



管理证书

ONTAP Mediator

NetApp
October 19, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/ontap-mediator/administer/regenerate-self-signed-certificate-task.html> on October 19, 2026. Always check docs.netapp.com for the latest.

目录

- 管理证书 1
 - 重新生成 ONTAP Mediator 主机的临时自签名证书 1
 - 将 ONTAP Mediator 自签名证书替换为受信任的第三方证书 2
 - 步骤 1：从颁发 CA 证书的第三方获取证书 3
 - 步骤 2：通过使用第三方 CA 证书签名来生成服务器证书 5
 - 步骤 3：在 ONTAP Mediator 配置中替换新的第三方 CA 证书和服务器证书 6
 - 步骤 4：（可选）为第三方证书使用其他路径或名称 10
 - 对 ONTAP Mediator 证书相关问题进行故障诊断 16
 - 验证证书过期时间 16
 - 验证 CA 认证中的 X509v3 扩展 16
 - 验证服务器证书和主题替代名称中的 X509v3 扩展 18
 - 验证私钥是否与证书匹配 20
 - 确认从特定 CA 证书创建了服务器证书 20

管理证书

重新生成 ONTAP Mediator 主机的临时自签名证书

当主机名或 IP 地址更改使现有证书无效时，为当前主机重新生成临时自签名证书。



此过程仅在运行 ONTAP Mediator 1.7 或更高版本的系统上受支持。

关于此任务

- 在已安装 ONTAP Mediator 的 Linux 主机上执行此任务。
- 只有在安装 ONTAP Mediator 后，由于主机的主机名或 IP 地址发生更改而导致生成的自签名证书过时，您才能执行此任务。
- 临时自签名证书被受信任的第三方证书替换后，请不要使用此任务重新生成证书。缺少自签名证书将导致此过程失败。

步骤

要为当前主机重新生成新的临时自签名证书，请执行以下步骤：

1. 重新启动 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
```

将 ONTAP Mediator 自签名证书替换为受信任的第三方证书

如果环境支持，请将自签名证书替换为由证书颁发机构颁发的可信证书。

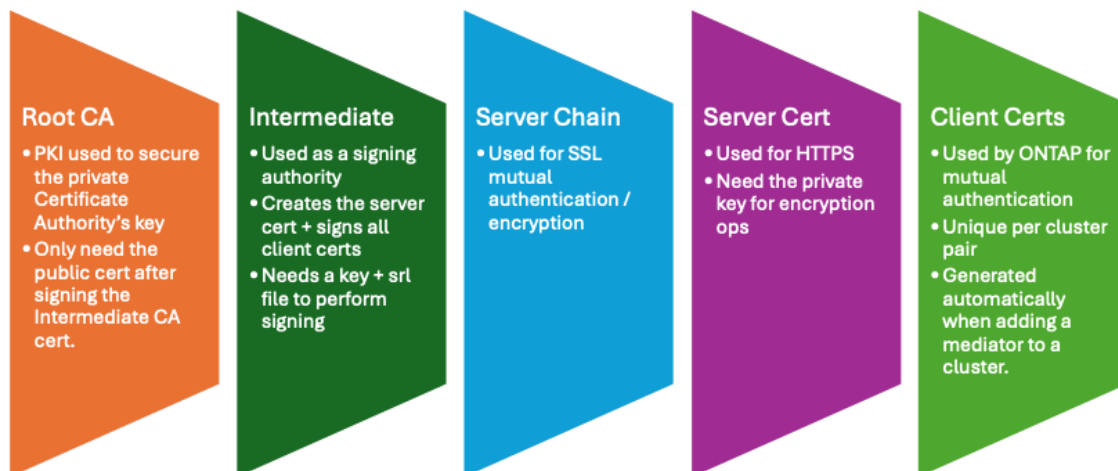


- 仅从 ONTAP 9.16.1 开始以及在某些较早的 ONTAP 补丁版本中支持第三方证书。请参阅["NetApp Bugs Online Bug ID CONTAP-243278"](#)。
- 仅在运行 ONTAP Mediator 1.7 或更高版本的系统上支持第三方证书。

关于此任务

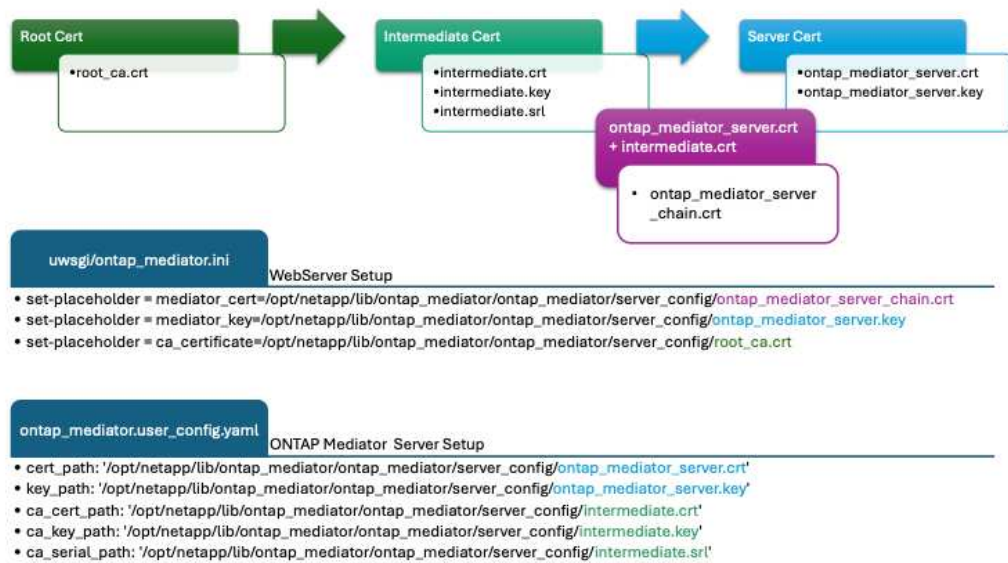
- 在已安装 ONTAP Mediator 的 Linux 主机上执行此任务。
- 如果需要将生成的自签名证书替换为从受信任的从属证书颁发机构（CA）获得的证书，则可以执行此任务。为了实现这一点，您应该有权访问受信任的公钥基础设施（PKI）机构。
- 下图显示了每个 ONTAP Mediator 证书的用途。

ONTAP Mediator Certificate Purposes



- 下图显示了 Web 服务器设置和 ONTAP Mediator 设置的配置。

ONTAP Mediator Certificates



步骤 1：从颁发 CA 证书的第三方获取证书

您可以通过以下步骤从 PKI 机构获取证书。

以下示例演示了将自签名证书参与者替换为位于
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/' 的第三方证书参与者。



本示例说明了 ONTAP Mediator 所需证书的必要标准。您可以通过与此过程不同的方式从 PKI 机构获取证书。请根据您的业务需求调整此过程。

ONTAP Mediator 1.9 及更高版本

1. 创建一个私钥 `intermediate.key` 和一个配置文件 `openssl_ca.cnf`，供 PKI 机构用于生成证书。
 - a. 生成私钥 `intermediate.key`:

示例

```
openssl genrsa -aes256 -out intermediate.key 4096
```
 - b. 配置文件 `openssl_ca.cnf` (位于
`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) 定义了生成的证书必须具有的属性。
2. 使用私钥和配置文件创建证书签名请求 `intermediate.csr`:

示例:

```
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. 将证书签名请求 `intermediate.csr` 发送给 PKI 机构进行签名。

PKI 机构验证请求并对 `.csr` 进行签名，从而生成证书 `intermediate.crt`。此外，您还需要从 PKI 机构获取对 `intermediate.crt` 证书进行签名的 `root\_ca.crt` 证书。



对于使用配置了 HTTPS 的 ONTAP Mediator 的 SnapMirror 活动同步集群和 MetroCluster IP 配置，您必须将 `intermediate.crt` 和 `root\_ca.crt` 证书添加到 ONTAP 集群。请参阅[“为 SnapMirror 活动同步配置 ONTAP 调解器和集群”](#)和[“为 MetroCluster IP 配置配置 ONTAP Mediator”](#)。

ONTAP Mediator 1.8 及更早版本

1. 创建私钥 `ca.key` 和配置文件 `openssl\_ca.cnf`，供 PKI 机构用来生成证书。

- a. 生成私钥 `ca.key`:

示例:

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

- b. 配置文件 `openssl\_ca.cnf` (位于
`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_ca.cnf`) 定义了生成的证书必须具有的属性。

2. 使用私钥和配置文件创建证书签名请求 `ca.csr`:

示例:

```
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. 将证书签名请求 `ca.csr` 发送给 PKI 机构进行签名。

PKI 机构验证请求并对 `.csr` 进行签名，从而生成证书 `ca.crt`。此外，您还需要从 PKI 机构获取

对 `ca.crt` 证书进行签名的 `root\_ca.crt` 证书。



对于 SnapMirror 活动同步集群，必须将 `ca.crt` 和 `root\_ca.crt` 证书添加到 ONTAP 集群。请参阅[“为 SnapMirror 活动同步配置 ONTAP 调解器和集群”](#)。

步骤 2：通过使用第三方 CA 证书签名来生成服务器证书

ONTAP Mediator 1.9 及更高版本

服务器证书必须由私钥 `intermediate.key` 和第三方证书 `intermediate.crt` 签名。此外，配置文件 `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_server.cnf` 包含某些属性，这些属性指定由 OpenSSL 颁发的服务器证书所需的属性。

以下命令可以生成服务器证书。

步骤

1. 要生成服务器证书签名请求（CSR），请从

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config 文件夹中运行以下命令：

```
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. 要从 CSR 生成服务器证书，请从

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config 文件夹中运行以下命令：



这些文件是从 PKI 机构获得的。如果使用不同的证书名称，请将 `intermediate.crt` 和 `intermediate.key` 替换为相关文件名。

```
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
```

- 该 `-CAcreateserial` 选项用于生成 `intermediate.srl` 文件。

ONTAP Mediator 1.8 及更早版本

服务器证书必须由私钥 `ca.key` 和第三方证书 `ca.crt` 签名。此外，配置文件 `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/openssl\_server.cnf` 包含某些属性，这些属性指定由 OpenSSL 颁发的服务器证书所需的属性。

以下命令可以生成服务器证书。

步骤

1. 要生成服务器证书签名请求（CSR），请从

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config 文件夹中运行以下命令：

```
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. 要从 CSR 生成服务器证书，请从

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config 文件夹中运行以下命令：



这些文件是从 PKI 机构获得的。如果使用不同的证书名称，请将 `ca.crt` 和 `ca.key` 替换为相关文件名。

```
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
```

- 该 `-CAcreateserial` 选项用于生成 `ca.srl` 文件。

步骤 3：在 ONTAP Mediator 配置中替换新的第三方 CA 证书和服务器证书

ONTAP Mediator 1.10 及更高版本

证书配置在位于

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml` 的配置文件中提供给 ONTAP Mediator。该文件包含以下属性：

```
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 是服务器证书变量。
- ca_cert_path、`ca\_key\_path` 和 `ca\_serial\_path` 是 CA 证书变量。

步骤

1. 将所有 intermediate.* 文件替换为第三方证书。

2. 从 `intermediate.crt` 和 `ontap\_mediator\_server.crt` 证书创建证书链:

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

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

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
```

- `ssl\_keyfile` 值是 `ontap\_mediator\_server.crt` 文件中的键路径, 即 `ontap\_mediator\_server.key`。
- `ssl\_certfile` 值是 `ontap\_mediator\_server\_chain.crt` 文件的路径。
- `ssl\_ca\_certs` 值是 `root\_ca.crt` 文件的路径。

4. 验证新生成的证书的以下属性设置是否正确:

- Linux 组所有者: `netapp:netapp`
- Linux 权限: `600`

5. 重新启动 ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP 调解器 1.9.1 和 1.9

证书配置在位于

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml` 的配置文件中提供给 ONTAP Mediator。该文件包含以下属性:

```
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 是服务器证书变量。
- ca_cert_path、`ca\_key\_path`和`ca\_serial\_path`是 CA 证书变量。

步骤

1. 将所有 intermediate.* 文件替换为第三方证书。
2. 从`intermediate.crt`和`ontap\_mediator\_server.crt`证书创建证书链：

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

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

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
```

- mediator_cert 值是 ontap_mediator_server_chain.crt 文件的路径。
- mediator_key value 是 ontap_mediator_server.crt 文件中的密钥路径，即`ontap\_mediator\_server.key`。
- ca_certificate 值是`root\_ca.crt`文件的路径。

4. 验证新生成的证书的以下属性设置是否正确：

- Linux 组所有者：netapp:netapp
- Linux 权限：600

5. 重新启动 ONTAP Mediator：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 及更早版本

证书配置在位于

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml`的配置文件中提供给 ONTAP Mediator。该文件包含以下属性：

```
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 是服务器证书变量。
- ca_cert_path、`ca\_key\_path`和`ca\_serial\_path`是 CA 证书变量。

步骤

1. 将所有 ca.* 文件替换为第三方证书。
2. 从`ca.crt`和`ontap\_mediator\_server.crt`证书创建证书链：

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

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

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
```

- mediator_cert 值是 ontap_mediator_server_chain.crt 文件的路径。
 - mediator_key value 是 ontap_mediator_server.crt`文件中的密钥路径，即`ontap_mediator_server.key`。
 - ca_certificate 值是`root\_ca.crt`文件的路径。
4. 验证新生成的证书的以下属性设置是否正确：
 - Linux 组所有者： netapp:netapp
 - Linux 权限： 600

5. 重新启动 ONTAP Mediator:

```
systemctl restart ontap_mediator
```

步骤 4: (可选) 为第三方证书使用其他路径或名称

ONTAP Mediator 1.10 及更高版本

您可以使用名称不同于 `intermediate.\*` 的第三方证书, 或者将第三方证书存储在其他位置。

步骤

1. 配置

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml 文件以覆盖 ontap_mediator.config.yaml 文件中的默认变量值。

如果您从 PKI 机构获取了 intermediate.crt, 并将其私钥 intermediate.key 存储在位置 `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config`, 则 `ontap\_mediator.user\_config.yaml` 文件应如下所示:



如果您使用 `intermediate.crt` 签署了 `ontap\_mediator\_server.crt` 证书, 则会生成 `intermediate.srl` 文件。有关详细信息, 请参见 [步骤 2: 通过使用第三方 CA 证书签名来生成服务器证书](#)。

```
[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. 如果您使用的证书结构中，`root_ca.crt` 证书提供了一个 `intermediate.crt` 证书来签署 `ontap_mediator_server.crt` 证书，请从 `intermediate.crt` 和 `ontap_mediator_server.crt` 证书创建证书链：



您应该在此过程的早期从 PKI 机构获取了 `'intermediate.crt'` 和 `'ontap_mediator_server.crt'` 证书。

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

- b. 更新 `'/opt/netapp/lib/ontap_mediator/unicorn/config.json'` 文件。

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
```

- `ssl_keyfile` 值是 `ontap_mediator_server.crt` 文件中的键路径，即 `ontap_mediator_server.key`。
- `ssl_certfile` 值是 `ontap_mediator_server_chain.crt` 文件的路径。
- `ssl_ca_certs` 值是 `root_ca.crt` 文件的路径。



对于使用配置了 HTTPS 的 ONTAP Mediator 的 SnapMirror 活动同步集群和 MetroCluster IP 配置，您必须将 `'intermediate.crt'` 和 `'root_ca.crt'` 证书添加到 ONTAP 集群。请参阅["为 SnapMirror 活动同步配置 ONTAP 调解器和集群"](#)和["为 MetroCluster IP 配置配置 ONTAP Mediator"](#)。

- c. 验证新生成的证书的以下属性设置是否正确：

- Linux 组所有者: netapp:netapp
- Linux 权限: 600

2. 在配置文件中更新证书时重新启动 ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP 调解器 1.9.1 和 1.9

您可以使用名称不同于 `intermediate.\*` 的第三方证书, 或者将第三方证书存储在其他位置。

步骤

1. 配置

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml 文件以覆盖 ontap_mediator.config.yaml 文件中的默认变量值。

如果您从 PKI 机构获取了 intermediate.crt, 并将其私钥 intermediate.key 存储在位置 `/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config`, 则 `ontap\_mediator.user\_config.yaml` 文件应如下所示:



如果您使用 `intermediate.crt` 签署了 `ontap\_mediator\_server.crt` 证书, 则会生成 `intermediate.srl` 文件。有关详细信息, 请参见 [步骤 2: 通过使用第三方 CA 证书签名来生成服务器证书](#)。

```
[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. 如果您使用的证书结构中，`root_ca.crt` 证书提供了一个 `intermediate.crt` 证书来签署 `ontap_mediator_server.crt` 证书，请从 `intermediate.crt` 和 `ontap_mediator_server.crt` 证书创建证书链：



您应该在此过程的早期从 PKI 机构获取了 `'intermediate.crt'` 和 `'ontap_mediator_server.crt'` 证书。

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

- b. 更新 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` 文件。

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
```

- `mediator_cert` 值是 `ontap_mediator_server_chain.crt` 文件的路径。
- `mediator_key` 值是 `ontap_mediator_server.crt` 文件中的键路径，即 `'ontap_mediator_server.key'`。
- `ca_certificate` 值是 `'root_ca.crt'` 文件的路径。



对于 SnapMirror 业务连续性 (SM-BC) 集群，必须将 `intermediate.crt` 和 `root_ca.crt` 证书添加到 ONTAP 集群。请参阅 ["为 SnapMirror 活动同步配置 ONTAP 调解器和集群"](#)。

- c. 验证新生成的证书的以下属性设置是否正确：

- Linux 组所有者： `netapp:netapp`
- Linux 权限： `600`

2. 在配置文件中更新证书时重新启动 ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 及更早版本

您可以使用名称不同于 `ca.\*` 的第三方证书，也可以将第三方证书存储在其他位置。

步骤

1. 配置

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml 文件以覆盖 ontap_mediator.config.yaml 文件中的默认变量值。

如果您从 PKI 机构获取了 ca.crt，并将其私钥 ca.key 存储在位置

`/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config`，则 `ontap\_mediator.user\_config.yaml` 文件应如下例所示：



如果您使用 `ca.crt` 对 `ontap\_mediator\_server.crt` 证书进行了签名，则会生成 `ca.srl` 文件。有关详细信息，请参见 [步骤 2: 通过使用第三方 CA 证书签名来生成服务器证书](#)。

```
[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. 如果您使用的证书结构中，`root_ca.crt` 证书提供了一个 `ca.crt` 证书来签署 `ontap_mediator_server.crt` 证书，请从 `ca.crt` 和 `ontap_mediator_server.crt` 证书创建证书链：



您应该在此过程的早期从 PKI 机构获得了 `'ca.crt'` 和 `'ontap_mediator_server.crt'` 证书。

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

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

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
```

- `mediator_cert` 值是 `ontap_mediator_server_chain.crt` 文件的路径。
- `mediator_key` 值是 `ontap_mediator_server.crt` 文件中的键路径，即 `'ontap_mediator_server.key'`。
- `ca_certificate` 值是 `'root_ca.crt'` 文件的路径。



对于 SnapMirror 业务连续性 (SM-BC) 集群，必须将 `'ca.crt'` 和 `'root_ca.crt'` 证书添加到 ONTAP 集群。请参阅["为 SnapMirror 活动同步配置 ONTAP 调解器和集群"](#)。

- c. 验证新生成的证书的以下属性设置是否正确：

- Linux 组所有者： `netapp:netapp`
- Linux 权限： `600`

2. 在配置文件中更新证书时重新启动 ONTAP Mediator：

```
systemctl restart ontap_mediator
```

对 ONTAP Mediator 证书相关问题进行故障诊断

在对证书问题进行故障排除时，使用这些检查来验证证书属性。

验证证书过期时间

使用以下命令来标识证书有效期范围。

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
```

验证 CA 认证中的 X509v3 扩展

使用以下命令验证 CA 认证中的 X509v3 扩展。

ONTAP Mediator 1.9 及更高版本

在 `openssl_ca.cnf` 中的 `v3_ca` 内定义的属性将在 `intermediate.crt` 中显示为 `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` 内定义的属性在 `ca.crt` 中显示为 `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
```

验证服务器证书和主题替代名称中的 **X509v3** 扩展

`openssl\_server.cnf` 配置文件中定义的 `v3\_req` 属性在证书中显示为 `X509v3 extensions`。

在以下示例中，您可以通过在安装了 ONTAP Mediator 的 Linux VM 上运行命令 `hostname -A` 和 `hostname -I` 来获取 `alt\_names` 部分中的变量。

请与网络管理员联系以获取变量的正确值。

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
```

验证私钥是否与证书匹配

您可以验证特定私钥是否与证书匹配。

分别在密钥和证书上使用以下 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
```

如果两者的 `-modulus` 属性匹配，则表明私钥和证书对是兼容的，并且可以协同工作。

确认从特定 CA 证书创建了服务器证书

您可以使用以下命令验证服务器证书是否是从特定 CA 证书创建的。

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
```

如果正在使用在线证书状态协议（OCSP）验证，请使用命令 ["openssl-verify"](#)。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。