ontap_mediator_server.key` ist.
 - Der ``ca_certificate`` Wert ist der Pfad der ``root_ca.crt`` Datei.
4. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:
 - Linux Gruppeninhaber: `netapp:netapp`
 - Linux-Berechtigungen: `600`

5. ONTAP Mediator neu starten:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 und früher

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` bereitgestellt. Die Datei enthält die folgenden Attribute:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
```

```
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'  
ca_serial_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- cert_path und key_path sind Serverzertifikatvariablen.
- ca_cert_path, ca_key_path und ca_serial_path sind CA-Zertifikatsvariablen.

Schritte

1. Alle ca.* Dateien durch die Zertifikate von Drittanbietern ersetzen.
2. Eine Zertifikatskette aus den ca.crt- und ontap_mediator_server.crt-Zertifikaten erstellen:

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

3. Die /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini Datei wird aktualisiert.

Aktualisieren Sie die Werte von mediator_cert, mediator_key und ca_certificate:

```
set-placeholder = mediator_cert =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_  
server_chain.crt
```

```
set-placeholder = mediator_key =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_  
server.key
```

```
set-placeholder = ca_certificate =  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der `mediator\_cert`Wert ist der Pfad der `ontap\_mediator\_server\_chain.crt`Datei.
 - Der mediator_key value ist der Schlüsselpfad in der ontap_mediator_server.crt-Datei, der ontap_mediator_server.key ist.
 - Der `ca\_certificate`Wert ist der Pfad der `root\_ca.crt`Datei.
4. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:
 - Linux Gruppeninhaber: netapp:netapp
 - Linux-Berechtigungen: 600
 5. ONTAP Mediator neu starten:

```
systemctl restart ontap_mediator
```

Schritt 4: Optional kann ein anderer Pfad oder Name für Ihre Drittanbieterzertifikate verwendet werden.

ONTAP Mediator 1.10 und höher

Sie können Zertifikate von Drittanbietern mit einem anderen Namen als intermediate.* verwenden

oder die Zertifikate von Drittanbietern an einem anderen Ort speichern.

Schritte

1. Die

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml-Datei wird so konfiguriert, dass die Standardwerte der Variablen in der ontap_mediator.config.yaml-Datei überschrieben werden.

Wenn Sie intermediate.crt von einer PKI-Zertifizierungsstelle erhalten haben und dessen privaten Schlüssel intermediate.key am Speicherort

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config ablegen, sollte die ontap_mediator.user_config.yaml Datei wie im folgenden Beispiel aussehen:



Wenn intermediate.crt zum Signieren des ontap_mediator_server.crt Zertifikats verwendet wurde, wird die intermediate.srl Datei generiert. Weitere Informationen finden Sie in [Schritt 2: Ein Serverzertifikat wird durch Signierung mit einer Drittanbieter-CA-Zertifizierung generiert.](#)

```
[root@mediator_host server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
```

```
diat.key'  
ca_serial_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme  
diat.srl'
```

- a. Wenn eine Zertifikatsstruktur verwendet wird, bei der das `root_ca.crt` Zertifikat ein `intermediate.crt` Zertifikat bereitstellt, das das `ontap_mediator_server.crt` Zertifikat signiert, wird eine Zertifikatskette aus den `intermediate.crt` und `ontap_mediator_server.crt` Zertifikaten erstellt:



Sie sollten die `intermediate.crt` und `ontap_mediator_server.crt` Zertifikate von einer PKI-Behörde bereits früher im Verfahren erhalten haben.

```
cat ontap_mediator_server.crt intermediate.crt >  
ontap_mediator_server_chain.crt
```

- b. Die `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` Datei wird aktualisiert.

Aktualisieren Sie die Werte von `ssl_keyfile`, `ssl_certfile` und `ssl_ca_certs`:

```
ssl_keyfile:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi  
at_server.key
```

```
ssl_certfile:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi  
at_server_chain.crt
```

```
ssl_ca_certs:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der `ssl_keyfile`-Wert ist der Schlüsselpfad in der `ontap_mediator_server.crt`-Datei, was `ontap_mediator_server.key` ist.
- Der `ssl_certfile`-Wert ist der Pfad der `ontap_mediator_server_chain.crt`-Datei.
- Der `ssl_ca_certs`-Wert ist der Pfad der `root_ca.crt`-Datei.



Für SnapMirror active sync Cluster und MetroCluster IP Konfigurationen, die ONTAP Mediator mit HTTPS verwenden, müssen Sie die `intermediate.crt` und `root_ca.crt` Zertifikate zu einem ONTAP Cluster hinzufügen. Informationen finden Sie unter ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#) und ["Den ONTAP Mediator für eine MetroCluster IP-Konfiguration konfigurieren"](#).

- c. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:

- Linux Gruppeninhaber: `netapp:netapp`
- Linux-Berechtigungen: `600`

2. ONTAP Mediator wird neu gestartet, wenn die Zertifikate in der Konfigurationsdatei aktualisiert

werden:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 und 1.9

Sie können Zertifikate von Drittanbietern mit einem anderen Namen als `intermediate.*` verwenden oder die Zertifikate von Drittanbietern an einem anderen Ort speichern.

Schritte

1. Die

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`-Datei wird so konfiguriert, dass die Standardwerte der Variablen in der `ontap_mediator.config.yaml`-Datei überschrieben werden.

Wenn Sie `intermediate.crt` von einer PKI-Zertifizierungsstelle erhalten haben und dessen privaten Schlüssel `intermediate.key` am Speicherort

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` ablegen, sollte die `ontap_mediator.user_config.yaml` Datei wie im folgenden Beispiel aussehen:



Wenn `intermediate.crt` zum Signieren des `ontap_mediator_server.crt` Zertifikats verwendet wurde, wird die `intermediate.srl` Datei generiert. Weitere Informationen finden Sie in [Schritt 2: Ein Serverzertifikat wird durch Signierung mit einer Drittanbieter-CA-Zertifizierung generiert](#).

```
[root@mediator_host server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
```

```
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- a. Wenn eine Zertifikatsstruktur verwendet wird, bei der das `root_ca.crt` Zertifikat ein `intermediate.crt` Zertifikat bereitstellt, das das `ontap_mediator_server.crt` Zertifikat signiert, wird eine Zertifikatskette aus den `intermediate.crt` und `ontap_mediator_server.crt` Zertifikaten erstellt:



Sie sollten die `intermediate.crt` und `ontap_mediator_server.crt` Zertifikate von einer PKI-Behörde bereits früher im Verfahren erhalten haben.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

- b. Die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei wird aktualisiert.

Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key` und `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt
```

```
set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
```

```
set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der ``mediator_cert`` Wert ist der Pfad der ``ontap_mediator_server_chain.crt`` Datei.
- Der `mediator_key`` Wert ist der Schlüsselpfad in der ``ontap_mediator_server.crt`` Datei, was ``ontap_mediator_server.key`` ist.
- Der ``ca_certificate`` Wert ist der Pfad der ``root_ca.crt`` Datei.



Für SnapMirror Business Continuity (SM-BC) Cluster müssen die `intermediate.crt` und `root_ca.crt` Zertifikate zu einem ONTAP Cluster hinzugefügt werden. Weitere Informationen unter ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#).

- c. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:

- Linux Gruppeninhaber: netapp:netapp

- Linux-Berechtigungen: 600

2. ONTAP Mediator wird neu gestartet, wenn die Zertifikate in der Konfigurationsdatei aktualisiert werden:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 und früher

Sie können Zertifikate von Drittanbietern mit einem anderen Namen als `ca.*` verwenden oder die Zertifikate von Drittanbietern an einem anderen Ort speichern.

Schritte

1. Die

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`-Datei wird so konfiguriert, dass die Standardwerte der Variablen in der `ontap_mediator.config.yaml`-Datei überschrieben werden.

Wenn Sie `ca.crt` von einer PKI-Zertifizierungsstelle erhalten haben und dessen privaten Schlüssel `ca.key` am Speicherort

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` ablegen, sollte die `ontap_mediator.user_config.yaml` Datei wie im folgenden Beispiel aussehen:



Wenn `ca.crt` zum Signieren des `ontap_mediator_server.crt` Zertifikats verwendet wurde, wird die `ca.srl` Datei generiert. Weitere Informationen finden Sie in [Schritt 2: Ein Serverzertifikat wird durch Signierung mit einer Drittanbieter-CA-Zertifizierung generiert](#).

```
[root@mediator_host server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
```

```
mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- a. Wenn eine Zertifikatsstruktur verwendet wird, bei der das `root_ca.crt` Zertifikat ein `ca.crt` Zertifikat bereitstellt, das das `ontap_mediator_server.crt` Zertifikat signiert, wird eine Zertifikatskette aus den `ca.crt` und `ontap_mediator_server.crt` Zertifikaten erstellt:



Sie sollten die `ca.crt` und `ontap_mediator_server.crt` Zertifikate von einer PKI-Behörde bereits früher im Verfahren erhalten haben.

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

- b. Die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei wird aktualisiert.

Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key` und `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server_chain.crt
```

```
set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server.key
```

```
set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der ``mediator_cert`` Wert ist der Pfad der ``ontap_mediator_server_chain.crt`` Datei.
- Der `mediator_key`` Wert ist der Schlüsselpfad in der ``ontap_mediator_server.crt`` Datei, was ``ontap_mediator_server.key`` ist.
- Der ``ca_certificate`` Wert ist der Pfad der ``root_ca.crt`` Datei.



Für SnapMirror Business Continuity (SM-BC) Cluster müssen die `ca.crt` und `root_ca.crt` Zertifikate zu einem ONTAP Cluster hinzugefügt werden. Weitere Informationen unter ["ONTAP Mediator und Cluster für SnapMirror active sync konfigurieren"](#).

- c. Es sollte sichergestellt sein, dass die folgenden Attribute der neu generierten Zertifikate korrekt gesetzt sind:

- Linux Gruppeninhaber: netapp:netapp

- Linux-Berechtigungen: 600

2. ONTAP Mediator wird neu gestartet, wenn die Zertifikate in der Konfigurationsdatei aktualisiert werden:

```
systemctl restart ontap_mediator
```

Fehlerbehebung bei ONTAP Mediator Problemen im Zusammenhang mit Zertifikaten

Mit diesen Prüfungen lassen sich die Zertifikatseigenschaften bei der Fehlerbehebung von Zertifikatsproblemen überprüfen.

Zertifikatsablauf überprüfen

Mit dem folgenden Befehl lässt sich der Gültigkeitszeitraum des Zertifikats ermitteln.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
    ...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

X509v3-Erweiterungen in der CA-Zertifizierung überprüfen

Mit dem folgenden Befehl lassen sich die X509v3-Erweiterungen in der CA-Zertifizierung überprüfen.

ONTAP Mediator 1.9 und höher

Die innerhalb von **v3_ca** in `openssl_ca.cnf` definierten Eigenschaften werden als X509v3 extensions in `intermediate.crt` angezeigt.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAP Mediator 1.8 und früher

Die innerhalb von **v3_ca** in `openssl_ca.cnf` definierten Eigenschaften werden als X509v3 extensions in `ca.crt` angezeigt.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
```

```

authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

            9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

            keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign

```

X509v3-Erweiterungen im Serverzertifikat und Subject Alt Names überprüfen

Die `v3_req` Eigenschaften, die in der `openssl_server.cnf` Konfigurationsdatei definiert sind, werden als `X509v3 extensions` im Zertifikat angezeigt.

Im folgenden Beispiel können die Variablen in den `alt_names` Abschnitten durch Ausführen der Befehle `hostname -A` und `hostname -I` auf der Linux-VM ermittelt werden, auf der ONTAP Mediator installiert ist.

Die korrekten Werte der Variablen sind beim Netzwerkadministrator zu erfragen.

ONTAP Mediator 1.9 und höher

```

[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints          = CA:false
extendedKeyUsage          = serverAuth
keyUsage                  = keyEncipherment, dataEncipherment
subjectAltName             = @alt_names

```

```

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...

    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Extended Key Usage:
            TLS Web Server Authentication
        X509v3 Key Usage:
            Key Encipherment, Data Encipherment
        X509v3 Subject Alternative Name:
            DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd

```

ONTAP Mediator 1.8 und früher

```

[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints          = CA:false
extendedKeyUsage          = serverAuth
keyUsage                  = keyEncipherment, dataEncipherment
subjectAltName            = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:

```

...

```
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  X509v3 Extended Key Usage:
    TLS Web Server Authentication
  X509v3 Key Usage:
    Key Encipherment, Data Encipherment
  X509v3 Subject Alternative Name:
    DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

Es wird überprüft, ob ein privater Schlüssel zu einem Zertifikat passt.

Es lässt sich überprüfen, ob ein bestimmter privater Schlüssel zu einem Zertifikat passt.

Die folgenden OpenSSL-Befehle werden jeweils auf den Schlüssel und das Zertifikat angewendet.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

Wenn das `-modulus`-Attribut bei beiden übereinstimmt, zeigt dies an, dass das private Schlüssel und Zertifikat Paar kompatibel ist und miteinander arbeiten kann.

Es sollte überprüft werden, ob ein Serverzertifikat von einem bestimmten CA-Zertifikat erstellt wurde.

Mit dem folgenden Befehl lässt sich überprüfen, ob das Serverzertifikat von einem bestimmten CA-Zertifikat erstellt wurde.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt
--untrusted intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
[root@mediator_host server_config]#
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

Wenn die Online Certificate Status Protocol (OCSP)-Validierung verwendet wird, kann der Befehl **"openssl-verify"** genutzt werden.

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.