



인증서 관리 ONTAP Mediator

NetApp
October 19, 2026

목차

인증서 관리	1
ONTAP Mediator 호스트용 임시 자체 서명 인증서를 다시 생성합니다.	1
ONTAP Mediator 자체 서명 인증서를 신뢰할 수 있는 타사 인증서로 교체하십시오.	2
1단계: CA 인증서를 발급하는 제3자 기관으로부터 인증서를 발급받으십시오.	3
2단계: 제3자 CA 인증서를 사용하여 서명함으로써 서버 인증서를 생성합니다.	5
3단계: ONTAP Mediator 구성에서 새로운 타사 CA 인증서 및 서버 인증서 교체.	6
4단계: 필요에 따라 타사 인증서에 다른 경로 또는 이름을 사용할 수 있습니다.	10
ONTAP Mediator 인증서 관련 문제 해결	16
인증서 만료 확인	16
CA 인증에서 X509v3 확장 기능을 확인합니다.	17
서버 인증서 및 주체 대체 이름에서 X509v3 확장 기능을 확인하십시오.	19
개인 키가 인증서와 일치하는지 확인하십시오	20
서버 인증서가 특정 CA 인증서로부터 생성되었는지 확인하십시오	21

인증서 관리

ONTAP Mediator 호스트용 임시 자체 서명 인증서를 다시 생성합니다.

호스트 이름이나 IP 주소 변경으로 기존 인증서가 무효화될 경우 현재 호스트에 대한 임시 자체 서명 인증서를 다시 생성합니다.



이 절차는 ONTAP Mediator 1.7 이상 버전이 실행되는 시스템에서만 지원됩니다.

이 작업 정보

- ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행하십시오.
- ONTAP Mediator를 설치한 후 호스트의 호스트 이름이나 IP 주소가 변경되어 생성된 자체 서명 인증서가 더 이상 유효하지 않게 된 경우에만 이 작업을 수행할 수 있습니다.
- 임시 자체 서명 인증서를 신뢰할 수 있는 타사 인증서로 교체한 후에는 이 작업을 사용하여 인증서를 다시 생성해서는 안 됩니다. 자체 서명 인증서가 없으면 이 절차가 실패합니다.

단계

현재 호스트에 대한 새 임시 자체 서명 인증서를 다시 생성하려면 다음 단계를 수행하십시오:

1. ONTAP Mediator를 재시작하십시오:

```
./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
```

ONTAP Mediator 자체 서명 인증서를 신뢰할 수 있는 타사 인증서로 교체하십시오

사용 환경에서 지원하는 경우, 자체 서명 인증서를 인증 기관에서 발급한 신뢰할 수 있는 인증서로 교체하십시오.

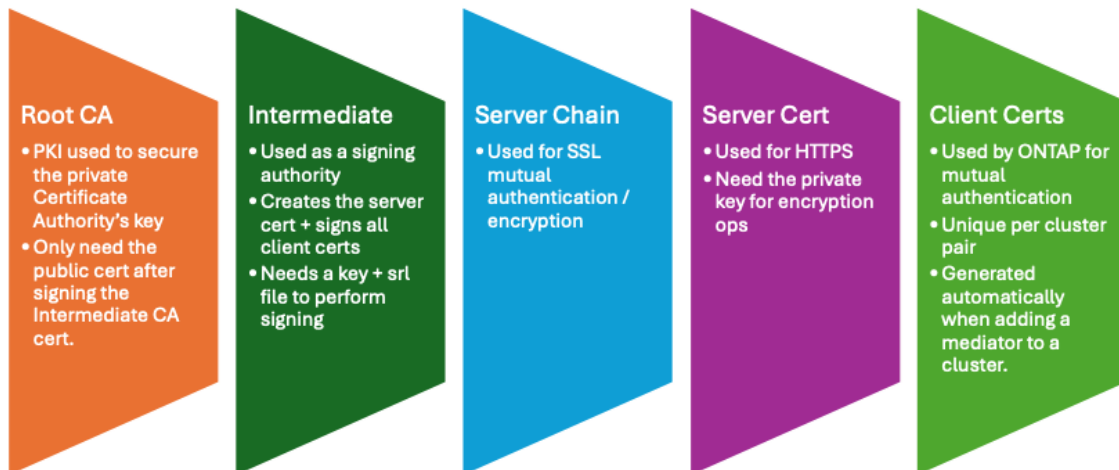


- 타사 인증서는 ONTAP 9.16.1 버전부터, 그리고 일부 이전 ONTAP 패치 릴리스에서만 지원됩니다. ["NetApp Bugs Online 버그 ID CONTAP-243278"](#)을(를) 참조하십시오.
- 타사 인증서는 ONTAP Mediator 1.7 이상 버전이 실행되는 시스템에서만 지원됩니다.

이 작업 정보

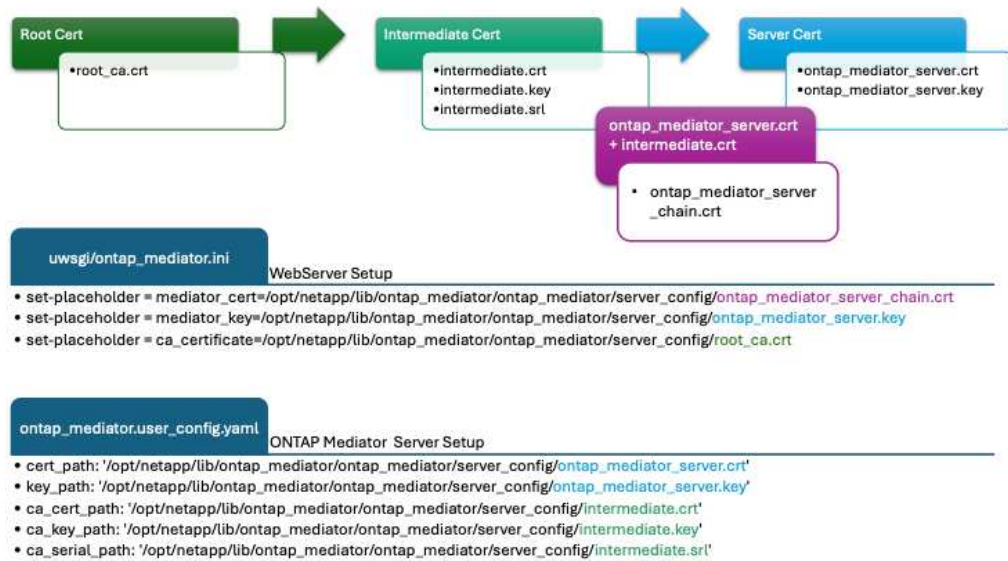
- ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행하십시오.
- 생성된 자체 서명 인증서를 신뢰할 수 있는 하위 인증 기관(CA)에서 발급받은 인증서로 교체해야 하는 경우 이 작업을 수행할 수 있습니다. 이를 위해서는 신뢰할 수 있는 공개 키 인프라(PKI) 기관에 대한 접근 권한이 있어야 합니다.
- 다음 이미지는 각 ONTAP Mediator 인증서의 용도를 보여줍니다.

ONTAP Mediator Certificate Purposes



- 다음 이미지는 웹 서버 설정 및 ONTAP Mediator 설정에 대한 구성을 보여줍니다.

ONTAP Mediator Certificates



1단계: CA 인증서를 발급하는 제3자 기관으로부터 인증서를 발급받으십시오.

다음 절차에 따라 PKI 기관으로부터 인증서를 발급받을 수 있습니다.

다음 예는 자체 서명 인증서 액터를 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`에 위치한 타사 인증서 액터로 교체하는 방법을 보여줍니다.



이 예시는 ONTAP Mediator에 필요한 인증서의 필수 요건을 설명합니다. PKI 기관으로부터 인증서를 발급받는 방법은 이 절차와 다를 수 있습니다. 비즈니스 요구 사항에 맞게 절차를 조정하십시오.

ONTAP Mediator 1.9 이상 버전

1. PKI 기관에서 인증서를 생성하는 데 사용할 개인 키 `intermediate.key` 및 구성 파일 `'openssl_ca.cnf'`을 생성합니다.

- a. 개인 키를 생성합니다 `intermediate.key`:

예

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

- b. 구성 파일 `openssl_ca.cnf`(`'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf'`에 위치)은 생성된 인증서가 반드시 가져야 하는 속성을 정의합니다.

2. 개인 키와 구성 파일을 사용하여 인증서 서명 요청을 생성합니다 `intermediate.csr`:

예:

```
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. 인증서 서명 요청 `intermediate.csr`을 PKI 기관에 보내 서명을 받으십시오.

PKI 기관은 요청을 확인하고 `.csr`에 서명하여 인증서 `intermediate.crt`를 생성합니다. 또한 PKI 기관에서 `intermediate.crt` 인증서에 서명한 `root\_ca.crt` 인증서를 받아야 합니다.



HTTPS로 구성된 ONTAP Mediator를 사용하는 SnapMirror 활성 동기화 클러스터 및 MetroCluster IP 구성의 경우, ONTAP 클러스터에 `intermediate.crt` 및 `root\_ca.crt` 인증서를 추가해야 합니다. **"SnapMirror 활성 동기화를 위해 ONTAP Mediator 및 클러스터를 구성합니다."** 및 **"ONTAP Mediator를 MetroCluster IP 구성에 맞게 구성합니다"**을(를) 참조하십시오.

ONTAP Mediator 1.8 이하 버전

1. PKI 기관에서 인증서를 생성하는 데 사용할 개인 키 `ca.key` 및 구성 파일 `openssl\_ca.cnf`을 생성합니다.

a. 개인 키를 생성합니다 `ca.key`:

예:

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

b. 구성 파일 `openssl\_ca.cnf`

(`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_ca.cnf`에 위치)은 생성된 인증서가 반드시 가져야 하는 속성을 정의합니다.

2. 개인 키와 구성 파일을 사용하여 인증서 서명 요청을 생성합니다 `ca.csr`:

예:

```
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. 인증서 서명 요청 `ca.csr`을 PKI 기관에 보내 서명을 받으십시오.

PKI 기관은 요청을 확인하고 `.csr`에 서명하여 인증서 `ca.crt`를 생성합니다. 또한 PKI 기관으로부터 `ca.crt` 인증서에 서명한 `root_ca.crt` 인증서를 받아야 합니다.



SnapMirror 활성화 동기화 클러스터의 경우 ONTAP 클러스터에 `ca.crt` 및 `root_ca.crt` 인증서를 추가해야 합니다. "[SnapMirror 활성화 동기화를 위해 ONTAP Mediator 및 클러스터를 구성합니다.](#)"을(를) 참조하십시오.

2단계: 제3자 CA 인증서를 사용하여 서명함으로써 서버 인증서를 생성합니다.

ONTAP Mediator 1.9 이상 버전

서버 인증서는 개인 키 `intermediate.key` 및 제3자 인증서 `intermediate.crt`로 서명되어야 합니다. 또한 구성 파일 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf`에는 OpenSSL에서 발급한 서버 인증서에 필요한 속성을 지정하는 특정 속성이 포함되어 있습니다.

다음 명령어를 사용하여 서버 인증서를 생성할 수 있습니다.

단계

1. 서버 인증서 서명 요청(CSR)을 생성하려면

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 폴더에서 다음 명령을 실행하십시오:

```
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. CSR에서 서버 인증서를 생성하려면

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 폴더에서 다음 명령을 실행하십시오:



이 파일들은 PKI 기관에서 가져온 것입니다. 다른 인증서 이름을 사용하는 경우, `intermediate.crt` 및 `intermediate.key`를 해당 파일 이름으로 바꾸십시오.

```
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
```

° `-CAcreateserial` 옵션은 `intermediate.srl` 파일을 생성하는 데 사용됩니다.

ONTAP Mediator 1.8 이하 버전

서버 인증서는 개인 키 `ca.key` 및 제3자 인증서 `ca.crt`로 서명되어야 합니다. 또한 구성 파일 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf`에는 OpenSSL에서 발급한 서버 인증서에 필요한 속성을 지정하는 특정 속성이 포함되어 있습니다.

다음 명령어를 사용하여 서버 인증서를 생성할 수 있습니다.

단계

1. 서버 인증서 서명 요청(CSR)을 생성하려면

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 폴더에서 다음 명령을

실행하십시오:

```
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. CSR에서 서버 인증서를 생성하려면

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config 폴더에서 다음 명령을 실행하십시오:



이 파일들은 PKI 기관에서 가져온 것입니다. 다른 인증서 이름을 사용하는 경우, ca.crt 및 'ca.key'를 해당 파일 이름으로 바꾸십시오.

```
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
```

° -CAcreateserial 옵션은 ca.srl 파일을 생성하는 데 사용됩니다.

3단계: ONTAP Mediator 구성에서 새로운 타사 CA 인증서 및 서버 인증서 교체

ONTAP Mediator 1.10 이상 버전

인증서 구성은

'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml'에 위치한 구성 파일에서 ONTAP Mediator에 제공됩니다. 이 파일에는 다음과 같은 속성이 포함되어 있습니다.

```
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 및 'key_path'는 서버 인증서 변수입니다.
- ca_cert_path, ca_key_path 및 'ca_serial_path'는 CA 인증서 변수입니다.

단계

1. 모든 `intermediate.*` 파일을 타사 인증서로 교체하십시오.
2. `intermediate.crt` 및 `ontap_mediator_server.crt` 인증서를 사용하여 인증서 체인을 생성합니다:

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

3. `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` 파일을 업데이트하십시오.

``ssl_keyfile`, `ssl_certfile` 및 `ssl_ca_certs`의 값을 업데이트하십시오:`

```
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
```

- 해당 `ssl_keyfile` 값은 `ontap_mediator_server.crt` 파일 내의 키 경로이며, 이는 ``ontap_mediator_server.key``입니다.
 - 해당 `ssl_certfile` 값은 `ontap_mediator_server_chain.crt` 파일의 경로입니다.
 - 해당 `ssl_ca_certs` 값은 `root_ca.crt` 파일의 경로입니다.
4. 새로 생성된 인증서의 다음 속성이 올바르게 설정되었는지 확인하십시오:
 - Linux 그룹 소유자: `netapp:netapp`
 - Linux 권한: `600`
 5. ONTAP Mediator를 재시작하십시오:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 및 1.9

인증서 구성은

``/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml``에 위치한 구성 파일에서 ONTAP Mediator에 제공됩니다. 이 파일에는 다음과 같은 속성이 포함되어 있습니다.

```
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 및 'key_path'는 서버 인증서 변수입니다.
- ca_cert_path, ca_key_path 및 'ca_serial_path'는 CA 인증서 변수입니다.

단계

1. 모든 intermediate.* 파일을 타사 인증서로 교체하십시오.
2. intermediate.crt 및 ontap_mediator_server.crt 인증서를 사용하여 인증서 체인을 생성합니다:

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

3. /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini 파일을 업데이트하십시오.

`mediator\_cert`, `mediator\_key` 및 `ca\_certificate`의 값을 업데이트하십시오:

```
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
```

- 해당 mediator_cert 값은 ontap_mediator_server_chain.crt 파일의 경로입니다.
 - mediator_key value`은(는) `ontap_mediator_server.crt 파일의 키 경로이며, 이는 `ontap\_mediator\_server.key`입니다.
 - 해당 ca_certificate 값은 root_ca.crt 파일의 경로입니다.
4. 새로 생성된 인증서의 다음 속성이 올바르게 설정되었는지 확인하십시오:
 - Linux 그룹 소유자: netapp:netapp
 - Linux 권한: 600

5. ONTAP Mediator를 재시작하십시오:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 이하 버전

인증서 구성은

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml`에 위치한 구성 파일에서 ONTAP Mediator에 제공됩니다. 이 파일에는 다음과 같은 속성이 포함되어 있습니다.

```
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/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 및 key_path는 서버 인증서 변수입니다.
- ca_cert_path, ca_key_path 및 ca_serial_path는 CA 인증서 변수입니다.

단계

1. 모든 ca.* 파일을 타사 인증서로 교체하십시오.
2. ca.crt 및 ontap_mediator_server.crt 인증서를 사용하여 인증서 체인을 생성합니다:

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

3. /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini 파일을 업데이트하십시오.

`mediator\_cert`, `mediator\_key` 및 `ca\_certificate`의 값을 업데이트하십시오:

```
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
```

- 해당 mediator_cert 값은 ontap_mediator_server_chain.crt 파일의 경로입니다.
- mediator_key value`은(는) `ontap_mediator_server.crt 파일의 키 경로이며, 이는 `ontap\_mediator\_server.key`입니다.
- 해당 ca_certificate 값은 root_ca.crt 파일의 경로입니다.

4. 새로 생성된 인증서의 다음 속성이 올바르게 설정되었는지 확인하십시오:

- Linux 그룹 소유자: netapp:netapp
- Linux 권한: 600

5. ONTAP Mediator를 재시작하십시오:

```
systemctl restart ontap_mediator
```

4단계: 필요에 따라 타사 인증서에 다른 경로 또는 이름을 사용할 수 있습니다.

ONTAP Mediator 1.10 이상 버전

`intermediate.\*` 이외의 다른 이름으로 타사 인증서를 사용하거나 다른 위치에 저장할 수 있습니다.

단계

1. /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml 파일을 구성하여 ontap_mediator.config.yaml 파일의 기본 변수 값을 재정의합니다.

PKI 기관으로부터 intermediate.crt`을(를) 발급받고 개인 키 `intermediate.key`을(를) /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config 위치에 저장하는 경우, ontap_mediator.user_config.yaml 파일은 다음 예와 같아야 합니다:



intermediate.crt`을(를) 사용하여 `ontap_mediator_server.crt 인증서에 서명한 경우 intermediate.srl 파일이 생성됩니다. 자세한 내용은 [2단계: 제3자 CA 인증서를 사용하여 서명함으로써 서버 인증서를 생성합니다](#).을(를) 참조하십시오.

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

```

- a. root_ca.crt 인증서가 ontap_mediator_server.crt 인증서에 서명하는 intermediate.crt 인증서를 제공하는 인증서 구조를 사용하는 경우, intermediate.crt 및 ontap_mediator_server.crt 인증서에서 인증서 체인을 생성하십시오.



절차의 이전 단계에서 PKI 기관으로부터 intermediate.crt 및 ontap_mediator_server.crt 인증서를 발급받았어야 합니다.

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

- b. /opt/netapp/lib/ontap_mediator/uvicorn/config.json 파일을 업데이트하십시오.

``ssl_keyfile``, ``ssl_certfile`` 및 ``ssl_ca_certs``의 값을 업데이트하십시오:

```

ssl_keyfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server.key

ssl_certfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server_chain.crt

```

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

- 해당 ssl_keyfile 값은 ontap_mediator_server.crt 파일 내의 키 경로이며, 이는 `ontap\_mediator\_server.key`입니다.
- 해당 ssl_certfile 값은 ontap_mediator_server_chain.crt 파일의 경로입니다.
- 해당 ssl_ca_certs 값은 root_ca.crt 파일의 경로입니다.



HTTPS로 구성된 ONTAP Mediator를 사용하는 SnapMirror 활성화 클러스터 및 MetroCluster IP 구성의 경우, ONTAP 클러스터에 intermediate.crt 및 root_ca.crt 인증서를 추가해야 합니다. "[SnapMirror 활성화 동기화를 위해 ONTAP Mediator 및 클러스터를 구성합니다.](#)" 및 "[ONTAP Mediator를 MetroCluster IP 구성에 맞게 구성합니다](#)"을(를) 참조하십시오.

c. 새로 생성된 인증서의 다음 속성이 올바르게 설정되었는지 확인하십시오:

- Linux 그룹 소유자: netapp:netapp
- Linux 권한: 600

2. 구성 파일에서 인증서가 업데이트되면 ONTAP Mediator를 다시 시작합니다:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 및 1.9

`intermediate.\*` 이외의 다른 이름으로 타사 인증서를 사용하거나 다른 위치에 저장할 수 있습니다.

단계

1. /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml 파일을 구성하여 ontap_mediator.config.yaml 파일의 기본 변수 값을 재정의합니다.

PKI 기관으로부터 intermediate.crt`을(를) 발급받고 개인 키 `intermediate.key`을(를) /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config 위치에 저장하는 경우, ontap_mediator.user_config.yaml 파일은 다음 예와 같아야 합니다:



intermediate.crt`을(를) 사용하여 `ontap_mediator_server.crt` 인증서에 서명한 경우 intermediate.srl 파일이 생성됩니다. 자세한 내용은 [2단계: 제3자 CA 인증서를 사용하여 서명함으로써 서버 인증서를 생성합니다.](#)을(를) 참조하십시오.

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

```

- a. root_ca.crt 인증서가 ontap_mediator_server.crt 인증서에 서명하는 intermediate.crt 인증서를 제공하는 인증서 구조를 사용하는 경우, intermediate.crt 및 ontap_mediator_server.crt 인증서에서 인증서 체인을 생성하십시오.



절차의 이전 단계에서 PKI 기관으로부터 intermediate.crt 및 ontap_mediator_server.crt 인증서를 발급받았어야 합니다.

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

- b. /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini 파일을 업데이트하십시오.

`mediator\_cert`, `mediator\_key` 및 `ca\_certificate`의 값을 업데이트하십시오:

```

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
```

- 해당 mediator_cert 값은 ontap_mediator_server_chain.crt 파일의 경로입니다.
- 해당 mediator_key 값은 ontap_mediator_server.crt 파일의 키 경로이며, 이는 `ontap\_mediator\_server.key`입니다.
- 해당 ca_certificate 값은 root_ca.crt 파일의 경로입니다.



SnapMirror Business Continuity(SM-BC) 클러스터의 경우 ONTAP 클러스터에 intermediate.crt 및 root_ca.crt 인증서를 추가해야 합니다. "SnapMirror 활성화 동기화를 위해 ONTAP Mediator 및 클러스터를 구성합니다."을(를) 참조하십시오.

c. 새로 생성된 인증서의 다음 속성이 올바르게 설정되었는지 확인하십시오:

- Linux 그룹 소유자: netapp:netapp
- Linux 권한: 600

2. 구성 파일에서 인증서가 업데이트되면 ONTAP Mediator를 다시 시작합니다:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 이하 버전

`ca.\*` 이외의 다른 이름으로 타사 인증서를 사용하거나 타사 인증서를 다른 위치에 저장할 수 있습니다.

단계

1. /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml 파일을 구성하여 ontap_mediator.config.yaml 파일의 기본 변수 값을 재정의합니다.

PKI 기관으로부터 ca.crt`을(를) 발급받아 해당 개인 키 `ca.key`를 위치
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config`에 저장한 경우,
`ontap\_mediator.user\_config.yaml` 파일은 다음 예와 같아야 합니다:



ca.crt`을(를) 사용하여 `ontap_mediator_server.crt` 인증서에 서명한 경우 ca.srl 파일이 생성됩니다. 자세한 내용은 [2단계: 제3자 CA 인증서를 사용하여 서명함으로써 서버 인증서를 생성합니다.](#)을(를) 참조하십시오.

```
[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/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. root_ca.crt 인증서가 ontap_mediator_server.crt 인증서에 서명하는 ca.crt 인증서를 제공하는 인증서 구조를 사용하는 경우, ca.crt 및 ontap_mediator_server.crt 인증서에서 인증서 체인을 생성하십시오.



절차의 이전 단계에서 PKI 기관으로부터 ca.crt 및 ontap_mediator_server.crt 인증서를 발급받았어야 합니다.

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

- b. /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini 파일을 업데이트하십시오.

`mediator\_cert`, `mediator\_key` 및 `ca\_certificate`의 값을 업데이트하십시오:

```
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
```

- 해당 mediator_cert 값은 ontap_mediator_server_chain.crt 파일의 경로입니다.
- 해당 mediator_key 값은 ontap_mediator_server.crt 파일의 키 경로이며, 이는 'ontap_mediator_server.key'입니다.
- 해당 ca_certificate 값은 root_ca.crt 파일의 경로입니다.



SnapMirror Business Continuity(SM-BC) 클러스터의 경우 ONTAP 클러스터에 ca.crt 및 root_ca.crt 인증서를 추가해야 합니다. "[SnapMirror 활성화 동기화를 위해 ONTAP Mediator 및 클러스터를 구성합니다.](#)"을(를) 참조하십시오.

c. 새로 생성된 인증서의 다음 속성이 올바르게 설정되었는지 확인하십시오:

- Linux 그룹 소유자: netapp:netapp
- Linux 권한: 600

2. 구성 파일에서 인증서가 업데이트되면 ONTAP Mediator를 다시 시작합니다:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 인증서 관련 문제 해결

인증서 문제를 해결할 때 이러한 검사를 사용하여 인증서 속성을 확인하십시오.

인증서 만료 확인

다음 명령어를 사용하여 인증서 유효 기간을 확인하십시오.

ONTAP Mediator 1.9 이상 버전

```
[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 이하 버전

```
[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
```

CA 인증서에서 X509v3 확장 기능을 확인합니다.

CA 인증서의 X509v3 확장 기능을 확인하려면 다음 명령어를 사용하십시오.

ONTAP Mediator 1.9 이상 버전

`openssl\_ca.cnf` 내의 `\*v3\_ca\*`에 정의된 속성은 `intermediate.crt`에서 `X509v3 extensions`으로 표시됩니다.

```
[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:
2F: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 이하 버전

`openssl\_ca.cnf` 내의 `\*v3\_ca\*`에서 정의된 속성은 `ca.crt` 내에서 `X509v3 extensions`로 표시됩니다.

```
[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
```

서버 인증서 및 주체 대체 이름에서 **X509v3** 확장 기능을 확인하십시오

`openssl\_server.cnf` 구성 파일에 정의된 `v3\_req` 속성은 인증서에 `X509v3 extensions`으로 표시됩니다.

다음 예에서는 ONTAP Mediator가 설치된 Linux VM에서 `hostname -A` 및 `hostname -I` 명령을 실행하여 `alt_names` 섹션의 변수를 가져올 수 있습니다.

변수의 정확한 값은 네트워크 관리자에게 문의하십시오.

ONTAP Mediator 1.9 이상 버전

```
[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 이하 버전

```
[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
```

개인 키가 인증서와 일치하는지 확인하십시오

특정 개인 키가 인증서와 일치하는지 확인할 수 있습니다.

다음 OpenSSL 명령어를 키와 인증서에 각각 적용하십시오.

ONTAP Mediator 1.9 이상 버전

```
[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 이하 버전

```
[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
```

양쪽의 -modulus 속성이 일치하면 개인 키와 인증서 쌍이 호환되어 서로 함께 작동할 수 있음을 나타냅니다.

서버 인증서가 특정 **CA** 인증서로부터 생성되었는지 확인하십시오

다음 명령어를 사용하여 서버 인증서가 특정 CA 인증서로부터 생성되었는지 확인할 수 있습니다.

ONTAP Mediator 1.9 이상 버전

```
[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 이하 버전

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

온라인 인증서 상태 프로토콜(OCSP) 유효성 검사를 사용하는 경우 "[openssl-verify](#)" 명령어를 사용하십시오.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.