



Gestiona certificados

ONTAP Mediator

NetApp
October 19, 2026

Tabla de contenidos

- Gestiona certificados 1
 - Regenerar un certificado temporal autofirmado para el host de ONTAP Mediator 1
 - Sustituir los certificados autofirmados de ONTAP Mediator por certificados de terceros de confianza 2
 - Paso 1: Obtener un certificado de una entidad externa que expida certificados de CA 3
 - Paso 2: Genera un certificado de servidor firmándolo con una certificación de CA de terceros 5
 - Paso 3: Sustituye el nuevo certificado de la entidad certificadora externa y el certificado del servidor en la configuración de ONTAP Mediator 6
 - Paso 4: si lo deseas, utiliza una ruta o un nombre diferente para tus certificados de terceros 10
- Solucionar problemas relacionados con los certificados de ONTAP Mediator 16
 - Verifica la fecha de caducidad del certificado 16
 - Verifica las extensiones X509v3 en la certificación de la CA 17
 - Verifica las extensiones X509v3 en el certificado del servidor y los nombres alternativos del sujeto 19
 - Comprueba que una clave privada coincida con un certificado 20
 - Comprueba que se haya creado un certificado de servidor a partir de un certificado de una CA concreta 21

Gestiona certificados

Regenerar un certificado temporal autofirmado para el host de ONTAP Mediator

Regenerar un certificado autofirmado temporal para el host actual cuando un cambio en el nombre de host o en la dirección IP invalide el certificado existente.



Este procedimiento solo es compatible con sistemas que ejecutan ONTAP Mediator 1.7 o una versión posterior.

Acerca de esta tarea

- Realiza esta tarea en el host Linux en el que hayas instalado ONTAP Mediator.
- Solo puedes realizar esta tarea si los certificados autofirmados generados han quedado obsoletos debido a cambios en el nombre de host o en la dirección IP del host después de instalar ONTAP Mediator.
- Una vez que el certificado autofirmado temporal haya sido sustituido por un certificado de confianza de un tercero, *no* utilices esta tarea para volver a generar un certificado. La ausencia de un certificado autofirmado provocará que este procedimiento falle.

Paso

Para generar un nuevo certificado temporal autofirmado para el host actual, realiza el siguiente paso:

1. Reinicia 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
```

Sustituir los certificados autofirmados de ONTAP Mediator por certificados de terceros de confianza

Si tu entorno lo permite, sustituye los certificados autofirmados por certificados de confianza emitidos por una autoridad de certificación.

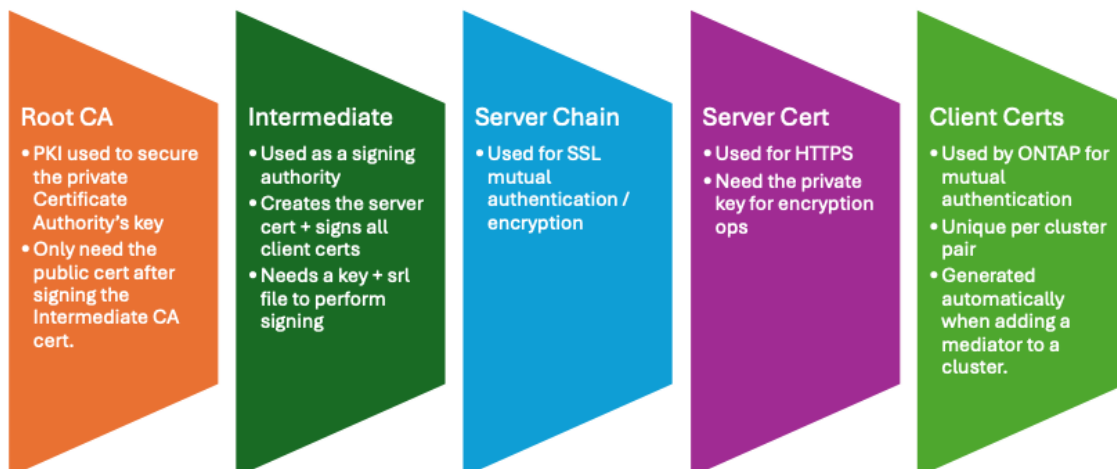


- Los certificados de terceros solo son compatibles a partir de ONTAP 9.16.1 y en algunas versiones de parche anteriores de ONTAP. Consulta ["ID de bug CONTAP-243278 de NetApp Bugs Online"](#).
- Los certificados de terceros solo son compatibles con sistemas que ejecutan ONTAP Mediator 1.7 o versiones posteriores.

Acerca de esta tarea

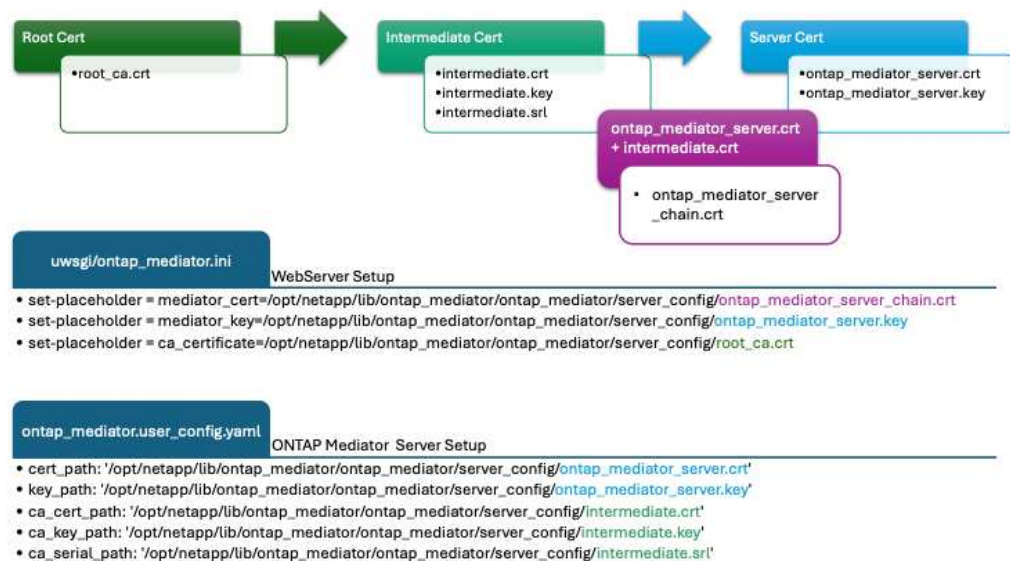
- Realiza esta tarea en el host Linux en el que hayas instalado ONTAP Mediator.
- Puedes realizar esta tarea si es necesario sustituir los certificados autofirmados generados por certificados obtenidos de una autoridad de certificación (CA) subordinada de confianza. Para ello, debes tener acceso a una autoridad de infraestructura de clave pública (PKI) de confianza.
- La siguiente imagen muestra la finalidad de cada certificado de ONTAP Mediator.

ONTAP Mediator Certificate Purposes



- La siguiente imagen muestra la configuración del servidor web y de ONTAP Mediator.

ONTAP Mediator Certificates



Paso 1: Obtener un certificado de una entidad externa que expida certificados de CA

Puedes obtener un certificado de una autoridad de PKI usando el siguiente procedimiento.

El siguiente ejemplo muestra cómo sustituir los certificados autofirmados por certificados de terceros ubicados en /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/.



El ejemplo ilustra los criterios necesarios para los certificados requeridos por ONTAP Mediator. Puedes obtener los certificados de una autoridad PKI mediante un procedimiento que podría ser diferente de este. Adapta el procedimiento según las necesidades de tu empresa.

ONTAP Mediator 1.9 y versiones posteriores

1. Crea una clave privada `intermediate.key` y un archivo de configuración `openssl_ca.cnf` que utilizará la autoridad PKI para generar un certificado.

- a. Genera la clave privada `intermediate.key`:

Ejemplo

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

- b. El archivo de configuración `openssl_ca.cnf` (ubicado en /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf) define las propiedades que debe tener el certificado generado.

2. Utiliza la clave privada y el archivo de configuración para crear una solicitud de firma de certificado `intermediate.csr`:

Ejemplo:

```
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-----
```

- Envía la solicitud de firma de certificado `intermediate.csr` a una autoridad de PKI para que la firme.

La autoridad de PKI verifica la solicitud y firma el `.csr`, generando el certificado `intermediate.crt`. Además, necesitas obtener el certificado `root_ca.crt` que firmó el certificado `intermediate.crt` de la autoridad de PKI.



Para los clústeres de SnapMirror active sync y las configuraciones IP de MetroCluster que usan ONTAP Mediator configurado con HTTPS, debes añadir los certificados `intermediate.crt` y `root_ca.crt` a un clúster de ONTAP. Consulta ["Configura ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror"](#) y ["Configura el ONTAP Mediator para una configuración IP de MetroCluster"](#).

ONTAP Mediator 1.8 y versiones anteriores

- Crea una clave privada `ca.key` y un archivo de configuración `openssl_ca.cnf` que utilizará la autoridad PKI para generar un certificado.

- Genera la clave privada `ca.key`:

Ejemplo:

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

- El archivo de configuración `openssl_ca.cnf` (ubicado en `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) define las propiedades que debe tener el certificado generado.

- Utiliza la clave privada y el archivo de configuración para crear una solicitud de firma de certificado `ca.csr`:

Ejemplo:

```
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. Envía la solicitud de firma de certificado `ca.csr` a una autoridad de PKI para que la firme.

La autoridad de PKI verifica la solicitud y firma el `.csr`, generando el certificado `ca.crt`. Además, necesitas obtener el certificado `root_ca.crt` que firmó el certificado `ca.crt` de la autoridad de PKI.



Para los clústeres de sincronización activa de SnapMirror, debes añadir los `ca.crt` y `root_ca.crt` certificados a un clúster ONTAP. Consulta ["Configura ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror"](#).

Paso 2: Genera un certificado de servidor firmándolo con una certificación de CA de terceros

ONTAP Mediator 1.9 y versiones posteriores

Un certificado de servidor debe estar firmado por la clave privada `intermediate.key` y el certificado de terceros `intermediate.crt`. Además, el archivo de configuración `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contiene ciertos atributos que especifican las propiedades necesarias para los certificados de servidor emitidos por OpenSSL.

Los siguientes comandos pueden generar un certificado de servidor.

Pasos

1. Para generar una solicitud de firma de certificado (CSR) de servidor, ejecuta el siguiente comando desde la carpeta `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`:

```
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 generar un certificado de servidor a partir de la CSR, ejecuta el siguiente comando desde la carpeta `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`:



Estos archivos se obtuvieron de una autoridad PKI. Si utilizas un nombre de certificado diferente, sustituye `intermediate.crt` y `intermediate.key` por los nombres de archivo correspondientes.

```
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
```

- La opción `-CAcreateserial` se utiliza para generar los archivos `intermediate.srl`.

ONTAP Mediator 1.8 y versiones anteriores

Un certificado de servidor debe estar firmado por la clave privada `ca.key` y el certificado de terceros `ca.crt`. Además, el archivo de configuración `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contiene ciertos atributos que especifican las propiedades necesarias para los certificados de servidor emitidos por OpenSSL.

Los siguientes comandos pueden generar un certificado de servidor.

Pasos

1. Para generar una solicitud de firma de certificado (CSR) de servidor, ejecuta el siguiente comando desde la carpeta `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`:

```
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 generar un certificado de servidor a partir de la CSR, ejecuta el siguiente comando desde la carpeta `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`:



Estos archivos se obtuvieron de una autoridad PKI. Si utilizas un nombre de certificado diferente, sustituye `ca.crt` y `ca.key` por los nombres de archivo correspondientes.

```
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
```

◦ La opción `-CAcreateserial` se utiliza para generar los archivos `ca.srl`.

Paso 3: Sustituye el nuevo certificado de la entidad certificadora externa y el certificado del servidor en la configuración de ONTAP Mediator

ONTAP Mediator 1.10 y versiones posteriores

La configuración del certificado se proporciona a ONTAP Mediator en el archivo de configuración ubicado en

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. El archivo incluye los siguientes 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/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` y `key_path` son variables de certificados de servidor.
- `ca_cert_path`, `ca_key_path` y `ca_serial_path` son variables de certificados de CA.

Pasos

1. Sustituye todos los archivos `intermediate.*` por los certificados de terceros.
2. Crea una cadena de certificados a partir de los certificados `intermediate.crt` y `ontap_mediator_server.crt`:

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

3. Actualiza el archivo `/opt/netapp/lib/ontap_mediator/uvicorn/config.json`.

Actualiza los valores de `ssl_keyfile`, `ssl_certfile` y `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
```

- El valor `ssl_keyfile` es la ruta clave en el archivo `ontap_mediator_server.crt`, que es `ontap_mediator_server.key`.
 - El valor `ssl_certfile` es la ruta del archivo `ontap_mediator_server_chain.crt`.
 - El valor `ssl_ca_certs` es la ruta del archivo `root_ca.crt`.
4. Comprueba que los siguientes atributos de los certificados recién generados estén configurados correctamente:
 - Titular del grupo Linux: `netapp:netapp`
 - Permisos de Linux: `600`
 5. Reinicia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 y 1.9

La configuración del certificado se proporciona a ONTAP Mediator en el archivo de configuración ubicado

en

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml. El archivo incluye los siguientes 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 y key_path son variables de certificados de servidor.
- ca_cert_path, ca_key_path y ca_serial_path son variables de certificados de CA.

Pasos

1. Sustituye todos los archivos intermediate.* por los certificados de terceros.
2. Crea una cadena de certificados a partir de los certificados intermediate.crt y ontap_mediator_server.crt:

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

3. Actualiza el archivo /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini.

Actualiza los valores de mediator_cert, mediator_key y 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
```

- El valor mediator_cert es la ruta del archivo ontap_mediator_server_chain.crt.

- La `mediator_key` value es la ruta clave en el archivo `ontap_mediator_server.crt`, que es `ontap_mediator_server.key`.
 - El valor `ca_certificate` es la ruta del archivo `root_ca.crt`.
4. Comprueba que los siguientes atributos de los certificados recién generados estén configurados correctamente:
 - Titular del grupo Linux: `netapp:netapp`
 - Permisos de Linux: `600`
 5. Reinicia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 y versiones anteriores

La configuración del certificado se proporciona a ONTAP Mediator en el archivo de configuración ubicado en

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. El archivo incluye los siguientes 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` y `key_path` son variables de certificados de servidor.
- `ca_cert_path`, `ca_key_path` y `ca_serial_path` son variables de certificados de CA.

Pasos

1. Sustituye todos los archivos `ca.*` por los certificados de terceros.
2. Crea una cadena de certificados a partir de los certificados `ca.crt` y `ontap_mediator_server.crt`:

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

3. Actualiza el archivo `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`.

Actualiza los valores de `mediator_cert`, `mediator_key` y `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
```

- El valor `mediator_cert` es la ruta del archivo `ontap_mediator_server_chain.crt`.
 - La `mediator_key` value es la ruta clave en el archivo `ontap_mediator_server.crt`, que es `ontap_mediator_server.key`.
 - El valor `ca_certificate` es la ruta del archivo `root_ca.crt`.
4. Comprueba que los siguientes atributos de los certificados recién generados estén configurados correctamente:
 - Titular del grupo Linux: `netapp:netapp`
 - Permisos de Linux: `600`
 5. Reinicia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Paso 4: si lo deseas, utiliza una ruta o un nombre diferente para tus certificados de terceros

ONTAP Mediator 1.10 y versiones posteriores

Puedes utilizar certificados de terceros con un nombre distinto de `intermediate.*` o almacenar los certificados de terceros en otra ubicación.

Pasos

1. Configura el archivo

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

 para anular los valores predeterminados de las variables en el archivo `ontap_mediator.config.yaml`.

Si obtuviste `intermediate.crt` de una autoridad PKI y guardas su clave privada `intermediate.key` en la ubicación

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

 el archivo `ontap_mediator.user_config.yaml` debería verse como en el siguiente ejemplo:

Si usaste `intermediate.crt` para firmar el `ontap_mediator_server.crt` certificado, se genera el archivo `intermediate.srl`. Consulta [Paso 2: Genera un certificado de servidor firmándolo con una certificación de CA de terceros](#) para obtener más información.

```
[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. Si utilizas una estructura de certificados en la que el certificado `root_ca.crt` proporciona un certificado `intermediate.crt` que firma el certificado `ontap_mediator_server.crt`, crea una cadena de certificados a partir de los certificados `intermediate.crt` y `ontap_mediator_server.crt`:



Deberías haber obtenido los `intermediate.crt` y `ontap_mediator_server.crt` certificados de una autoridad de PKI en una fase anterior del procedimiento.

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

- b. Actualiza el archivo `/opt/netapp/lib/ontap_mediator/uvicorn/config.json`.

Actualiza los valores de `ssl_keyfile`, `ssl_certfile` y `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
```

- El valor `ssl_keyfile` es la ruta clave en el archivo `ontap_mediator_server.crt`, que es `ontap_mediator_server.key`.
- El valor `ssl_certfile` es la ruta del archivo `ontap_mediator_server_chain.crt`.
- El valor `ssl_ca_certs` es la ruta del archivo `root_ca.crt`.



Para los clústeres de SnapMirror active sync y las configuraciones IP de MetroCluster que usan ONTAP Mediator configurado con HTTPS, debes añadir los certificados `intermediate.crt` y `root_ca.crt` a un clúster de ONTAP. Consulta ["Configura ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror"](#) y ["Configura el ONTAP Mediator para una configuración IP de MetroCluster"](#).

c. Comprueba que los siguientes atributos de los certificados recién generados estén configurados correctamente:

- Titular del grupo Linux: `netapp:netapp`
- Permisos de Linux: `600`

2. Reinicia ONTAP Mediator cuando se actualicen los certificados en el archivo de configuración:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 y 1.9

Puedes utilizar certificados de terceros con un nombre distinto de `intermediate.*` o almacenar los certificados de terceros en otra ubicación.

Pasos

1. Configura el archivo

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.  
user_config.yaml para anular los valores predeterminados de las variables en el archivo  
ontap_mediator.config.yaml.
```

Si obtuviste `intermediate.crt` de una autoridad PKI y guardas su clave privada `intermediate.key` en la ubicación

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config, el archivo  
ontap_mediator.user_config.yaml debería verse como en el siguiente ejemplo:
```



Si usaste `intermediate.crt` para firmar el `ontap_mediator_server.crt`

certificado, se genera el archivo `intermediate.srl`. Consulta [Paso 2: Genera un certificado de servidor firmándolo con una certificación de CA de terceros](#) para obtener más información.

```
[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. Si utilizas una estructura de certificados en la que el certificado `root_ca.crt` proporciona un certificado `intermediate.crt` que firma el certificado `ontap_mediator_server.crt`, crea una cadena de certificados a partir de los certificados `intermediate.crt` y `ontap_mediator_server.crt`:



Deberías haber obtenido los `intermediate.crt` y `ontap_mediator_server.crt` certificados de una autoridad de PKI en una fase anterior del procedimiento.

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

- b. Actualiza el archivo `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`.

Actualiza los valores de `mediator_cert`, `mediator_key` y `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server_chain.crt
```

```
set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server.key
```

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

- El valor `mediator_cert` es la ruta del archivo `ontap_mediator_server_chain.crt`.
- El valor `mediator_key` es la ruta clave en el archivo `ontap_mediator_server.crt`, que es `ontap_mediator_server.key`.
- El valor `ca_certificate` es la ruta del archivo `root_ca.crt`.



Para los clústeres de SnapMirror Business Continuity (SM-BC), debes añadir los certificados `intermediate.crt` y `root_ca.crt` a un clúster ONTAP. Consulta ["Configura ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror"](#).

- c. Comprueba que los siguientes atributos de los certificados recién generados estén configurados correctamente:

- Titular del grupo Linux: `netapp:netapp`
- Permisos de Linux: `600`

2. Reinicia ONTAP Mediator cuando se actualicen los certificados en el archivo de configuración:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 y versiones anteriores

Puedes utilizar certificados de terceros con un nombre distinto de `ca.*` o almacenar los certificados de terceros en otra ubicación.

Pasos

1. Configura el archivo

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` para anular los valores predeterminados de las variables en el archivo `ontap_mediator.config.yaml`.

Si obtuviste `ca.crt` de una autoridad PKI y guardas su clave privada `ca.key` en la ubicación `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, el archivo `ontap_mediator.user_config.yaml` debería verse como en el siguiente ejemplo:



Si usaste `ca.crt` para firmar el `ontap_mediator_server.crt` certificado, se genera el archivo `ca.srl`. Consulta [Paso 2: Genera un certificado de servidor firmándolo con una certificación de CA de terceros](#) para obtener más información.

```
[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. Si utilizas una estructura de certificados en la que el certificado `root_ca.crt` proporciona un certificado `ca.crt` que firma el certificado `ontap_mediator_server.crt`, crea una cadena de certificados a partir de los certificados `ca.crt` y `ontap_mediator_server.crt`:



Deberías haber obtenido los `ca.crt` y `ontap_mediator_server.crt` certificados de una autoridad de PKI en una fase anterior del procedimiento.

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

- b. Actualiza el archivo `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`.

Actualiza los valores de `mediator_cert`, `mediator_key` y `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
```

- El valor `mediator_cert` es la ruta del archivo `ontap_mediator_server_chain.crt`.
- El valor `mediator_key` es la ruta clave en el archivo `ontap_mediator_server.crt`, que es `ontap_mediator_server.key`.
- El valor `ca_certificate` es la ruta del archivo `root_ca.crt`.



Para los clústeres de SnapMirror Business Continuity (SM-BC), debes añadir los certificados `ca.crt` y `root_ca.crt` a un clúster ONTAP. Consulta ["Configura ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror"](#).

c. Comprueba que los siguientes atributos de los certificados recién generados estén configurados correctamente:

- Titular del grupo Linux: `netapp:netapp`
- Permisos de Linux: `600`

2. Reinicia ONTAP Mediator cuando se actualicen los certificados en el archivo de configuración:

```
systemctl restart ontap_mediator
```

Solucionar problemas relacionados con los certificados de ONTAP Mediator

Utiliza estas comprobaciones para verificar las propiedades de los certificados a la hora de resolver problemas relacionados con ellos.

Verifica la fecha de caducidad del certificado

Utiliza el siguiente comando para identificar el período de validez del certificado.

ONTAP Mediator 1.9 y versiones 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
```

ONTAP Mediator 1.8 y versiones 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
```

Verifica las extensiones X509v3 en la certificación de la CA

Utiliza el siguiente comando para comprobar las extensiones X509v3 en la certificación de la CA.

ONTAP Mediator 1.9 y versiones posteriores

Las propiedades definidas dentro de **v3_ca** en `openssl_ca.cnf` se muestran como X509v3 extensions en `intermediate.crt`.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:
```

```

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
    X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

    X509v3 Basic Constraints: critical
        CA:TRUE
    X509v3 Key Usage: critical
        Digital Signature, Certificate Sign, CRL Sign

```

ONTAP Mediator 1.8 y versiones anteriores

Las propiedades definidas dentro de **v3_ca** en `openssl_ca.cnf` se muestran como X509v3 extensions en `ca.crt`.

```

[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign

```

Verifica las extensiones X509v3 en el certificado del servidor y los nombres alternativos del sujeto

Las v3_req propiedades definidas en el openssl_server.cnf archivo de configuración se muestran como X509v3 extensions en el certificado.

En el siguiente ejemplo, puedes obtener las variables en las secciones alt_names ejecutando los comandos hostname -A y hostname -I en la máquina virtual Linux en la que está instalado ONTAP Mediator.

Consulta con tu administrador de red cuáles son los valores correctos de las variables.

ONTAP Mediator 1.9 y versiones 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
```

ONTAP Mediator 1.8 y versiones 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
```

Comprueba que una clave privada coincida con un certificado

Puedes comprobar si una clave privada concreta coincide con un certificado.

Utiliza los siguientes comandos de OpenSSL en la clave y el certificado, respectivamente.

ONTAP Mediator 1.9 y versiones 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
```

ONTAP Mediator 1.8 y versiones 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
```

Si el atributo `-modulus` coincide en ambos casos, indica que la clave privada y el certificado son compatibles y pueden funcionar juntos.

Comprueba que se haya creado un certificado de servidor a partir de un certificado de una CA concreta

Puedes utilizar el siguiente comando para comprobar que el certificado del servidor se ha creado a partir de un certificado de una CA concreta.

ONTAP Mediator 1.9 y versiones 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]#
```

ONTAP Mediator 1.8 y versiones anteriores

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

Si se utiliza la validación mediante el Protocolo de estado de certificados en línea (OCSP), usa el comando `"openssl-verify"`.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.