



管理憑證 ONTAP Mediator

NetApp
October 19, 2026

目錄

管理憑證	1
為 ONTAP Mediator 主機重新產生臨時自簽名憑證	1
將 ONTAP Mediator 自簽名憑證替換為受信任的第三方憑證	2
步驟 1：從核發 CA 憑證的第三方取得憑證	3
步驟 2：使用第三方 CA 認證簽署來產生伺服器憑證	5
步驟 3：在 ONTAP Mediator 組態中取代新的第三方 CA 憑證和伺服器憑證	6
步驟 4：視需要，為您的第三方憑證使用不同的路徑或名稱	10
疑難排解 ONTAP 中介器憑證相關問題	16
驗證憑證到期	16
驗證 CA 認證中的 X509v3 擴充	16
驗證伺服器憑證和主旨備用名稱中的 X509v3 擴充	18
驗證私鑰是否與憑證相符	20
確認伺服器憑證是由特定的 CA 憑證建立	20

管理憑證

為 ONTAP Mediator 主機重新產生臨時自簽名憑證

當主機名稱或 IP 位址變更導致現有憑證失效時，為目前主機重新產生臨時自簽章憑證。



此程序僅在執行 ONTAP Mediator 1.7 或更新版本的系統上支援。

關於此任務

- 在安裝了 ONTAP Mediator 的 Linux 主機上執行此工作。
- 只有當安裝 ONTAP Mediator 後，由於主機的主機名稱或 IP 位址發生更改，導致產生的自簽名憑證失效時，才能執行此工作。
- 在臨時自我簽署憑證被受信任的第三方憑證取代後，您_不得_使用此工作重新產生憑證。缺少自我簽署憑證會導致此程序失敗。

步驟

若要為目前主機重新產生新的臨時自簽憑證，請執行下列步驟：

1. 重新啟動 ONTAP 中介器：

```
./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
```

將 ONTAP Mediator 自簽名憑證替換為受信任的第三方憑證

如果您的環境支援，請將自簽名憑證取代為由憑證授權單位所核發的受信任憑證。

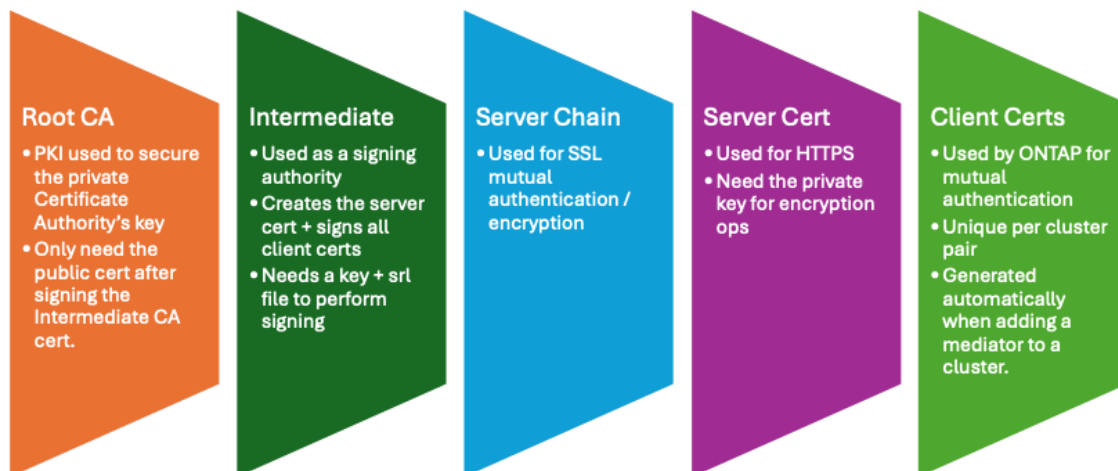


- 第三方憑證僅從 ONTAP 9.16.1 版本開始，以及在一些較早的 ONTAP 修補程式版本中才受支援。請參閱 ["NetApp Bugs Online Bug ID CONTAP-243278"](#)。
- 第三方憑證僅在執行 ONTAP Mediator 1.7 或更新版本的系統上支援。

關於此任務

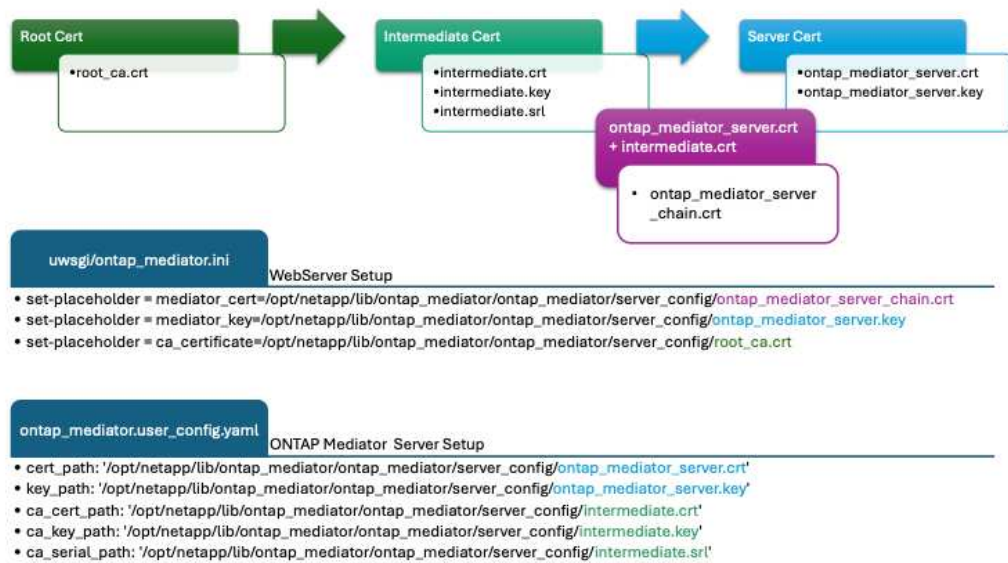
- 在安裝了 ONTAP Mediator 的 Linux 主機上執行此工作。
- 如果需要將產生的自簽章憑證取代為從受信任的下級憑證授權單位 (CA) 取得的憑證，則可以執行此工作。為此，您需要擁有受信任的公開金鑰基礎架構 (PKI) 授權單位的存取權。
- 下列映像顯示每個 ONTAP Mediator 憑證的用途。

ONTAP Mediator Certificate Purposes



- 下列映像顯示 Web 伺服器設定與 ONTAP Mediator 設定的組態。

ONTAP Mediator Certificates



步驟 1：從核發 CA 憑證的第三方取得憑證

您可以使用以下步驟從 PKI 機構取得憑證。

以下範例示範如何將自簽名憑證提供者替換為位於
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/' 的第三方憑證提供者。



此範例說明了 ONTAP Mediator 所需憑證的必要條件。您可以從 PKI 機構取得憑證，其方式可能與此程序不同。請根據您的業務需求調整程序。

ONTAP Mediator 1.9 及更高版本

1. 建立私鑰 `intermediate.key` 和組態檔案 `openssl_ca.cnf`，供 PKI 機構產生憑證時使用。

- a. 產生私鑰 `intermediate.key`：

範例

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

- b. 組態檔案 `openssl_ca.cnf` (位於
`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) 定義了產生的憑證必須具有的屬性。

2. 使用私鑰和組態檔案建立憑證簽署請求 `intermediate.csr`：

範例：

```
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. 將憑證簽署請求發送 `intermediate.csr` 給 PKI 機構進行簽署。

PKI 授權單位驗證請求並對 `.csr` 進行簽署，以產生憑證 `intermediate.crt`。此外，您還需要從 PKI 授權單位取得對 `intermediate.crt` 憑證進行簽署的 `root\_ca.crt` 憑證。



對於使用設定為 HTTPS 的 ONTAP Mediator 的 SnapMirror 作用中同步叢集和 MetroCluster IP 組態，您必須將 `intermediate.crt` 和 `root\_ca.crt` 憑證新增至 ONTAP 叢集。請參閱 ["設定 ONTAP 中介器和叢集以進行 SnapMirror 作用中同步"](#) 和 ["設定 ONTAP Mediator 以進行 MetroCluster IP 組態"](#)。

ONTAP Mediator 1.8 及更早版本

1. 建立私鑰 `ca.key` 和組態檔案 `openssl\_ca.cnf`，供 PKI 機構產生憑證時使用。

- a. 產生私鑰 `ca.key`：

範例：

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

- b. 組態檔案 `openssl\_ca.cnf`（位於
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_ca.cnf`）定義了產生的憑證必須具有的屬性。

2. 使用私鑰和組態檔案建立憑證簽署請求 `ca.csr`：

範例：

```
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. 將憑證簽署請求 `ca.csr` 發送給 PKI 機構進行簽署。

PKI 授權單位驗證請求並為 `.csr` 簽署，產生憑證 `ca.crt`。此外，您還需要從 PKI 授權單位取得

已簽署 `ca.crt` 憑證的 `root\_ca.crt` 憑證。



對於 SnapMirror 作用中同步叢集，您必須將 `ca.crt` 和 `root\_ca.crt` 憑證新增至 ONTAP 叢集。請參閱["設定 ONTAP 中介器和叢集以進行 SnapMirror 作用中同步"](#)。

步驟 2：使用第三方 CA 認證簽署來產生伺服器憑證

ONTAP Mediator 1.9 及更高版本

伺服器憑證必須由私鑰 `intermediate.key` 和第三方憑證 `intermediate.crt` 簽署。此外，組態檔案 `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_server.cnf` 包含某些屬性，用於指定 OpenSSL 所發出的伺服器憑證所需的特性。

以下命令可以產生伺服器憑證。

步驟

1. 若要產生伺服器憑證簽署要求（CSR），請從
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` 資料夾執行下列命令：

```
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. 若要從 CSR 產生伺服器憑證，請從
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` 資料夾執行下列命令：



這些檔案是從 PKI 機構取得的。如果您使用的是不同的憑證名稱，請將
`intermediate.crt` 和 `intermediate.key` 替換為相關的檔案名稱。

```
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 選項用於產生 `intermediate.srl` 檔案。

ONTAP Mediator 1.8 及更早版本

伺服器憑證必須由私鑰 `ca.key` 和第三方憑證 `ca.crt` 簽署。此外，組態檔案 `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_server.cnf` 包含某些屬性，用於指定 OpenSSL 所發出的伺服器憑證所需的特性。

以下命令可以產生伺服器憑證。

步驟

1. 若要產生伺服器憑證簽署要求（CSR），請從
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` 資料夾執行下列命令：

```
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. 若要從 CSR 產生伺服器憑證，請從

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config 資料夾執行下列命令：



這些檔案是從 PKI 授權單位取得。如果您使用的是不同的憑證名稱，請將 `ca.crt` 和 `ca.key` 替換為相關的檔案名稱。

```
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
```

◦ 此 -CAcreateserial 選項用於產生 ca.srl 檔案。

步驟 3：在 ONTAP Mediator 組態中取代新的第三方 CA 憑證和伺服器憑證

ONTAP Mediator 1.10 及更高版本

憑證組態透過位於

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml 的組態檔案提供給 ONTAP Mediator。該檔案包含下列屬性：

```
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 和 key_path 是伺服器憑證變數。
- ca_cert_path、ca_key_path 和 ca_serial_path 是 CA 憑證變數。

步驟

1. 將所有 `intermediate.\*` 檔案替換為第三方憑證。

2. 從 `intermediate.crt` 和 `ontap\_mediator\_server.crt` 憑證建立憑證鏈：

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

3. 更新 `/opt/netapp/lib/ontap\_mediator/uvicorn/config.json` 檔案。

更新 `ssl\_keyfile`、`ssl\_certfile` 和 `ssl\_ca\_certs` 的值：

```
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
```

- 該 `ssl\_keyfile` 值是 `ontap\_mediator\_server.crt` 檔案中的鍵路徑，即 `ontap\_mediator\_server.key`。
- 該 `ssl\_certfile` 值是 `ontap\_mediator\_server\_chain.crt` 檔案的路徑。
- 該 `ssl\_ca\_certs` 值是 `root\_ca.crt` 檔案的路徑。

4. 請驗證新產生的憑證的以下屬性是否設定正確：

- Linux 群組所有者：`netapp:netapp`
- Linux 權限：`600`

5. 重新啟動 ONTAP 中介器：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 和 1.9

憑證組態透過位於

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 的組態檔案提供給 ONTAP Mediator。該檔案包含下列屬性：

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

- cert_path 和 key_path 是伺服器憑證變數。
- ca_cert_path、ca_key_path 和 ca_serial_path 是 CA 憑證變數。

步驟

1. 將所有 `intermediate.\*` 檔案替換為第三方憑證。
2. 從 `intermediate.crt` 和 `ontap\_mediator\_server.crt` 憑證建立憑證鏈：

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

3. 更新 `/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini` 檔案。

更新 mediator_cert、`mediator\_key` 和 `ca\_certificate` 的值：

```
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
```

- 該 `mediator\_cert` 值是 `ontap\_mediator\_server\_chain.crt` 檔案的路徑。
 - mediator_key value 是 ontap_mediator_server.crt 檔案中的關鍵路徑，即 ontap_mediator_server.key。
 - 該 `ca\_certificate` 值是 `root\_ca.crt` 檔案的路徑。
4. 請驗證新產生的憑證的以下屬性是否設定正確：
 - Linux 群組所有者：netapp:netapp
 - Linux 權限：600
 5. 重新啟動 ONTAP 中介器：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 及更早版本

憑證組態透過位於

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml 的組態檔案提供給 ONTAP Mediator。該檔案包含下列屬性：

```

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 和 key_path 是伺服器憑證變數。
- ca_cert_path、ca_key_path 和 ca_serial_path 是 CA 憑證變數。

步驟

1. 將所有 `ca.\*` 檔案替換為第三方憑證。
2. 從 ca.crt 和 ontap_mediator_server.crt 憑證建立憑證鏈：

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

3. 更新 `/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini` 檔案。

更新 mediator_cert、`mediator\_key` 和 `ca\_certificate` 的值：

```
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
```

- 該 `mediator\_cert` 值是 `ontap\_mediator\_server\_chain.crt` 檔案的路徑。
 - mediator_key value 是 ontap_mediator_server.crt 檔案中的關鍵路徑，即 ontap_mediator_server.key。
 - 該 `ca\_certificate` 值是 `root\_ca.crt` 檔案的路徑。
4. 請驗證新產生的憑證的以下屬性是否設定正確：
 - Linux 群組所有者：netapp:netapp
 - Linux 權限：600

5. 重新啟動 ONTAP 中介器：

```
systemctl restart ontap_mediator
```

步驟 4：視需要，為您的第三方憑證使用不同的路徑或名稱

ONTAP Mediator 1.10 及更高版本

您可以使用名稱不同於 `intermediate.*` 的第三方憑證，或將第三方憑證儲存在不同的位置。

步驟

1. 設定

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` 檔案以置換 `ontap_mediator.config.yaml` 檔案中的預設變數值。

如果您從 PKI 機構取得 `intermediate.crt`，並將其私鑰 `intermediate.key` 儲存在位置 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`，則 `ontap_mediator.user_config.yaml` 檔案應類似於以下範例：



如果您使用 `intermediate.crt` 來簽署 `ontap_mediator_server.crt` 憑證，則會產生 `intermediate.srl` 檔案。請參閱 [步驟 2：使用第三方 CA 認證簽署來產生伺服器憑證](#) 以取得詳細資訊。

```
[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
```

```

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'

```

- a. 如果您使用的憑證結構中，root_ca.crt 憑證提供 intermediate.crt 憑證來簽署 ontap_mediator_server.crt 憑證，請從 intermediate.crt 和 ontap_mediator_server.crt 憑證建立憑證鏈：



您應該在先前的程序中，從 PKI 授權單位取得 `intermediate.crt` 和 `ontap\_mediator\_server.crt` 憑證。

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

- b. 更新 /opt/netapp/lib/ontap_mediator/uvicorn/config.json 檔案。

更新 ssl_keyfile、`ssl\_certfile` 和 `ssl\_ca\_certs` 的值：

```

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

```

- 該 ssl_keyfile 值是 ontap_mediator_server.crt 檔案中的鍵路徑，即 ontap_mediator_server.key。
- 該 `ssl\_certfile` 值是 `ontap\_mediator\_server\_chain.crt` 檔案的路徑。
- 該 ssl_ca_certs 值是 root_ca.crt 檔案的路徑。



對於使用設定為 HTTPS 的 ONTAP Mediator 的 SnapMirror 作用中同步叢集和 MetroCluster IP 組態，您必須將 `intermediate.crt` 和 `root\_ca.crt` 憑證新增至 ONTAP 叢集。請參閱 ["設定 ONTAP 中介器和叢集以進行 SnapMirror 作用中同步"](#) 和 ["設定 ONTAP Mediator 以進行 MetroCluster IP 組態"](#)。

- c. 請驗證新產生的憑證的以下屬性是否設定正確：

- Linux 群組所有者：netapp:netapp

- Linux 權限：600

2. 當組態檔案中的憑證更新後，請重新啟動 ONTAP Mediator：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 和 1.9

您可以使用名稱不同於 `intermediate.*` 的第三方憑證，或將第三方憑證儲存在不同的位置。

步驟

1. 設定

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` 檔案以置換 `ontap_mediator.config.yaml` 檔案中的預設變數值。

如果您從 PKI 機構取得 `intermediate.crt`，並將其私鑰 `intermediate.key` 儲存在位置 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`，則 `ontap_mediator.user_config.yaml` 檔案應類似於以下範例：



如果您使用 `intermediate.crt` 來簽署 `ontap_mediator_server.crt` 憑證，則會產生 `intermediate.srl` 檔案。請參閱 [步驟 2：使用第三方 CA 認證簽署來產生伺服器憑證](#) 以取得詳細資訊。

```
[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. 如果您使用的憑證結構中，root_ca.crt 憑證提供 intermediate.crt 憑證來簽署 ontap_mediator_server.crt 憑證，請從 intermediate.crt 和 ontap_mediator_server.crt 憑證建立憑證鏈：



您應該在先前的程序中，從 PKI 授權單位取得 `intermediate.crt` 和 `ontap\_mediator\_server.crt` 憑證。

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

- b. 更新 `/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini` 檔案。

更新 mediator_cert、mediator_key 和 ca_certificate 的值：

```
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
```

- 該 `mediator\_cert` 值是 `ontap\_mediator\_server\_chain.crt` 檔案的路徑。
- 該 mediator_key 值是 ontap_mediator_server.crt 檔案中的鍵路徑，即 ontap_mediator_server.key。
- 該 `ca\_certificate` 值是 `root\_ca.crt` 檔案的路徑。



對於 SnapMirror 業務連續性 (SM-BC) 叢集，您必須將 `intermediate.crt` 和 `root\_ca.crt` 憑證新增至 ONTAP 叢集。請參閱[設定 ONTAP 中介器和叢集以進行 SnapMirror 作用中同步](#)。

- c. 請驗證新產生的憑證的以下屬性是否設定正確：

- Linux 群組所有者：netapp:netapp
- Linux 權限：600

2. 當組態檔案中的憑證更新後，請重新啟動 ONTAP Mediator：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 及更早版本

您可以使用名稱不同於 `ca.*` 的第三方憑證，或將第三方憑證儲存在不同的位置。

步驟

1. 設定

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` 檔案以置換 `ontap_mediator.config.yaml` 檔案中的預設變數值。

如果您從 PKI 機構取得了 `ca.crt`，並將其私鑰 `ca.key` 儲存在位置

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`，則該 `ontap_mediator.user_config.yaml` 檔案應如下例所示：



如果您使用 `ca.crt` 簽署 `ontap_mediator_server.crt` 憑證，則會產生 `ca.srl` 檔案。如需詳細資訊，請參閱 [步驟 2：使用第三方 CA 認證簽署來產生伺服器憑證](#)。

```
[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. 如果您使用的憑證結構中，root_ca.crt 憑證提供 ca.crt 憑證來簽署 ontap_mediator_server.crt 憑證，請從 ca.crt 和 ontap_mediator_server.crt 憑證建立憑證鏈：



您應該在此程序稍早從 PKI 授權單位取得 ca.crt 和 ontap_mediator_server.crt 憑證。

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

- b. 更新 '/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini' 檔案。

更新 mediator_cert、mediator_key 和 ca_certificate 的值：

```
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
```

- 該 mediator_cert 值是 ontap_mediator_server_chain.crt 檔案的路徑。
- 該 mediator_key 值是 ontap_mediator_server.crt 檔案中的鍵路徑，即 ontap_mediator_server.key。
- 該 ca_certificate 值是 root_ca.crt 檔案的路徑。



對於 SnapMirror 業務連續性 (SM-BC) 叢集，您必須將 ca.crt 和 root_ca.crt 憑證新增至 ONTAP 叢集。請參閱 ["設定 ONTAP 中介器和叢集以進行 SnapMirror 作用中同步"](#)。

- c. 請驗證新產生的憑證的以下屬性是否設定正確：

- Linux 群組所有者：netapp:netapp
- Linux 權限：600

2. 當組態檔案中的憑證更新後，請重新啟動 ONTAP Mediator：

```
systemctl restart ontap_mediator
```

疑難排解 ONTAP 中介器憑證相關問題

在疑難排解憑證問題時，請使用這些檢查來驗證憑證屬性。

驗證憑證到期

使用下列命令來識別憑證有效範圍。

ONTAP Mediator 1.9 及更高版本

```
[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 及更早版本

```
[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
```

驗證 CA 認證中的 X509v3 擴充

使用下列命令驗證 CA 認證中的 X509v3 擴充。

ONTAP Mediator 1.9 及更高版本

在 `openssl_ca.cnf` 中的 ``v3_ca`` 內定義的屬性，會在 ``intermediate.crt`` 中顯示為 ``X509v3 extensions``。

```
[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 及更早版本

在 `openssl_ca.cnf` 中的 `v3_ca` 內定義的屬性，會在 `ca.crt` 中顯示為 `X509v3 extensions`。

```
[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

驗證伺服器憑證和主旨備用名稱中的 **X509v3** 擴充

`openssl\_server.cnf` 組態檔案中定義的 `v3\_req` 屬性會在憑證中顯示為 `X509v3 extensions`。

在以下範例中，您可以透過在安裝了 ONTAP Mediator 的 Linux VM 上執行命令 `hostname -A` 和 `hostname -I`，來取得 `alt\_names` 區段中的變數。

請向網路管理員諮詢變數的正確值。

ONTAP Mediator 1.9 及更高版本

```
[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 及更早版本

```
[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
```

驗證私鑰是否與憑證相符

您可以驗證某個私鑰是否與憑證相符。

分別對金鑰和憑證使用以下 OpenSSL 命令。

ONTAP Mediator 1.9 及更高版本

```
[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 及更早版本

```
[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
```

如果兩者的 `-modulus` 屬性相符，則表示私密金鑰和憑證配對相容，可以互相配合使用。

確認伺服器憑證是由特定的 CA 憑證建立

您可以使用下列命令來驗證伺服器憑證是否由特定的 CA 憑證建立。

ONTAP Mediator 1.9 及更高版本

```
[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 及更早版本

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

如果使用線上憑證狀態協定（OCSP）驗證，請使用命令 "[openssl-verify](#)"。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。