



証明書管理 ONTAP Mediator

NetApp
October 19, 2026

目次

証明書管理	1
ONTAP Mediatorホスト用の一時的な自己署名証明書を再生成する	1
ONTAP Mediatorの自己署名証明書を信頼できる第三者機関の証明書に置き換える	2
ステップ1：CA証明書を発行するサードパーティから証明書を取得する	3
ステップ2：サードパーティのCA証明書で署名してサーバー証明書を生成する	5
ステップ3：ONTAP Mediator構成で新しいサードパーティCA証明書とサーバー証明書を置き換える	6
ステップ4：オプションで、サードパーティの証明書に別のパスまたは名前を使用します	10
ONTAP Mediatorの証明書関連の問題のトラブルシューティング	16
証明書の有効期限を確認する	16
CA 証明書における X509v3 拡張の検証	17
サーバー証明書とサブジェクトの代替名における X509v3 拡張機能を検証する	19
秘密鍵が証明書と一致していることを確認する	21
サーバー証明書が特定のCA証明書から作成されたことを確認する	21

証明書の管理

ONTAP Mediatorホスト用の一時的な自己署名証明書を再生成する

ホスト名またはIPアドレスの変更により既存の証明書が無効になった場合、現在のホスト用の一時的な自己署名証明書を再生成します。



この手順は、ONTAP Mediator 1.7以降を実行しているシステムでのみサポートされます。

タスク概要

- この作業は、ONTAP Mediator をインストールした Linux ホストで実行してください。
- このタスクは、ONTAP Mediator のインストール後にホストのホスト名または IP アドレスが変更されたために、生成された自己署名証明書が古くなった場合にのみ実行できます。
- 一時的な自己署名証明書を信頼できるサードパーティの証明書に置き換えた後は、このタスクを使用して証明書を再生成し_ない_でください。自己署名証明書がない場合、この手順は失敗します。

手順

現在のホストの一時的な自己署名証明書を新たに再生成するには、以下の手順を実行します。

1. ONTAP Mediatorを再起動します：

```
./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の自己署名証明書を信頼できる第三者機関の証明書に置き換える

お使いの環境が対応している場合は、自己署名証明書を認証局が発行した信頼できる証明書に置き換えてください。

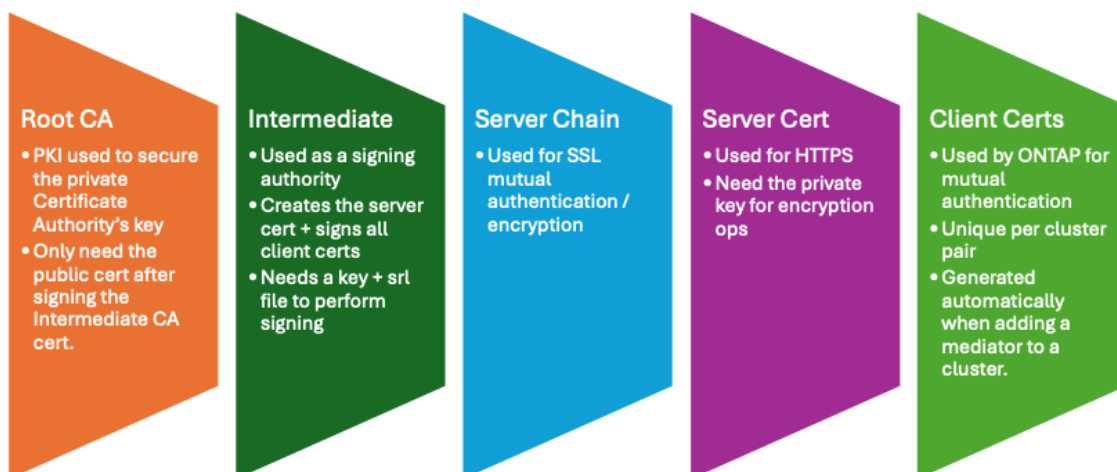


- サードパーティ証明書はONTAP 9.16.1以降およびそれ以前の一部のONTAPパッチリリースでのみサポートされます。["NetApp Bugs Online バグID CONTAP-243278"](#)を参照してください。
- サードパーティの証明書は、ONTAP Mediator 1.7以降を実行しているシステムでのみサポートされます。

タスク概要

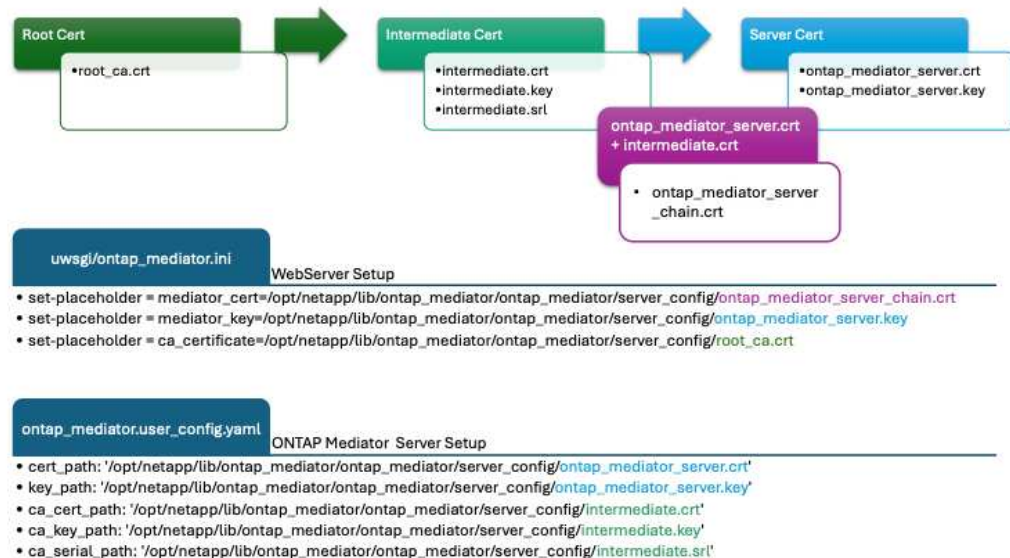
- この作業は、ONTAP Mediator をインストールした Linux ホストで実行してください。
- 生成された自己署名証明書を、信頼できる従属証明機関（CA）から取得した証明書に置き換える必要がある場合に、このタスクを実行できます。これを行うには、信頼できる公開鍵基盤（PKI）機関にアクセスする必要があります。
- 次の図は、各ONTAP Mediator証明書の目的を示しています。

ONTAP Mediator Certificate Purposes



- 次の図は、Web サーバのセットアップと ONTAP Mediator のセットアップの構成を示しています。

ONTAP Mediator Certificates



ステップ1：CA証明書を発行するサードパーティから証明書を取得する

以下の手順に従って、PKI 機関から証明書を取得できます。

次の例は、自己署名証明書アクターを `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/` にあるサードパーティ証明書アクターに置き換える方法を示しています。



この例では、ONTAP Mediatorに必要な証明書の必要な基準を示しています。PKI認証局から証明書を取得する方法は、この手順とは異なる場合があります。ビジネスニーズに応じて手順を調整してください。

ONTAP Mediator 1.9以降

1. PKI 機関が証明書を生成するために使用する秘密キー `intermediate.key` と構成ファイル `openssl\_ca.cnf` を作成します。
 - a. 秘密鍵を生成します intermediate.key：

例

```
openssl genrsa -aes256 -out intermediate.key 4096
```
 - b. 構成ファイル openssl_ca.cnf (

```
`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`
```

にありますが) は、生成される証明書に必要なプロパティを定義します。
2. 秘密鍵と構成ファイルを使用して証明書署名要求を作成します intermediate.csr：

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. 証明書署名要求 `intermediate.csr` をPKI機関に送信して署名をもらいます。

PKI機関はリクエストを検証し、`.csr`に署名して証明書を生成します `intermediate.crt`。さらに、PKI機関から `intermediate.crt` 証明書に署名した `root\_ca.crt` 証明書を取得する必要があります。



HTTPSで構成されたONTAP Mediatorを使用するSnapMirrorアクティブ同期クラスターおよびMetroCluster IP構成の場合は、ONTAPクラスターに `intermediate.crt` および `root\_ca.crt` 証明書を追加する必要があります。["SnapMirror アクティブ同期のためにONTAP Mediator とクラスターを設定する"](#)および["MetroCluster IP構成用のONTAP Mediatorを構成します"](#)を参照してください。

ONTAP Mediator 1.8 以前

1. PKI 機関が証明書を生成するために使用する秘密キー `ca.key` と構成ファイル `openssl\_ca.cnf` を作成します。
 - a. 秘密鍵を生成します ca.key :

例：


```
openssl genrsa -aes256 -out ca.key 4096
```
 - b. 構成ファイル openssl_ca.cnf (
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_ca.cnf` にあります) は、
生成される証明書に必要なプロパティを定義します。
2. 秘密鍵と構成ファイルを使用して証明書署名要求を作成します ca.csr :

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. 証明書署名要求 `ca.csr` をPKI機関に送信して署名をもらいます。

PKI機関はリクエストを検証し、`.csr` に署名して証明書を生成します `ca.crt`。さらに、PKI機関から `ca.crt` 証明書に署名した `root\_ca.crt` 証明書を取得する必要があります。



SnapMirrorアクティブ同期クラスタの場合は、ONTAPクラスタに `ca.crt` および `root\_ca.crt` 証明書を追加する必要があります。["SnapMirror アクティブ同期のために ONTAP Mediator とクラスタを設定する"](#)を参照してください。

ステップ2：サードパーティのCA証明書で署名してサーバー証明書を生成する

ONTAP Mediator 1.9以降

サーバー証明書は、秘密鍵 `intermediate.key` とサードパーティの証明書 `intermediate.crt` によって署名されている必要があります。さらに、構成ファイル

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_server.cnf` には、OpenSSL によって発行されるサーバー証明書に必要なプロパティを指定する特定の属性が含まれています。

次のコマンドでサーバー証明書を生成できます。

手順

1. サーバー証明書署名要求（CSR）を生成するには、
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` フォルダーから次のコマンドを実行します：

```
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. CSR からサーバー証明書を生成するには、
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` フォルダーから次のコマンドを実行します：



これらのファイルはPKI認証局から取得されました。異なる証明書名を使用している場合は、`intermediate.crt` と `intermediate.key` を該当するファイル名に置き換えてください。

```
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` オプションは `intermediate.srl` ファイルを生成するために使用されます。

ONTAP Mediator 1.8 以前

サーバー証明書は、秘密鍵 `ca.key` とサードパーティの証明書 `ca.crt` によって署名されている必要があります。さらに、構成ファイル

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_server.cnf` には、OpenSSL によ

って発行されるサーバー証明書に必要なプロパティを指定する特定の属性が含まれています。

次のコマンドでサーバー証明書を生成できます。

手順

1. サーバー証明書署名要求（CSR）を生成するには、
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` フォルダから次のコマンドを実行します：

```
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. CSR からサーバー証明書を生成するには、
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` フォルダから次のコマンドを実行します：



これらのファイルはPKI認証局から取得されました。異なる証明書名を使用している場合は、`ca.crt`と`ca.key`を該当するファイル名に置き換えてください。

```
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` オプションは `ca.srl` ファイルを生成するために使用されます。

ステップ3：ONTAP Mediator構成で新しいサードパーティCA証明書とサーバ証明書を置き換える

ONTAP Mediator 1.10以降

証明書の設定は、

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml`にある設定ファイルでONTAP Mediatorに提供されます。このファイルには、以下の属性が含まれます：

```
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/intermediate.srl'
```

- `cert\_path`および`key\_path`はサーバー証明書変数です。
- `ca\_cert\_path`、`ca\_key\_path`、および`ca\_serial\_path`はCA証明書変数です。

手順

1. すべての`intermediate.\*`ファイルをサードパーティの証明書に置き換えます。
2. `intermediate.crt`および`ontap\_mediator\_server.crt`証明書から証明書チェーンを作成します：

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

3. `/opt/netapp/lib/ontap\_mediator/unicorn/config.json`ファイルを更新します。

`ssl\_keyfile`、`ssl\_certfile`、および`ssl\_ca\_certs`の値を更新します：

```
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
```

- `ssl\_keyfile`値は`ontap\_mediator\_server.crt`ファイル内のキーパスで、`ontap\_mediator\_server.key`です。
 - `ssl\_certfile`値は`ontap\_mediator\_server\_chain.crt`ファイルのパスです。
 - `ssl\_ca\_certs`値は`root\_ca.crt`ファイルのパスです。
4. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：
 - Linux グループのオーナー: netapp:netapp
 - Linux の権限: 600
 5. ONTAP Mediatorを再起動します：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 および 1.9

証明書の設定は、

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml`にある設定ファイルでONTAP Mediatorに提供されます。このファイルには、以下の属性が含まれます：

```

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` および `key\_path` はサーバー証明書変数です。
- `ca\_cert\_path`、`ca\_key\_path`、および `ca\_serial\_path` は CA 証明書変数です。

手順

1. すべての `intermediate.\*` ファイルをサードパーティの証明書に置き換えます。
2. `intermediate.crt` および `ontap\_mediator\_server.crt` 証明書から証明書チェーンを作成します：

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

3. `/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini` ファイルを更新します。

`mediator\_cert`、`mediator\_key`、および
`ca\_certificate` の値を更新します：

```

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

```

- `mediator\_cert` 値は `ontap\_mediator\_server\_chain.crt` ファイルのパスです。
- `mediator\_key value` は `ontap\_mediator\_server.crt` ファイル内のキーパスです
`ontap\_mediator\_server.key`。

◦ `ca\_certificate` 値は `root\_ca.crt` ファイルのパスです。

4. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

◦ Linux グループのオーナー: netapp:netapp

◦ Linux の権限: 600

5. ONTAP Mediatorを再起動します：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 以前

証明書の設定は、

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml`にある設定ファイルでONTAP Mediatorに提供されます。このファイルには、以下の属性が含まれます：

```
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` および `key\_path` はサーバー証明書変数です。

• `ca\_cert\_path`、`ca\_key\_path`、および `ca\_serial\_path` は CA 証明書変数です。

手順

1. すべての `ca.\*` ファイルをサードパーティの証明書に置き換えます。

2. `ca.crt` および `ontap\_mediator\_server.crt` 証明書から証明書チェーンを作成します：

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

3. `/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini` ファイルを更新します。

`mediator\_cert`、`mediator\_key`、および
`ca\_certificate` の値を更新します：

```
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
```

- `mediator\_cert`値は `ontap\_mediator\_server\_chain.crt` ファイルのパスです。
- `mediator\_key` value`は `ontap_mediator_server.crt` ファイル内のキーパスです
`ontap\_mediator\_server.key`。
- `ca\_certificate`値は `root\_ca.crt` ファイルのパスです。

4. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

- Linux グループのオーナー: netapp:netapp
- Linux の権限: 600

5. ONTAP Mediatorを再起動します：

```
systemctl restart ontap_mediator
```

ステップ4：オプションで、サードパーティの証明書に別のパスまたは名前を使用します

ONTAP Mediator 1.10以降

`intermediate.\*`以外の別の名前でサードパーティの証明書を使用したり、別の場所に保存したりすることもできます。

手順

1. `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.user\_config.yaml` ファイルを設定して、`ontap\_mediator.config.yaml` ファイル内のデフォルトの変数値を上書きします。

`intermediate.crt`をPKI機関から取得し、その秘密鍵 `intermediate.key`を
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config`の場所に
保存する場合、
`ontap\_mediator.user\_config.yaml`ファイルは次の例のようになります：



`intermediate.crt`を使用して `ontap\_mediator\_server.crt` 証明書に署名した場合、
`intermediate.srl` ファイルが生成されます。詳細については、[ステップ2：サードパーティのCA証明書で署名してサーバー証明書を生成する](#)を参照してください。

```
[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` 証明書が `ontap\_mediator\_server.crt` 証明書に署名する `intermediate.crt` 証明書を提供している場合は、`intermediate.crt` 証明書と `ontap\_mediator\_server.crt` 証明書から証明書チェーンを作成します：



手順の早い段階で、PKI 機関から `intermediate.crt` 証明書と `ontap\_mediator\_server.crt` 証明書を取得しておく必要があります。

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

- b. `/opt/netapp/lib/ontap\_mediator/unicorn/config.json` ファイルを更新します。

`ssl\_keyfile`、`ssl\_certfile`、および
`ssl\_ca\_certs` の値を更新します：

```
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
```

- `ssl\_keyfile`値は `ontap\_mediator\_server.crt` ファイル内のキープスで、`ontap\_mediator\_server.key` です。
- `ssl\_certfile`値は `ontap\_mediator\_server\_chain.crt` ファイルのパスです。
- `ssl\_ca\_certs`値は `root\_ca.crt` ファイルのパスです。



HTTPSで構成されたONTAP Mediatorを使用するSnapMirrorアクティブ同期クラスタおよびMetroCluster IP構成の場合は、ONTAPクラスタに `intermediate.crt` および `root\_ca.crt` 証明書を追加する必要があります。"[SnapMirror アクティブ同期のために ONTAP Mediator とクラスタを設定する](#)"および"[MetroCluster IP構成用のONTAP Mediatorを構成します](#)"を参照してください。

c. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

- Linux グループのオーナー: netapp:netapp
- Linux の権限: 600

2. 設定ファイルで証明書が更新されたら、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 および 1.9

`intermediate.\*` 以外の別の名前でサードパーティの証明書を使用したり、別の場所に保存したりすることもできます。

手順

1. `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.user\_config.yaml` ファイルを設定して、`ontap\_mediator.config.yaml` ファイル内のデフォルトの変数値を上書きします。

`intermediate.crt` をPKI機関から取得し、その秘密鍵 `intermediate.key` を `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config` の場所に保存する場合、`ontap\_mediator.user\_config.yaml` ファイルは次の例のようになります：



`intermediate.crt` を使用して `ontap\_mediator\_server.crt` 証明書に署名した場合、`intermediate.srl` ファイルが生成されます。詳細については、[ステップ2：サードパー](#)

```
[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`` 証明書が ``ontap_mediator_server.crt`` 証明書に署名する ``intermediate.crt`` 証明書を提
供する証明書構造を使用している場合は、``intermediate.crt`` 証明書と
``ontap_mediator_server.crt`` 証明書から証明書チェーンを作成します：



手順の早い段階で、PKI 機関から ``intermediate.crt`` 証明書と
``ontap_mediator_server.crt`` 証明書を取得しておく必要があります。

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

b. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ファイルを更新します。

``mediator_cert``、``mediator_key``、および
``ca_certificate`` の値を更新します：

```
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
```

- ``mediator_cert`` 値は ``ontap_mediator_server_chain.crt`` ファイルのパスです。
- ``mediator_key`` 値は ``ontap_mediator_server.crt`` ファイル内のキープスで、``ontap_mediator_server.key`` です。
- ``ca_certificate`` 値は ``root_ca.crt`` ファイルのパスです。



SnapMirrorビジネス継続性（SM-BC）クラスタの場合は、``intermediate.crt`` および ``root_ca.crt`` 証明書をONTAPクラスタに追加する必要があります。["SnapMirror アクティブ同期のために ONTAP Mediator とクラスタを設定する"](#)を参照してください。

c. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

- Linux グループのオーナー: `netapp:netapp`
- Linux の権限: `600`

2. 設定ファイルで証明書が更新されたら、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 以前

``ca.*`` 以外の別の名前でサードパーティの証明書を使用したり、別の場所に保存したりすることもできます。

手順

1. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` ファイルを設定して、``ontap_mediator.config.yaml`` ファイル内のデフォルトの変数値を上書きします。

``ca.crt`` をPKI機関から取得し、その秘密鍵 ``ca.key`` を
`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`` の場所に
保存する場合、

`ontap\_mediator.user\_config.yaml` ファイルは次の例のようになります：



`ca.crt` を使用して `ontap\_mediator\_server.crt` 証明書に署名した場合、`ca.srl` ファイルが生成されます。詳細については、[ステップ2：サードパーティのCA証明書で署名してサーバー証明書を生成する](#)を参照してください。

```
[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` 証明書が `ontap\_mediator\_server.crt` 証明書に署名する `ca.crt` 証明書を提供する証明書構造を使用している場合は、`ca.crt` 証明書と `ontap\_mediator\_server.crt` 証明書から証明書チェーンを作成します：



手順の早い段階で、PKI 機関から `ca.crt` 証明書と `ontap\_mediator\_server.crt` 証明書を取得しておく必要があります。

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

b. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ファイルを更新します。

``mediator_cert``、``mediator_key``、および
``ca_certificate`` の値を更新します：

```
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
```

- ``mediator_cert`` 値は ``ontap_mediator_server_chain.crt`` ファイルのパスです。
- ``mediator_key`` 値は ``ontap_mediator_server.crt`` ファイル内のキーパスで、``ontap_mediator_server.key`` です。
- ``ca_certificate`` 値は ``root_ca.crt`` ファイルのパスです。



SnapMirrorビジネス継続性（SM-BC）クラスタの場合は、``ca.crt`` および ``root_ca.crt`` 証明書をONTAPクラスタに追加する必要があります。["SnapMirror アクティブ同期のために ONTAP Mediator とクラスタを設定する"](#)を参照してください。

c. 新しく生成された証明書の次の属性が正しく設定されていることを確認します：

- Linux グループのオーナー: `netapp:netapp`
- Linux の権限: `600`

2. 設定ファイルで証明書が更新されたら、ONTAP Mediator を再起動します。

```
systemctl restart ontap_mediator
```

ONTAP Mediatorの証明書関連の問題のトラブルシューティング

証明書の問題をトラブルシューティングする際には、これらのチェック項目を使用して証明書のプロパティを確認してください。

証明書の有効期限を確認する

証明書の有効範囲を識別するには、次のコマンドを使用します。

ONTAP Mediator 1.9以降

```
[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 以前

```
[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 証明書における X509v3 拡張の検証

次のコマンドを使用して、CA 証明書の X509v3 拡張機能を検証します。

ONTAP Mediator 1.9以降

`openssl\_ca.cnf`内の `\*v3\_ca\*`で定義されたプロパティは、
`intermediate.crt`では `X509v3 extensions`として表示されます。

```
[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 以前

`openssl\_ca.cnf`内の`\*v3\_ca\*`で定義されたプロパティは、`ca.crt`では`X509v3 extensions`として表示されます。

```
[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
```

サーバー証明書とサブジェクトの代替名における **X509v3** 拡張機能を検証する

`openssl\_server.cnf`構成ファイルで定義された `v3\_req` プロパティは、証明書内で `X509v3 extensions` として表示されます。

次の例では、ONTAP Mediator がインストールされている Linux VM で `hostname -A` および `hostname -I` コマンドを実行することで、`alt\_names` セクション内の変数を取得できます。

変数の正しい値については、ネットワーク管理者に確認してください。

ONTAP Mediator 1.9以降

```
[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 以前

```
[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
```

秘密鍵が証明書と一致していることを確認する

特定の秘密鍵が証明書と一致するかどうかを確認できます。

キーと証明書に対してそれぞれ次の OpenSSL コマンドを使用します。

ONTAP Mediator 1.9以降

```
[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 以前

```
[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
```

両方の `-modulus` 属性が一致する場合、秘密鍵と証明書のペアに互換性があり、相互に動作できることを示します。

サーバー証明書が特定のCA証明書から作成されたことを確認する

次のコマンドを使用して、サーバー証明書が特定のCA証明書から作成されていることを確認できます。

ONTAP Mediator 1.9以降

```
[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 以前

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

```
ontap_mediator_server.crt: OK
```

オンライン証明書ステータス プロトコル（OCSP）検証を使用している場合は、コマンド"[openssl-verify](#)"を使用します。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。