



Gérer les certificats

ONTAP Mediator

NetApp
October 19, 2026

Sommaire

Gérer les certificats	1
Régénérez un certificat temporaire auto-signé pour l'hôte ONTAP Mediator	1
Remplacez les certificats auto-signés d'ONTAP Mediator par des certificats tiers de confiance	2
Étape 1 : Obtenir un certificat auprès d'un organisme tiers délivrant un certificat d'autorité de certification	3
Étape 2 : Générez un certificat de serveur en le signant à l'aide d'une certification d'autorité de certification tierce	5
Étape 3 : Remplacez le nouveau certificat d'autorité de certification tierce et le certificat du serveur dans la configuration de ONTAP Mediator.	6
Étape 4 : Vous pouvez, si vous le souhaitez, utiliser un chemin d'accès ou un nom différent pour vos certificats tiers	10
Résoudre les problèmes liés aux certificats d'ONTAP Mediator	16
Vérifier l'expiration du certificat	16
Vérifier les extensions X509v3 dans le certificat de l'autorité de certification	17
Vérifiez les extensions X509v3 dans le certificat du serveur et les noms alternatifs du sujet	19
Vérifiez qu'une clé privée correspond à un certificat	21
Vérifiez qu'un certificat de serveur est créé à partir d'un certificat d'autorité de certification particulier ..	21

Gérer les certificats

Régénérez un certificat temporaire auto-signé pour l'hôte ONTAP Mediator

Régénérer un certificat auto-signé temporaire pour l'hôte actuel lorsqu'un changement de nom de l'hôte ou d'adresse IP invalide le certificat existant.



Cette procédure n'est prise en charge que sur les systèmes exécutant ONTAP Mediator 1.7 ou une version ultérieure.

À propos de cette tâche

- Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.
- Vous pouvez effectuer cette tâche uniquement si les certificats auto-signés générés sont devenus obsolètes en raison de modifications apportées au nom de l'hôte ou à l'adresse IP de l'hôte après l'installation d'ONTAP Mediator.
- Une fois le certificat auto-signé temporaire remplacé par un certificat tiers de confiance, vous ne devez *pas* utiliser cette tâche pour régénérer un certificat. L'absence de certificat auto-signé entraînera l'échec de cette procédure.

Étape

Pour régénérer un nouveau certificat temporaire auto-signé pour l'hôte actuel, procédez comme suit :

1. Redémarrer 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
```

Remplacez les certificats auto-signés d'ONTAP Mediator par des certificats tiers de confiance

Si votre environnement le permet, remplacez les certificats auto-signés par des certificats de confiance émis par une autorité de certification.

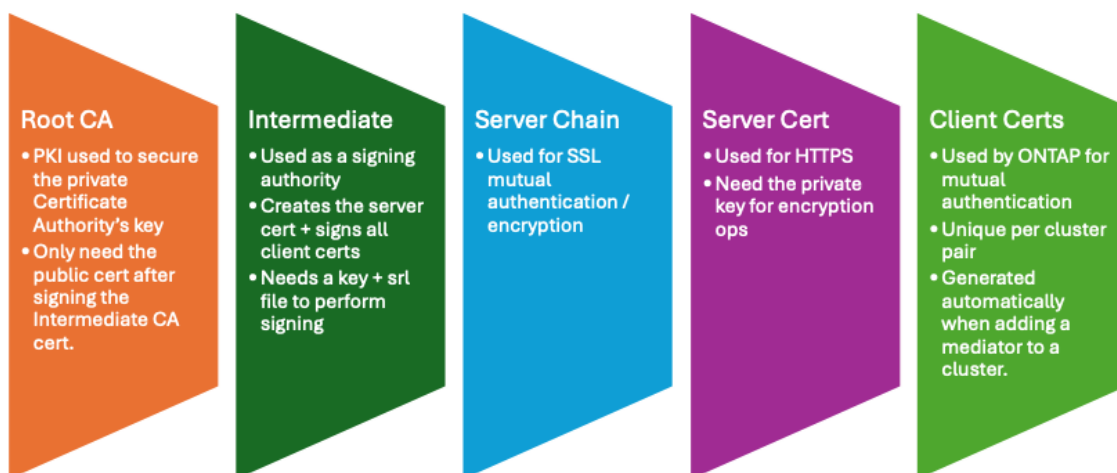


- Les certificats tiers ne sont pris en charge qu'à partir d'ONTAP 9.16.1 et dans certaines versions correctives antérieures d'ONTAP. Voir ["NetApp Identifiant du bogue Bugs Online CONTAP-243278"](#).
- Les certificats tiers ne sont pris en charge que sur les systèmes exécutant ONTAP Mediator 1.7 ou une version ultérieure.

À propos de cette tâche

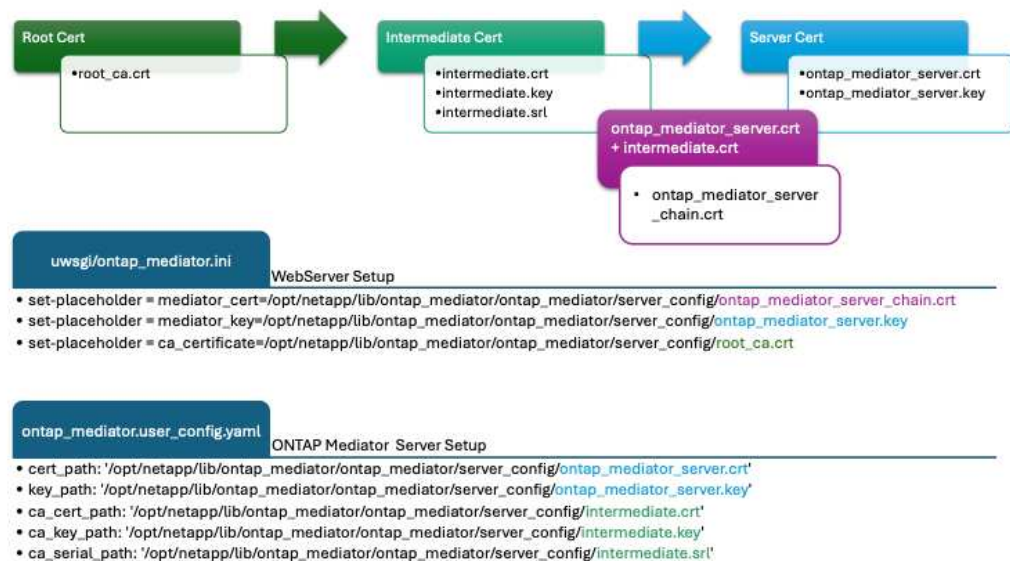
- Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.
- Vous pouvez effectuer cette opération si les certificats auto-signés générés doivent être remplacés par des certificats obtenus auprès d'une autorité de certification (CA) subordonnée de confiance. Pour ce faire, vous devez avoir accès à une autorité d'infrastructure à clés publiques (PKI) de confiance.
- L'image suivante illustre la finalité de chaque certificat ONTAP Mediator.

ONTAP Mediator Certificate Purposes



- L'image suivante illustre la configuration du serveur web et d'ONTAP Mediator.

ONTAP Mediator Certificates



Étape 1 : Obtenir un certificat auprès d'un organisme tiers délivrant un certificat d'autorité de certification

Vous pouvez obtenir un certificat auprès d'une autorité PKI en suivant la procédure ci-dessous.

L'exemple suivant illustre le remplacement des acteurs de certificats auto-signés par les acteurs de certificats tiers situés à /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/.



Cet exemple illustre les critères nécessaires pour les certificats requis pour ONTAP Mediator. Vous pouvez obtenir les certificats auprès d'une autorité PKI d'une manière qui peut différer de cette procédure. Adaptez la procédure en fonction de vos besoins métier.

ONTAP Mediator 1.9 et versions ultérieures

1. Créez une clé privée `intermediate.key` et un fichier de configuration `openssl_ca.cnf` que l'autorité PKI utilisera pour générer un certificat.

- a. Générer la clé privée `intermediate.key`:

Exemple

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

- b. Le fichier de configuration `openssl_ca.cnf` (situé à /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf) définit les propriétés que le certificat généré doit avoir.

2. Utilisez la clé privée et le fichier de configuration pour créer une demande de signature de certificat `intermediate.csr`:

Exemple :

```
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. Envoyez la demande de signature de certificat `intermediate.csr` à une autorité PKI pour signature.

L'autorité PKI vérifie la requête et la signe `.csr`, générant ainsi le certificat `intermediate.crt`. De plus, vous devez obtenir auprès de l'autorité PKI le certificat `root_ca.crt` qui a signé le certificat `intermediate.crt`.



Pour les clusters SnapMirror active sync et les configurations IP MetroCluster utilisant ONTAP Mediator configuré avec HTTPS, vous devez ajouter les `intermediate.crt` et `root_ca.crt` certificats à un cluster ONTAP. Voir ["Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror"](#) et ["Configurez le médiateur ONTAP pour une configuration IP MetroCluster"](#).

ONTAP Mediator 1.8 et versions antérieures

1. Créez une clé privée `ca.key` et un fichier de configuration `openssl_ca.cnf` qui seront utilisés par l'autorité PKI pour générer un certificat.

- a. Générer la clé privée `ca.key` :

Exemple :

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

- b. Le fichier de configuration `openssl_ca.cnf` (situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) définit les propriétés que le certificat généré doit avoir.

2. Utilisez la clé privée et le fichier de configuration pour créer une demande de signature de certificat `ca.csr`:

Exemple :

```
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. Envoyez la demande de signature de certificat `ca.csr` à une autorité PKI pour sa signature.

L'autorité PKI vérifie la requête et signe la `.csr`, générant le certificat `ca.crt`. De plus, vous devez obtenir auprès de l'autorité PKI le `root_ca.crt` certificat qui a signé le `ca.crt` certificat.



Pour les clusters de synchronisation active SnapMirror, vous devez ajouter les certificats `ca.crt` et `root_ca.crt` à un cluster ONTAP. Voir ["Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror"](#).

Étape 2 : Générez un certificat de serveur en le signant à l'aide d'une certification d'autorité de certification tierce

ONTAP Mediator 1.9 et versions ultérieures

Un certificat serveur doit être signé par la clé privée `intermediate.key` et le certificat tiers `intermediate.crt`. De plus, le fichier de configuration `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contient certains attributs qui spécifient les propriétés requises pour les certificats serveur émis par OpenSSL.

Les commandes suivantes permettent de générer un certificat serveur.

Étapes

1. Pour générer une demande de signature de certificat de serveur (CSR), exécutez la commande suivante depuis le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` dossier :

```
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. Pour générer un certificat serveur à partir de la CSR, exécutez la commande suivante depuis le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` dossier :



Ces fichiers proviennent d'une autorité de certification PKI. Si vous utilisez un autre nom de certificat, remplacez `intermediate.crt` et `intermediate.key` par les noms de fichiers correspondants.

```
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
```

- L'option `-CAcreateserial` permet de générer les `intermediate.srl` fichiers.

ONTAP Mediator 1.8 et versions antérieures

Un certificat serveur doit être signé par la clé privée `ca.key` et le certificat tiers `ca.crt`. De plus, le fichier de configuration

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contient certains attributs qui spécifient les propriétés requises pour les certificats serveur émis par OpenSSL.

Les commandes suivantes permettent de générer un certificat serveur.

Étapes

1. Pour générer une demande de signature de certificat de serveur (CSR), exécutez la commande suivante depuis le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` dossier :

```
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. Pour générer un certificat serveur à partir de la CSR, exécutez la commande suivante depuis le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` dossier:



Ces fichiers ont été obtenus auprès d'une autorité PKI. Si vous utilisez un autre nom de certificat, remplacez `ca.crt` et `ca.key` par les noms de fichiers correspondants.

```
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
```

° L' `-CAcreateserial` option permet de générer les `ca.srl` fichiers.

Étape 3 : Remplacez le nouveau certificat d'autorité de certification tierce et le certificat du serveur dans la configuration de ONTAP Mediator.

ONTAP Mediator 1.10 et versions ultérieures

La configuration du certificat est fournie à ONTAP Mediator dans le fichier de configuration situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. Le fichier comprend les attributs suivants :

```
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` et `key_path` sont des variables de certificat serveur.
- `ca_cert_path`, `ca_key_path` et `ca_serial_path` sont des variables de certificat d'autorité de certification.

Étapes

1. Remplacez tous `intermediate.*` les fichiers par les certificats tiers.
2. Créez une chaîne de certificats à partir des certificats `intermediate.crt` et `ontap_mediator_server.crt`:

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

3. Mettez à jour le `/opt/netapp/lib/ontap_mediator/unicorn/config.json` fichier.

Mettez à jour les valeurs de `ssl_keyfile`, `ssl_certfile` et `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
```

- La `ssl_keyfile` valeur correspond au chemin d'accès à la clé dans le `ontap_mediator_server.crt` fichier, qui est `ontap_mediator_server.key`.
 - La `ssl_certfile` valeur correspond au chemin d'accès du `ontap_mediator_server_chain.crt` fichier.
 - La `ssl_ca_certs` valeur correspond au chemin d'accès du `root_ca.crt` fichier.
4. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :
 - Propriétaire du groupe Linux: `netapp:netapp`
 - Autorisations Linux: `600`
 5. Redémarrer ONTAP Mediator :

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 et 1.9

La configuration du certificat est fournie à ONTAP Mediator dans le fichier de configuration situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. Le fichier comprend les attributs suivants :

```
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` et `key_path` sont des variables de certificat serveur.
- `ca_cert_path`, `ca_key_path` et `ca_serial_path` sont des variables de certificat d'autorité de certification.

Étapes

1. Remplacez tous `intermediate.*` les fichiers par les certificats tiers.
2. Créez une chaîne de certificats à partir des certificats `intermediate.crt` et `ontap_mediator_server.crt`:

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

3. Mettez à jour le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Mettez à jour les valeurs de `mediator_cert`, `mediator_key` et `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
```

- La `mediator_cert` valeur correspond au chemin d'accès du `ontap_mediator_server_chain.crt` fichier.
- Le `mediator_key` value est le chemin d'accès principal dans le fichier `ontap_mediator_server.crt`, qui est `ontap_mediator_server.key`.
- La `ca_certificate` valeur correspond au chemin d'accès du `root_ca.crt` fichier.

4. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :

- Propriétaire du groupe Linux: `netapp:netapp`
- Autorisations Linux: `600`

5. Redémarrer ONTAP Mediator :

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 et versions antérieures

La configuration du certificat est fournie à ONTAP Mediator dans le fichier de configuration situé à `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.conf.yaml`. Le fichier comprend les attributs suivants :

```
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` et `key_path` sont des variables de certificat serveur.
- `ca_cert_path`, `ca_key_path` et `ca_serial_path` sont des variables de certificat d'autorité de certification.

Étapes

1. Remplacez tous `ca.*` les fichiers par les certificats tiers.
2. Créez une chaîne de certificats à partir des certificats `ca.crt` et `ontap_mediator_server.crt` :

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

3. Mettez à jour le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Mettez à jour les valeurs de `mediator_cert`, `mediator_key` et `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
```

- La `mediator_cert` valeur correspond au chemin d'accès du `ontap_mediator_server_chain.crt` fichier.
- Le `mediator_key` value est le chemin d'accès principal dans le fichier `ontap_mediator_server.crt`, qui est `ontap_mediator_server.key`.
- La `ca_certificate` valeur correspond au chemin d'accès du `root_ca.crt` fichier.

4. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :

- Propriétaire du groupe Linux: `netapp:netapp`
- Autorisations Linux: `600`

5. Redémarrer ONTAP Mediator :

```
systemctl restart ontap_mediator
```

Étape 4 : Vous pouvez, si vous le souhaitez, utiliser un chemin d'accès ou un nom différent pour vos certificats tiers

ONTAP Mediator 1.10 et versions ultérieures

Vous pouvez utiliser des certificats tiers avec un nom autre que `intermediate.*` ou stocker les certificats tiers dans un autre emplacement.

Étapes

1. Configurez le

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` fichier pour remplacer les valeurs par défaut des variables dans le `ontap_mediator.config.yaml` fichier.

Si vous avez obtenu `intermediate.crt` auprès d'une autorité PKI et que vous stockez sa clé privée `intermediate.key` à l'emplacement

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, le fichier `ontap_mediator.user_config.yaml` devrait ressembler à l'exemple suivant :



Si vous avez utilisé `intermediate.crt` pour signer le `ontap_mediator_server.crt` certificat, le fichier `intermediate.srl` est généré. Consultez [Étape 2 : Générez un certificat de serveur en le signant à l'aide d'une certification d'autorité de certification tierce](#) pour plus d'informations.

```
[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 vous utilisez une structure de certificats où le `root_ca.crt` certificat fournit un `intermediate.crt` certificat qui signe le `ontap_mediator_server.crt` certificat, créez une chaîne de certificats à partir des `intermediate.crt` et `ontap_mediator_server.crt` certificats :



Vous auriez dû obtenir les `intermediate.crt` et `ontap_mediator_server.crt` certificats auprès d'une autorité PKI plus tôt dans la procédure.

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

b. Mettez à jour le `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` fichier.

Mettez à jour les valeurs de `ssl_keyfile`, `ssl_certfile` et `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
```

- La `ssl_keyfile` valeur correspond au chemin d'accès à la clé dans le `ontap_mediator_server.crt` fichier, qui est `ontap_mediator_server.key`.
- La `ssl_certfile` valeur correspond au chemin d'accès du `ontap_mediator_server_chain.crt` fichier.
- La `ssl_ca_certs` valeur correspond au chemin d'accès du `root_ca.crt` fichier.



Pour les clusters SnapMirror active sync et les configurations IP MetroCluster utilisant ONTAP Mediator configuré avec HTTPS, vous devez ajouter les `intermediate.crt` et `root_ca.crt` certificats à un cluster ONTAP. Voir ["Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror"](#) et ["Configurez le médiateur ONTAP pour une configuration IP MetroCluster"](#).

c. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :

- Propriétaire du groupe Linux: `netapp:netapp`
- Autorisations Linux: `600`

2. Redémarrez ONTAP Mediator une fois les certificats mis à jour dans le fichier de configuration :

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 et 1.9

Vous pouvez utiliser des certificats tiers avec un nom autre que `intermediate.*` ou stocker les certificats tiers dans un autre emplacement.

Étapes

1. Configurez le

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

 fichier pour remplacer les valeurs par défaut des variables dans le `ontap_mediator.config.yaml` fichier.

Si vous avez obtenu `intermediate.crt` auprès d'une autorité PKI et que vous stockez sa clé privée `intermediate.key` à l'emplacement

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

 le fichier `ontap_mediator.user_config.yaml` devrait ressembler à l'exemple suivant :



Si vous avez utilisé `intermediate.crt` pour signer le `ontap_mediator_server.crt` certificat, le fichier `intermediate.srl` est généré. Consultez [Étape 2 : Générez un certificat de serveur en le signant à l'aide d'une certification d'autorité de certification tierce](#) pour plus d'informations.

```
[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 vous utilisez une structure de certificats où le `root_ca.crt` certificat fournit un `intermediate.crt` certificat qui signe le `ontap_mediator_server.crt` certificat, créez une chaîne de certificats à partir des `intermediate.crt` et `ontap_mediator_server.crt` certificats :



Vous auriez dû obtenir les `intermediate.crt` et

ontap_mediator_server.crt certificats auprès d'une autorité PKI plus tôt dans la procédure.

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

b. Mettez à jour le /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini fichier.

Mettez à jour les valeurs de mediator_cert, mediator_key et 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
```

- La mediator_cert valeur correspond au chemin d'accès du ontap_mediator_server_chain.crt fichier.
- La mediator_key valeur correspond au chemin d'accès à la clé dans le ontap_mediator_server.crt fichier, qui est ontap_mediator_server.key.
- La ca_certificate valeur correspond au chemin d'accès du root_ca.crt fichier.



Pour les clusters de continuité d'activité SnapMirror Business Continuity (SM-BC), vous devez ajouter les certificats intermediate.crt et root_ca.crt à un cluster ONTAP. Voir ["Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror"](#).

c. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :

- Propriétaire du groupe Linux: netapp:netapp
- Autorisations Linux: 600

2. Redémarrez ONTAP Mediator une fois les certificats mis à jour dans le fichier de configuration :

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 et versions antérieures

Vous pouvez utiliser des certificats tiers avec un nom autre que ca.* ou stocker les certificats tiers dans un emplacement différent.

Étapes

1. Configurez le

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml fichier pour remplacer les valeurs par défaut des variables dans le ontap_mediator.config.yaml fichier.

Si vous avez obtenu `ca.crt` auprès d'une autorité PKI et que vous stockez sa clé privée `ca.key` à l'emplacement `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, le fichier `ontap_mediator.user_config.yaml` devrait ressembler à l'exemple suivant :



Si vous avez utilisé `ca.crt` pour signer le `ontap_mediator_server.crt` certificat, le `ca.srl` fichier est généré. Consultez [Étape 2 : Générez un certificat de serveur en le signant à l'aide d'une certification d'autorité de certification tierce](#) pour plus d'informations.

```
[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 vous utilisez une structure de certificats où le `root_ca.crt` certificat fournit un `ca.crt` certificat qui signe le `ontap_mediator_server.crt` certificat, créez une chaîne de certificats à partir du `ca.crt` et du `ontap_mediator_server.crt` certificat :



Vous auriez dû obtenir les `ca.crt` et `ontap_mediator_server.crt` certificats

après d'une autorité PKI plus tôt dans la procédure.

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

b. Mettez à jour le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Mettez à jour les valeurs de `mediator_cert`, `mediator_key` et `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
```

- La `mediator_cert` valeur correspond au chemin d'accès du `ontap_mediator_server_chain.crt` fichier.
- La `mediator_key` valeur correspond au chemin d'accès à la clé dans le `ontap_mediator_server.crt` fichier, qui est `ontap_mediator_server.key`.
- La `ca_certificate` valeur correspond au chemin d'accès du `root_ca.crt` fichier.



Pour les clusters SnapMirror Business Continuity (SM-BC), vous devez ajouter les `ca.crt` et `root_ca.crt` certificats à un cluster ONTAP. Voir "[Configurez ONTAP Mediator et les clusters pour la synchronisation active SnapMirror](#)".

c. Vérifiez que les attributs suivants des certificats nouvellement générés sont correctement définis :

- Propriétaire du groupe Linux: `netapp:netapp`
- Autorisations Linux: `600`

2. Redémarrez ONTAP Mediator une fois les certificats mis à jour dans le fichier de configuration :

```
systemctl restart ontap_mediator
```

Résoudre les problèmes liés aux certificats d'ONTAP Mediator

Utilisez ces vérifications pour contrôler les propriétés du certificat lors du dépannage des problèmes de certificat.

Vérifier l'expiration du certificat

Utilisez la commande suivante pour identifier la plage de validité du certificat.

ONTAP Mediator 1.9 et versions ultérieures

```
[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 et versions antérieures

```
[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
```

Vérifier les extensions X509v3 dans le certificat de l'autorité de certification

Utilisez la commande suivante pour vérifier les extensions X509v3 dans le certificat de l'autorité de certification.

ONTAP Mediator 1.9 et versions ultérieures

Les propriétés définies dans **v3_ca** dans `openssl_ca.cnf` sont affichées comme X509v3 extensions dans `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 et versions antérieures

Les propriétés définies dans **v3_ca** dans `openssl_ca.cnf` sont affichées comme X509v3 extensions dans `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
```

Vérifiez les extensions X509v3 dans le certificat du serveur et les noms alternatifs du sujet

Les v3_req propriétés définies dans le openssl_server.cnf fichier de configuration sont affichées telles qu'elles figurent X509v3 extensions dans le certificat.

Dans l'exemple suivant, vous pouvez obtenir les variables dans les sections alt_names en exécutant les commandes hostname -A et hostname -I sur la machine virtuelle Linux sur laquelle ONTAP Mediator est installé.

Vérifiez auprès de votre administrateur réseau les valeurs correctes des variables.

ONTAP Mediator 1.9 et versions ultérieures

```
[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 et versions antérieures

```
[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
```

Vérifiez qu'une clé privée correspond à un certificat

Vous pouvez vérifier si une clé privée particulière correspond à un certificat.

Utilisez les commandes OpenSSL suivantes respectivement sur la clé et le certificat.

ONTAP Mediator 1.9 et versions ultérieures

```
[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 et versions antérieures

```
[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 l'attribut `-modulus` correspond pour les deux, cela indique que la paire clé privée-certificat est compatible et peut fonctionner ensemble.

Vérifiez qu'un certificat de serveur est créé à partir d'un certificat d'autorité de certification particulier

Vous pouvez utiliser la commande suivante pour vérifier que le certificat du serveur est créé à partir d'un certificat d'autorité de certification spécifique.

ONTAP Mediator 1.9 et versions ultérieures

```
[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 et versions antérieures

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

```
ontap_mediator_server.crt  
ontap_mediator_server.crt: OK
```

Si la validation du protocole OCSP (Online Certificate Status Protocol) est utilisée, utilisez la commande ["openssl-verify"](#).

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.