



Administrar ONTAP Mediator

ONTAP Mediator

NetApp
October 19, 2026

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

Tabla de contenidos

Administrar ONTAP Mediator	1
Actualizar ONTAP Mediator	1
Actualizar ONTAP Mediator	1
Actualizar el sistema operativo host y reinstalar o actualizar ONTAP Mediator	9
Configurar los atributos de ONTAP Mediator	14
Parámetros configurables de ONTAP Mediator	14
Instalar certificados SSL de terceros	15
Configurar la protección contra ataques a la contraseña	17
Configurar las reglas de complejidad de las contraseñas	17
Configurar el umbral de espacio libre	18
Configura el espacio reservado para los registros	18
Cambiar el nombre de usuario y la contraseña de ONTAP Mediator	19
Cambiar el nombre de usuario	19
Cambiar la contraseña	20
Iniciar y detener ONTAP Mediator	21
Detener ONTAP Mediator	21
Iniciar ONTAP Mediator	21
Comprobar el estado de ONTAP Mediator	22
Comprueba el estado del servicio	22
Confirma los puertos de escucha	23
Gestiona certificados	23
Regenerar un certificado temporal autofirmado para el host de ONTAP Mediator	23
Sustituir los certificados autofirmados de ONTAP Mediator por certificados de terceros de confianza ..	24
Solucionar problemas relacionados con los certificados de ONTAP Mediator	39
Mantenimiento del sistema operativo del host para ONTAP Mediator	44
Reinicia el host	45
Actualizaciones del paquete del host	45
Actualiza el núcleo del sistema operativo del host	45
Realiza el mantenimiento del host	46
Cambios en el nombre de host o la dirección IP	48
Desinstalar ONTAP Mediator	49

Administrar ONTAP Mediator

Actualizar ONTAP Mediator

Actualizar ONTAP Mediator

Para actualizar ONTAP Mediator a una versión más reciente sin actualizar el sistema operativo del host, descarga el paquete de instalación de la nueva versión y ejecuta el instalador en el host en el que ya está instalado ONTAP Mediator.



Si necesitas actualizar el sistema operativo del host a una nueva versión y reinstalar o actualizar ONTAP Mediator como parte de ese proceso, consulta ["Actualizar el SO host y ONTAP Mediator"](#) en su lugar.

Antes de empezar

- Comprueba que tu host cumpla los requisitos previos descritos en ["Prepárate para instalar ONTAP Mediator"](#), incluidos los requisitos del host, el firewall y el sistema operativo.
- Descarga el paquete de instalación de la nueva versión. Consulta ["Descarga el paquete de instalación de ONTAP Mediator"](#).
- NetApp recomienda verificar la firma digital del nuevo paquete de instalación. Consulta ["Comprueba la firma digital del paquete de instalación de ONTAP Mediator"](#).

Acerca de esta tarea

Revisa la siguiente información antes de actualizar ONTAP Mediator.

- Deberías actualizar ONTAP Mediator a la última versión. Las versiones anteriores siguen funcionando con todas las versiones de ONTAP, pero las más recientes incluyen parches de seguridad para componentes de terceros.
- Cuando actualizas a una nueva versión de ONTAP Mediator que incluye el paquete SCST, el instalador actualiza automáticamente a la versión recomendada de SCST, a menos que haya disponible una versión superior. Para instrucciones sobre cómo instalar manualmente una versión superior de SCST, consulta ["Mantenimiento del sistema operativo del host para ONTAP Mediator"](#). Para las versiones compatibles, consulta el ["Matriz de compatibilidad de SCST"](#).



- Si la actualización falla, puede que tengas que probar una versión más reciente de ONTAP Mediator.
- A partir del 15 de junio de 2025, no puedes instalar ni actualizar ONTAP Mediator 1.9 y 1.8 porque sus certificados de firma de código han caducado. Si la actualización falla, usa en su lugar la versión de parche ONTAP Mediator 1.9.1.
- A partir de ONTAP 9.19.1 y ONTAP Mediator 1.12, tienes la opción de instalar ONTAP Mediator con compatibilidad con iSCSI y HTTPS, o compatibilidad solo con HTTPS. Si eliges instalar ONTAP Mediator con compatibilidad solo con HTTPS, el paquete SCST no se instala.
- Si actualizas desde ONTAP Mediator 1.11 o anterior con SCST instalado y eliges la opción solo HTTPS durante la actualización, el paquete SCST se desinstala y la nueva versión de ONTAP Mediator no contiene el paquete SCST.
- Si tienes previsto utilizar ONTAP Mediator para supervisar varias configuraciones de IP de MetroCluster, la compatibilidad depende de tu tipo de Mediator, la versión de ONTAP y el sistema operativo. Consulta

"Utiliza ONTAP Mediator para supervisar varias configuraciones de MetroCluster IP" para obtener más información.

- La instalación de ONTAP Mediator con soporte solo para HTTPS es compatible con los siguientes casos de uso:
 - Tienes previsto utilizar ONTAP Mediator únicamente para supervisar tus clústeres de sincronización activa de SnapMirror.
 - Tienes pensado configurar ONTAP Mediator con HTTPS para supervisar una o varias configuraciones de IP de MetroCluster.
- ONTAP Mediator debe estar instalado con soporte para iSCSI y HTTPS en el siguiente escenario:
 - Tienes previsto configurar ONTAP Mediator con iSCSI para supervisar una o varias configuraciones IP de MetroCluster.
- Al ejecutar el instalador en una instalación existente de ONTAP Mediator, este detecta la versión actual y te pide que confirmes la actualización:

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

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

- Como parte de la actualización, el instalador crea un paquete de soporte con la configuración previa a la actualización y migra la base de datos antes de actualizar el software ONTAP Mediator.
- En los casos de uso de automatización, puedes usar el comando `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 -y` para saltarte las indicaciones del instalador.

Pasos

1. Ejecuta el instalador de la nueva versión y sigue las instrucciones que te vayan apareciendo:

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



Para omitir la comprobación de la firma durante la actualización, utiliza el comando `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 --skip-code-signature -check`

El instalador detecta la instalación existente y te pide que actualices, luego instala los paquetes necesarios y migra tu configuración.

▼ Ejemplo de actualización de ONTAP Mediator con HTTPS y soporte iSCSI (salida de consola)

```
[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 polycoreutils-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 ~]#

▼ Ejemplo de actualización de ONTAP Mediator con soporte solo para HTTPS (salida de consola)

```
[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 polycoreutils-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 ~]#
```

Actualizar el sistema operativo host y reinstalar o actualizar ONTAP Mediator

Para actualizar el sistema operativo host de ONTAP Mediator con SCST instalado a una versión posterior, debes desinstalar ONTAP Mediator. Después de la actualización del sistema operativo, puedes reinstalar tu versión actual de ONTAP Mediator o actualizar a una versión más reciente.

Acerca de esta tarea

- Esta tarea se aplica a las versiones de ONTAP Mediator con SCST instalado. Si instalaste ONTAP Mediator 1.12 o posterior con soporte solo para HTTPS, el paquete SCST no está instalado y puedes actualizar el sistema operativo host sin afectar a ONTAP Mediator. Consulta la documentación del proveedor del sistema operativo host para ver las instrucciones de actualización del sistema operativo.
- Si solo necesitas actualizar el kernel del sistema operativo del host a una versión compatible sin pasar a una nueva versión del sistema operativo, consulta ["Mantenimiento del sistema operativo del host para ONTAP Mediator"](#) en su lugar.
- Antes de actualizar el sistema operativo del host para ONTAP Mediator con la herramienta leapp-upgrade, ["desinstalar ONTAP Mediator"](#). La herramienta comprueba si hay nuevas versiones de RPM en los repositorios registrados.
- El instalador de ONTAP Mediator instala un archivo .rpm, que la herramienta leapp-upgrade incluye en la búsqueda. Dado que el instalador descomprime el archivo en lugar de descargarlo de un repositorio registrado, la herramienta no puede encontrar una actualización. Debes utilizar la herramienta leapp-upgrade para desinstalar el paquete.

Pasos

1. Haz una copia de seguridad de los archivos de registro:

```
[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. Realiza la actualización con la herramienta 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. Vuelve a instalar ONTAP Mediator:



Realiza el resto de los pasos inmediatamente después de reinstalar ONTAP Mediator para evitar la pérdida de los archivos de registro.

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

ONTAP Mediator: Self Extracting Installer

..<snip installation>..
[rootmediator-host ~]#
```

4. Detén ontap_mediator:

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

5. Sustituye los archivos de registro:

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

6. Inicia ontap_mediator:

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

7. Vuelve a conectar todos los clústeres de ONTAP al ONTAP Mediator actualizado:

MetroCluster sobre IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
Status      Status
-----
-----
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
Connection
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

Para la sincronización activa de SnapMirror, no necesitas reinstalar los certificados TLS almacenados fuera de /opt/netapp. Haz una copia de seguridad y restaura los certificados almacenados en /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      Owing
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

```

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

....

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

....

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::>
```

Información relacionada

- ["security certificate delete"](#)
- ["instalación de certificado de seguridad"](#)
- ["security certificate show"](#)
- ["snapmirror mediator add"](#)
- ["snapmirror mediator remove"](#)
- ["storage iscsi-initiator show"](#)

Configurar los atributos de ONTAP Mediator

Puedes configurar los atributos del lado del host de ONTAP Mediator, incluidas las opciones relacionadas con los certificados y las anulaciones de configuración.

Parámetros configurables de ONTAP Mediator

ONTAP Mediator admite varios parámetros configurables. Los valores predeterminados de estos parámetros se proporcionan en un archivo `low_space_threshold_mib: 10` de solo lectura. El archivo se encuentra en:

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

Todos los valores que se introduzcan en el `ontap_mediator.user_config.yaml` anularán los valores predeterminados y se mantendrán en todas las actualizaciones de ONTAP Mediator.

Después de modificar `ontap_mediator.user_config.yaml`, reinicia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Los atributos de ONTAP Mediator descritos en esta sección se pueden modificar si es necesario.



No debes cambiar los demás valores predeterminados del `ontap_mediator.config.yaml` porque los valores modificados no se conservan durante las actualizaciones de ONTAP Mediator.

Modifica los atributos de ONTAP Mediator copiando las variables necesarias en el archivo `ontap_mediator.user_config.yaml` para anular la configuración predeterminada.

Instalar certificados SSL de terceros

Puedes sustituir los certificados autofirmados predeterminados por certificados SSL de terceros modificando los archivos de configuración de ONTAP Mediator.

Para sustituir los certificados autofirmados predeterminados por certificados SSL de terceros, modifica determinados atributos en los siguientes archivos:

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

Las variables de estos archivos sirven para controlar los archivos de certificados que utiliza ONTAP Mediator.

ONTAP Mediator 1.9 y versiones posteriores

Las variables predeterminadas que figuran en la siguiente tabla están incluidas en el archivo `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`.

Variable	Ruta
<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>
<code>ca_key_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key</code>
<code>ca_serial_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl</code>
<code>cert_valid_days</code>	1095
<code>x509_passin_pwd</code>	pass:ontap

- `cert_valid_days` se utiliza para establecer la fecha de caducidad de los certificados de cliente. El valor máximo es de tres años (1095 días).
- `x509_passin_pwd` es la frase de contraseña del certificado de cliente firmado.

Las variables predeterminadas que figuran en la siguiente tabla están incluidas en el archivo `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`.

Variable	Ruta
<code>mediator_cert</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt</code>
<code>mediator_key</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>

ONTAP Mediator 1.8 y versiones anteriores

Las variables predeterminadas que figuran en la siguiente tabla están incluidas en el archivo `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`.

Variable	Ruta
<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/ca.crt</code>
<code>ca_key_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key</code>
<code>ca_serial_path</code>	<code>/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl</code>
<code>cert_valid_days</code>	1095
<code>x509_passin_pwd</code>	<code>pass:ontap</code>

- `cert_valid_days` se utiliza para establecer la fecha de caducidad de los certificados de cliente. El valor máximo es de tres años (1095 días).
- `x509_passin_pwd` es la frase de contraseña del certificado de cliente firmado.

Las variables predeterminadas que figuran en la siguiente tabla están incluidas en el archivo `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`.

Variable	Ruta
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 modificas estos atributos, reinicia ONTAP Mediator para aplicar los cambios. Para obtener instrucciones detalladas sobre cómo sustituir los certificados predeterminados por certificados de terceros, consulta ["Sustituir los certificados autofirmados por certificados de terceros de confianza"](#).

Configurar la protección contra ataques a la contraseña

Los siguientes ajustes ofrecen protección contra ataques de adivinación de contraseñas por fuerza bruta.

Para activar la función, asigna un valor a `window_seconds` y a `retry_limit`.

Ejemplos:

- Da un margen de 5 minutos para que se hagan conjeturas y luego restablece el recuento a cero fallos:

```
authentication_lock_window_seconds: 300
```

- Bloquea la cuenta si se producen cinco fallos dentro del plazo establecido:

```
authentication_retry_limit: 5
```

- Reduce el impacto de los ataques de fuerza bruta para adivinar contraseñas estableciendo un retraso que ocurre antes de rechazar cada intento, lo que ralentiza los ataques.

```
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
```

Configurar las reglas de complejidad de las contraseñas

Los siguientes campos controlan las reglas de complejidad de la contraseña de la cuenta de usuario de la API de 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)
```

Configura los parámetros de espacio en disco y de registro de ONTAP Mediator, incluidos el umbral de espacio libre y el espacio reservado para registros.

Configurar el umbral de espacio libre

Hay ajustes que controlan el espacio libre necesario en el `/opt/netapp/lib/ontap_mediator` disco.

Si el espacio es inferior al umbral establecido, el servicio emite un evento de advertencia.

```
low_space_threshold_mib: 10
```

Configura el espacio reservado para los registros

La función `RESERVE_LOG_SPACE` se controla mediante ajustes específicos. De forma predeterminada, la instalación de ONTAP Mediator crea un espacio en disco independiente para los registros. El instalador crea un nuevo archivo de tamaño fijo con un total de 700MB de espacio en disco para usarlo exclusivamente para el registro de ONTAP Mediator.

Para desactivar esta función y usar el espacio en disco predeterminado, realiza los siguientes pasos:

1. Cambia el valor de `RESERVE_LOG_SPACE` de 1 a 0 en el siguiente archivo:

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

- a. Ejecuta el siguiente comando:

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

```
RESERVE_LOG_SPACE=0
```

b. Reinicia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Para volver a activar la función, cambia el valor de 0 a 1 y reinicia Mediator.



Al cambiar de espacio en disco, no se eliminan los registros existentes. Todos los registros anteriores se respaldan y luego se mueven al espacio en disco actual después de cambiar y reiniciar el Mediator.

Cambiar el nombre de usuario y la contraseña de ONTAP Mediator

Cambia el nombre de usuario o la contraseña de ONTAP Mediator desde el host Linux en el que está instalado ONTAP Mediator.

Cambiar el nombre de usuario

Puedes cambiar el nombre de usuario usando el siguiente procedimiento.

Acerca de esta tarea

Realiza esta tarea en el host Linux en el que hayas instalado ONTAP Mediator.

Si no consigues ejecutar este comando, es posible que tengas que hacerlo utilizando la ruta completa, como se muestra en el siguiente ejemplo:

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

Pasos

Cambia el nombre de usuario eligiendo una de las siguientes opciones:

- **Opción (a):** Ejecuta el comando `mediator_change_user` y responde a las preguntas tal y como se muestra en el siguiente ejemplo:

```
[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 ~]#
```

- **Opción (b):** Ejecuta el siguiente comando:

```
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 ~]#
```

Cambiar la contraseña

Puedes cambiar la contraseña usando el siguiente procedimiento.

Acerca de esta tarea

Realiza esta tarea en el host Linux en el que hayas instalado ONTAP Mediator.

Si no consigues ejecutar este comando, es posible que tengas que hacerlo utilizando la ruta completa, como se muestra en el siguiente ejemplo:

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

Pasos

Cambia la contraseña eligiendo una de las siguientes opciones:

- **Opción (a):** Ejecuta el comando `mediator_change_password` y responde a las preguntas como se muestra en el siguiente ejemplo:

```
[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 ~]#
```

- **Opción (b):** Ejecuta el siguiente comando:

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

El ejemplo muestra que la contraseña se cambia de "mediator1" a "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 ~]#
```

Iniciar y detener ONTAP Mediator

Detén o reinicia ONTAP Mediator y SCST cuando necesites realizar tareas de mantenimiento en el host o volver a activar el servicio.

Detener ONTAP Mediator

Para detener ONTAP Mediator, sigue estos pasos:

Pasos

1. Detén ONTAP Mediator:

```
systemctl stop ontap_mediator
```

2. Detén SCST:

```
systemctl stop mediator-scst
```

3. Desactiva ONTAP Mediator y SCST:

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

Iniciar ONTAP Mediator

Para volver a activar ONTAP Mediator, sigue estos pasos:

Pasos

1. Habilitar ONTAP Mediator y SCST:

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

2. Inicia SCST:

```
systemctl start mediator-scst
```

3. Inicia ONTAP Mediator:

```
systemctl start ontap_mediator
```

Comprobar el estado de ONTAP Mediator

Comprueba que ONTAP Mediator funcione correctamente.

Comprueba el estado del servicio

Pasos

1. Ver el estado de ONTAP Mediator:

a. Ejecuta el siguiente comando:

```
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. Consulta el estado del servicio SCST:



Si instalaste ONTAP Mediator 1.12 o posterior con soporte solo para HTTPS, el paquete SCST no está instalado y puedes omitir esta tarea.

```
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 ~]#
```

Confirma los puertos de escucha

1. Comprueba los puertos que utiliza 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
```

Gestiona certificados

Regenerar un certificado temporal autofirmado para el host de ONTAP Mediator

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



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

Acerca de esta tarea

- Realiza esta tarea en el host Linux en el que hayas instalado ONTAP Mediator.
- Solo puedes realizar esta tarea si los certificados autofirmados generados han quedado obsoletos debido a cambios en el nombre de host o en la dirección IP del host después de instalar ONTAP Mediator.

- Una vez que el certificado autofirmado temporal haya sido sustituido por un certificado de confianza de un tercero, *no* utilices esta tarea para volver a generar un certificado. La ausencia de un certificado autofirmado provocará que este procedimiento falle.

Paso

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

1. Reinicia ONTAP Mediator:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

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

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



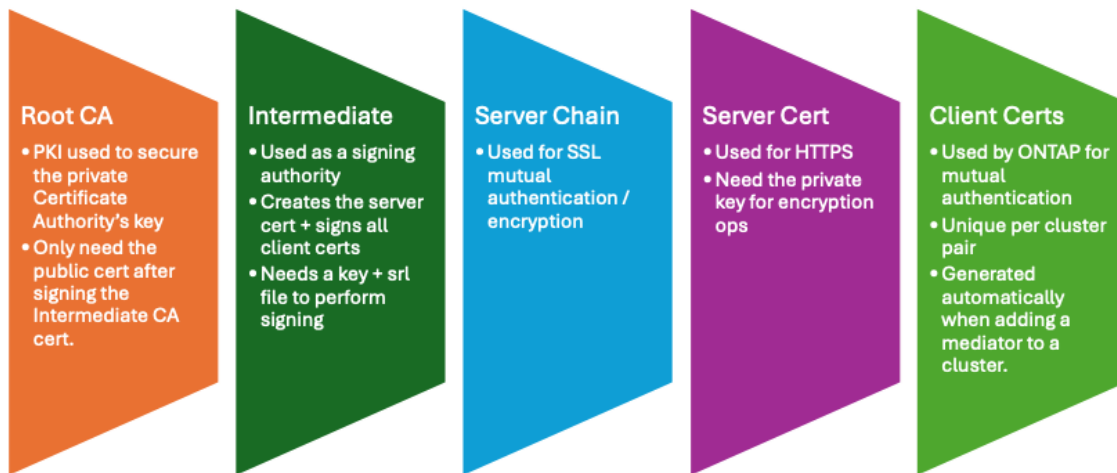
- Los certificados de terceros solo son compatibles a partir de ONTAP 9.16.1 y en algunas versiones de parche anteriores de ONTAP. Consulta ["ID de bug CONTAP-243278 de NetApp Bugs Online"](#).

- Los certificados de terceros solo son compatibles con sistemas que ejecutan ONTAP Mediator 1.7 o versiones posteriores.

Acerca de esta tarea

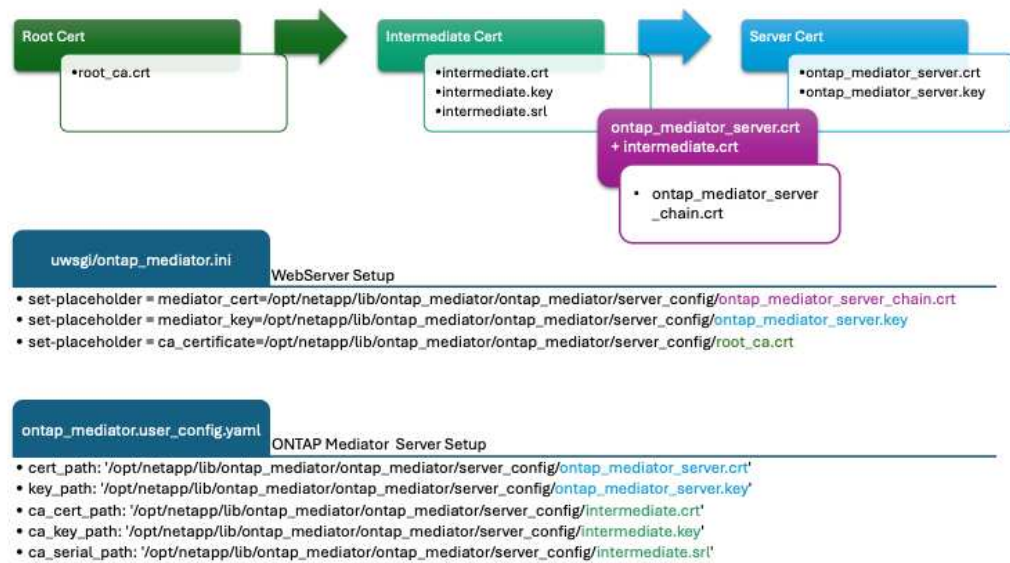
- Realiza esta tarea en el host Linux en el que hayas instalado ONTAP Mediator.
- Puedes realizar esta tarea si es necesario sustituir los certificados autofirmados generados por certificados obtenidos de una autoridad de certificación (CA) subordinada de confianza. Para ello, debes tener acceso a una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

ONTAP Mediator Certificate Purposes



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

ONTAP Mediator Certificates



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

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

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



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

ONTAP Mediator 1.9 y versiones posteriores

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

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

Ejemplo

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

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

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

Ejemplo:

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@mediator_host server_config]# openssl req -key
intermediate.key -new -config openssl_ca.cnf -out intermediate.csr
Enter pass phrase for intermediate.key:
[root@mediator_host server_config]# cat intermediate.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

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

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



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

ONTAP Mediator 1.8 y versiones anteriores

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

Ejemplo:

```
openssl genrsa -aes256 -out ca.key 4096
```
 - b. El archivo de configuración `openssl_ca.cnf` (ubicado en `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) define las propiedades que debe tener el certificado generado.
2. Utiliza la clave privada y el archivo de configuración para crear una solicitud de firma de certificado `ca.csr`:

Ejemplo:

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@mediator_host server_config]# openssl req -key ca.key -new
-config openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@mediator_host server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
```

-----END CERTIFICATE REQUEST-----

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

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



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

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

ONTAP Mediator 1.9 y versiones posteriores

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

Los siguientes comandos pueden generar un certificado de servidor.

Pasos

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

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey  
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out  
ontap_mediator_server.csr
```

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



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

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA  
intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095  
-req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
```

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

ONTAP Mediator 1.8 y versiones anteriores

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

emitidos por OpenSSL.

Los siguientes comandos pueden generar un certificado de servidor.

Pasos

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

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey  
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out  
ontap_mediator_server.csr
```

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



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

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt  
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in  
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

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

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

ONTAP Mediator 1.10 y versiones posteriores

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

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. El archivo incluye los siguientes atributos:

```
cert_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi  
ator_server.crt'  
key_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi  
ator_server.key'  
ca_cert_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.crt'  
ca_key_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.key'  
ca_serial_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
```

```
te.srl'
```

- `cert_path` y `key_path` son variables de certificados de servidor.
- `ca_cert_path`, `ca_key_path` y `ca_serial_path` son variables de certificados de CA.

Pasos

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

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

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

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

```
ssl_keyfile:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_  
server.key
```

```
ssl_certfile:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_  
server_chain.crt
```

```
ssl_ca_certs:  
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

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

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 y 1.9

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

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. El archivo incluye los siguientes atributos:

```

cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_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` y `key_path` son variables de certificados de servidor.
- `ca_cert_path`, `ca_key_path` y `ca_serial_path` son variables de certificados de CA.

Pasos

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

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

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

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

```

set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt

```

```

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key

```

```

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

```

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

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

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

5. Reinicia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 y versiones anteriores

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

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml. El archivo incluye los siguientes atributos:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- cert_path y key_path son variables de certificados de servidor.
- ca_cert_path, ca_key_path y ca_serial_path son variables de certificados de CA.

Pasos

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

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

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

Actualiza los valores de mediator_cert, mediator_key y ca_certificate:

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

set-placeholder = mediator_key =
```

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
```

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

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

```
systemctl restart ontap_mediator
```

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

ONTAP Mediator 1.10 y versiones posteriores

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

Pasos

1. Configura el archivo

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

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

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



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

```
[root@mediator_host server_config]# cat  
ontap_mediator.user_config.yaml
```

```
# This config file can be used to override the default settings in  
ontap_mediator.config.yaml
```

```
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

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



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

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

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

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

```
ssl_keyfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
```

```
or_server.key
```

```
ssl_certfile:
```

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt
```

```
ssl_ca_certs:
```

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

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



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

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

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

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

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 y 1.9

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

Pasos

1. Configura el archivo

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

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

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

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

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

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

```
[root@mediator_host server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

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



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

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

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

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

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

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

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

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



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

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

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

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

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 y versiones anteriores

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

Pasos

1. Configura el archivo

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

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



Si usaste `ca.crt` para firmar el `ontap_mediator_server.crt` certificado, se genera el archivo `ca.srl`. Consulta [Paso 2: Genera un certificado de servidor](#)

```
[root@mediator_host server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

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



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

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

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

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

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

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key

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

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



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

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

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

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

```
systemctl restart ontap_mediator
```

Solucionar problemas relacionados con los certificados de ONTAP Mediator

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

Verifica la fecha de caducidad del certificado

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

ONTAP Mediator 1.9 y versiones posteriores

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
    ...
        Validity
```

```
Not Before: Feb 22 19:57:25 2024 GMT
Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP Mediator 1.8 y versiones anteriores

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

Verifica las extensiones X509v3 en la certificación de la CA

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

ONTAP Mediator 1.9 y versiones posteriores

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

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

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

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

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

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

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

ONTAP Mediator 1.8 y versiones anteriores

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

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

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

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

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

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

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

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

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

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

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

ONTAP Mediator 1.9 y versiones posteriores

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

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints          = CA:false
extendedKeyUsage          = serverAuth
keyUsage                  = keyEncipherment, dataEncipherment
subjectAltName            = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1  = 1.2.3.4
IP.2  = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
    ...

    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Extended Key Usage:
            TLS Web Server Authentication
        X509v3 Key Usage:
            Key Encipherment, Data Encipherment
        X509v3 Subject Alternative Name:
            DNS:abc.company.com, DNS:abc-v6.company.com, IP
            Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP Mediator 1.8 y versiones anteriores

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

```
[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints          = CA:false
extendedKeyUsage          = serverAuth
keyUsage                  = keyEncipherment, dataEncipherment
subjectAltName            = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
    ...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
                Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

Comprueba que una clave privada coincida con un certificado

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

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

ONTAP Mediator 1.9 y versiones posteriores

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
```

```
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP Mediator 1.8 y versiones anteriores

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in  
ca.key | openssl md5  
Enter pass phrase for ca.key:  
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc  
[root@mediator_host server_config]# openssl x509 -noout -modulus -in  
ca.crt | openssl md5  
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

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

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

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

ONTAP Mediator 1.9 y versiones posteriores

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

ONTAP Mediator 1.8 y versiones anteriores

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

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

Mantenimiento del sistema operativo del host para ONTAP Mediator

Asegúrate de que el sistema operativo host de ONTAP Mediator se mantenga regularmente para lograr un rendimiento óptimo.

Reinicia el host

Reinicia el host solo cuando los clústeres estén en buen estado. Los clústeres no pueden responder a los fallos mientras ONTAP Mediator esté desconectado. Programa una hora para el mantenimiento antes de reiniciar.

ONTAP Mediator se reanuda automáticamente durante un reinicio y vuelve a establecer las relaciones configuradas previamente con los clústeres de ONTAP.

Actualizaciones del paquete del host

Actualiza cualquier biblioteca o paquete de yum, excepto el kernel. Reinicia el host si es necesario para que los cambios surtan efecto. Programa una ventana de servicio antes de reiniciar el host.

Si instalas el `yum-utils` paquete, usa el comando `needs-restarting` para detectar si algún cambio en los paquetes requiere un reinicio.

Reinicia el sistema tras actualizar las dependencias de ONTAP Mediator, ya que los cambios no surten efecto de forma inmediata.

Actualiza el núcleo del sistema operativo del host

SCST debe compilarse para el núcleo que estás usando. Para actualizar el sistema operativo, debes programar tiempo para el mantenimiento.

Antes de empezar

Los siguientes requisitos se aplican cuando el paquete SCST se instala con ONTAP Mediator.

- Puedes actualizar todos los paquetes de biblioteca, excepto el kernel, pero es posible que tengas que reiniciar para aplicar los cambios en ONTAP Mediator. Programa un tiempo de inactividad si necesitas reiniciar.
- Debes mantener actualizado el núcleo del sistema operativo. Actualiza el núcleo a una versión compatible incluida en "[Matriz de versiones de ONTAP Mediator](#)". Debes reiniciar el sistema, así que planifica una ventana de mantenimiento para la interrupción del servicio.
 - Desinstala el módulo del núcleo SCST antes de reiniciar y luego vuelve a instalarlo.
 - Prepara una versión compatible de SCST para reinstalarla antes de iniciar la actualización del núcleo del sistema operativo.



Si instalaste ONTAP Mediator 1.12 o una versión posterior con soporte solo para HTTPS, el paquete SCST no se instala y el kernel del sistema operativo host se puede actualizar sin afectar a ONTAP Mediator. Consulta la documentación de tu sistema operativo host para ver las instrucciones de actualización.

Pasos

Sigue estos pasos para actualizar el kernel del sistema operativo del host.



Antes de actualizar el kernel, comprueba que el sistema operativo y la versión de ONTAP Mediator sean compatibles. Para conocer las versiones compatibles, consulta "[Matriz de compatibilidad con sistemas operativos](#)".

1. Detén ONTAP Mediator.

2. Desinstala el paquete SCST, consulta [Realiza el mantenimiento del host](#). (SCST no ofrece ningún mecanismo de actualización).
3. Actualiza el sistema operativo y reinicia.
4. Vuelve a instalar el paquete SCST.
5. Vuelve a activar ONTAP Mediator.

Realiza el mantenimiento del host

Actualizar el kernel de la VM puede provocar problemas de compatibilidad con los módulos de SCST. Desinstala y vuelve a instalar SCST manualmente.



Si instalaste ONTAP Mediator 1.12 o posterior con soporte solo para HTTPS, el paquete SCST no está instalado y puedes omitir esta tarea.

Paso 1: desinstala SCST

Para desinstalar SCST, utiliza el paquete tar correspondiente a tu versión de ONTAP Mediator.

Pasos

1. Descarga el paquete SCST correspondiente (tal y como se indica en la siguiente tabla) y descomprímelo.

En esta versión ...	Utiliza este paquete 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. Accede al paquete de código abierto desde el ["Descargas de SCST en SourceForge"](#).
 - b. Selecciona **Download released versions**.
 - c. Descomprime el paquete en tu máquina virtual.
2. Ejecuta los siguientes comandos de desinstalación en el directorio `scst`:
 - a. `systemctl stop mediator-scst`

- b. `make scstadm_uninstall`
- c. `make iscsi_uninstall`
- d. `make usr_uninstall`
- e. `make scst_uninstall`
- f. `depmod`

Paso 2: Instalar SCST

Para instalar SCST manualmente, necesitas el paquete tar de SCST que se utiliza para la versión instalada de ONTAP Mediator (consulta el [Tabla SCST](#)).

Acerca de esta tarea

- Realiza este paso antes de instalar el ONTAP Mediator. Si la versión de SCST que estás usando es más reciente que la versión incluida con el instalador de ONTAP Mediator, el instalador omite este paso.
- En algunos escenarios, la instalación predeterminada de SCST en el sistema operativo actualizado puede fallar porque el sistema operativo actualizado requiere un parche.

A partir de ONTAP Mediator 1.12.1, si la instalación falla, puedes usar la herramienta de reparación de SCST ubicada en `/usr/local/bin/mediator_repair_scst` para reparar la instalación.

Si el sistema operativo actualizado requiere un parche, la herramienta lo incluye para la versión de SCST que se suministra en el paquete ONTAP Mediator. La `mediator_repair_scst` herramienta es una herramienta independiente que está separada del instalador principal y viene empaquetada dentro del archivo de ONTAP Mediator `tgz`. No afecta la instalación ni las rutas de actualización de ONTAP Mediator.

Pasos

1. Ejecuta los siguientes comandos de instalación en el `scst` directorio:

- a. `make 2release`
- b. `make scst_install`
- c. `make usr_install`
- d. `make iscsi_install`
- e. `make scstadm_install`
- f. `depmod`



Si estás realizando una instalación inicial y deseas preinstalar ONTAP Mediator, ejecuta el siguiente comando antes de continuar con el siguiente paso:

```
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 instalas SCST antes que ONTAP Mediator durante una instalación inicial, omite este

paso. El instalador aplica los parches pertinentes de SCST.

2. Opcionalmente, si el arranque seguro está activado, antes de reiniciar, realiza los siguientes pasos:

a. Determina el nombre de cada archivo para los `scst_vdisk`, `scst` y `iscsi_scst` módulos:

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

b. Determina la versión del kernel:

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

c. Firma cada archivo de módulo con el kernel:

```
[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. Instala la clave UEFI junto con el firmware.

Las instrucciones para instalar la clave UEFI se encuentran en:

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

La clave UEFI generada se encuentra en:

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

3. Reinicia el sistema:

```
reboot
```

Cambios en el nombre de host o la dirección IP

Acerca de esta tarea

- Realiza esta tarea en el host Linux en el que hayas instalado ONTAP Mediator.
- Hazlo solo si los certificados autofirmados ya no son válidos debido a que el nombre de host o la dirección IP han cambiado tras instalar ONTAP Mediator.

- Una vez que el certificado autofirmado temporal haya sido sustituido por un certificado de confianza de terceros, *no* utilices esta tarea para volver a generar un certificado. Si no dispones de un certificado autofirmado, no puedes usar este procedimiento.

Paso

Crea un certificado autofirmado temporal para el host actual:

1. Reinicia ONTAP Mediator:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

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

Desinstalar ONTAP Mediator

Si es necesario, desinstala ONTAP Mediator después de desconectarlo de ONTAP.

Antes de empezar

Debes desconectar ONTAP Mediator de ONTAP antes de quitarlo.

Acerca de esta tarea

Realiza esta tarea en el host Linux en el que hayas instalado ONTAP Mediator.

Si no consigues ejecutar este comando, es posible que tengas que hacerlo utilizando la ruta completa, como se muestra en el siguiente ejemplo:

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

Paso

1. Desinstala 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 ~]#
```

Información de copyright

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

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

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

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

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

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

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

Información de la marca comercial

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