



Gerenciar certificados

ONTAP Mediator

NetApp
October 19, 2026

Índice

Gerenciar certificados	1
Regenere um certificado autoassinado temporário para o host do ONTAP Mediator	1
Substitua os certificados autoassinados do ONTAP Mediator por certificados confiáveis de terceiros	2
Passo 1: obtenha um certificado de um terceiro que emita um certificado de CA	3
Etapa 2: gere um certificado de servidor assinando-o com uma autoridade certificadora (CA) de terceiro	5
Etapa 3: substitua o novo certificado da CA de terceiros e o certificado do servidor na configuração do ONTAP Mediator	6
Passo 4: opcionalmente, use um caminho ou nome diferente para seus certificados de terceiros	10
Solução de problemas relacionados a certificados do ONTAP Mediator	16
Verificar a expiração do certificado	16
Verifique as extensões X509v3 na certificação da Autoridade de Certificação	17
Verificar extensões X509v3 no certificado do servidor e nomes alternativos do assunto	18
Verifique se a chave privada corresponde a um certificado	20
Verifique se um certificado de servidor foi criado a partir de um certificado de CA específico	21

Gerenciar certificados

Regenere um certificado autoassinado temporário para o host do ONTAP Mediator

Regenere um certificado temporário autoassinado para o host atual quando uma alteração no nome do host ou no endereço IP invalidar o certificado existente.



Este procedimento só é compatível com sistemas que executam o ONTAP Mediator 1.7 ou posterior.

Sobre esta tarefa

- Execute esta tarefa no host Linux onde você instalou o ONTAP Mediator.
- Você só pode executar esta tarefa se os certificados autoassinados gerados tiverem se tornado obsoletos devido a alterações no nome do host ou no endereço IP do host após a instalação do ONTAP Mediator.
- Após o certificado autoassinado temporário ser substituído por um certificado confiável de terceiro, você *não* deve usar esta tarefa para regenerar um certificado. A ausência de um certificado autoassinado fará com que este procedimento falhe.

Etapas

Para gerar um novo certificado autoassinado temporário para o host atual, execute a seguinte etapa:

1. Reinicie o 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
```

Substitua os certificados autoassinados do ONTAP Mediator por certificados confiáveis de terceiros

Se o seu ambiente suportar, substitua os certificados autoassinados por certificados confiáveis emitidos por uma autoridade certificadora.

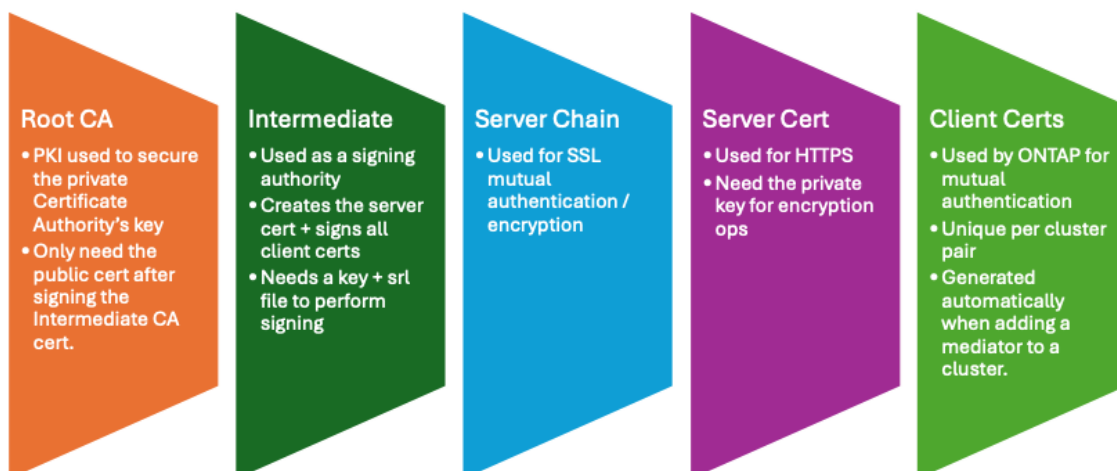


- Os certificados de terceiros são suportados apenas a partir do ONTAP 9.16.1 e em algumas versões de patch anteriores do ONTAP. Consulte "[NetApp ID do bug no Bugs Online CONTAP-243278](#)".
- Os certificados de terceiros são suportados apenas em sistemas que executam o ONTAP Mediator 1.7 ou posterior.

Sobre esta tarefa

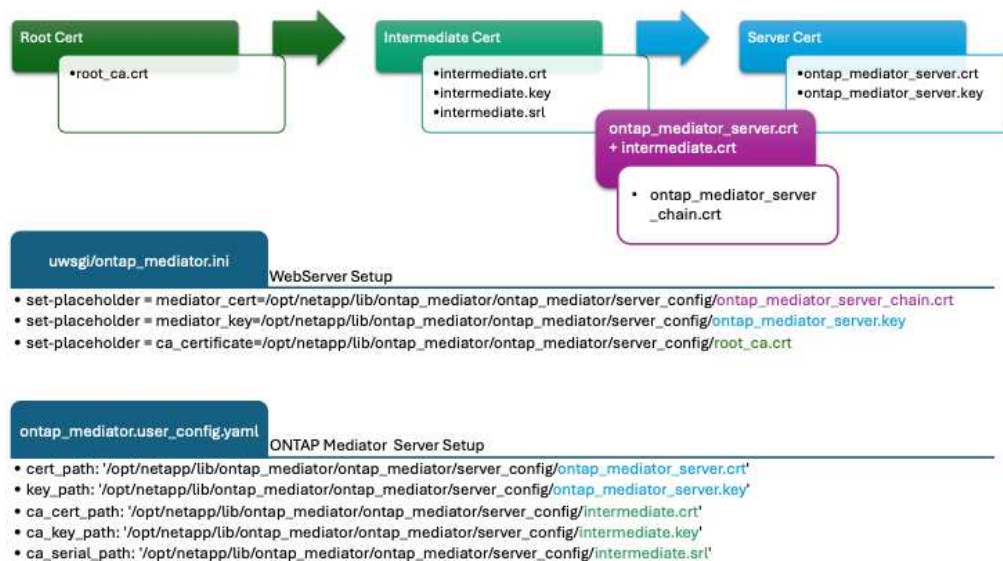
- Execute esta tarefa no host Linux onde você instalou o ONTAP Mediator.
- Você pode realizar essa tarefa se os certificados autoassinados gerados precisarem ser substituídos por certificados obtidos de uma autoridade de certificação (AC) subordinada confiável. Para isso, você deve ter acesso a uma autoridade de infraestrutura de chave pública (PKI) confiável.
- A imagem a seguir mostra as finalidades de cada certificado do ONTAP Mediator.

ONTAP Mediator Certificate Purposes



- A imagem a seguir mostra a configuração da instalação do servidor web e do ONTAP Mediator.

ONTAP Mediator Certificates



Passo 1: obtenha um certificado de um terceiro que emita um certificado de CA

Você pode obter um certificado de uma autoridade PKI seguindo o procedimento abaixo.

O exemplo a seguir demonstra a substituição das entidades de certificado autoassinado pelas entidades de certificado de terceiro localizadas em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`.



O exemplo ilustra os critérios necessários para os certificados exigidos para o ONTAP Mediator. Você pode obter os certificados de uma autoridade de Infraestrutura de Chaves Públicas (PKI) de uma forma que pode ser diferente deste procedimento. Ajuste o procedimento de acordo com as necessidades do seu negócio.

O ONTAP Mediator 1.9 e versões posteriores

1. Crie uma chave privada `intermediate.key` e um arquivo de configuração `openssl_ca.cnf` que serão utilizados pela autoridade PKI para gerar um certificado.
 - a. Gere a chave privada `intermediate.key`:

Exemplo

```
openssl genrsa -aes256 -out intermediate.key 4096
```
 - b. O arquivo de configuração `openssl_ca.cnf` (localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) define as propriedades que o certificado gerado deve ter.
2. Utilize a chave privada e o arquivo de configuração para criar uma solicitação de assinatura de certificado `intermediate.csr`:

Exemplo:

```
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. Envie a solicitação de assinatura do certificado `intermediate.csr` a uma autoridade de PKI para que ela o assine.

A autoridade de PKI verifica a solicitação e assina o `.csr`, gerando o certificado `intermediate.crt`. Além disso, você precisa obter o `root_ca.crt` certificado que assinou o `intermediate.crt` certificado da autoridade de PKI.



Para clusters do SnapMirror active sync e configurações IP do MetroCluster que usam o ONTAP Mediator configurado com HTTPS, você deve adicionar os certificados `intermediate.crt` e `root_ca.crt` a um cluster do ONTAP. Consulte ["Configure o ONTAP Mediator e os clusters para a sincronização ativa do SnapMirror"](#) e ["Configure o ONTAP Mediator para uma configuração IP do MetroCluster"](#).

O ONTAP Mediator 1.8 e versões anteriores

1. Crie uma chave privada `ca.key` e um arquivo de configuração `openssl_ca.cnf` que serão usados pela autoridade PKI para gerar um certificado.

- a. Gere a chave privada `ca.key`:

Exemplo:

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

- b. O arquivo de configuração `openssl_ca.cnf` (localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) define as propriedades que o certificado gerado deve ter.

2. Use a chave privada e o arquivo de configuração para criar uma solicitação de assinatura de certificado `ca.csr`:

Exemplo:

```
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. Envie a solicitação de assinatura do certificado `ca.csr` a uma autoridade de Infraestrutura de Chaves Públicas (PKI) para que ela o assine.

A autoridade de PKI verifica a solicitação e assina o `.csr`, gerando o certificado `ca.crt`. Além disso, você precisa obter o certificado `root_ca.crt` que assinou o certificado `ca.crt` da autoridade de PKI.



Para clusters do SnapMirror active sync, você deve adicionar os certificados `ca.crt` e `root_ca.crt` a um cluster do ONTAP. Consulte ["Configure o ONTAP Mediator e os clusters para a sincronização ativa do SnapMirror"](#).

Etapa 2: gere um certificado de servidor assinando-o com uma autoridade certificadora (CA) de terceiro

O ONTAP Mediator 1.9 e versões posteriores

Um certificado de servidor deve ser assinado pela chave privada `intermediate.key` e pelo certificado de terceiro `intermediate.crt`. Além disso, o arquivo de configuração `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contém certos atributos que especificam as propriedades necessárias para os certificados de servidor emitidos pelo OpenSSL.

Os comandos a seguir podem gerar um certificado de servidor.

Passos

1. Para gerar uma solicitação de assinatura de certificado do servidor (CSR), execute o seguinte comando a partir da `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` pasta:

```
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. Para gerar um certificado de servidor a partir do CSR, execute o seguinte comando na pasta `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`:



Esses arquivos foram obtidos de uma autoridade de PKI. Se você estiver usando um nome de certificado diferente, substitua `intermediate.crt` por `<certificate_name>` e `intermediate.key` por `<filename>` pelos nomes de arquivo relevantes.

```
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
```

- A `-CAcreateserial` opção é usada para gerar os `intermediate.srl` arquivos.

O ONTAP Mediator 1.8 e versões anteriores

Um certificado de servidor deve ser assinado pela chave privada `ca.key` e pelo certificado de terceiro `ca.crt`. Além disso, o arquivo de configuração `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contém certos atributos que especificam as propriedades necessárias para os certificados de servidor emitidos pelo OpenSSL.

Os comandos a seguir podem gerar um certificado de servidor.

Passos

1. Para gerar uma solicitação de assinatura de certificado do servidor (CSR), execute o seguinte comando a partir da `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` pasta:

```
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. Para gerar um certificado de servidor a partir do CSR, execute o seguinte comando na `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` pasta:



Esses arquivos foram obtidos de uma autoridade PKI. Se você estiver usando um nome de certificado diferente, substitua `ca.crt`<certificate_name> e `ca.key`<filename> pelos nomes de arquivo relevantes.

```
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
```

- A `-CAcreateserial` opção é usada para gerar os `ca.srl` arquivos.

Etapa 3: substitua o novo certificado da CA de terceiros e o certificado do servidor na configuração do ONTAP Mediator

O ONTAP Mediator 1.10 e versões posteriores

A configuração do certificado é fornecida ao ONTAP Mediator no arquivo de configuração localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. O arquivo inclui os seguintes atributos:

```
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/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'
```

- `cert_path` e `key_path` são variáveis de certificado do servidor.
- `ca_cert_path`, `ca_key_path` e `ca_serial_path` são variáveis de certificado CA.

Passos

1. Substitua todos `intermediate.*` os arquivos pelos certificados de terceiros.
2. Crie uma cadeia a partir dos `intermediate.crt` e `ontap_mediator_server.crt` certificados:

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

3. Atualize o `/opt/netapp/lib/ontap_mediator/unicorn/config.json` arquivo.

Atualize os valores de `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
```

- O `ssl_keyfile` valor é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
 - O `ssl_certfile` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
 - O `ssl_ca_certs` valor é o caminho do `root_ca.crt` arquivo.
4. Verifique se os seguintes atributos dos certificados recém-gerados estão configurados corretamente:
 - Proprietário do grupo Linux: `netapp:netapp`
 - Permissões do Linux: `600`
 5. Reinicie o ONTAP Mediator:

```
systemctl restart ontap_mediator
```

O ONTAP Mediator 1.9.1 e 1.9

A configuração do certificado é fornecida ao ONTAP Mediator no arquivo de configuração localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. O arquivo inclui os seguintes atributos:

```
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/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'
```

- `cert_path` e `key_path` são variáveis de certificado do servidor.
- `ca_cert_path`, `ca_key_path` e `ca_serial_path` são variáveis de certificado CA.

Passos

1. Substitua todos `intermediate.*` os arquivos pelos certificados de terceiros.
2. Crie uma cadeia a partir dos `intermediate.crt` e `ontap_mediator_server.crt` certificados:

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

3. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` arquivo.

Atualize os valores de `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
```

- O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.

- O `mediator_key` value é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
- O `ca_certificate` valor é o caminho do `root_ca.crt` arquivo.

4. Verifique se os seguintes atributos dos certificados recém-gerados estão configurados corretamente:

- Proprietário do grupo Linux: `netapp:netapp`
- Permissões do Linux: `600`

5. Reinicie o ONTAP Mediator:

```
systemctl restart ontap_mediator
```

O ONTAP Mediator 1.8 e versões anteriores

A configuração do certificado é fornecida ao ONTAP Mediator no arquivo de configuração localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. O arquivo inclui os seguintes atributos:

```
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` são variáveis de certificado do servidor.
- `ca_cert_path`, `ca_key_path` e `ca_serial_path` são variáveis de certificado CA.

Passos

1. Substitua todos `ca.*` os arquivos pelos certificados de terceiros.
2. Crie uma cadeia de certificados a partir dos `ca.crt` e `ontap_mediator_server.crt` certificados:

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

3. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` arquivo.

Atualize os valores de `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
```

- O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
 - O `mediator_key value` é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
 - O `ca_certificate` valor é o caminho do `root_ca.crt` arquivo.
4. Verifique se os seguintes atributos dos certificados recém-gerados estão configurados corretamente:
 - Proprietário do grupo Linux: `netapp:netapp`
 - Permissões do Linux: `600`

5. Reinicie o ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Passo 4: opcionalmente, use um caminho ou nome diferente para seus certificados de terceiros

O ONTAP Mediator 1.10 e versões posteriores

Você pode usar certificados de terceiros com um nome diferente de `intermediate.*` ou armazenar os certificados de terceiros em um local diferente.

Passos

1. Configure o

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` arquivo para substituir os valores padrão das variáveis no `ontap_mediator.config.yaml` arquivo.

Se você obteve `intermediate.crt` de uma autoridade PKI e armazena sua chave privada `intermediate.key` no local

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, o arquivo `ontap_mediator.user_config.yaml` deve ser semelhante ao exemplo a seguir:



Se você usou `intermediate.crt` para assinar o `ontap_mediator_server.crt` certificado, o arquivo `intermediate.srl` é gerado. Veja [Etapa 2: gere um certificado de servidor assinando-o com uma autoridade certificadora \(CA\) de terceiro](#) para obter mais informações.

```
[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 você estiver usando uma estrutura de certificado em que o `root_ca.crt` certificado fornece um `intermediate.crt` certificado que assina o `ontap_mediator_server.crt` certificado, crie uma cadeia de certificados a partir dos `intermediate.crt` e `ontap_mediator_server.crt` certificados:



Você deveria ter obtido anteriormente no procedimento os certificados `intermediate.crt` e `ontap_mediator_server.crt` de uma autoridade PKI.

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

- b. Atualize o `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` arquivo.

Atualize os valores de `ssl_keyfile`, `ssl_certfile`, e `ssl_ca_certs`:

```

ssl_keyfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi

```

```
or_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
```

- O `ssl_keyfile` valor é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
- O `ssl_certfile` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
- O `ssl_ca_certs` valor é o caminho do `root_ca.crt` arquivo.



Para clusters do SnapMirror active sync e configurações IP do MetroCluster que usam o ONTAP Mediator configurado com HTTPS, você deve adicionar os certificados `intermediate.crt` e `root_ca.crt` a um cluster do ONTAP. Consulte ["Configure o ONTAP Mediator e os clusters para a sincronização ativa do SnapMirror"](#) e ["Configure o ONTAP Mediator para uma configuração IP do MetroCluster"](#).

c. Verifique se os seguintes atributos dos certificados recém-gerados estão configurados corretamente:

- Proprietário do grupo Linux: `netapp:netapp`
- Permissões do Linux: `600`

2. Reinicie o ONTAP Mediator quando os certificados forem atualizados no arquivo de configuração:

```
systemctl restart ontap_mediator
```

O ONTAP Mediator 1.9.1 e 1.9

Você pode usar certificados de terceiros com um nome diferente de `intermediate.*` ou armazenar os certificados de terceiros em um local diferente.

Passos

1. Configure o

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml
```

 arquivo para substituir os valores padrão das variáveis no `ontap_mediator.config.yaml` arquivo.

Se você obteve `intermediate.crt` de uma autoridade PKI e armazena sua chave privada `intermediate.key` no local

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config,
```

 o arquivo `ontap_mediator.user_config.yaml` deve ser semelhante ao exemplo a seguir:

Se você usou `intermediate.crt` para assinar o `ontap_mediator_server.crt` certificado, o arquivo `intermediate.srl` é gerado. Veja [Etapa 2: gere um certificado de servidor assinando-o com uma autoridade certificadora \(CA\) de terceiro](#) para obter mais informações.

```
[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 você estiver usando uma estrutura de certificado em que o `root_ca.crt` certificado fornece um `intermediate.crt` certificado que assina o `ontap_mediator_server.crt` certificado, crie uma cadeia de certificados a partir dos `intermediate.crt` e `ontap_mediator_server.crt` certificados:



Você deveria ter obtido anteriormente no procedimento os certificados `intermediate.crt` e `ontap_mediator_server.crt` de uma autoridade PKI.

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

- b. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` arquivo.

Atualize os valores de `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
```

- O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
- O `mediator_key` valor é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
- O `ca_certificate` valor é o caminho do `root_ca.crt` arquivo.



Para clusters do SnapMirror Business Continuity (SM-BC), você deve adicionar os `intermediate.crt` e `root_ca.crt` certificados a um cluster do ONTAP. Consulte ["Configure o ONTAP Mediator e os clusters para a sincronização ativa do SnapMirror"](#).

c. Verifique se os seguintes atributos dos certificados recém-gerados estão configurados corretamente:

- Proprietário do grupo Linux: `netapp:netapp`
- Permissões do Linux: `600`

2. Reinicie o ONTAP Mediator quando os certificados forem atualizados no arquivo de configuração:

```
systemctl restart ontap_mediator
```

O ONTAP Mediator 1.8 e versões anteriores

Você pode usar certificados de terceiro com um nome diferente de `ca.*` ou armazenar os certificados de terceiro em um local diferente.

Passos

1. Configure o

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.  
user_config.yaml
```

 arquivo para substituir os valores padrão das variáveis no `ontap_mediator.config.yaml` arquivo.

Se você obteve `ca.crt` de uma autoridade de PKI e armazena a chave privada `ca.key` no local `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, o `ontap_mediator.user_config.yaml` arquivo deve ter a seguinte aparência:



Se você usou `ca.crt` para assinar o `ontap_mediator_server.crt` certificado, o arquivo `ca.srl` é gerado. Consulte [Etapa 2: gere um certificado de servidor assinando-o com uma autoridade certificadora \(CA\) de terceiro](#) para obter mais informações.

```
[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 você estiver usando uma estrutura de certificado em que o `root_ca.crt` certificado fornece um `ca.crt` certificado que assina o `ontap_mediator_server.crt` certificado, crie uma cadeia a partir dos certificados `ca.crt` e `ontap_mediator_server.crt`:



Você deveria ter obtido os `ca.crt` e `ontap_mediator_server.crt` certificados de uma autoridade PKI anteriormente no procedimento.

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

- b. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` arquivo.

Atualize os valores de `mediator_cert`, `mediator_key` e `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
```

```
or_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
```

- O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
- O `mediator_key` valor é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
- O `ca_certificate` valor é o caminho do `root_ca.crt` arquivo.



Para clusters do SnapMirror Business Continuity (SM-BC), você deve adicionar os `ca.crt` e `root_ca.crt` certificados a um cluster do ONTAP. Consulte ["Configure o ONTAP Mediator e os clusters para a sincronização ativa do SnapMirror"](#).

c. Verifique se os seguintes atributos dos certificados recém-gerados estão configurados corretamente:

- Proprietário do grupo Linux: `netapp:netapp`
- Permissões do Linux: `600`

2. Reinicie o ONTAP Mediator quando os certificados forem atualizados no arquivo de configuração:

```
systemctl restart ontap_mediator
```

Solução de problemas relacionados a certificados do ONTAP Mediator

Use estas verificações para confirmar as propriedades do certificado ao solucionar problemas relacionados a certificados.

Verificar a expiração do certificado

Use o seguinte comando para identificar o intervalo de validade do certificado.

O ONTAP Mediator 1.9 e versões posteriores

```
[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
```

O ONTAP Mediator 1.8 e versões anteriores

```
[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
```

Verifique as extensões X509v3 na certificação da Autoridade de Certificação

Use o seguinte comando para verificar as extensões X509v3 no certificado da CA.

O ONTAP Mediator 1.9 e versões posteriores

As propriedades definidas em **v3_ca** em `openssl_ca.cnf` são exibidas como X509v3 extensions em `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
```

O ONTAP Mediator 1.8 e versões anteriores

As propriedades definidas em **v3_ca** em `openssl_ca.cnf` são exibidas como X509v3 extensions em `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
```

Verificar extensões X509v3 no certificado do servidor e nomes alternativos do assunto

As `v3_req` propriedades definidas no `openssl_server.cnf` arquivo de configuração são exibidas como

X509v3 extensions no certificado.

No exemplo a seguir, você pode obter as variáveis nas `alt_names` seções executando os comandos `hostname -A` e `hostname -I` na máquina virtual Linux na qual o ONTAP Mediator está instalado.

Consulte seu administrador de rede para obter os valores corretos das variáveis.

O ONTAP Mediator 1.9 e versões posteriores

```
[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
```

O ONTAP Mediator 1.8 e versões anteriores

```
[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

```

Verifique se a chave privada corresponde a um certificado

Você pode verificar se uma determinada chave privada corresponde a um certificado.

Use os seguintes comandos OpenSSL na chave e no certificado, respectivamente.

O ONTAP Mediator 1.9 e versões posteriores

```

[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
```

O ONTAP Mediator 1.8 e versões anteriores

```
[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 o `-modulus` atributo de ambos corresponder, isso indica que o par de chave privada e certificado é compatível e pode funcionar em conjunto.

Verifique se um certificado de servidor foi criado a partir de um certificado de CA específico

Você pode usar o seguinte comando para verificar se o certificado do servidor foi criado a partir de um certificado de CA específico.

O ONTAP Mediator 1.9 e versões posteriores

```
[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]#
```

O ONTAP Mediator 1.8 e versões anteriores

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

Se você estiver usando a validação do Protocolo de Status de Certificado Online (OCSP), use o comando `"openssl-verify"`.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.