



Gestisci i certificati

ONTAP Mediator

NetApp
October 19, 2026

Sommario

- Gestisci i certificati 1
 - Rigenera un certificato temporaneo autofirmato per l’host ONTAP Mediator 1
 - Sostituisci i certificati autofirmati di ONTAP Mediator con certificati attendibili di terze parti 2
 - Passaggio 1: Ottieni un certificato da una terza parte che emette un certificato CA..... 3
 - Passaggio 2: Genera un certificato server firmandolo con un’autorità di certificazione (CA) di terze parti 5
 - Passaggio 3: sostituisci il nuovo certificato CA di terze parti e il certificato del server nella configurazione di ONTAP Mediator 6
 - Passaggio 4: Facoltativamente, usa un percorso o un nome diverso per i certificati di terze parti 10
- Risolvi i problemi relativi ai certificati di ONTAP Mediator 16
 - Verifica la scadenza del certificato 16
 - Verifica le estensioni X509v3 nel certificato CA..... 17
 - Verifica le estensioni X509v3 nel certificato del server e nei Subject Alternative Name 18
 - Verifica che la chiave privata corrisponda al certificato 20
 - Verifica che il certificato del server sia stato creato a partire da un certificato CA specifico 21

Gestisci i certificati

Rigenera un certificato temporaneo autofirmato per l'host ONTAP Mediator

Rigenera un certificato temporaneo autofirmato per l'host corrente quando una modifica dell'host name o dell'indirizzo IP invalida il certificato esistente.



Questa procedura è supportata solo sui sistemi che eseguono ONTAP Mediator 1.7 o versioni successive.

Informazioni su questa attività

- Esegui questa operazione sull'host Linux su cui hai installato ONTAP Mediator.
- Puoi eseguire questa operazione solo se i certificati autofirmati generati sono diventati obsoleti a causa di modifiche all'hostname o all'indirizzo IP dell'host dopo aver installato ONTAP Mediator.
- Dopo aver sostituito il certificato temporaneo autofirmato con un certificato di terze parti attendibile, non usare questa procedura per rigenerare un certificato. L'assenza di un certificato autofirmato causerà l'errore di questa procedura.

Passaggio

Per rigenerare un nuovo certificato temporaneo autofirmato per l'host corrente, esegui il seguente passaggio:

1. Riavvia ONTAP Mediator:

```
./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
```

Sostituisci i certificati autofirmati di ONTAP Mediator con certificati attendibili di terze parti

Se il tuo ambiente lo consente, sostituisci i certificati autofirmati con certificati attendibili emessi da un'autorità di certificazione.

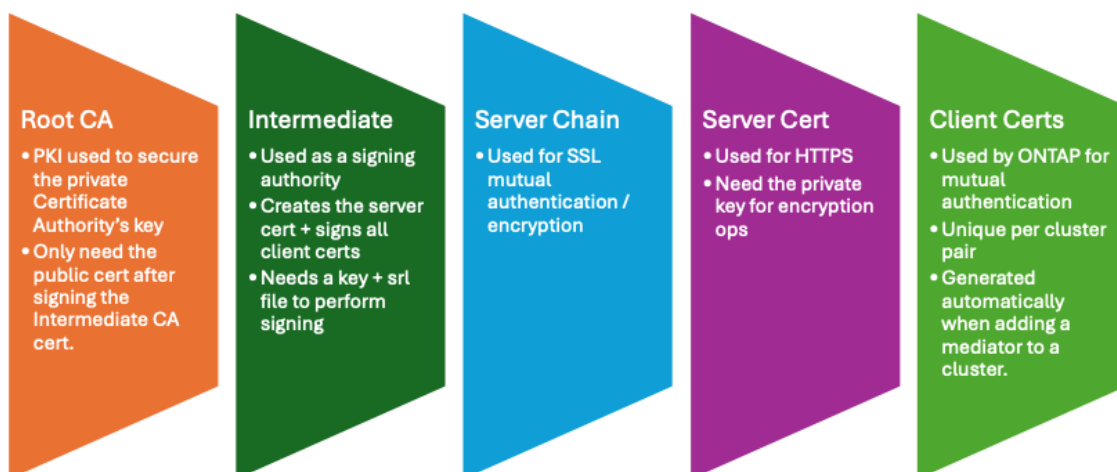


- I certificati di terze parti sono supportati solo a partire da ONTAP 9.16.1 e in alcune release patch precedenti di ONTAP. Consulta ["ID bug Bugs Online NetApp CONTAP-243278"](#).
- I certificati di terze parti sono supportati solo sui sistemi che eseguono ONTAP Mediator 1.7 o versioni successive.

Informazioni su questa attività

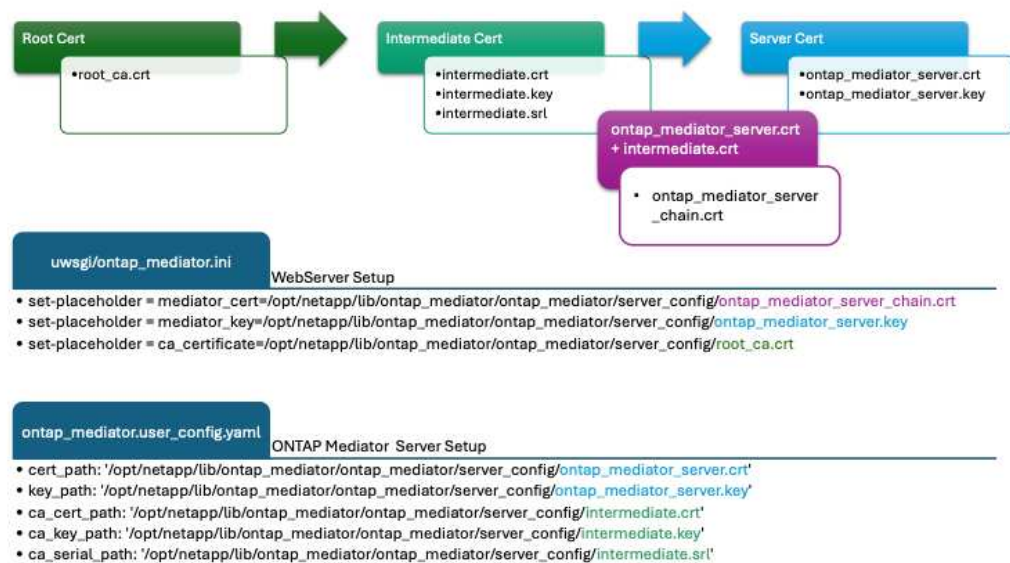
- Esegui questa operazione sull'host Linux su cui hai installato ONTAP Mediator.
- Puoi eseguire questa operazione se i certificati autofirmati generati devono essere sostituiti con certificati ottenuti da un'autorità di certificazione (CA) subordinata attendibile. Per farlo, devi avere accesso a un'autorità attendibile dell'infrastruttura a chiave pubblica (PKI).
- L'immagine seguente mostra le finalità di ciascun certificato ONTAP Mediator.

ONTAP Mediator Certificate Purposes



- L'immagine seguente mostra la configurazione per l'installazione del server web e di ONTAP Mediator.

ONTAP Mediator Certificates



Passaggio 1: Ottieni un certificato da una terza parte che emette un certificato CA

Puoi ottenere un certificato da un'autorità PKI seguendo la procedura descritta di seguito.

L'esempio seguente mostra come sostituire i componenti del certificato autofirmato con quelli del certificato di terze parti che si trovano in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`.



L'esempio illustra i criteri necessari per i certificati richiesti per ONTAP Mediator. Puoi ottenere i certificati da un'autorità PKI seguendo una procedura che potrebbe differire da quella descritta. Adatta la procedura alle tue esigenze aziendali.

ONTAP Mediator 1.9 e versioni successive

1. Crea una chiave privata `intermediate.key` e un file di configurazione `openssl_ca.cnf` che verranno utilizzati dall'autorità PKI per generare un certificato.

- a. Genera la chiave privata `intermediate.key`:

Esempio

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

- b. Il file di configurazione `openssl_ca.cnf` (situato in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definisce le proprietà che il certificato generato deve possedere.

2. Usa la chiave privata e il file di configurazione per creare una richiesta di firma del certificato `intermediate.csr`:

Esempio:

```
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. Invia la richiesta di firma del certificato `intermediate.csr` a un'autorità PKI per farla firmare.

L'autorità PKI verifica la richiesta e firma il `.csr`, generando il certificato `intermediate.crt`. Inoltre, devi ottenere dall'autorità PKI il certificato `root_ca.crt` che ha firmato il certificato `intermediate.crt`.



Per i cluster di sincronizzazione attiva di SnapMirror e le configurazioni IP di MetroCluster che utilizzano ONTAP Mediator configurato con HTTPS, devi aggiungere i certificati `intermediate.crt` e `root_ca.crt` a un cluster ONTAP. Vedi ["Configura ONTAP Mediator e i cluster per SnapMirror active sync"](#) e ["Configura il mediatore ONTAP per una configurazione IP MetroCluster"](#).

ONTAP Mediator 1.8 e versioni precedenti

1. Crea una chiave privata `ca.key` e un file di configurazione `openssl_ca.cnf` che l'autorità PKI userà per generare un certificato.
 - a. Genera la chiave privata `ca.key`:
Esempio:

```
openssl genrsa -aes256 -out ca.key 4096
```
 - b. Il file di configurazione `openssl_ca.cnf` (situato in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definisce le proprietà che il certificato generato deve possedere.
2. Usa la chiave privata e il file di configurazione per creare una richiesta di firma del certificato `ca.csr`:

Esempio:

```
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. Invia la richiesta di firma del certificato `ca.csr` a un'autorità PKI per la firma.

L'autorità PKI verifica la richiesta e firma il documento `.csr`, generando il certificato `ca.crt`. Inoltre, devi ottenere dall'autorità PKI il certificato `root_ca.crt` che ha firmato il certificato `ca.crt`.



Per i cluster con sincronizzazione attiva di SnapMirror, devi aggiungere i `ca.crt` e `root_ca.crt` certificati a un cluster ONTAP. Vedi "[Configura ONTAP Mediator e i cluster per SnapMirror active sync](#)".

Passaggio 2: Genera un certificato server firmandolo con un'autorità di certificazione (CA) di terze parti

ONTAP Mediator 1.9 e versioni successive

Un certificato server deve essere firmato con la chiave privata `intermediate.key` e il certificato di terze parti `intermediate.crt`. Inoltre, il file di configurazione `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contiene determinati attributi che specificano le proprietà richieste per i certificati server emessi da OpenSSL.

I seguenti comandi possono generare un certificato del server.

Passaggi

1. Per generare una richiesta di firma del certificato del server (CSR), esegui il seguente comando dalla `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` cartella:

```
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. Per generare un certificato server dal CSR, esegui il seguente comando dalla `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` cartella:



Questi file provengono da un'autorità PKI. Se utilizzi un nome di certificato diverso, sostituisci `intermediate.crt` e `intermediate.key` con i nomi file pertinenti.

```
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
```

° L'opzione `-CAcreateserial` viene utilizzata per generare i file `intermediate.srl`.

ONTAP Mediator 1.8 e versioni precedenti

Un certificato server deve essere firmato con la chiave privata `ca.key` e con il certificato di terze parti `ca.crt`. Inoltre, il file di configurazione `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contiene determinati attributi che specificano le proprietà richieste per i certificati server emessi da

OpenSSL.

I seguenti comandi possono generare un certificato del server.

Passaggi

1. Per generare una richiesta di firma del certificato del server (CSR), esegui il seguente comando dalla /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config cartella:

```
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. Per generare un certificato server dal CSR, esegui il seguente comando dalla /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`cartella:



Hai ottenuto questi file da un'autorità PKI. Se usi un nome di certificato diverso, sostituisci `ca.crt` e `ca.key` con i nomi di file pertinenti.

```
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
```

° L'-CAcreateserial`opzione serve a generare il `ca.srl file.

Passaggio 3: sostituisci il nuovo certificato CA di terze parti e il certificato del server nella configurazione di ONTAP Mediator

ONTAP Mediator 1.10 e versioni successive

La configurazione del certificato viene fornita a ONTAP Mediator nel file di configurazione situato in /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml. Il file include i seguenti attributi:

```
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` e `key_path` sono variabili del certificato del server.
- `ca_cert_path`, `ca_key_path`, e `ca_serial_path` sono variabili del certificato CA.

Passaggi

1. Sostituisci tutti `intermediate.*` i file con i certificati di terze parti.
2. Crea una catena di certificati dai `intermediate.crt` e `ontap_mediator_server.crt` certificati:

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

3. Aggiorna il `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` file.

Aggiorna i valori di `ssl_keyfile`, `ssl_certfile`, e `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
```

- Il `ssl_keyfile` valore è il percorso della chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
 - Il `ssl_certfile` valore corrisponde al percorso del `ontap_mediator_server_chain.crt` file.
 - Il `ssl_ca_certs` valore corrisponde al percorso del `root_ca.crt` file.
4. Verifica che i seguenti attributi dei certificati appena generati siano impostati correttamente:
 - Proprietario del gruppo Linux: `netapp:netapp`
 - Permessi Linux: `600`
 5. Riavvia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 e 1.9

La configurazione del certificato viene fornita a ONTAP Mediator nel file di configurazione situato in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. Il file include i seguenti attributi:

```
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` e `key_path` sono variabili del certificato del server.
- `ca_cert_path`, `ca_key_path`, e `ca_serial_path` sono variabili del certificato CA.

Passaggi

1. Sostituisci tutti `intermediate.*` i file con i certificati di terze parti.
2. Crea una catena di certificati dai `intermediate.crt` e `ontap_mediator_server.crt` certificati:

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

3. Aggiorna il `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Aggiorna i valori di `mediator_cert`, `mediator_key` e `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

```

- Il `mediator_cert` valore corrisponde al percorso del `ontap_mediator_server_chain.crt` file.
- Il `mediator_key` value è il percorso chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- Il `ca_certificate` valore è il percorso del `root_ca.crt` file.

4. Verifica che i seguenti attributi dei certificati appena generati siano impostati correttamente:

- Proprietario del gruppo Linux: `netapp:netapp`

◦ Permessi Linux: 600

5. Riavvia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 e versioni precedenti

La configurazione del certificato viene fornita a ONTAP Mediator nel file di configurazione situato in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.conf.yaml`. Il file include i seguenti attributi:

```
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` e `key_path` sono variabili del certificato del server.
- `ca_cert_path`, `ca_key_path`, e `ca_serial_path` sono variabili del certificato CA.

Passaggi

1. Sostituisci tutti `ca.*` i file con i certificati di terze parti.
2. Crea una catena di certificati dai certificati `ca.crt` e `ontap_mediator_server.crt`:

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

3. Aggiorna il `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Aggiorna i valori di `mediator_cert`, `mediator_key` e `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
```

- Il `mediator_cert` valore corrisponde al percorso del `ontap_mediator_server_chain.crt` file.
 - Il `mediator_key` value è il percorso chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
 - Il `ca_certificate` valore è il percorso del `root_ca.crt` file.
4. Verifica che i seguenti attributi dei certificati appena generati siano impostati correttamente:
 - Proprietario del gruppo Linux: `netapp:netapp`
 - Permessi Linux: `600`
 5. Riavvia ONTAP Mediator:


```
systemctl restart ontap_mediator
```

Passaggio 4: Facoltativamente, usa un percorso o un nome diverso per i certificati di terze parti

ONTAP Mediator 1.10 e versioni successive

Puoi utilizzare certificati di terze parti con un nome diverso da `intermediate.*` oppure archiviare i certificati di terze parti in una posizione diversa.

Passaggi

1. Configura il

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file per sovrascrivere i valori predefiniti delle variabili nel `ontap_mediator.config.yaml` file.

Se hai ottenuto `intermediate.crt` da un'autorità PKI e memorizzi la sua chiave privata `intermediate.key` nella posizione

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, il `ontap_mediator.user_config.yaml` file dovrebbe essere simile al seguente esempio:



Se hai usato `intermediate.crt` per firmare il `ontap_mediator_server.crt` certificato, viene generato il file `intermediate.srl`. Consulta [Passaggio 2: Genera un certificato server firmandolo con un'autorità di certificazione \(CA\) di terze parti](#) per ulteriori informazioni.

```
[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. Se utilizzi una struttura di certificati in cui il `root_ca.crt` certificato fornisce un `intermediate.crt` certificato che firma il `ontap_mediator_server.crt` certificato, crea una catena di certificati dai certificati `intermediate.crt` e `ontap_mediator_server.crt`:



Avresti dovuto ottenere i `intermediate.crt` e `ontap_mediator_server.crt` certificati da un'autorità PKI in una fase precedente della procedura.

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

- b. Aggiorna il `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` file.

Aggiorna i valori di `ssl_keyfile`, `ssl_certfile`, e `ssl_ca_certs`:

```

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
```

- Il `ssl_keyfile` valore è il percorso della chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- Il `ssl_certfile` valore corrisponde al percorso del `ontap_mediator_server_chain.crt` file.
- Il `ssl_ca_certs` valore corrisponde al percorso del `root_ca.crt` file.



Per i cluster di sincronizzazione attiva di SnapMirror e le configurazioni IP di MetroCluster che utilizzano ONTAP Mediator configurato con HTTPS, devi aggiungere i certificati `intermediate.crt` e `root_ca.crt` a un cluster ONTAP. Vedi ["Configura ONTAP Mediator e i cluster per SnapMirror active sync"](#) e ["Configura il mediatore ONTAP per una configurazione IP MetroCluster"](#).

c. Verifica che i seguenti attributi dei certificati appena generati siano impostati correttamente:

- Proprietario del gruppo Linux: `netapp:netapp`
- Permessi Linux: `600`

2. Riavvia ONTAP Mediator quando i certificati vengono aggiornati nel file di configurazione:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 e 1.9

Puoi utilizzare certificati di terze parti con un nome diverso da `intermediate.*` oppure archiviare i certificati di terze parti in una posizione diversa.

Passaggi

1. Configura il

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file per sovrascrivere i valori predefiniti delle variabili nel `ontap_mediator.config.yaml` file.

Se hai ottenuto `intermediate.crt` da un'autorità PKI e memorizzi la sua chiave privata `intermediate.key` nella posizione

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, il `ontap_mediator.user_config.yaml` file dovrebbe essere simile al seguente esempio:



Se hai usato `intermediate.crt` per firmare il `ontap_mediator_server.crt` certificato, viene generato il file `intermediate.srl`. Consulta [Passaggio 2: Genera un certificato server firmandolo con un'autorità di certificazione \(CA\) di terze parti](#) per ulteriori informazioni.

```
[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. Se utilizzi una struttura di certificati in cui il `root_ca.crt` certificato fornisce un `intermediate.crt` certificato che firma il `ontap_mediator_server.crt` certificato, crea una catena di certificati dai certificati `intermediate.crt` e `ontap_mediator_server.crt`:



Avresti dovuto ottenere i `intermediate.crt` e `ontap_mediator_server.crt` certificati da un'autorità PKI in una fase precedente della procedura.

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

- b. Aggiorna il `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Aggiorna i valori di `mediator_cert`, `mediator_key` e `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_mediator_server.key
```

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

- Il `mediator_cert` valore corrisponde al percorso del `ontap_mediator_server_chain.crt` file.
- Il `mediator_key` valore è il percorso della chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- Il `ca_certificate` valore è il percorso del `root_ca.crt` file.



Per i cluster SnapMirror Business Continuity (SM-BC), devi aggiungere i certificati `intermediate.crt` e `root_ca.crt` a un cluster ONTAP. Vedi ["Configura ONTAP Mediator e i cluster per SnapMirror active sync"](#).

c. Verifica che i seguenti attributi dei certificati appena generati siano impostati correttamente:

- Proprietario del gruppo Linux: `netapp:netapp`
- Permessi Linux: `600`

2. Riavvia ONTAP Mediator quando i certificati vengono aggiornati nel file di configurazione:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 e versioni precedenti

Puoi utilizzare certificati di terze parti con un nome diverso da `ca.*` oppure archiviare i certificati di terze parti in una posizione diversa.

Passaggi

1. Configura il

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file per sovrascrivere i valori predefiniti delle variabili nel `ontap_mediator.config.yaml` file.

Se hai ottenuto `ca.crt` da un'autorità PKI e memorizzi la relativa chiave privata `ca.key` nella posizione `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, il `ontap_mediator.user_config.yaml` file dovrebbe essere simile al seguente esempio:



Se hai usato `ca.crt` per firmare il `ontap_mediator_server.crt` certificato, viene generato il file `ca.srl`. Consulta [Passaggio 2: Genera un certificato server firmandolo con un'autorità di certificazione \(CA\) di terze parti](#) per ulteriori informazioni.

```
[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. Se utilizzi una struttura di certificati in cui il `root_ca.crt` certificato fornisce un `ca.crt` certificato che firma il `ontap_mediator_server.crt` certificato, crea una catena di certificati dai `ca.crt` e `ontap_mediator_server.crt` certificati:



Avresti dovuto ottenere i `ca.crt` e `ontap_mediator_server.crt` certificati da un'autorità PKI in una fase precedente della procedura.

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

- b. Aggiorna il `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Aggiorna i valori di `mediator_cert`, `mediator_key` e `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
```

- Il `mediator_cert` valore corrisponde al percorso del `ontap_mediator_server_chain.crt` file.
- Il `mediator_key` valore è il percorso della chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- Il `ca_certificate` valore è il percorso del `root_ca.crt` file.



Per i cluster SnapMirror Business Continuity (SM-BC), devi aggiungere i certificati `ca.crt` e `root_ca.crt` a un cluster ONTAP. Vedi ["Configura ONTAP Mediator e i cluster per SnapMirror active sync"](#).

c. Verifica che i seguenti attributi dei certificati appena generati siano impostati correttamente:

- Proprietario del gruppo Linux: `netapp:netapp`
- Permessi Linux: `600`

2. Riavvia ONTAP Mediator quando i certificati vengono aggiornati nel file di configurazione:

```
systemctl restart ontap_mediator
```

Risolvi i problemi relativi ai certificati di ONTAP Mediator

Usa questi controlli per verificare le proprietà del certificato durante la risoluzione dei problemi dei certificati.

Verifica la scadenza del certificato

Usa il seguente comando per identificare l'intervallo di validità del certificato.

ONTAP Mediator 1.9 e versioni successive

```
[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 e versioni precedenti

```
[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
```

Verifica le estensioni X509v3 nel certificato CA

Usa il seguente comando per verificare le estensioni X509v3 nel certificato della CA.

ONTAP Mediator 1.9 e versioni successive

Le proprietà definite all'interno di **v3_ca** in `openssl_ca.cnf` vengono visualizzate come X509v3 extensions in `intermediate.crt`.

```
[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 e versioni precedenti

Le proprietà definite all'interno di **v3_ca** in `openssl_ca.cnf` vengono visualizzate come X509v3 extensions in `ca.crt`.

```
[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
```

Verifica le estensioni X509v3 nel certificato del server e nei Subject Alternative Name

Le `v3_req` proprietà definite nel `openssl_server.cnf` file di configurazione sono visualizzate come X509v3 extensions nel certificato.

Nell'esempio seguente, puoi ottenere le variabili nelle `alt_names` sezioni eseguendo i comandi `hostname -A` e `hostname -I` sulla VM Linux su cui è installato ONTAP Mediator.

Verifica con il tuo amministratore di rete i valori corretti delle variabili.

ONTAP Mediator 1.9 e versioni successive

```
[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 e versioni precedenti

```
[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

```

Verifica che la chiave privata corrisponda al certificato

Puoi verificare se una determinata chiave privata corrisponde a un certificato.

Usa i seguenti comandi OpenSSL rispettivamente sulla chiave e sul certificato.

ONTAP Mediator 1.9 e versioni successive

```

[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 e versioni precedenti

```
[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
```

Se l'attributo `-modulus` per entrambi corrisponde, significa che la coppia chiave privata-certificato è compatibile e può funzionare insieme.

Verifica che il certificato del server sia stato creato a partire da un certificato CA specifico

Puoi usare il seguente comando per verificare che il certificato del server sia stato creato da un certificato CA specifico.

ONTAP Mediator 1.9 e versioni successive

```
[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 e versioni precedenti

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

Se utilizzi la convalida OCSP (Online Certificate Status Protocol), usa il comando `"openssl-verify"`.

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.