



Administrer ONTAP Mediator

ONTAP Mediator

NetApp
October 19, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/ontap-mediator/administer/upgrade-ontap-mediator-task.html> on October 19, 2026. Always check docs.netapp.com for the latest.

Sommaire

Administrer ONTAP Mediator	1
Mettre à niveau ONTAP Mediator	1
Mettre à niveau ONTAP Mediator	1
Mettez à niveau le système d'exploitation hôte et réinstallez ou mettez à niveau ONTAP Mediator	9
Configurer les attributs de ONTAP Mediator	14
Paramètres configurables du médiateur ONTAP	14
Installer des certificats SSL tiers	15
Configurer la protection contre les attaques par mot de passe	17
Configurer les règles de complexité des mots de passe	18
Configurer le seuil d'espace libre	18
Configurer l'espace de journalisation réservé	18
Modifier le nom d'utilisateur et le mot de passe du médiateur ONTAP	19
Changer le nom d'utilisateur	19
Changer le mot de passe	20
Démarrer et arrêter ONTAP Mediator	21
Arrêtez ONTAP Mediator	21
Démarrer ONTAP Mediator	21
Vérifier l'état de santé de ONTAP Mediator	22
Vérifiez l'état du service	22
Vérifiez les ports d'écoute	23
Gérer les certificats	24
Régénérez un certificat temporaire auto-signé pour l'hôte ONTAP Mediator	24
Remplacez les certificats auto-signés d'ONTAP Mediator par des certificats tiers de confiance	25
Résoudre les problèmes liés aux certificats d'ONTAP Mediator	39
Maintenir le système d'exploitation hôte pour ONTAP Mediator	45
Redémarrez l'hôte	45
Mises à jour du package hôte	45
Mettre à niveau le noyau du système d'exploitation hôte	45
Effectuer la maintenance de l'hôte	46
Modifications du nom d'hôte ou de l'adresse IP de l'hôte	49
Désinstaller ONTAP Mediator	50

Administrer ONTAP Mediator

Mettre à niveau ONTAP Mediator

Mettre à niveau ONTAP Mediator

Pour mettre à niveau ONTAP Mediator vers une version plus récente sans mettre à niveau le système d'exploitation hôte, téléchargez le package d'installation de la nouvelle version et exécutez le programme d'installation sur l'hôte sur lequel ONTAP Mediator est déjà installé.



Si vous devez mettre à niveau le système d'exploitation hôte vers une nouvelle version et réinstaller ou mettre à niveau ONTAP Mediator dans le cadre de ce processus, consultez plutôt ["Mettez à niveau le système d'exploitation hôte et ONTAP Mediator"](#).

Avant de commencer

- Vérifiez que votre hôte répond aux prérequis décrits dans ["Préparez-vous à installer ONTAP Mediator"](#), y compris les exigences relatives à l'hôte, au pare-feu et au système d'exploitation.
- Téléchargez le package d'installation de la nouvelle version. Consultez ["Téléchargez le package d'installation d'ONTAP Mediator"](#).
- NetApp recommande de vérifier la signature du code du nouveau package d'installation. Voir ["Vérifiez la signature du code du package d'installation d'ONTAP Mediator"](#).

À propos de cette tâche

Veuillez consulter les informations suivantes avant de mettre à niveau ONTAP Mediator.

- Vous devez mettre à niveau ONTAP Mediator vers la dernière version. Les versions antérieures restent compatibles avec toutes les versions d'ONTAP, mais les versions plus récentes intègrent des correctifs de sécurité pour les composants tiers.
- Lors de la mise à niveau vers une nouvelle version d'ONTAP Mediator incluant le package SCST, le programme d'installation effectue automatiquement la mise à niveau vers la version SCST recommandée, sauf si une version supérieure est disponible. Pour obtenir des instructions sur l'installation manuelle d'une version SCST supérieure, consultez ["Maintenir le système d'exploitation hôte pour ONTAP Mediator"](#). Pour les versions prises en charge, consultez le ["Matrice de prise en charge SCST"](#).



- Si la mise à niveau échoue, vous devrez peut-être essayer une version plus récente d'ONTAP Mediator.
- À compter du 15 juin 2025, vous ne pourrez plus installer ni mettre à niveau ONTAP Mediator 1.9 et 1.8, car leurs certificats de signature de code ont expiré. Si la mise à niveau échoue, utilisez plutôt la version de correctif ONTAP Mediator 1.9.1.
- À partir d'ONTAP 9.19.1 et ONTAP Mediator 1.12, vous avez la possibilité d'installer ONTAP Mediator avec la prise en charge d'iSCSI et d'HTTPS, ou uniquement avec la prise en charge d'HTTPS. Si vous choisissez d'installer ONTAP Mediator avec la prise en charge d'HTTPS uniquement, le package SCST n'est pas installé.
- Si vous effectuez une mise à niveau depuis ONTAP Mediator 1.11 ou une version antérieure avec SCST installé, et que vous choisissez l'option HTTPS uniquement lors de la mise à niveau, le package SCST est désinstallé et la nouvelle version d'ONTAP Mediator ne contient pas le package SCST.

- Si vous prévoyez d'utiliser ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster, la prise en charge dépend de votre type de Mediator, de la version d'ONTAP et du système d'exploitation. Consultez ["Utilisez ONTAP Mediator pour surveiller plusieurs configurations IP MetroCluster"](#) pour plus d'informations.
- L'installation ONTAP Mediator avec prise en charge du protocole HTTPS uniquement est prise en charge pour les cas d'utilisation suivants :
 - Vous prévoyez d'utiliser uniquement ONTAP Mediator pour surveiller vos clusters de synchronisation active SnapMirror.
 - Vous prévoyez de configurer ONTAP Mediator avec HTTPS pour surveiller une ou plusieurs configurations IP MetroCluster.
- ONTAP Mediator doit être installé avec la prise en charge d'iSCSI et de HTTPS dans le scénario suivant :
 - Vous prévoyez de configurer ONTAP Mediator avec iSCSI pour surveiller une ou plusieurs configurations IP MetroCluster.
- Lorsque vous exécutez le programme d'installation sur une installation existante de ONTAP Mediator, il détecte la version actuelle et vous invite à confirmer la mise à niveau :

```
ONTAP Mediator will be upgraded from version <current-version> to <new-version>.
```

```
Do you wish to continue? Y(es)/n(o) :
```

- Dans le cadre de la mise à niveau, le programme d'installation capture un ensemble de support de votre configuration antérieure à la mise à niveau et migre la base de données avant de mettre à niveau le logiciel ONTAP Mediator.
- Pour les cas d'utilisation d'automatisation, vous pouvez utiliser la commande `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 -y` pour ignorer les invites de l'installateur.

Étapes

1. Exécutez le programme d'installation de la nouvelle version et répondez aux invites comme demandé :

```
./ontap-mediator-1.12.1/ontap-mediator-1.12.1
```



Pour ignorer la vérification de signature lors de la mise à niveau, utilisez la `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 --skip-code-signature-check` commande

Le programme d'installation détecte l'installation existante et vous invite à la mettre à niveau, puis installe les paquets requis et migre votre configuration.

▼ Exemple de mise à niveau d'ONTAP Mediator avec prise en charge HTTPS et iSCSI (sortie console)

```
[root@mediator_host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
```

Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls

+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API
(mediatoradmin).

Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall

+ Installing required packages.

Last metadata expiration check: 0:03:56 ago on Mon 20 Apr 2026
02:49:08 PM EDT.

Package openssl-1:3.5.1-7.el9_7.x86_64 is already installed.

Package openssl-devel-1:3.5.1-7.el9_7.x86_64 is already installed.

Package kernel-devel-5.14.0-611.45.1.el9_7.x86_64 is already
installed.

Package kernel-modules-core-5.14.0-611.45.1.el9_7.x86_64 is already
installed.

Package gcc-11.5.0-11.el9.x86_64 is already installed.

Package make-1:4.3-8.el9.x86_64 is already installed.

Package which-2.21-30.el9_6.x86_64 is already installed.

Package libselinux-utils-3.6-3.el9.x86_64 is already installed.

Package patch-2.7.6-16.el9.x86_64 is already installed.

Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.

Package perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch is already
installed.

Package bzip2-1.0.8-10.el9_5.x86_64 is already installed.

Package efibootmgr-16-12.el9.x86_64 is already installed.

Package mokutil-2:0.7.2-1.el9.x86_64 is already installed.

Package python3-pip-21.3.1-1.el9.noarch is already installed.

Package elfutils-libelf-devel-0.193-1.el9.x86_64 is already installed.

Package policycoreutils-python-utils-3.6-3.el9.noarch is already

```

installed.
Package python3.12-3.12.12-4.el9_7.2.x86_64 is already installed.
Package python3.12-devel-3.12.12-4.el9_7.2.x86_64 is already
installed.
Dependencies resolved.
Nothing to do.
Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.uigddi/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20260420145003.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20260420145003.log)

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
    OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
[root@mediator_host ~]# ontap-mediator-1.12.1/ontap-mediator-1.12.1

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
    Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
+ Unpacking the ONTAP Mediator installer
+ ONTAP_MEDIATOR_INSTALL_HTTPS_ONLY is set to '0', args are: ''
+ Starting ONTAP Mediator install/update process: previous
installation_mode is ''

```

ONTAP Mediator can be installed with iSCSI and HTTPS support, or support for HTTPS only.

Do you wish to install ONTAP Mediator with iSCSI and HTTPS support?

Y(es)/n(o): yes

ONTAP Mediator will be installed with mode: ISCSI_HTTPS

+ Selected install package mode: ISCSI_HTTPS

ONTAP Mediator will be upgraded from version 1.11.0 to 1.12.1.

Do you wish to continue? Y(es)/n(o): yes

Capturing support_bundle to save pre-upgrade configuration. API Credentials are required.

Mediator API User Name: mediatoradmin

Password: Running plugins, please wait...

Creating tar archive...

Support bundle has been generated at

/opt/netapp/data/support_bundles/scs001097036-1_1776711598_BASIC.tgz

Testing the DB can be upgraded

Cloning database...

Cloning successful.

Verifying database is up-to-date...

Database out-of-date.Migrations are necessary:

Current revision: 0d5dcf349b27, Head revision: 758e4873c40d

Performing database migrations against clone...

Migrations successful.

Database upgrade operation complete.

+ Adding python312 specific packages

+ Upgrading ONTAP Mediator. (Log: /root/ontap_mediator.gwaGmU/ontap-mediator-1.12.1/ontap-mediator-1.12.1/upgrade_20260420145942.log)

+ Note: ONTAP Mediator generated a self-signed server certificate for temporary use on

this host. If the DNS name or IP address for the host is changed, the certificate

will no longer be valid. The default certificates should be replaced with secure

trusted certificates signed by a known certificate authority prior to use for production.

For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for the current

OS. Using 'yum update' to upgrade the kernel might cause service interruption.

```
For more information, see /opt/netapp/lib/ontap_mediator/README
[root@mediator_host ~]#
```

▼ **Exemple de mise à niveau d'ONTAP Mediator avec prise en charge de HTTPS uniquement (sortie console)**

```
[root@mediator_host~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API
(mediatoradmin).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall

+ Installing required packages.

Last metadata expiration check: 0:33:41 ago on Tue 21 Apr 2026
10:48:35 AM EDT.
Package openssl-1:3.5.1-7.el9_7.x86_64 is already installed.
Package openssl-devel-1:3.5.1-7.el9_7.x86_64 is already installed.
Package kernel-devel-5.14.0-611.45.1.el9_7.x86_64 is already
installed.
Package kernel-modules-core-5.14.0-611.45.1.el9_7.x86_64 is already
installed.
Package gcc-11.5.0-11.el9.x86_64 is already installed.
```

```
Package make-1:4.3-8.el9.x86_64 is already installed.
Package which-2.21-30.el9_6.x86_64 is already installed.
Package libselinux-utils-3.6-3.el9.x86_64 is already installed.
Package patch-2.7.6-16.el9.x86_64 is already installed.
Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.
Package perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch is already
installed.
Package bzip2-1.0.8-10.el9_5.x86_64 is already installed.
Package efibootmgr-16-12.el9.x86_64 is already installed.
Package mokutil-2:0.7.2-1.el9.x86_64 is already installed.
Package python3-pip-21.3.1-1.el9.noarch is already installed.
Package elfutils-libelf-devel-0.193-1.el9.x86_64 is already installed.
Package policycoreutils-python-utils-3.6-3.el9.noarch is already
installed.
Package python3.12-3.12.12-4.el9_7.2.x86_64 is already installed.
Package python3.12-devel-3.12.12-4.el9_7.2.x86_64 is already
installed.
Dependencies resolved.
Nothing to do.
Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.JclgnS/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20260421112205.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20260421112205.log)

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
    OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
[root@mediator_host~]#
```

```
[root@mediator_host~]# tar -zxvf ontap-mediator-1.12.1.tgz
ontap-mediator-1.12.1/
ontap-mediator-1.12.1/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.12.1/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.12.1/ONTAP-Mediator-production.pub
ontap-mediator-1.12.1/ontap-mediator-1.12.1
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig
ontap-mediator-1.12.1/ontap-mediator-1.12.1.tsr
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig.tsr
[root@mediator_host~]#
[root@mediator_host~]# ontap-mediator-1.12.1/ontap-mediator-1.12.1
--https-only
```

ONTAP Mediator: Self Extracting Installer

```
+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
+ Unpacking the ONTAP Mediator installer
+ ONTAP_MEDIATOR_INSTALL_HTTPS_ONLY is set to '1', args are: ''
+ Starting ONTAP Mediator install/update process: previous
installation_mode is ''
+ Selected install package mode: HTTPS_ONLY
ONTAP Mediator will be upgraded from version 1.11.0 to 1.12.1.
```

```
Do you wish to continue? Y(es)/n(o): yes
Capturing support_bundle to save pre-upgrade configuration. API
Credentials are required.
```

```
  Mediator API User Name: mediatoradmin
```

```
    Password: Running plugins, please wait...
```

```
Creating tar archive...
```

```
Support bundle has been generated at
```

```
/opt/netapp/data/support_bundles/scs001097036-1_1776785423_BASIC.tgz
```

```
Testing the DB can be upgraded
```

```
Cloning database...
```

```
Cloning successful.
```

```
Verifying database is up-to-date...
```

```
Database out-of-date.Migrations are necessary:
```

```
Current revision: 0d5dcf349b27, Head revision: 758e4873c40d
```

```
Performing database migrations against clone...
```

```

Migrations successful.
Database upgrade operation complete.
+ Adding python312 specific packages
+ Upgrading ONTAP Mediator. (Log: /root/ontap_mediator.cRy0mN/ontap-
mediator-1.12.1/ontap-mediator-1.12.1/upgrade_20260421113003.log)
fapolicyd not installed or no rules.d directory found, skipping
fapolicyd configuration
    ONTAP Mediator rsyslog and logging rotation enabled
+ Upgrade successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/upgrade_20260421113003.log)\n

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
    OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README

[root@mediator_host ~]#

```

Mettez à niveau le système d'exploitation hôte et réinstallez ou mettez à niveau ONTAP Mediator

Pour mettre à niveau le système d'exploitation hôte pour ONTAP Mediator avec SCST installé vers une version ultérieure, vous devez désinstaller ONTAP Mediator. Après la mise à niveau du système d'exploitation, vous pouvez réinstaller votre version actuelle de ONTAP Mediator ou effectuer une mise à niveau vers une version plus récente.

À propos de cette tâche

- Cette tâche s'applique aux versions d'ONTAP Mediator avec SCST installé. Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure avec prise en charge de HTTPS uniquement, le package SCST n'est pas installé et vous pouvez mettre à niveau le système d'exploitation hôte sans affecter ONTAP Mediator. Consultez la documentation du fournisseur du système d'exploitation hôte pour obtenir les instructions de mise à niveau.
- Si vous devez uniquement mettre à jour le noyau du système d'exploitation hôte vers une version prise en charge sans passer à une nouvelle version du système d'exploitation, consultez plutôt ["Maintenir le système d'exploitation hôte pour ONTAP Mediator"](#).

- Avant de mettre à niveau le système d'exploitation hôte d'ONTAP Mediator avec l'outil leapp-upgrade, "[désinstaller ONTAP Mediator](#)". L'outil vérifie la présence de nouvelles versions RPM dans les dépôts enregistrés.
- Le programme d'installation d'ONTAP Mediator installe un fichier .rpm, que l'outil leapp-upgrade inclut dans la recherche. Comme le programme d'installation décompresse le fichier au lieu de le télécharger depuis un dépôt enregistré, l'outil ne peut pas trouver de mise à niveau. Vous devez utiliser l'outil leapp-upgrade pour désinstaller le package.

Étapes

1. Sauvegardez les fichiers journaux :

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Effectuez la mise à niveau avec l'outil leapp-upgrade :

```
[rootmediator-host ~]# leapp preupgrade --target 9.8
..<snip upgrade checks>..
..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 9.8
..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. Réinstaller ONTAP Mediator:



Effectuez les étapes restantes immédiatement après la réinstallation de ONTAP Mediator afin d'éviter toute perte de fichiers journaux.

```
[rootmediator-host ~]# ontap-mediator-1.12.1/ontap-mediator-1.12.1
```

```
ONTAP Mediator: Self Extracting Installer
```

```
....  
[rootmediator-host ~]#
```

4. Arrêtez ontap_mediator:

```
[rootmediator-host ~]# systemctl stop ontap_mediator  
[rootmediator-host ~]#
```

5. Remplacez les fichiers journaux :

```
[rootmediator-host ~]# tar -xf ontap_mediator_file_backup.tgz -C  
/opt/netapp/lib/ontap_mediator  
[rootmediator-host ~]#
```

6. Démarrer ontap_mediator:

```
[rootmediator-host ~]# systemctl start ontap_mediator  
[rootmediator-host ~]#
```

7. Reconnectez tous les clusters ONTAP à ONTAP Mediator mis à niveau :

MetroCluster sur IP

```
siteA::> metrocluster configuration-settings mediator show  
Mediator IP      Port      Node      Configuration  
Connection  
  
-----  
-----  
172.31.40.122  
31784      siteA-node2      true      false  
           siteA-node1      true      false  
           siteB-node2      true      false  
           siteB-node2      true      false  
  
siteA::> metrocluster configuration-settings mediator remove  
Removing the mediator and disabling Automatic Unplanned Switchover. It  
may take a few minutes to complete.  
Please enter the username for the mediator: mediatoradmin  
Please enter the password for the mediator:  
Confirm the mediator password:  
Automatic Unplanned Switchover is disabled for all nodes...
```

Removing mediator mailboxes...
Successfully removed the mediator.

```
siteA::> metrocluster configuration-settings mediator add -mediator  
-address 172.31.40.122
```

Adding the mediator and enabling Automatic Unplanned Switchover. It may take a few minutes to complete.

Please enter the username for the mediator: mediatoradmin

Please enter the password for the mediator:

Confirm the mediator password:

Successfully added the mediator.

```
siteA::> metrocluster configuration-settings mediator show
```

Mediator IP	Port	Node	Configuration	Status	Status
172.31.40.122	31784	siteA-node2	true	true	
		siteA-node1	true	true	
		siteB-node2	true	true	
		siteB-node2	true	true	

```
siteA::>
```

SnapMirror active sync

Pour SnapMirror active sync, vous n'avez pas besoin de réinstaller les certificats TLS stockés en dehors de /opt/netapp. Sauvegardez et restaurez les certificats stockés dans /opt/netapp.

```
peer1::> snapmirror mediator show
```

Mediator Address	Peer Cluster	Connection Status	Quorum Status
172.31.49.237	peer2	unreachable	true

```
peer1::> snapmirror mediator remove -mediator-address 172.31.49.237  
-peer-cluster peer2
```

Info: [Job 39] 'mediator remove' job queued

```
peer1::> job show -id 39
```

Job ID	Name	Owning Vserver	Node	State
39	mediator remove	peer1	peer1-node1	Success

Description: Removing entry in mediator

```

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver      Serial Number      Certificate Name      Type
-----
peer1
4A790360081F41145E14C5D7CE721DC6C210007F
ONTAPMediatorCA      server-
ca
Certificate Authority: ONTAP Mediator CA
Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer

```

```
-cluster peer2 -username mediatoradmin
```

Notice: Enter the mediator password.

Enter the password:

Enter the password again:

Info: [Job: 43] 'mediator add' job queued

```
peer1::> job show -id 43
```

Job	ID	Name	Owning Vserver	Node	State
43		mediator add	peer1	peer1-node2	Success
		Description: Creating a mediator entry			

```
peer1::> snapmirror mediator show
```

Mediator	Address	Peer	Cluster	Connection	Status	Quorum	Status
172.31.49.237		peer2		connected		true	

```
peer1::>
```

Informations connexes

- ["security certificate delete"](#)
- ["installation du certificat de sécurité"](#)
- ["security certificate show"](#)
- ["snapmirror mediator add"](#)
- ["snapmirror mediator remove"](#)
- ["storage iscsi-initiator show"](#)

Configurer les attributs de ONTAP Mediator

Vous pouvez configurer les attributs côté hôte de ONTAP Mediator, y compris les paramètres liés aux certificats et les remplacements de configuration.

Paramètres configurables du médiateur ONTAP

ONTAP Mediator prend en charge plusieurs paramètres configurables. Les valeurs par défaut de ces paramètres sont fournies dans un `low_space_threshold_mib`: 10 fichier en lecture seule. Le fichier se trouve à l'emplacement suivant :

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

Toutes les valeurs placées dans le `ontap_mediator.user_config.yaml` remplaceront les valeurs par défaut et seront conservées lors de toutes les mises à niveau d'ONTAP Mediator.

Après avoir modifié `ontap_mediator.user_config.yaml`, redémarrez ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Les attributs du médiateur ONTAP décrits dans cette section peuvent être modifiés si nécessaire.



Les autres valeurs par défaut dans le `ontap_mediator.config.yaml` ne doivent pas être modifiées, car les valeurs modifiées ne sont pas conservées lors des mises à niveau d'ONTAP Mediator.

Vous modifiez les attributs de ONTAP Mediator en copiant les variables requises dans le fichier `ontap_mediator.user_config.yaml` afin de remplacer les paramètres par défaut.

Installer des certificats SSL tiers

Vous pouvez remplacer les certificats auto-signés par défaut par des certificats SSL tiers en modifiant les fichiers de configuration de ONTAP Mediator.

Pour remplacer les certificats auto-signés par défaut par des certificats SSL tiers, vous devez modifier certains attributs dans les fichiers suivants :

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

Les variables contenues dans ces fichiers servent à contrôler les fichiers de certificats utilisés par ONTAP Mediator.

ONTAP Mediator 1.9 et versions ultérieures

Les variables par défaut répertoriées dans le tableau suivant sont incluses dans le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` fichier.

Variable	Chemin
<code>cert_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt</code>
<code>key_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key</code>
<code>ca_cert_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt</code>

Variable	Chemin
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_valid_days	1095
x509_passin_pwd	pass:ontap

- cert_valid_days sert à définir la durée de validité des certificats clients. La valeur maximale est de trois ans (1095 jours).
- x509_passin_pwd est la phrase de passe du certificat client signé.

Les variables par défaut répertoriées dans le tableau suivant sont incluses dans le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Variable	Chemin
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/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

ONTAP Mediator 1.8 et versions antérieures

Les variables par défaut répertoriées dans le tableau suivant sont incluses dans le `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` fichier.

Variable	Chemin
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

Variable	Chemin
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- cert_valid_days sert à définir la durée de validité des certificats clients. La valeur maximale est de trois ans (1095 jours).
- x509_passin_pwd est la phrase de passe du certificat client signé.

Les variables par défaut répertoriées dans le tableau suivant sont incluses dans le `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` fichier.

Variable	Chemin
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/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

Si vous modifiez ces attributs, redémarrez ONTAP Mediator pour appliquer les modifications. Pour obtenir des instructions détaillées sur la façon de remplacer les certificats par défaut par des certificats tiers, consultez ["Remplacez les certificats auto-signés par des certificats tiers de confiance"](#).

Configurer la protection contre les attaques par mot de passe

Les paramètres suivants offrent une protection contre les attaques par force brute visant à deviner les mots de passe.

Pour activer cette fonctionnalité, définissez une valeur pour `window_seconds` et `retry_limit`.

Exemples :

- Accordez une fenêtre de 5 minutes pour les tentatives, puis réinitialisez le compteur des échecs à zéro :

```
authentication_lock_window_seconds: 300
```

- Bloquez le compte si cinq échecs se produisent dans la période définie:

```
authentication_retry_limit: 5
```

- Réduisez l'impact des attaques de devinette de mots de passe par force brute en instaurant un délai avant le rejet de chaque tentative, ce qui ralentit les attaques.

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0    # seconds (float) to delay
```

```
failed_auth_attempts_prior_to_response, 0 = no delay
authentication_lock_window_seconds: null # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null # number of retries to allow
before locking API access, null = unlimited
```

Configurer les règles de complexité des mots de passe

Les champs suivants contrôlent les règles de complexité du mot de passe du compte utilisateur de l'API ONTAP Mediator.

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0 # min. uppercase characters

password_lowercase_chars: 1 # min. lowercase character

password_special_chars: 1 # min. non-letter, non-digit

password_nonletter_chars: 2 # min. non-letter characters (digits,
specials, anything)
```

Configurez les paramètres d'espace disque et d'espace de journalisation pour ONTAP Mediator, y compris le seuil d'espace libre et l'espace de journalisation réservé.

Configurer le seuil d'espace libre

Il existe des paramètres permettant de contrôler l'espace libre requis sur le `/opt/netapp/lib/ontap_mediator` disque.

Si l'espace est inférieur au seuil défini, le service émet un événement d'avertissement.

```
low_space_threshold_mib: 10
```

Configurer l'espace de journalisation réservé

Cette `RESERVE_LOG_SPACE` fonctionnalité est contrôlée par des paramètres spécifiques. Par défaut, l'installation de ONTAP Mediator crée un espace disque distinct pour les journaux. Le programme d'installation crée un nouveau fichier de taille fixe avec un total de 700MB d'espace disque destiné explicitement à la journalisation de ONTAP Mediator.

Pour désactiver cette fonctionnalité et utiliser l'espace disque par défaut, procédez comme suit :

1. Modifiez la valeur de `RESERVE_LOG_SPACE` de 1 à 0 dans le fichier suivant :

```
/opt/netapp/lib/ontap_mediator/tools/mediator_env
```

a. Exécutez la commande suivante :

```
cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep  
"RESERVE_LOG_SPACE"
```

```
RESERVE_LOG_SPACE=0
```

b. Redémarrer ONTAP Mediator :

```
systemctl restart ontap_mediator
```

Pour réactiver la fonctionnalité, modifiez la valeur de 0 à 1 et redémarrez le Mediator.



Le passage d'un espace disque à un autre ne supprime pas les journaux existants. Tous les journaux précédents sont sauvegardés puis déplacés vers l'espace disque actuel après le basculement et le redémarrage du Mediator.

Modifier le nom d'utilisateur et le mot de passe du médiateur ONTAP

Modifiez le nom d'utilisateur ou le mot de passe de ONTAP Mediator depuis l'hôte Linux sur lequel ONTAP Mediator est installé.

Changer le nom d'utilisateur

Vous pouvez modifier le nom d'utilisateur en suivant la procédure suivante.

À propos de cette tâche

Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.

Si vous ne parvenez pas à exécuter cette commande, vous devrez peut-être l'exécuter en utilisant le chemin complet comme indiqué dans l'exemple suivant :

```
/usr/local/bin/mediator_username
```

Étapes

Modifiez votre nom d'utilisateur en choisissant l'une des options suivantes :

- **Option (a)** : Exécutez la commande `mediator_change_user` et répondez aux invites comme indiqué dans l'exemple suivant :

```
[root@mediator-host ~]# mediator_change_user  
Modify the Mediator API username by entering the following values:
```

```
Mediator API User Name: mediatoradmin
Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- **Option (b):** Exécutez la commande suivante:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

Changer le mot de passe

Vous pouvez modifier le mot de passe en suivant la procédure ci-dessous.

À propos de cette tâche

Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.

Si vous ne parvenez pas à exécuter cette commande, vous devrez peut-être l'exécuter en utilisant le chemin complet comme indiqué dans l'exemple suivant :

```
/usr/local/bin/mediator_change_password
```

Étapes

Modifiez le mot de passe en choisissant l'une des options suivantes :

- **Option (a):** Exécutez la `mediator_change_password` commande et répondez aux invites comme indiqué dans l'exemple suivant :

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
Mediator API User Name: mediatoradmin
Old Password:
New Password:
Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- **Option (b):** Exécutez la commande suivante:

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1  
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

L'exemple montre que le mot de passe est modifié de « mediator1 » à « mediator2 ».

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin  
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2  
mediator_change_password  
The password has been updated successfully.  
[root@mediator-host ~]#
```

Démarrer et arrêter ONTAP Mediator

Arrêtez ou redémarrez ONTAP Mediator et SCST lorsque vous devez effectuer la maintenance de l'hôte ou réactiver le service.

Arrêtez ONTAP Mediator

Pour arrêter ONTAP Mediator, procédez comme suit :

Étapes

1. Arrêter ONTAP Mediator:

```
systemctl stop ontap_mediator
```

2. Arrêter SCST:

```
systemctl stop mediator-scst
```

3. Désactiver ONTAP Mediator et SCST:

```
systemctl disable ontap_mediator mediator-scst
```

Démarrer ONTAP Mediator

Pour réactiver ONTAP Mediator, procédez comme suit :

Étapes

1. Activez ONTAP Mediator et SCST:

```
systemctl enable ontap_mediator mediator-scst
```

2. Démarrer SCST:

```
systemctl start mediator-scst
```

3. Démarrer ONTAP Mediator :

```
systemctl start ontap_mediator
```

Vérifier l'état de santé de ONTAP Mediator

Vérifiez qu'ONTAP Mediator fonctionne normalement.

Vérifiez l'état du service

Étapes

1. Consultez l'état d'ONTAP Mediator :

a. Exécutez la commande suivante :

```
systemctl status ontap_mediator
```

```
[root@mediator_host ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
└─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
```

```
[root@mediator_host ~]#
```

b. Consultez l'état du service SCST:



Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le package SCST n'est pas installé et vous pouvez ignorer cette tâche.

```
systemctl status mediator-scst
```

+

```
[root@mediator_host ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service; enabled;
 vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1 weeks 0
 days ago
     Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
 status=0/SUCCESS)
    Main PID: 286662 (iscsi-scstd)
         Tasks: 1 (limit: 49473)
        Memory: 1.2M
         CGroup: /system.slice/mediator-scst.service
                 └─286662 /usr/local/sbin/iscsi-scstd

[root@mediator_host ~]#
```

Vérifiez les ports d'écoute

1. Veuillez confirmer les ports utilisés par ONTAP Mediator :

```
netstat -anlt | grep -E '3260|31784'
```

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

tcp        0      0 0.0.0.0:31784      0.0.0.0:*        LISTEN
tcp        0      0 0.0.0.0:3260      0.0.0.0:*        LISTEN
tcp6       0      0 :::3260          :::*             LISTEN
```

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.

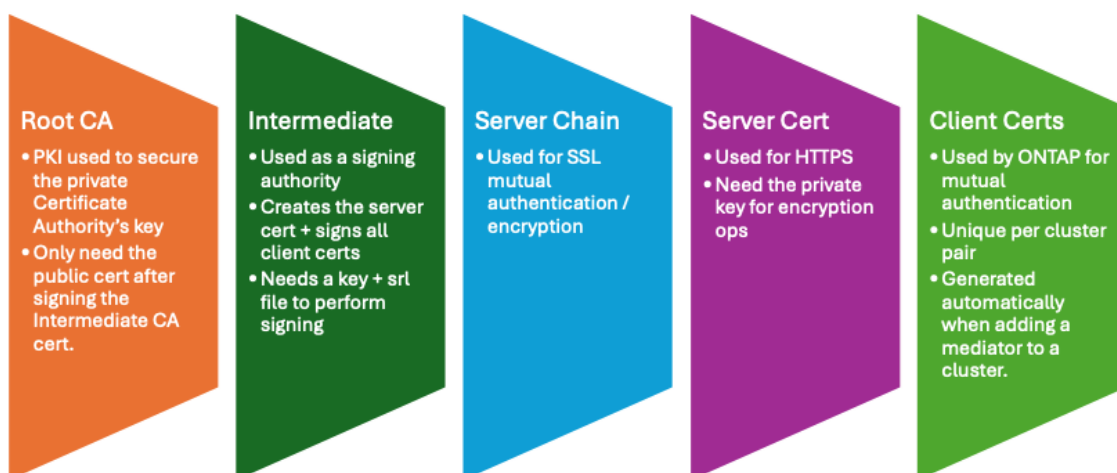


- Les certificats tiers ne sont pris en charge qu'à partir d'ONTAP 9.16.1 et dans certaines versions correctives antérieures d'ONTAP. Voir "[NetApp Identifiant du bogue Bugs Online CONTAP-243278](#)".
- Les certificats tiers ne sont pris en charge que sur les systèmes exécutant ONTAP Mediator 1.7 ou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

À propos de cette tâche

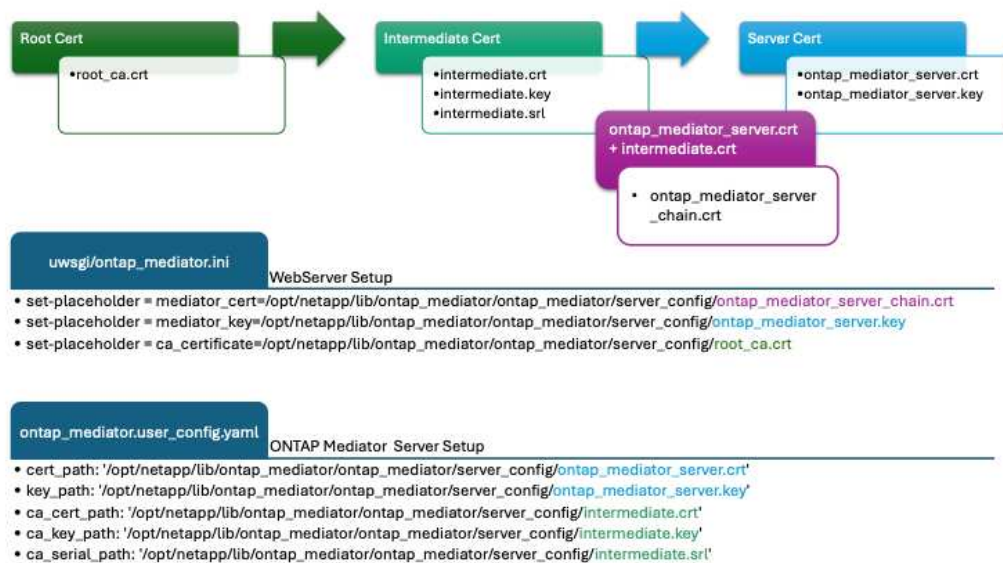
- Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.
- Vous pouvez effectuer cette opération si les certificats auto-signés générés doivent être remplacés par des certificats obtenus auprès d'une autorité de certification (CA) subordonnée de confiance. Pour ce faire, 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/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/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.
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_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/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.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/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.crt
```

```
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

```
[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 auprès 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"`.

Maintenir le système d'exploitation hôte pour ONTAP Mediator

Assurez-vous que le système d'exploitation hôte de ONTAP Mediator bénéficie d'une maintenance régulière afin d'obtenir des performances optimales.

Redémarrez l'hôte

Redémarrez l'hôte uniquement lorsque les clusters sont opérationnels. Les clusters ne peuvent pas réagir aux pannes lorsque ONTAP Mediator est hors ligne. Planifiez une maintenance avant de redémarrer.

ONTAP Mediator reprend automatiquement son activité lors d'un redémarrage et rétablit les relations précédemment configurées avec les clusters ONTAP.

Mises à jour du package hôte

Mettez à jour toute bibliothèque ou tout paquet yum, à l'exception du noyau. Redémarrez l'hôte si nécessaire pour que les modifications prennent effet. Planifiez une fenêtre de maintenance avant de redémarrer l'hôte.

Si vous installez le `yum-utils` paquet, utilisez la `needs-restarting` commande pour détecter si des modifications apportées au paquet nécessitent un redémarrage.

Redémarrez après la mise à jour des dépendances d'ONTAP Mediator, car les modifications ne prennent pas effet immédiatement.

Mettre à niveau le noyau du système d'exploitation hôte

SCST doit être compilé pour le noyau que vous utilisez. Pour mettre à jour le système d'exploitation, vous devez planifier du temps pour la maintenance.

Avant de commencer

Les exigences suivantes s'appliquent lorsque le package SCST est installé avec ONTAP Mediator.

- Vous pouvez mettre à jour tous les paquets de bibliothèque, à l'exception du noyau, mais un redémarrage peut être nécessaire pour appliquer les modifications dans ONTAP Mediator. Prévoyez une interruption si vous devez redémarrer.
- Il est recommandé de maintenir le noyau du système d'exploitation à jour. Mettez à niveau le noyau vers une version prise en charge répertoriée dans "[Matrice des versions d'ONTAP Mediator](#)". Un redémarrage du système est nécessaire ; prévoyez donc une interruption de service pour la maintenance.
 - Désinstallez le module du noyau SCST avant de redémarrer, puis réinstallez-le après le redémarrage.
 - Préparez une version compatible de SCST à réinstaller avant de commencer la mise à niveau du noyau du système d'exploitation.



Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le paquet SCST n'est pas installé et le noyau du système d'exploitation hôte peut être mis à niveau sans incidence sur ONTAP Mediator. Consultez la documentation de votre système d'exploitation hôte pour obtenir les instructions de mise à niveau.

Étapes

Suivez ces étapes pour mettre à niveau le noyau du système d'exploitation hôte.



Avant de mettre à niveau le noyau, vérifiez que le système d'exploitation et la version d'ONTAP Mediator sont compatibles. Pour connaître les versions prises en charge, consultez le "[Matrice de prise en charge des systèmes d'exploitation](#)".

1. Arrêtez ONTAP Mediator.
2. Désinstallez le package SCST, voir [Effectuer la maintenance de l'hôte](#). (SCST ne propose pas de mécanisme de mise à niveau.)
3. Mettez à jour le système d'exploitation, puis redémarrez.
4. Réinstallez le package SCST.
5. Réactivez ONTAP Mediator.

Effectuer la maintenance de l'hôte

La mise à jour du noyau de la machine virtuelle peut entraîner des problèmes de compatibilité avec les modules SCST. Désinstallez puis réinstallez SCST manuellement.



Si vous avez installé ONTAP Mediator 1.12 ou une version ultérieure prenant uniquement en charge HTTPS, le package SCST n'est pas installé et vous pouvez ignorer cette tâche.

Étape 1 : Désinstaller SCST

Pour désinstaller SCST, utilisez l'archive tar correspondant à votre version d'ONTAP Mediator.

Étapes

1. Téléchargez le paquet SCST approprié (comme indiqué dans le tableau suivant) et extrayez-le.

Pour cette version ...	Utilisez ce bundle tar...
ONTAP Mediator 1.12.1	scst-3.10.tar.gz
ONTAP Mediator 1.12	scst-3.10.tar.gz
ONTAP Mediator 1.11	scst-3.9.tar.gz
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

- a. Accédez au package open source depuis le "[Téléchargements SCST sur sourceforge](#)".

- b. Sélectionnez **Télécharger les versions publiées**.
 - c. Extrayez l'archive sur votre VM.
2. Exécutez les commandes de désinstallation suivantes dans le `scst` répertoire :
 - a. `systemctl stop mediator-scst`
 - b. `make scstadm_uninstall`
 - c. `make iscsi_uninstall`
 - d. `make usr_uninstall`
 - e. `make scst_uninstall`
 - f. `depmod`

Étape 2 : Installer SCST

Pour installer manuellement SCST, vous avez besoin du paquet tar SCST utilisé pour la version installée d'ONTAP Mediator (voir le [Table SCST](#)).

À propos de cette tâche

- Effectuez cette étape avant d'installer ONTAP Mediator. Si la version de SCST que vous utilisez est plus récente que la version fournie avec le programme d'installation de ONTAP Mediator, celui-ci ignore cette étape.
- Dans certains scénarios, l'installation par défaut de SCST sur le système d'exploitation mis à niveau peut échouer car le système d'exploitation mis à niveau nécessite un correctif.

À partir d'ONTAP Mediator 1.12.1, si l'installation échoue, vous pouvez utiliser l'outil de réparation SCST situé dans `/usr/local/bin/mediator_repair_scst` pour réparer l'installation.

Si le système d'exploitation mis à niveau nécessite un correctif, l'outil le contient pour la version de SCST fournie avec le package ONTAP Mediator. L'`mediator_repair_scst` outil est un outil autonome distinct du programme d'installation principal et est inclus dans le fichier ONTAP Mediator `.tgz`. Il n'affecte pas l'installation ni les chemins de mise à niveau d'ONTAP Mediator.

Étapes

1. Exécutez les commandes d'installation suivantes dans le `scst` répertoire:
 - a. `make 2release`
 - b. `make scst_install`
 - c. `make usr_install`
 - d. `make iscsi_install`
 - e. `make scstadm_install`
 - f. `depmod`



Si vous effectuez une première installation et souhaitez préinstaller ONTAP Mediator, exécutez la commande suivante avant de passer à l'étape suivante :

```
mkdir -p
```

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

g. `cp scst/src/certs/scst_module_key.der`

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
```

h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`



Si vous préinstallez SCST avant ONTAP Mediator lors d'une première installation, ignorez cette étape. Le programme d'installation applique les correctifs SCST nécessaires.

2. Si vous le souhaitez, si le démarrage sécurisé est activé, avant de redémarrer, effectuez les étapes suivantes :

a. Déterminez le nom de chaque fichier pour les modules `scst_vdisk`, `scst` et `iscsi_scst` :

```
[root@localhost ~]# modinfo -n scst_vdisk
[root@localhost ~]# modinfo -n scst
[root@localhost ~]# modinfo -n iscsi_scst
```

b. Déterminez la version du noyau :

```
[root@localhost ~]# uname -r
```

c. Signez chaque fichier de module avec le noyau:

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

d. Installez la clé UEFI avec le micrologiciel.

Les instructions pour installer la clé UEFI se trouvent à l'adresse suivante :

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

La clé UEFI générée se trouve à l'emplacement suivant :

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. Redémarrez le système :

Modifications du nom d'hôte ou de l'adresse IP de l'hôte

À propos de cette tâche

- Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.
- Ne faites cela que si les certificats auto-signés ne sont plus valides parce que le nom d'hôte ou l'adresse IP changent après l'installation de ONTAP Mediator.
- Une fois le certificat temporaire auto-signé remplacé par un certificat tiers de confiance, vous ne devez *pas* utiliser cette tâche pour régénérer un certificat. Si vous ne possédez pas de certificat auto-signé, vous ne pouvez pas utiliser cette procédure.

Étape

Créez un certificat auto-signé temporaire pour l'hôte actuel :

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
```

```
[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

Désinstaller ONTAP Mediator

Si nécessaire, désinstallez ONTAP Mediator après l'avoir déconnecté d'ONTAP.

Avant de commencer

Vous devez déconnecter ONTAP Mediator d'ONTAP avant de le supprimer.

À propos de cette tâche

Effectuez cette tâche sur l'hôte Linux sur lequel vous avez installé ONTAP Mediator.

Si vous ne parvenez pas à exécuter cette commande, vous devrez peut-être l'exécuter en utilisant le chemin complet comme indiqué dans l'exemple suivant :

```
/usr/local/bin/uninstall_ontap_mediator
```

Étape

1. Désinstaller ONTAP Mediator :

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator

ONTAP Mediator: Self Extracting Uninstaller

+ Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
+ Remove successful.
[root@mediator-host ~]#
```

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.