



Documentación de ONTAP Mediator

ONTAP Mediator

NetApp
October 19, 2026

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

Tabla de contenidos

Documentación de ONTAP Mediator	1
Notas de publicación	2
Novedades de ONTAP Mediator	2
Matriz de compatibilidad de ONTAP Mediator	4
Matriz de compatibilidad con sistemas operativos	4
Matriz de compatibilidad de SCST	7
Empezar	9
Conoce ONTAP Mediator	9
Cómo funciona ONTAP Mediator	9
Servicios de ONTAP Mediator	9
Herramientas a disposición del administrador del sistema	9
SCST y actualizaciones del núcleo	10
Soporte para HTTPS e iSCSI	10
Guía de inicio rápido de ONTAP Mediator	10
¿Qué sigue?	11
Instala y configura	12
Resumen del proceso de instalación de ONTAP Mediator	12
Prepárate para instalar ONTAP Mediator	12
Requisitos de instalación	13
Requisitos del host	14
Requisitos de cortafuegos y redes	14
Requisitos OS	15
Instala ONTAP Mediator cuando el arranque seguro de UEFI esté activado	16
Proporcionar acceso al repositorio para la instalación de ONTAP Mediator	17
Descarga el paquete de instalación de ONTAP Mediator	25
Verifica la firma del código de ONTAP Mediator	26
Instala el paquete de instalación de ONTAP Mediator	28
Registrar la clave de seguridad para UEFI Secure Boot	46
Firmar los módulos del kernel de SCST	47
Comprueba el estado de la instalación de ONTAP Mediator	48
Usa ONTAP Mediator	50
Utiliza ONTAP Mediator para la sincronización activa de SnapMirror y MetroCluster IP	50
Supervisar las relaciones de sincronización activa de SnapMirror	50
Supervisa las configuraciones IP de MetroCluster	50
Administrar ONTAP Mediator	52
Actualizar ONTAP Mediator	52
Actualizar ONTAP Mediator	52
Actualizar el sistema operativo host y reinstalar o actualizar ONTAP Mediator	60
Configurar los atributos de ONTAP Mediator	65
Parámetros configurables de ONTAP Mediator	65
Instalar certificados SSL de terceros	66
Configurar la protección contra ataques a la contraseña	68
Configurar las reglas de complejidad de las contraseñas	68

Configurar el umbral de espacio libre	69
Configura el espacio reservado para los registros.	69
Cambiar el nombre de usuario y la contraseña de ONTAP Mediator	70
Cambiar el nombre de usuario	70
Cambiar la contraseña	71
Iniciar y detener ONTAP Mediator	72
Detener ONTAP Mediator	72
Iniciar ONTAP Mediator	72
Comprobar el estado de ONTAP Mediator.	73
Comprueba el estado del servicio	73
Confirma los puertos de escucha	74
Gestiona certificados	74
Regenerar un certificado temporal autofirmado para el host de ONTAP Mediator	74
Sustituir los certificados autofirmados de ONTAP Mediator por certificados de terceros de confianza	75
Solucionar problemas relacionados con los certificados de ONTAP Mediator	90
Mantenimiento del sistema operativo del host para ONTAP Mediator.	95
Reinicia el host.	96
Actualizaciones del paquete del host.	96
Actualiza el núcleo del sistema operativo del host	96
Realiza el mantenimiento del host.	97
Cambios en el nombre de host o la dirección IP	99
Desinstalar ONTAP Mediator	100
Avisos legales	102
Copyright	102
Marcas registradas.	102
Patentes	102
Política de privacidad.	102
Código abierto	102
ONTAP Mediator para MetroCluster IP y la sincronización activa de SnapMirror	102

Documentación de ONTAP Mediator

Notas de publicación

Novedades de ONTAP Mediator

Cada versión incluye nuevas mejoras para ONTAP Mediator.



Para obtener información sobre las versiones del sistema operativo y de SCST, consulta ["Matriz de soporte"](#).

Versión de ONTAP Mediator	Mejoras
1.12.1	• Soporte para RHEL: ◦ Compatible: 10.1 y 9.7. ◦ Recomendado: 10.2, 10.0, 9.8, 9.6, 9.4 y 8.10. • Soporte para Rocky Linux 10.2, 9.8 y 8.10. • Soporte para Oracle Linux 10.1 y 9.8 con ambos kernels rhck y uek. • A partir de ONTAP Mediator 1.12.1 y ONTAP 9.19.1, una única instancia de ONTAP Mediator configurada con HTTPS puede supervisar simultáneamente las siguientes configuraciones: ◦ Un máximo de diez configuraciones IP de cuatro nodos o cinco de ocho nodos de MetroCluster si se instalan en un host con una CPU de 8 núcleos y al menos 16 GB de RAM. Consulta "Utiliza ONTAP Mediator para supervisar varias configuraciones de MetroCluster IP". ◦ Una configuración IP de MetroCluster de cuatro nodos y una relación entre iguales activa de SnapMirror si se instala en un host con una CPU de 2 núcleos. Consulta "Configura ONTAP Mediator para SnapMirror active sync". • Incluye una nueva herramienta para reparar una instalación de SCST dañada. Después de instalar ONTAP Mediator, puedes encontrar la herramienta en <code>/usr/local/bin/mediator_repair_scst</code>. Puedes usar la herramienta después de una actualización del sistema operativo, si el sistema operativo actualizado requiere un parche de SCST que no está disponible en el paquete predeterminado de SCST.
1,12	• Soporte para RHEL: ◦ Compatible: 10.1 y 9.7. ◦ Recomendado: 10.2, 10.0, 9.8, 9.6, 9.4 y 8.10. • Soporte para Rocky Linux 10.2, 9.8 y 8.10. • Soporte para Oracle Linux 10.1 y 9.7 con ambos kernels rhck y uek. • A partir de ONTAP 9.19.1 y ONTAP Mediator 1.12, puedes configurar un ONTAP Mediator que use HTTPS para la comunicación en configuraciones IP de MetroCluster. HTTPS ofrece mayor seguridad al cifrar sesiones completas usando SSL/TLS. Puedes elegir instalar ONTAP Mediator con soporte solo para HTTPS. El paquete SCST no se instala si usas este método de instalación. "Más información sobre las opciones de instalación de HTTPS e iSCSI para ONTAP Mediator".

1,11	• Soporte para RHEL 10.1, 10.0, 9.7, 9.6, 9.4 y 8.10. • Soporte para Rocky Linux 10.1, 9.7 y 8.10. • Soporte para Oracle Linux 10.0 y 9.6 con ambos kernels rhck y uek. • Añade compatibilidad con IPv6 para las configuraciones IP de MetroCluster. • Añade compatibilidad con fapolicyd.
1,10	• Soporte para RHEL 10.0, 9.6, 9.4 y 8.10. • Soporte para Rocky Linux 10.0, 9.6 y 8.10. • Actualiza la versión base de Python de Python 3.9 a Python 3.12.
1.9.1	• Soporte para RHEL: ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 y 8.4. ◦ Recomendado: 9.5, 9.4, 9.2, 9.0, 8.10 y 8.8. • Compatibilidad con Rocky Linux 9.5 y 8.10. • Agrega nuevos certificados para la verificación de firmas de código. • Se ha añadido compatibilidad para omitir las comprobaciones de firma de código con la marca <code>-skip-code-signature-check</code>. • El instalador muestra avisos cuando detecta certificados de firma de código caducados.
1,9	• Soporte para RHEL: ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 y 8.4. ◦ Recomendado: 9.5, 9.4, 9.2, 9.0, 8.10 y 8.8. • Compatibilidad con Rocky Linux 9.5 y 8.10. • Compatibilidad con FIPS para RHEL y Rocky Linux. • Se añadieron mejoras de rendimiento para una mayor escalabilidad. • Se mejoraron los nombres de archivo para simplificar la configuración de los certificados firmados por PKI.
1,8	• Soporte para RHEL: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4. ◦ Versiones recomendadas: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 y 8.8. • Compatibilidad con Rocky Linux 9.4 y 8.10.
1,7	• Soporte para RHEL: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4. ◦ Recomendado: 9.3, 9.2, 9.1, 9.0, 8.9 y 8.8. • Compatibilidad con Rocky Linux 9.3 y 8.9. • Compatibilidad con datos SAN (Subject Alternative Name) en certificados autofirmados y certificados firmados por terceros.

1,6	• Actualizaciones de Python 3.9. • Soporte para RHEL: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4. ◦ Recomendado: 9.2, 9.1, 9.0 y 8.8. • Compatibilidad con Rocky Linux 9.2 y 8.8. • Se ha dejado de ofrecer soporte para todas las versiones de RHEL 7.x y CentOS.
1,5	• Compatibilidad con RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6. • Compatibilidad con CentOS 7.9, 7.8, 7.7 y 7.6. • Incluye advertencias de obsolescencia para RHEL 7.x / CentOS 7.x. • Optimiza la velocidad para sistemas de sincronización activa de SnapMirror a gran escala. • Se ha añadido una firma criptográfica de código al instalador.
1,4	• Compatibilidad con RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6. • Compatibilidad con CentOS 7.9, 7.8, 7.7 y 7.6. • Se ha añadido compatibilidad con el arranque seguro (SB) del firmware basado en UEFI.
1,3	• Compatibilidad con RHEL 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6. • Compatibilidad con CentOS 7.9, 7.8, 7.7 y 7.6.
1,2	• Soporte para RHEL 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6. • Compatibilidad con CentOS 7.9, 7.8, 7.7 y 7.6. • Compatibilidad con buzones de correo HTTPs. • Para usar con ONTAP 9.8+ MCC-IP AUSO y sincronización activa ZRTO de SnapMirror.
1,1	• Compatibilidad con RHEL 8.0 y 7.6. • Compatibilidad con CentOS 7.6. • Elimina las dependencias de Perl.
1,0	• Compatibilidad con buzones de correo iSCSI. • Para su uso con ONTAP 9.7+ MCC-IP AUSO. • Compatibilidad con RHEL/CentOS 7.6.

Matriz de compatibilidad de ONTAP Mediator

La matriz de compatibilidad de ONTAP Mediator incluye información sobre la compatibilidad con las versiones del sistema operativo y de SCST.

Matriz de compatibilidad con sistemas operativos

En la siguiente tabla se enumeran los sistemas operativos compatibles con cada versión de ONTAP Mediator.

Sistema operativo para ONT AP Mediador	1.12.1	1,12	1,11	1,10	1.9.1	1,9	1,8	1,7	1,6	1,5	1,4	1,3	1,2	1,1	1,0
RHEL 10.2	Sí	Sí	No	No	No	No	No	No	No	No	No	No	No	No	No
RHEL 10.1	Compatible	Compatible	Sí	No	No	No	No	No	No	No	No	No	No	No	No
RHEL 10.0	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No	No	No	No	No
RHEL 9.8	Sí	Sí	No	No	No	No	No	No	No	No	No	No	No	No	No
RHEL 9.7	Compatible	Compatible	Sí	No	No	No	No	No	No	No	No	No	No	No	No
RHEL 9.6	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No	No	No	No	No
RHEL 9.5	No	No	No	No	Sí	No	No	No	No	No	No	No	No	No	No
RHEL 9.4	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No	No
RHEL 9.3	No	No	No	No	No	No	Sí	Sí	No	No	No	No	No	No	No
RHEL 9.2	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No
RHEL 9.1	No	No	No	No	No	No	Sí	Sí	Sí	No	No	No	No	No	No
RHEL 9.0	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No
RHEL 8.10	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No	No
RHEL 8.9	No	No	No	No	Compatible	Compatible	Sí	Sí	No	No	No	No	No	No	No
RHEL 8.8	No	No	No	No	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No

RHE L 8.7	No	No	No	No	Com patibl e	Com patibl e	Sí	Sí	Sí	No	No	No	No	No	No
RHE L 8.6	No	No	No	No	Com patibl e	Com patibl e	Sí	Sí	Sí	No	No	No	No	No	No
RHE L 8.5	No	No	No	No	Com patibl e	Com patibl e	Sí	Sí	Sí	Sí	Sí	No	No	No	No
RHE L 8.4	No	No	No	No	Com patibl e	Com patibl e	Sí	Sí	Sí	Sí	Sí	No	No	No	No
RHE L 8.3	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Sí	Sí	Sí	No	No	No
RHE L 8.2	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Sí	Sí	Sí	No	No	No
RHE L 8.1	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Sí	Sí	Sí	Sí	No	No
RHE L 8.0	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Sí	Sí	Sí	Sí	Sí	No
RHE L y Cent OS 7.9	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Sí	Sí	Sí	Com patibl e	No	No
RHE L y Cent OS 7.8	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Sí	Sí	Sí	Sí	No	No
RHE L y Cent OS 7.7	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Sí	Sí	Sí	Sí	No	No
RHE L y Cent OS 7.6	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Obso leto	Sí	Sí	Sí	Sí	Sí	Sí (solo RHE L)
Cent OS 8 y strea m	No	No	No	No	No	No	No	No	No	No	No	No	N/A	N/A	N/A

Rock y Linux 10	Sí (10.2)	Sí (10.2)	Sí (10.0 y 10.1)	Sí	No	No	No	No	No	No	No	No	No	No	No
Rock y Linux 9	Sí (9.8)	Sí (9.8)	Sí (9.7)	Sí (9.6 y 9.4)	Sí (9.5)	Sí (9.5)	Sí (9.4)	Sí (9.3)	Sí (9.2)	N/A	N/A	N/A	N/A	N/A	N/A
Rock y Linux 8	Sí (8.10)	Sí (8.10)	Sí (8.10)	Sí (8.10)	Sí (8.10)	Sí (8.10)	Sí (8.10)	Sí (8.9)	Sí (8.8)	N/A	N/A	N/A	N/A	N/A	N/A
Oracle Linux 10	Sí (10.1)	Sí (10.1)	Sí (10.0)	No	No	No	No	No	No	No	No	No	No	No	No
Oracle Linux 9	Sí (9.8)	Sí (9.7)	Sí (9.6)	No	No	No	No	No	No	No	No	No	No	No	No

- «Sí» significa que el sistema operativo es el recomendado para la instalación de ONTAP Mediator y que es totalmente compatible y tiene soporte.
- «No» significa que el sistema operativo y ONTAP Mediator no son compatibles.
- "Compatible" significa que Red Hat ya no ofrece soporte para estas versiones de RHEL, pero aún puedes instalar ONTAP Mediator en ellas.
- ONTAP Mediator 1.6 añade compatibilidad con Rocky Linux 9 y 8.
- ONTAP Mediator 1.5 fue la última versión compatible con los sistemas operativos de la rama RHEL 7.x.
- CentOS 8 se eliminó de todas las versiones debido a su cambio de rama. CentOS Stream se consideró que no es un sistema operativo adecuado para producción. No se planea soporte.

Matriz de compatibilidad de SCST

La siguiente tabla muestra la versión de SCST compatible con cada versión de ONTAP Mediator.

Versión de ONTAP Mediator	Versión de SCST compatible
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

Versión de ONTAP Mediator	Versión de SCST compatible
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 1.2	scst-3.4.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

Empezar

Conoce ONTAP Mediator

ONTAP Mediator admite las funciones de ONTAP al proporcionar un almacenamiento persistente y protegido para los metadatos de alta disponibilidad (HA), una funcionalidad de consulta síncrona del estado de los nodos para facilitar la determinación del quórum y al actuar como proxy de ping para comprobar la capacidad de respuesta de las controladoras.



Esta documentación se refiere a la versión local de ONTAP Mediator. Para obtener información sobre ONTAP Cloud Mediator, disponible a partir de ONTAP 9.17.1, consulta "[SnapMirror documentación de active sync](#)".

Cómo funciona ONTAP Mediator

ONTAP Mediator se ejecuta en un host Linux situado en un tercer dominio de fallo, independiente de tus clústeres de ONTAP, donde proporciona un almacén persistente y aislado para los metadatos de alta disponibilidad. ONTAP utiliza este almacén, junto con las funciones de consulta del estado de los nodos y de proxy de ping de Mediator, para supervisar las relaciones de sincronización activa de SnapMirror y las configuraciones IP de MetroCluster.

- ONTAP Mediator utiliza el LIF de gestión de nodos y el LIF de gestión de clúster para comunicarse con cada clúster a través de múltiples rutas redundantes. Esto permite a ONTAP distinguir entre un fallo total del sitio y un único fallo de enlace InterSwitch (ISL).
- En la sincronización activa de SnapMirror, si un clúster pierde la conexión tanto con su par como con ONTAP Mediator, ONTAP considera que el par es inaccesible y puede conmutar automáticamente a la copia superviviente.
- En las configuraciones IP de MetroCluster, ONTAP Mediator facilita una conmutación de sitios automática no planificada asistida por Mediator (MAUSO) al almacenar información de estado sobre los nodos de MetroCluster y ayudar a determinar el curso de acción adecuado durante un fallo.

Servicios de ONTAP Mediator

ONTAP Mediator ofrece dos servicios `systemctl` adicionales:

- **`ontap_mediator.service`**

Mantiene el servidor de la API de REST para gestionar las relaciones de ONTAP.

- **`mediator-scst.service`**

Controla el inicio y el apagado del módulo iSCSI (SCST).

Herramientas a disposición del administrador del sistema

Herramientas a disposición del administrador del sistema:

- **`/usr/local/bin/mediator_change_password`**

Establece una nueva contraseña de la API cuando se proporcionan el nombre de usuario y la contraseña actuales de la API.

- **`/usr/local/bin/mediator_change_user`**

Establece un nuevo nombre de usuario de la API cuando se facilitan el nombre de usuario y la contraseña actuales de la API.

- **`/usr/local/bin/mediator_generate_support_bundle`**

Genera un archivo tgz local que contiene toda la información de soporte útil necesaria para comunicarte con el soporte al cliente de NetApp. Esto incluye la configuración de la aplicación, los registros y algo de información del sistema. Los paquetes se generan en el disco local y pueden transferirse manualmente, según sea necesario. Ubicación de almacenamiento: `/opt/netapp/data/support_bundles/`

- **`/usr/local/bin/uninstall_ontap_mediator`**

Elimina el paquete ONTAP Mediator y el módulo del núcleo SCST. Esto incluye toda la configuración, los registros y los datos del buzón.

- **`/usr/local/bin/mediator_unlock_user`**

Desbloquea la cuenta de usuario de la API si se ha alcanzado el límite de reintentos de autenticación. Esta función se utiliza para impedir la deducción de contraseñas mediante ataques de fuerza bruta. Solicita al usuario que introduzca el nombre de usuario y la contraseña correctos.

- **`/usr/local/bin/mediator_add_user`**

(Solo para soporte técnico) Se utiliza para añadir el usuario de la API durante la instalación.

SCST y actualizaciones del núcleo

ONTAP Mediator utiliza SCST para proporcionar iSCSI para la comunicación en las configuraciones de IP de MetroCluster. El paquete SCST es un módulo del kernel que se compila durante la instalación. Es posible que tengas que volver a instalar SCST después de las actualizaciones del kernel. Como alternativa, desinstala ONTAP Mediator, luego vuelve a instalar y reconfigura la relación de ONTAP. Consulta "[SCST: un subsistema de destino SCSI genérico para Linux](#)" para saber más sobre SCST.



Deberías coordinar cualquier actualización del kernel del SO del servidor con una ventana de mantenimiento en ONTAP.

Soporte para HTTPS e iSCSI

A partir de ONTAP 9.19.1 y ONTAP Mediator 1.12, puedes configurar un ONTAP Mediator que use HTTPS o iSCSI para supervisar una configuración IP de MetroCluster. Puedes elegir instalar ONTAP Mediator con soporte tanto para iSCSI como para HTTPS, o solo para HTTPS. Si ONTAP Mediator se instala con soporte solo para HTTPS, el paquete SCST no se instala. Consulta "[Opciones de instalación HTTPS e iSCSI para ONTAP Mediator](#)" para obtener más información.

Guía de inicio rápido de ONTAP Mediator

Para empezar a utilizar ONTAP Mediator, debes instalar el software y configurarlo para

que funcione con tu entorno ONTAP.

1

Instala ONTAP Mediator

"[Instalar ONTAP Mediator](#)" en tu sistema y asegúrate de que se cumplan todas las dependencias necesarias.

2

Comprueba la instalación de ONTAP Mediator

"[Comprueba que la instalación de ONTAP Mediator se haya realizado correctamente](#)" comprobando el estado del servicio y revisando los registros en busca de posibles errores o advertencias.

3

Configura ONTAP Mediator para tu entorno ONTAP

Dependiendo de si quieres "[Utiliza ONTAP Mediator para MetroCluster IP, SnapMirror active sync o ambas cosas](#)", sigue los pasos de configuración correspondientes para asegurarte de que todos los ajustes necesarios se apliquen correctamente.

¿Qué sigue?

Ahora puedes usar ONTAP Mediator para supervisar las configuraciones IP de MetroCluster, las configuraciones de sincronización activa de SnapMirror o ambas. Para obtener más información, consulta "[SnapMirror documentación de active sync](#)" y "[MetroCluster documentación](#)".

Instala y configura

Resumen del proceso de instalación de ONTAP Mediator

La instalación de ONTAP Mediator incluye la preparación para la instalación, la configuración del acceso a los repositorios, la descarga del paquete de instalación, la verificación de la firma del código y la instalación del paquete ONTAP Mediator.

1

"Prepárate para instalar ONTAP Mediator"

Para instalar ONTAP Mediator, debes asegurarte de cumplir todos los requisitos previos.

2

"Proporciona acceso al repositorio"

Debes habilitar el acceso a los repositorios para que ONTAP Mediator pueda acceder a los paquetes necesarios durante el proceso de instalación.

3

"Descarga el paquete de instalación de ONTAP Mediator"

Descarga el paquete de instalación de ONTAP Mediator desde la página de descargas de ONTAP Mediator.

4

"Comprueba la firma digital del paquete de instalación de ONTAP Mediator"

NetApp recomienda verificar la firma del código de ONTAP Mediator antes de instalar el paquete de instalación de ONTAP Mediator.

5

"Instala el paquete de instalación de ONTAP Mediator"

Descarga el paquete de instalación y ejecuta el instalador en el host.

6

"Comprueba la instalación de ONTAP Mediator"

Una vez instalado ONTAP Mediator, comprueba que se esté ejecutando correctamente.

Prepárate para instalar ONTAP Mediator

Para instalar ONTAP Mediator, debes cumplir todos los requisitos previos, descargar el paquete de instalación y ejecutar el instalador en el host.



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

Requisitos de instalación

Revisa los siguientes requisitos antes de instalar ONTAP Mediator.



- ONTAP Mediator 1.8 y versiones anteriores no es compatible con el modo FIPS de Red Hat Enterprise Linux (RHEL) e impide que se instale correctamente. Puedes comprobar si el modo FIPS está activado con el comando `fips-mode-setup --check`. Puedes desactivar el modo FIPS con el comando `fips-mode-setup --disable`. Reinicia el sistema después de desactivar el modo FIPS para instalar correctamente ONTAP Mediator 1.8 o versiones anteriores.
- Si la instalación falla, es posible que tengas que probar con una versión más reciente de ONTAP Mediator.
- A partir del 15 de junio de 2025, no puedes instalar ni actualizar ONTAP Mediator 1.9 ni 1.8 porque sus certificados de firma de código han caducado. Si la instalación falla, usa en su lugar la versión de parche ONTAP Mediator 1.9.1.

- Si instalas el paquete `yum-utils`, puedes usar el comando `needs-restarting`.
- A partir de ONTAP Mediator 1.11, se admite IPv6 para las configuraciones IP de MetroCluster.

Opciones de instalación HTTPS e iSCSI para ONTAP Mediator

Antes de instalar ONTAP Mediator, revisa la siguiente información:

- En ONTAP Mediator, el paquete SCST se usa para proporcionar iSCSI para la comunicación en configuraciones IP de MetroCluster. El paquete SCST es un módulo del kernel que se compila durante la instalación. A partir de ONTAP 9.19.1 y Mediator 1.12, puedes configurar un ONTAP Mediator que use HTTPS en lugar de iSCSI para supervisar una configuración IP de MetroCluster.
- 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.

Requisitos del host

Sigue estos requisitos al instalar RHEL o Rocky Linux y configurar los repositorios correspondientes.



Si modificas el proceso de instalación o configuración, es posible que tengas que realizar pasos adicionales.

Requisitos de la distribución de Linux

- Instala RHEL o Rocky Linux siguiendo las prácticas recomendadas de Red Hat. Dado que CentOS 8.x ha llegado al final de su ciclo de vida, no se recomiendan las versiones compatibles con CentOS 8.x.
- Al instalar ONTAP Mediator, asegúrate de que el sistema tenga acceso al repositorio necesario para que el programa de instalación pueda descargar e instalar todas las dependencias de software necesarias.
- Para que el instalador de yum pueda encontrar el software del que depende en los repositorios de RHEL, registra el sistema durante la instalación o después con una suscripción válida de Red Hat.



Consulta la documentación de Red Hat Subscription Manager para obtener más información.

Requisitos de cortafuegos y redes

ONTAP Mediator utiliza una serie de puertos para comunicarse con servicios específicos.

- Si estás usando un cortafuegos de terceros:
 - El acceso HTTPS debe estar activado.
 - Debe configurarse para permitir el acceso en los puertos 31784 y 3260.

Si usas el cortafuegos predeterminado de Red Hat o CentOS, el cortafuegos se configura automáticamente durante la instalación de Mediator.

- En hosts Linux sin acceso a internet, asegúrate de que los paquetes necesarios estén disponibles en un repositorio local.

Si utilizas el Protocolo de control de agregación de enlaces (LACP) en un entorno Linux, configura el kernel y establece `sysctl net.ipv4.conf.all.arp_ignore` en 2.

La siguiente tabla enumera los puertos que debes permitir en tu cortafuegos:



- El puerto iSCSI solo es necesario en una configuración IP de MetroCluster.
- El puerto 22/tcp no es necesario para el funcionamiento normal, pero puedes habilitarlo temporalmente para mantenimiento y deshabilitarlo cuando la sesión de mantenimiento haya terminado.

Puertos/servicios	Fuente	Dirección	Destino	Propósito
22/tcp	Host de gestión	Entrada	ONTAP Mediator	(Opcional) gestión de SSH / ONTAP Mediator
31784/tcp	cluster-mgmt y node-mgmt LIFs	Entrada	Servidor web ONTAP Mediator	(Obligatorio) API de REST (HTTPS)

3260/tcp	LIF de gestión de nodos	Entrada	Objetivos iSCSI de ONTAP Mediator	(Requerido para las configuraciones IP de MetroCluster) conexión de datos iSCSI para los buzones
----------	-------------------------	---------	-----------------------------------	--



Para una sincronización activa de SnapMirror o MetroCluster IP ONTAP Mediator que usa HTTPS para la comunicación, ONTAP no requiere que el puerto 3260 esté habilitado o conectado.

Requisitos OS

Tu sistema operativo debe cumplir los siguientes requisitos:

- Instalación física o máquina virtual de 64 bits
- 8 GB de RAM
- 1 GB de espacio en disco (para la instalación de aplicaciones, los registros del servidor y la base de datos)
- Usuario: Acceso root

Consulta ["Matriz de compatibilidad con sistemas operativos"](#) para ver los sistemas operativos compatibles con cada versión de ONTAP Mediator.

Paquetes necesarios para el sistema operativo

ONTAP Mediator requiere los siguientes paquetes:



Los paquetes vienen preinstalados o el instalador de ONTAP Mediator los instala automáticamente.

Todas las versiones de RHEL/CentOS	Paquetes adicionales para RHEL 10.x / Rocky Linux 10	Paquetes adicionales para RHEL 9.x / Rocky Linux 9	Paquetes adicionales para RHEL 8.x / Rocky Linux 8
------------------------------------	--	--	--

• openssl • openssl-devel • kernel-devel-\$ (uname -r) • gcc • hacer • libselinux-utils • parche • bzip2 • perl-Data-Dumper • perl-ExtUtils- MakeMaker • efibootmgr • mokutil	• python3.12 • python3.12-devel	• elfutils-libelf-devel • policycoreutils-python- utils • python3 • python3-devel	• elfutils-libelf-devel • policycoreutils-python- utils • redhat-lsb-core • python39 • python39-devel
--	--	--	---

El paquete de instalación de Mediator es un archivo tar comprimido y autoextraíble que incluye:

- Un archivo RPM que contiene todas las dependencias que no se pueden obtener del repositorio de la versión compatible.
- Un script de instalación.

Se recomienda disponer de un certificado SSL válido.



- La versión del kernel debe coincidir con la versión del sistema operativo.
- No actualices el kernel más allá de la versión del sistema operativo compatible con tu versión de ONTAP Mediator, ya que es posible que el módulo SCST probado no funcione.

Instala ONTAP Mediator cuando el arranque seguro de UEFI esté activado

ONTAP Mediator se puede instalar en un sistema tanto si tiene activado el arranque seguro UEFI como si no.

Acerca de esta tarea

- Puedes desactivar el arranque seguro de UEFI antes de instalar ONTAP Mediator si no es necesario o si estás solucionando problemas relacionados con la instalación de ONTAP Mediator. Desactiva la opción de arranque seguro de UEFI en la configuración de tu equipo.
- Si instalaste ONTAP Mediator 1.12 o posterior con soporte solo para HTTPS, el paquete SCST no está instalado y puedes omitir esta tarea.



Para obtener instrucciones detalladas sobre cómo desactivar UEFI Secure Boot, consulta la documentación del sistema operativo de tu host.

Para instalar ONTAP Mediator con UEFI Secure Boot activado, debes registrar una clave de seguridad antes de que el servicio pueda iniciarse. La clave se genera durante la fase de compilación de la instalación de SCST y se guarda como un par de claves pública-privada en tu equipo. Usa la utilidad `mokutil` para añadir la clave pública como una Machine Owner Key (MOK) a tu firmware UEFI, lo que permite que el sistema confíe en el módulo firmado y lo cargue. Guarda la frase de contraseña `mokutil` en un lugar seguro, ya que la

necesitarás al reiniciar tu sistema para activar la MOK.

Pasos

1. Comprueba si el arranque seguro de UEFI está activado en tu sistema:

```
mokutil --sb-state
```

Los resultados indican si UEFI Secure Boot está activado en este sistema.

Si...	Ir a...
El arranque seguro de UEFI está activado	
El arranque seguro de UEFI está desactivado	"Proporcionar acceso al repositorio para la instalación de ONTAP Mediator"



- Se te pedirá que crees una frase de contraseña que deberás guardar en un lugar seguro. Necesitarás esta frase de contraseña para habilitar la clave en el UEFI Boot Manager.
- ONTAP Mediator 1.2.0 y las versiones anteriores no admiten este modo.

2. Si la utilidad `mokutil` no está instalada, ejecuta el siguiente comando:

```
yum install mokutil
```

¿Y ahora qué?

["Proporcionar acceso al repositorio para la instalación de ONTAP Mediator"](#)

Proporcionar acceso al repositorio para la instalación de ONTAP Mediator

Debes habilitar el acceso a los repositorios para que ONTAP Mediator pueda acceder a los paquetes necesarios durante el proceso de instalación.

Pasos

1. Determina a qué repositorios debes acceder, como se muestra en la siguiente tabla:

Si tu sistema operativo es...	Debes facilitar el acceso a estos repositorios...
Oracle Linux 10.x	• ol-10-for-x86_64-baseos-rpms • ol-10-for-x86_64-appstream-rpms
Oracle Linux 9.x	• ol-9-for-x86_64-baseos-rpms • ol-9-for-x86_64-appstream-rpms
RHEL 10.x	• rhel-10-for-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms

RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 7.x	• rhel-7-server-optional-rpms
CentOS 7.x	• C7.6.1810 - Repositorio base
Rocky Linux 10	• appstream • baseos
Rocky Linux 9	• appstream • baseos
Rocky Linux 8	• appstream • baseos

2. Utiliza uno de los siguientes procedimientos para habilitar el acceso a los repositorios mencionados arriba, así ONTAP Mediator puede acceder a los paquetes necesarios durante el proceso de instalación.



Si ONTAP Mediator depende de módulos de Python presentes en los repositorios "extras" y "optional", es posible que necesite acceder a los archivos `rhel-X-for-x86_64-extras-rpms` y `rhel-X-for-x86_64-optional-rpms`.

▼ Procedimiento para el sistema operativo Oracle Linux 10.x

Usa este procedimiento si tu sistema operativo es **Oracle Linux 10.x** para habilitar el acceso a los repositorios:

Pasos

- a. Suscríbete al repositorio requerido:

```
subscription-manager repos --enable ol-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable ol-10-for-x86_64-appstream-rpms
```

El siguiente ejemplo muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable ol-10-for-x86_64-baseos-rpms
Repository 'ol-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable ol-10-for-x86_64-appstream-rpms
Repository 'ol-10-for-x86_64-appstream-rpms' is enabled for this system.
```

b. Ejecuta el siguiente comando para ver la lista de repositorios habilitados:

```
yum repolist
```

Los repositorios recién suscritos deberían aparecer en la lista.

▼ Procedimiento para el sistema operativo Oracle Linux 9.x

Usa este procedimiento si tu sistema operativo es **Oracle Linux 9.x** para habilitar el acceso a los repositorios:

Pasos

a. Suscríbete al repositorio requerido:

```
subscription-manager repos --enable ol-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable ol-9-for-x86_64-appstream-rpms
```

El siguiente ejemplo muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable ol-9-for-x86_64-baseos-rpms
Repository 'ol-9-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable ol-9-for-x86_64-appstream-rpms
Repository 'ol-9-for-x86_64-appstream-rpms' is enabled for this system.
```

b. Ejecuta el siguiente comando para ver la lista de repositorios habilitados:

```
yum repolist
```

Los repositorios recién suscritos deberían aparecer en la lista.

▼ Procedimiento para el sistema operativo RHEL 10.x

Sigue este procedimiento si tu sistema operativo es **RHEL 10.x** para habilitar el acceso a los repositorios:

Pasos

a. Suscríbete al repositorio requerido:

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
```

El siguiente ejemplo muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this system.
```

b. Ejecuta el siguiente comando para ver la lista de repositorios habilitados:

```
yum repolist
```

Los repositorios recién suscritos deberían aparecer en la lista.

▼ Procedimiento para el sistema operativo RHEL 9.x

Sigue este procedimiento si tu sistema operativo es **RHEL 9.x** para habilitar el acceso a los repositorios:

Pasos

a. Suscríbete al repositorio requerido:

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

El siguiente ejemplo muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this system.
```

b. Ejecuta el siguiente comando para ver la lista de repositorios habilitados:

```
yum repolist
```

Los repositorios recién suscritos deberían aparecer en la lista.

▼ Procedimiento para el sistema operativo RHEL 8.x

Sigue este procedimiento si tu sistema operativo es **RHEL 8.x** para habilitar el acceso a los repositorios:

Pasos

a. Suscríbete al repositorio requerido:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

El siguiente ejemplo muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this system.
```

b. Ejecuta el siguiente comando para ver la lista de repositorios habilitados:

```
yum repolist
```

Los repositorios recién suscritos deberían aparecer en la lista.

▼ Procedimiento para el sistema operativo RHEL 7.x

Sigue este procedimiento si tu sistema operativo es **RHEL 7.x** para habilitar el acceso a los repositorios:

Pasos

a. Suscríbete al repositorio requerido:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

El siguiente ejemplo muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

b. Ejecuta el siguiente comando para ver la lista de repositorios habilitados:

```
yum repolist
```

El siguiente ejemplo muestra la ejecución de este comando. El repositorio "rhel-7-server-optional-rpms" debería aparecer en la lista.

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group |
26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo |
2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db |
8.3 MB  00:00:01
repo id                                repo name
status
rhel-7-server-optional-rpms/7Server/x86_64  Red Hat Enterprise Linux
7 Server - Optional (RPMs)  19,447
rhel-7-server-rpms/7Server/x86_64          Red Hat Enterprise Linux
7 Server (RPMs)  26,758
repolist: 46,205
[root@localhost ~]#
```

▼ Procedimiento para el sistema operativo CentOS 7.x

Usa este procedimiento si tu sistema operativo es **CentOS 7.x** para habilitar el acceso a los repositorios:



Los siguientes ejemplos muestran un repositorio para CentOS 7.6 y es posible que no funcionen con otras versiones de CentOS. Utiliza el repositorio base para tu versión de CentOS.

Pasos

a. Añade el repositorio C7.6.1810 - Base. El repositorio C7.6.1810 - Base vault contiene el paquete

"kernel-devel" necesario para ONTAP Mediator.

b. Agrega las siguientes líneas a /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

c. Ejecuta el siguiente comando para ver la lista de repositorios habilitados:

```
yum repolist
```

El siguiente ejemplo muestra la ejecución de este comando. El repositorio CentOS-7.6.1810 - Base debería aparecer en la lista.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: distro.ibiblio.org
* extras: distro.ibiblio.org
* updates: ewr.edge.kernel.org
C7.6.1810-base | 3.6 kB 00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz | 166 kB 00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db | 6.0 MB 00:00:04
repo id repo name status
C7.6.1810-base/x86_64 CentOS-7.6.1810 - Base 10,019
base/7/x86_64 CentOS-7 - Base 10,097
extras/7/x86_64 CentOS-7 - Extras 307
updates/7/x86_64 CentOS-7 - Updates 1,010
repolist: 21,433
[root@localhost ~]#
```

▼ Procedimiento para los sistemas operativos Rocky Linux 10, 9 u 8

Sigue este procedimiento si tu sistema operativo es **Rocky Linux 10**, **Rocky Linux 9** o **Rocky Linux 8** para habilitar el acceso a los repositorios:

Pasos

a. Suscríbete a los repositorios necesarios:

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

b. Realiza una operación de clean:

```
dnf clean all
```

c. Verifica la lista de repositorios:

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                                repo name
appstream                             Rocky Linux 10 - AppStream
baseos                                Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                                repo name
appstream                             Rocky Linux 9 - AppStream
baseos                                Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                                repo name
appstream                             Rocky Linux 8 - AppStream
baseos                                Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

¿Y ahora qué?

["Descarga el paquete de instalación de ONTAP Mediator"](#)

Descarga el paquete de instalación de ONTAP Mediator

Descarga el paquete de instalación de ONTAP Mediator e instálalo.

Pasos

1. Descarga el paquete de instalación de ONTAP Mediator desde la página de descargas de ONTAP Mediator.

["Página de descarga de ONTAP Mediator"](#)

2. Coloca el paquete de instalación de Mediator en el directorio de trabajo actual:

```
ls ontap-mediator-1.12.1.tgz
```

```
ontap-mediator-1.12.1.tgz
```



En las versiones 1.4 y anteriores de ONTAP Mediator, el instalador se llama ontap-mediator.

Si tu sistema no tiene conexión a internet, asegúrate de que el instalador pueda acceder a los paquetes necesarios.

3. Si es necesario, traslada el paquete de instalación de Mediator al directorio de instalación.
4. Descomprime el paquete de instalación:

```
tar xvfz ontap-mediator-1.12.1.tgz
```

```
ontap-mediator-1.12.1/  
ontap-mediator-1.12.1/csc-prod-ONTAP-Mediator.pem  
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/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.tsr  
ontap-mediator-1.12.1/ontap-mediator-1.12.1.tsr  
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig
```

¿Y ahora qué?

["Verifica la firma del código de ONTAP Mediator"](#)

Verifica la firma del código de ONTAP Mediator

NetApp recomienda verificar la firma del código de ONTAP Mediator antes de la instalación. Este paso es opcional.

Antes de empezar

Asegúrate de que tu sistema cumple estos requisitos antes de verificar la firma del código de ONTAP Mediator.



- A partir del 15 de junio de 2025, no puedes instalar ni actualizar a ONTAP Mediator 1.9 y 1.8 porque los certificados de verificación de firma de código han caducado. En su lugar, instala o actualiza a ONTAP Mediator 1.10 o posterior.
- Si el sistema no cumple los requisitos que se indican a continuación, no es necesario realizar el proceso de verificación y puedes acceder directamente a ["Instala el paquete de instalación de ONTAP Mediator"](#).

- Versiones de openssl 1.0.2 a 3.0 para la verificación básica
- openssl versión 1.1.0 o posterior para las operaciones de la Autoridad de Sello de Tiempo (TSA)
- Acceso público a internet para la verificación de OCSP

El paquete de descarga incluye los siguientes archivos:

Archivo	Descripción
ONTAP-Mediator-production.pub	La clave pública utilizada para verificar la firma
csc-prod-chain-ONTAP-Mediator.pem	La cadena de confianza de la CA de certificación pública
csc-prod-ONTAP-Mediator.pem	El certificado utilizado para generar la clave
ontap-mediator-1.12.1	El ejecutable de instalación del producto para la versión 1.12
ontap-mediator-1.12.1.sig	La firma del instalador, a la que se le ha aplicado un hash SHA-256 y luego se ha firmado con RSA usando la clave csc-prod
ontap-mediator-1.12.1.sig.tsr	La solicitud de revocación que utilizará OCSCP para la firma del instalador
ontap-mediator-1.12.1.tsr	El archivo de solicitud de firma con marca de tiempo
tsa-prod-ONTAP-Mediator.pem	El certificado público del TSR
tsa-prod-chain-ONTAP-Mediator.pem	La cadena de certificados públicos de la CA para el TSR

Pasos

1. Realiza la comprobación de revocación en `csc-prod-ONTAP-Mediator.pem` utilizando Online Certificate Status Protocol (OCSP).
 - a. Busca la URL de OCSP del certificado. Es posible que los certificados de desarrollador no proporcionen un URI:

```
openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
```

- b. Genera una solicitud OSCP para el certificado.

```
openssl ocsf -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout req.der
```

- c. Conéctate al OSCP Manager para enviar la solicitud OSCP:

```
openssl ocsf -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-chain-ONTAP-Mediator.pem
```

2. Comprueba la cadena de confianza del CSC y las fechas de caducidad con respecto al host local:

```
openssl verify
```



La versión de openssl PATH debe tener un cert.pem válido (que no sea autofirmado).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath ${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath ${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem
```

El comando falla si el certificado de comprobación de la firma del código o el certificado de marca de tiempo ha caducado o no es válido. Descarga una versión más reciente de ONTAP Mediator.

3. Verifica los archivos `ontap-mediator-1.12.1.sig.tsr` y `ontap-mediator-1.12.1.tsr` usando los certificados asociados:

OpenSSL 3.x

```
openssl ts -verify -data ontap-mediator-1.12.1.sig -in ontap-mediator-1.12.1.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-ONTAP-Mediator.pem
```

OpenSSL 1.x

```
openssl ts -verify -data ontap-mediator-1.12.1 -in ontap-mediator-
```

```
1.12.1.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```



.tsr archivos contienen la respuesta de marca de tiempo asociada al instalador y la firma de código. El procesamiento confirma que la marca de tiempo tiene una firma válida de TSA y que tu archivo de entrada no ha cambiado. Tu equipo realiza la verificación localmente. No necesitas acceder a los servidores de TSA.

4. Verifica las firmas con la clave:

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature  
ontap-mediator-1.12.1.sig ontap-mediator-1.12.1
```

¿Y ahora qué?

["Instala el paquete de instalación de ONTAP Mediator"](#)

Instala el paquete de instalación de ONTAP Mediator

Para instalar ONTAP Mediator, debes obtener el paquete de instalación y ejecutar el instalador en el host.



Para actualizar una instalación existente de ONTAP Mediator, consulta ["Actualizar ONTAP Mediator"](#) en su lugar.

Acerca de esta tarea

- 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.
- Durante la instalación o actualización a ONTAP Mediator 1.12 o posterior, el instalador te pedirá que respondas a lo siguiente:

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

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

Y(es)/n(o):

- Responde **Yes** si planeas usar ONTAP Mediator configurado con iSCSI para monitorear una o más configuraciones IP de MetroCluster.
- Responde **No** si tienes previsto usar ONTAP Mediator solo para la sincronización activa de SnapMirror, o si planeas configurar ONTAP Mediator con HTTPS para monitorear una o más configuraciones de IP de MetroCluster.

Alternativamente, puedes usar la opción `--https-only` en el comando `./ontap-mediator-1.12.1/ontap-mediator-1.12.1` para especificar solo HTTPS.

- 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 y responde a las indicaciones según se requiera:

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

```
[root@mediator_host ~]# ./ontap-mediator-1.12.1/ontap-mediator-1.12.1
```



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

El programa de instalación crea las cuentas necesarias e instala los paquetes requeridos. Si ONTAP Mediator ya está instalado, el programa de instalación te pedirá que actualices; para ver los pasos y ejemplos específicos de la actualización, consulta ["Actualizar ONTAP Mediator"](#).

▼ Ejemplo de instalación de ONTAP Mediator con soporte HTTPS e iSCSI (salida de consola)

```
[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/ONTAP-Mediator-production.pub
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-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 ~]# 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

+ Checking that required ports 3260 and 31784 are free

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

Would you like to use the default account names: netapp + mediatoradmin? (Y(es)/n(o)): yes

Enter ONTAP Mediator user account (mediatoradmin) password:

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

+ Checking if SELinux is in enforcing mode

SELinux is set to Enforcing. ONTAP Mediator server requires modifying the SELinux context of the file

/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to 'bin_t'.

This is necessary to start the ONTAP Mediator service while SELinux is set to Enforcing.

Allow SELinux context change? Y(es)/n(o): yes
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.

+ Checking for default Linux firewall

+ Installing required packages.

Last metadata expiration check: 2:16:00 ago on Tue 24 Mar 2026
12:58:28 PM EDT.

Package openssl-1:3.5.1-7.0.1.el9_7.x86_64 is already installed.

Package openssl-devel-1:3.5.1-7.0.1.el9_7.x86_64 is already installed.

Package kernel-uek-devel-6.12.0-109.67.6.el9uek.x86_64 is already
installed.

Package gcc-11.5.0-11.0.2.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-16-12.0.1.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 python3.12-3.12.12-4.0.1.el9_7.1.x86_64 is already installed.

Package python3.12-devel-3.12.12-4.0.1.el9_7.1.x86_64 is already
installed.

Package gcc-toolset-14-14.0-2.el9.x86_64 is already installed.

Dependencies resolved.

=====

Package	Architecture	Version
Repository	Size	

=====

Installing:

efibootmgr	x86_64	18-
------------	--------	-----

8.el10	baseos	47 k
mokutil	x86_64	
2:0.7.2-1.el10	baseos	48 k
patch	x86_64	2.7.6-
26.el10	appstream	131 k
perl-ExtUtils-MakeMaker	noarch	2:7.70-
513.el10	appstream	295 k
python3-devel	x86_64	
3.12.12-4.el10_1	appstream	329 k
python3-pip	noarch	23.3.2-
7.el10	appstream	3.2 M
Upgrading:		
libselinux	x86_64	3.9-
1.el10	baseos	97 k
libselinux-utils	x86_64	3.9-
1.el10	baseos	122 k
libsemanage	x86_64	3.9-
1.el10	baseos	122 k
libsepol	x86_64	3.9-
1.el10	baseos	348 k
policycoreutils	x86_64	3.9-
1.el10	baseos	224 k
policycoreutils-python-utils	noarch	3.9-
1.el10	appstream	51 k
python-unversioned-command	noarch	
3.12.12-4.el10_1	appstream	11 k
python3	x86_64	
3.12.12-4.el10_1	baseos	28 k
python3-libs	x86_64	
3.12.12-4.el10_1	baseos	9.4 M
python3-libselinux	x86_64	3.9-
1.el10	appstream	200 k
python3-libsemanage	x86_64	3.9-
1.el10	appstream	81 k
python3-policycoreutils	noarch	3.9-
1.el10	appstream	2.2 M
Installing dependencies:		
annobin-docs	noarch	12.99-
1.el10	appstream	88 k
annobin-plugin-gcc	x86_64	12.99-
1.el10	appstream	998 k
dwz	x86_64	0.16-
1.el10	appstream	139 k
efi-filesystem	noarch	6-
7.el10.rocky.0.1	baseos	7.8 k
efi-srpm-macros	noarch	6-

7.el10.rocky.0.1	appstream	22 k
efivar-libs	x86_64	39-
3.el10	baseos	127 k
fonts-srpm-macros	noarch	
1:2.0.5-18.el10	appstream	26 k
forge-srpm-macros	noarch	0.4.0-
6.el10	appstream	20 k
gcc-plugin-annobin	x86_64	14.3.1-
2.1.el10	appstream	67 k
go-srpm-macros	noarch	3.6.0-
7.el10_1	appstream	27 k
kernel-srpm-macros	noarch	1.0-
26.el10	appstream	9.4 k
lua-srpm-macros	noarch	1-
15.el10	appstream	8.8 k
ocaml-srpm-macros	noarch	10-
4.el10	appstream	9.2 k
openblas-srpm-macros	noarch	2-
19.el10	appstream	7.7 k
package-notes-srpm-macros	noarch	0.5-
13.el10	appstream	9.2 k
perl-AutoSplit	noarch	5.74-
512.2.el10_0	appstream	21 k
perl-Benchmark	noarch	1.25-
512.2.el10_0	appstream	27 k
perl-CPAN-Meta-Requirements	noarch	2.143-
11.el10	appstream	35 k
perl-CPAN-Meta-YAML	noarch	0.018-
512.el10	appstream	26 k
perl-Devel-PPPort	x86_64	3.72-
512.el10	appstream	219 k
perl-ExtUtils-Command	noarch	2:7.70-
513.el10	appstream	14 k
perl-ExtUtils-Constant	noarch	0.25-
512.2.el10_0	appstream	43 k
perl-ExtUtils-Install	noarch	2.22-
511.el10	appstream	43 k
perl-ExtUtils-Manifest	noarch	1:1.75-
511.el10	appstream	34 k
perl-ExtUtils-ParseXS	noarch	1:3.51-
512.el10	appstream	189 k
perl-File-Compare	noarch	
1.100.800-512.2.el10_0	appstream	13 k
perl-File-Copy	noarch	2.41-
512.2.el10_0	appstream	20 k
perl-I18N-Langinfo	x86_64	0.24-

512.2.el10_0	appstream	25 k
perl-JSON-PP	noarch	1:4.16-
512.el10	appstream	66 k
perl-Test-Harness	noarch	1:3.48-
512.el10	appstream	282 k
perl-lib	x86_64	0.65-
512.2.el10_0	appstream	15 k
perl-srpm-macros	noarch	1-
57.el10	appstream	8.5 k
perl-version	x86_64	
8:0.99.32-4.el10	appstream	63 k
pyproject-srpm-macros	noarch	1.16.2-
1.el10	appstream	14 k
python-srpm-macros	noarch	3.12-
10.el10	appstream	23 k
python3-pyparsing	noarch	3.1.1-
7.el10	baseos	271 k
qt6-srpm-macros	noarch	6.9.1-
1.el10	appstream	9.6 k
redhat-rpm-config	noarch	293-
1.el10.rocky.0.2	appstream	78 k
rust-toolset-srpm-macros	noarch	1.88.0-
1.el10	appstream	12 k
systemtap-sdt-devel	x86_64	5.3-
3b.el10	appstream	69 k
systemtap-sdt-dtrace	x86_64	5.3-
3b.el10	appstream	70 k
Installing weak dependencies:		
perl-CPAN-Meta	noarch	
2.150010-511.el10	appstream	197 k
perl-Encode-Locale	noarch	1.05-
31.el10	appstream	18 k
perl-Time-HiRes	x86_64	
4:1.9777-511.el10	appstream	58 k
perl-devel	x86_64	
4:5.40.2-512.2.el10_0	appstream	770 k
perl-doc	noarch	5.40.2-
512.2.el10_0	appstream	4.9 M

Transaction Summary

```

=====
=====

```

Install 52 Packages

Upgrade 12 Packages

Total download size: 26 M

```
Is this ok [y/N]: y
Downloading Packages:
(1/64): efi-filesystem-6-7.el10.rocky.0.1.noarch.rpm
206 kB/s | 7.8 kB      00:00
(2/64): efibootmgr-18-8.el10.x86_64.rpm
1.2 MB/s | 47 kB      00:00
(3/64): efivar-libs-39-3.el10.x86_64.rpm
2.8 MB/s | 127 kB     00:00
(4/64): mokutil-0.7.2-1.el10.x86_64.rpm
6.4 MB/s | 48 kB      00:00
(5/64): annobin-docs-12.99-1.el10.noarch.rpm
11 MB/s | 88 kB       00:00
(6/64): python3-pyparsing-3.1.1-7.el10.noarch.rpm
13 MB/s | 271 kB      00:00
(7/64): dwz-0.16-1.el10.x86_64.rpm
12 MB/s | 139 kB      00:00
(8/64): efi-srpm-macros-6-7.el10.rocky.0.1.noarch.rpm
2.7 MB/s | 22 kB      00:00
(9/64): fonts-srpm-macros-2.0.5-18.el10.noarch.rpm
5.1 MB/s | 26 kB      00:00
(10/64): forge-srpm-macros-0.4.0-6.el10.noarch.rpm
4.3 MB/s | 20 kB      00:00
(11/64): gcc-plugin-annobin-14.3.1-2.1.el10.x86_64.rpm
10 MB/s | 67 kB       00:00
(12/64): go-srpm-macros-3.6.0-7.el10_1.noarch.rpm
4.7 MB/s | 27 kB      00:00
(13/64): kernel-srpm-macros-1.0-26.el10.noarch.rpm
2.0 MB/s | 9.4 kB     00:00
(14/64): lua-srpm-macros-1-15.el10.noarch.rpm
2.0 MB/s | 8.8 kB     00:00
(15/64): ocaml-srpm-macros-10-4.el10.noarch.rpm
2.0 MB/s | 9.2 kB     00:00
(16/64): annobin-plugin-gcc-12.99-1.el10.x86_64.rpm
16 MB/s | 998 kB      00:00
(17/64): openblas-srpm-macros-2-19.el10.noarch.rpm
432 kB/s | 7.7 kB     00:00
(18/64): package-notes-srpm-macros-0.5-13.el10.noarch.rpm
519 kB/s | 9.2 kB     00:00
(19/64): perl-AutoSplit-5.74-512.2.el10_0.noarch.rpm
4.5 MB/s | 21 kB      00:00
(20/64): patch-2.7.6-26.el10.x86_64.rpm
14 MB/s | 131 kB      00:00
(21/64): perl-Benchmark-1.25-512.2.el10_0.noarch.rpm
3.5 MB/s | 27 kB      00:00
(22/64): perl-CPAN-Meta-Requirements-2.143-11.el10.noarch.rpm
10 MB/s | 35 kB       00:00
```

```
(23/64): perl-CPAN-Meta-YAML-0.018-512.el10.noarch.rpm
5.3 MB/s | 26 kB      00:00
(24/64): perl-CPAN-Meta-2.150010-511.el10.noarch.rpm
12 MB/s | 197 kB     00:00
(25/64): perl-Encode-Locale-1.05-31.el10.noarch.rpm
2.6 MB/s | 18 kB     00:00
(26/64): perl-ExtUtils-Command-7.70-513.el10.noarch.rpm
3.0 MB/s | 14 kB     00:00
(27/64): perl-Devel-PPPort-3.72-512.el10.x86_64.rpm
13 MB/s | 219 kB     00:00
(28/64): perl-ExtUtils-Constant-0.25-512.2.el10_0.noarch.rpm
4.9 MB/s | 43 kB     00:00
(29/64): perl-ExtUtils-Install-2.22-511.el10.noarch.rpm
4.7 MB/s | 43 kB     00:00
(30/64): perl-ExtUtils-Manifest-1.75-511.el10.noarch.rpm
6.2 MB/s | 34 kB     00:00
(31/64): perl-File-Compare-1.100.800-512.2.el10_0.noarch.rpm
4.2 MB/s | 13 kB     00:00
(32/64): perl-ExtUtils-MakeMaker-7.70-513.el10.noarch.rpm
17 MB/s | 295 kB     00:00
(33/64): perl-ExtUtils-ParseXS-3.51-512.el10.noarch.rpm
11 MB/s | 189 kB     00:00
(34/64): perl-File-Copy-2.41-512.2.el10_0.noarch.rpm
1.7 MB/s | 20 kB     00:00
(35/64): perl-Il8N-Langinfo-0.24-512.2.el10_0.x86_64.rpm
5.0 MB/s | 25 kB     00:00
(36/64): perl-JSON-PP-4.16-512.el10.noarch.rpm
9.3 MB/s | 66 kB     00:00
(37/64): perl-Time-HiRes-1.9777-511.el10.x86_64.rpm
11 MB/s | 58 kB     00:00
(38/64): perl-Test-Harness-3.48-512.el10.noarch.rpm
13 MB/s | 282 kB     00:00
(39/64): perl-lib-0.65-512.2.el10_0.x86_64.rpm
4.4 MB/s | 15 kB     00:00
(40/64): perl-srpm-macros-1-57.el10.noarch.rpm
2.7 MB/s | 8.5 kB    00:00
(41/64): perl-devel-5.40.2-512.2.el10_0.x86_64.rpm
19 MB/s | 770 kB     00:00
(42/64): perl-version-0.99.32-4.el10.x86_64.rpm
4.3 MB/s | 63 kB     00:00
(43/64): pyproject-srpm-macros-1.16.2-1.el10.noarch.rpm
4.5 MB/s | 14 kB     00:00
(44/64): python-srpm-macros-3.12-10.el10.noarch.rpm
5.1 MB/s | 23 kB     00:00
(45/64): python3-devel-3.12.12-4.el10_1.x86_64.rpm
20 MB/s | 329 kB     00:00
```

```

(46/64): qt6-srpm-macros-6.9.1-1.el10.noarch.rpm
3.0 MB/s | 9.6 kB      00:00
(47/64): redhat-rpm-config-293-1.el10.rocky.0.2.noarch.rpm
16 MB/s | 78 kB       00:00
(48/64): rust-toolset-srpm-macros-1.88.0-1.el10.noarch.rpm
3.6 MB/s | 12 kB      00:00
(49/64): systemtap-sdt-devel-5.3-3b.el10.x86_64.rpm
11 MB/s | 69 kB       00:00
(50/64): systemtap-sdt-dtrace-5.3-3b.el10.x86_64.rpm
16 MB/s | 70 kB       00:00
(51/64): libselinux-3.9-1.el10.x86_64.rpm
10 MB/s | 97 kB       00:00
(52/64): libselinux-utils-3.9-1.el10.x86_64.rpm
14 MB/s | 122 kB      00:00
(53/64): libsemanage-3.9-1.el10.x86_64.rpm
13 MB/s | 122 kB      00:00
(54/64): libsepol-3.9-1.el10.x86_64.rpm
18 MB/s | 348 kB      00:00
(55/64): python3-pip-23.3.2-7.el10.noarch.rpm
21 MB/s | 3.2 MB      00:00
(56/64): policycoreutils-3.9-1.el10.x86_64.rpm
4.3 MB/s | 224 kB     00:00
(57/64): python3-3.12.12-4.el10_1.x86_64.rpm
5.7 MB/s | 28 kB      00:00
(58/64): policycoreutils-python-utils-3.9-1.el10.noarch.rpm
6.7 MB/s | 51 kB      00:00
(59/64): perl-doc-5.40.2-512.2.el10_0.noarch.rpm
17 MB/s | 4.9 MB      00:00
(60/64): python-unversioned-command-3.12.12-4.el10_1.noarch.rpm
175 kB/s | 11 kB      00:00
(61/64): python3-libselinux-3.9-1.el10.x86_64.rpm
16 MB/s | 200 kB      00:00
(62/64): python3-libsemanage-3.9-1.el10.x86_64.rpm
7.0 MB/s | 81 kB      00:00
(63/64): python3-policycoreutils-3.9-1.el10.noarch.rpm
28 MB/s | 2.2 MB      00:00
(64/64): python3-libs-3.12.12-4.el10_1.x86_64.rpm
31 MB/s | 9.4 MB      00:00
-----
-----
Total
19 MB/s | 26 MB      00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.

```

Running transaction

```
Preparing      :
1/1
  Upgrading     : python3-libs-3.12.12-4.el10_1.x86_64
1/76
  Upgrading     : python-unversioned-command-3.12.12-
4.el10_1.noarch
2/76
  Upgrading     : python3-3.12.12-4.el10_1.x86_64
3/76
  Upgrading     : libsepol-3.9-1.el10.x86_64
4/76
  Upgrading     : libselinux-3.9-1.el10.x86_64
5/76
  Running scriptlet: libselinux-3.9-1.el10.x86_64
5/76
  Installing    : perl-version-8:0.99.32-4.el10.x86_64
6/76
  Installing    : perl-File-Copy-2.41-512.2.el10_0.noarch
7/76
  Installing    : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
8/76
  Upgrading     : libsemanage-3.9-1.el10.x86_64
9/76
  Upgrading     : python3-libselinux-3.9-1.el10.x86_64
10/76
  Installing    : perl-Time-HiRes-4:1.9777-511.el10.x86_64
11/76
  Installing    : perl-JSON-PP-1:4.16-512.el10.noarch
12/76
  Installing    : perl-File-Compare-1.100.800-512.2.el10_0.noarch
13/76
  Installing    : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
14/76
  Installing    : efivar-libs-39-3.el10.x86_64
15/76
  Upgrading     : python3-libsemanage-3.9-1.el10.x86_64
16/76
  Installing    : perl-ExtUtils-Command-2:7.70-513.el10.noarch
17/76
  Installing    : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
18/76
  Upgrading     : libselinux-utils-3.9-1.el10.x86_64
19/76
  Upgrading     : policycoreutils-3.9-1.el10.x86_64
20/76
```

```
Running scriptlet: policycoreutils-3.9-1.el10.x86_64
20/76
  Upgrading      : python3-policycoreutils-3.9-1.el10.noarch
21/76
  Installing     : python3-pyparsing-3.1.1-7.el10.noarch
22/76
  Installing     : systemtap-sdt-dtrace-5.3-3b.el10.x86_64
23/76
  Installing     : systemtap-sdt-devel-5.3-3b.el10.x86_64
24/76
  Installing     : python3-pip-23.3.2-7.el10.noarch
25/76
  Installing     : rust-toolset-srpm-macros-1.88.0-1.el10.noarch
26/76
  Installing     : qt6-srpm-macros-6.9.1-1.el10.noarch
27/76
  Installing     : pyproject-srpm-macros-1.16.2-1.el10.noarch
28/76
  Installing     : perl-srpm-macros-1-57.el10.noarch
29/76
  Installing     : perl-lib-0.65-512.2.el10_0.x86_64
30/76
  Installing     : perl-doc-5.40.2-512.2.el10_0.noarch
31/76
  Installing     : perl-I18N-Langinfo-0.24-512.2.el10_0.x86_64
32/76
  Installing     : perl-Encode-Locale-1.05-31.el10.noarch
33/76
  Installing     : perl-ExtUtils-Constant-0.25-512.2.el10_0.noarch
34/76
  Installing     : perl-Devel-PPPort-3.72-512.el10.x86_64
35/76
  Installing     : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
36/76
  Installing     : perl-CPAN-Meta-2.150010-511.el10.noarch
37/76
  Installing     : perl-Benchmark-1.25-512.2.el10_0.noarch
38/76
  Installing     : perl-Test-Harness-1:3.48-512.el10.noarch
39/76
  Installing     : perl-AutoSplit-5.74-512.2.el10_0.noarch
40/76
  Installing     : package-notes-srpm-macros-0.5-13.el10.noarch
41/76
  Installing     : openblas-srpm-macros-2-19.el10.noarch
42/76
```

```

Installing      : ocaml-srpm-macros-10-4.el10.noarch
43/76
Installing      : lua-srpm-macros-1-15.el10.noarch
44/76
Installing      : kernel-srpm-macros-1.0-26.el10.noarch
45/76
Installing      : gcc-plugin-annobin-14.3.1-2.1.el10.x86_64
46/76
Installing      : efi-srpm-macros-6-7.el10.rocky.0.1.noarch
47/76
Installing      : dwz-0.16-1.el10.x86_64
48/76
Installing      : annobin-docs-12.99-1.el10.noarch
49/76
Installing      : annobin-plugin-gcc-12.99-1.el10.x86_64
50/76
Installing      : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/76
Installing      : forge-srpm-macros-0.4.0-6.el10.noarch
52/76
Installing      : go-srpm-macros-3.6.0-7.el10_1.noarch
53/76
Installing      : python-srpm-macros-3.12-10.el10.noarch
54/76
Installing      : redhat-rpm-config-293-1.el10.rocky.0.2.noarch
55/76
Running scriptlet: redhat-rpm-config-293-1.el10.rocky.0.2.noarch
55/76
Installing      : perl-ExtUtils-Install-2.22-511.el10.noarch
56/76
Installing      : perl-devel-4:5.40.2-512.2.el10_0.x86_64
57/76
Installing      : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
58/76
Installing      : efi-filesystem-6-7.el10.rocky.0.1.noarch
59/76
Installing      : efibootmgr-18-8.el10.x86_64
60/76
Installing      : python3-devel-3.12.12-4.el10_1.x86_64
61/76
Upgrading       : polycoreutils-python-utils-3.9-1.el10.noarch
62/76
Installing      : mokutil-2:0.7.2-1.el10.x86_64
63/76
Installing      : patch-2.7.6-26.el10.x86_64
64/76

```

```

Cleanup          : policycoreutils-python-utils-3.8-1.el10.noarch
65/76
Cleanup          : python3-policycoreutils-3.8-1.el10.noarch
66/76
Running scriptlet: policycoreutils-3.8-1.el10.x86_64
67/76
Cleanup          : policycoreutils-3.8-1.el10.x86_64
67/76
Cleanup          : python3-libsemanage-3.8.1-1.el10_0.x86_64
68/76
Cleanup          : libsemanage-3.8.1-1.el10_0.x86_64
69/76
Cleanup          : python3-libselinux-3.8-2.el10_0.x86_64
70/76
Cleanup          : libselinux-utils-3.8-2.el10_0.x86_64
71/76
Cleanup          : python3-3.12.9-2.el10_0.2.x86_64
72/76
Cleanup          : libselinux-3.8-2.el10_0.x86_64
73/76
Cleanup          : python-unversioned-command-3.12.9-
2.el10_0.2.noarch
74/76
Cleanup          : libsepol-3.8-1.el10.x86_64
75/76
Cleanup          : python3-libs-3.12.9-2.el10_0.2.x86_64
76/76
Running scriptlet: python3-libs-3.12.9-2.el10_0.2.x86_64
76/76

Upgraded:
  libselinux-3.9-1.el10.x86_64
libselinux-utils-3.9-1.el10.x86_64
  libsemanage-3.9-1.el10.x86_64
libsepol-3.9-1.el10.x86_64
  policycoreutils-3.9-1.el10.x86_64
policycoreutils-python-utils-3.9-1.el10.noarch
  python-unversioned-command-3.12.12-4.el10_1.noarch
python3-3.12.12-4.el10_1.x86_64
  python3-libs-3.12.12-4.el10_1.x86_64
python3-libselinux-3.9-1.el10.x86_64
  python3-libsemanage-3.9-1.el10.x86_64
python3-policycoreutils-3.9-1.el10.noarch
Installed:
  annobin-docs-12.99-1.el10.noarch
annobin-plugin-gcc-12.99-1.el10.x86_64

```

dwz-0.16-1.el10.x86_64	efi-
filesystem-6-7.el10.rocky.0.1.noarch	
efi-srpm-macros-6-7.el10.rocky.0.1.noarch	
efibootmgr-18-8.el10.x86_64	
efivar-libs-39-3.el10.x86_64	
fonts-srpm-macros-1:2.0.5-18.el10.noarch	
forge-srpm-macros-0.4.0-6.el10.noarch	gcc-
plugin-annobin-14.3.1-2.1.el10.x86_64	
go-srpm-macros-3.6.0-7.el10_1.noarch	
kernel-srpm-macros-1.0-26.el10.noarch	
lua-srpm-macros-1-15.el10.noarch	
mokutil-2:0.7.2-1.el10.x86_64	
ocaml-srpm-macros-10-4.el10.noarch	
openblas-srpm-macros-2-19.el10.noarch	
package-notes-srpm-macros-0.5-13.el10.noarch	
patch-2.7.6-26.el10.x86_64	
perl-AutoSplit-5.74-512.2.el10_0.noarch	
perl-Benchmark-1.25-512.2.el10_0.noarch	
perl-CPAN-Meta-2.150010-511.el10.noarch	
perl-CPAN-Meta-Requirements-2.143-11.el10.noarch	
perl-CPAN-Meta-YAML-0.018-512.el10.noarch	
perl-Devel-PPPort-3.72-512.el10.x86_64	
perl-Encode-Locale-1.05-31.el10.noarch	
perl-ExtUtils-Command-2:7.70-513.el10.noarch	
perl-ExtUtils-Constant-0.25-512.2.el10_0.noarch	
perl-ExtUtils-Install-2.22-511.el10.noarch	
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch	
perl-ExtUtils-Manifest-1:1.75-511.el10.noarch	
perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch	
perl-File-Compare-1.100.800-512.2.el10_0.noarch	
perl-File-Copy-2.41-512.2.el10_0.noarch	
perl-I18N-Langinfo-0.24-512.2.el10_0.x86_64	
perl-JSON-PP-1:4.16-512.el10.noarch	
perl-Test-Harness-1:3.48-512.el10.noarch	
perl-Time-HiRes-4:1.9777-511.el10.x86_64	
perl-devel-4:5.40.2-512.2.el10_0.x86_64	
perl-doc-5.40.2-512.2.el10_0.noarch	
perl-lib-0.65-512.2.el10_0.x86_64	
perl-srpm-macros-1-57.el10.noarch	
perl-version-8:0.99.32-4.el10.x86_64	
pyproject-srpm-macros-1.16.2-1.el10.noarch	
python-srpm-macros-3.12-10.el10.noarch	
python3-devel-3.12.12-4.el10_1.x86_64	
python3-pip-23.3.2-7.el10.noarch	
python3-pyparsing-3.1.1-7.el10.noarch	qt6-
srpm-macros-6.9.1-1.el10.noarch	

```
redhat-rpm-config-293-1.el10.rocky.0.2.noarch
rust-toolset-srpm-macros-1.88.0-1.el10.noarch
systemtap-sdt-devel-5.3-3b.el10.x86_64
systemtap-sdt-dtrace-5.3-3b.el10.x86_64
```

Complete!

OS package installations finished

OS package installations finished

+ Installing ONTAP Mediator. (Log:

/root/ontap_mediator.pJBcIv/ontap-mediator-1.12.1/ontap-mediator-1.12.1/install_20260324151410.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_20260324151410.log)

+ WARNING: This system supports UEFI

Secure Boot (SB) is currently disabled on this system.

If SB is enabled in the future, SCST will not work

unless the following action is taken:

Using the keys in

/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow instructions in

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

to sign the SCST kernel module. Note that reboot will be needed.

SCST will not start automatically when Secure Boot is enabled and not configured properly.

+ 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 instalación de ONTAP Mediator con soporte solo para HTTPS (salida de consola)

```
[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 ~]# 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
Error querying OCSP responder
40E72F35407F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:596:
40E72F35407F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:1045:server=http://ocsp.entrust.net:80

WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate

Continue without code signature checking (only recommended if
integrity has been established manually)? y(es)/N(o): yes
SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ 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
```

```
+ Checking that required port 31784 is free
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API
(mediatoradmin).
```

```
Would you like to use the default account names: netapp +
mediatoradmin? (Y(es)/n(o)): yes
```

```
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: 0:38:52 ago on Mon 20 Apr 2026
11:23:22 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 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.CJqNqu/ontap-
mediator-1.12.1/ontap-mediator-1.12.1/install_20260420120204.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_20260420120204.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
[root@mediator_host ~]#
```

Registrar la clave de seguridad para UEFI Secure Boot

A partir de ONTAP Mediator 1.4, el mecanismo de arranque seguro (Secure Boot) está habilitado en los sistemas UEFI. Cuando el arranque seguro está habilitado, debes seguir algunos pasos adicionales para registrar la clave de seguridad después de la instalación.



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

Pasos

1. Sigue las instrucciones del archivo README para firmar el módulo del kernel SCST:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modul
e-signing
```

2. Busca las claves necesarias:

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



Tras la instalación, el sistema muestra los archivos README y la ubicación de la clave.

3. Añade la clave pública a la lista MOK:

```
mokutil --import  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_  
key.der
```



Puedes dejar la clave privada en su ubicación predeterminada o trasladarla a una ubicación segura. Debes mantener la clave pública en su ubicación actual para que Boot Manager pueda utilizarla. Para obtener más información, consulta el archivo README.module-signing:

```
[root@hostname ~]# ls  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/  
README.module-signing scst_module_key.der scst_module_key.priv
```

4. Reinicia el equipo y usa el gestor de arranque UEFI de tu dispositivo para aprobar el nuevo MOK. Necesitarás la frase de contraseña proporcionada para la utilidad `mokutil` en ["Instala ONTAP Mediator cuando el arranque seguro de UEFI esté activado"](#).

Firmar los módulos del kernel de SCST

Una vez instalado ONTAP Mediator, si `systemctl status mediator-scst` muestra `failed (inactive)`, sigue estos pasos para firmar el módulo del kernel 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.

Pasos

1. Durante el proceso de compilación, se genera un par de claves pública y privada en el directorio `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`. Ejecuta el siguiente comando para ver las claves generadas:

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

```
README.module-signing scst_module_key.der scst_module_key.priv
```

2. Inicia el proceso de importación de la clave pública al repositorio de claves de la UEFI ejecutando el siguiente comando:

```
mokutil --import  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_  
key.der
```

La utilidad `mokutil` te pide que introduzcas una contraseña dos veces.

3. El software `mokutil` solicita una contraseña temporal para usarla con esta clave durante el proceso de importación.
4. Comprueba si el proceso de importación ha comenzado con el siguiente comando y, a continuación, reinicia el sistema. El bootloader inicia el EFI MOK manager.

```
mokutil --list-new
```

5. Utiliza los menús de la pantalla para activar la clave del módulo del kernel SCST. Después de arrancar, ejecuta el siguiente comando. Una vez que se inicia el servicio, se firman los módulos del kernel SCST.

```
systemctl status mediator-scst
```

¿Y ahora qué?

["Comprueba el estado de la instalación de ONTAP Mediator"](#)

Comprueba el estado de la instalación de ONTAP Mediator

Una vez instalado ONTAP Mediator, comprueba que se esté ejecutando correctamente.

Pasos

1. Ver el estado de ONTAP Mediator:

```
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
```

2. Consulta el estado de SCST:

```
systemctl status mediator-scst
```



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

```
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
```

3. Comprueba los puertos que utiliza ONTAP Mediator:

```
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
```

¿Qué sigue?

Una vez instalado y comprobado ONTAP Mediator, puedes continuar con las siguientes tareas de configuración posteriores a la instalación:

- ["Utiliza ONTAP Mediator para la sincronización activa de SnapMirror y MetroCluster IP"](#)
- ["Configurar los atributos de ONTAP Mediator"](#) (Opcional)

Usa ONTAP Mediator

Utiliza ONTAP Mediator para la sincronización activa de SnapMirror y MetroCluster IP

ONTAP Mediator se ejecuta en un host Linux en un tercer dominio de fallos, independiente de tus clústeres de ONTAP, donde proporciona un almacén persistente y aislado para los metadatos de alta disponibilidad (HA). ONTAP utiliza este almacén, junto con las funciones de consulta del estado de los nodos y de proxy de ping de Mediator, para supervisar las relaciones de sincronización activa de SnapMirror y las configuraciones IP de MetroCluster.



Esta documentación se refiere a la versión on-premises de ONTAP Mediator. Para obtener información sobre ONTAP Cloud Mediator, disponible a partir de ONTAP 9.17.1, consulta ["SnapMirror documentación de active sync"](#).

Supervisar las relaciones de sincronización activa de SnapMirror

SnapMirror active sync utiliza ONTAP Mediator como testigo pasivo de las copias principal y espejo en un grupo de consistencia. Si se produce una partición de red o una de las copias deja de estar disponible, SnapMirror active sync consulta a ONTAP Mediator para determinar qué copia sigue atendiendo la E/S y detiene la E/S en la otra copia.

A partir de ONTAP 9.8, puedes utilizar cualquier versión de ONTAP Mediator para supervisar una relación de sincronización activa de SnapMirror.



Para conocer los límites en cuanto al número de pares de clústeres de sincronización activa de SnapMirror que puede supervisar una sola instancia de ONTAP Mediator, consulta ["Límites de objetos para ONTAP SnapMirror active sync"](#).

["Configura ONTAP Mediator para SnapMirror active sync"](#)

Supervisa las configuraciones IP de MetroCluster

En una configuración IP de MetroCluster, ONTAP Mediator almacena información de estado sobre los nodos de MetroCluster en LUN de buzón y ayuda a los nodos con una conmutación de sitios automática no planificada asistida por Mediator (MAUSO) en caso de desastre o de situaciones específicas de fallo.

A partir de ONTAP 9.19.1 y ONTAP Mediator 1.12, puedes configurar un ONTAP Mediator que use HTTPS para la comunicación a fin de supervisar tu configuración IP de MetroCluster. Al configurar ONTAP Mediator con el protocolo iSCSI, puedes usar cualquier versión de ONTAP Mediator para supervisar una configuración IP de MetroCluster.



Para conocer los límites en cuanto al número de configuraciones de IP de MetroCluster que puede supervisar una única instancia de ONTAP Mediator, consulte ["Utiliza ONTAP Mediator para supervisar varias configuraciones de MetroCluster IP"](#)

["Configura ONTAP Mediator para una configuración IP de MetroCluster"](#)

Información relacionada

- ["Arquitectura de sincronización activa de ONTAP SnapMirror"](#)
- ["Descubre cómo ONTAP Mediator admite la conmutación de sitios automática no planificada en una configuración IP de MetroCluster"](#)

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.



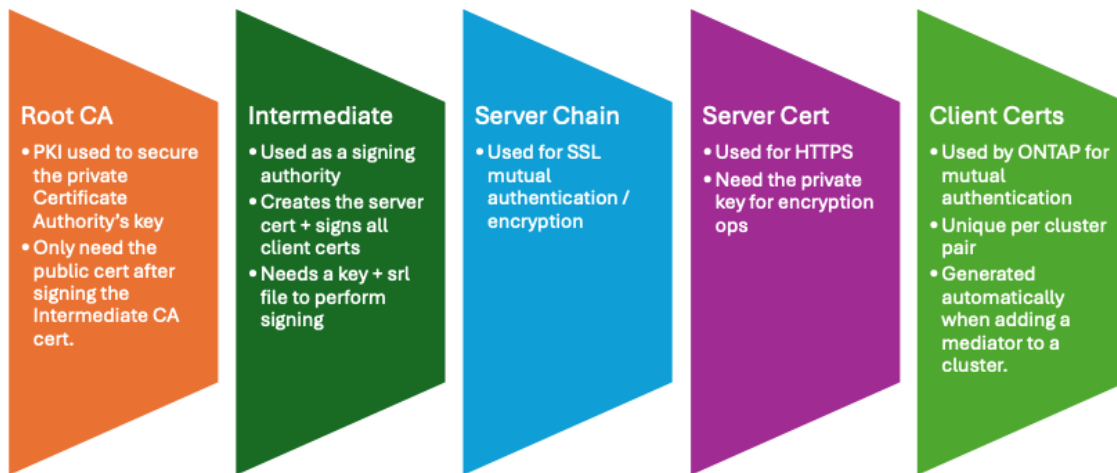
- Los certificados de terceros solo son compatibles a partir de ONTAP 9.16.1 y en algunas versiones de parche anteriores de ONTAP. Consulta ["ID de bug CONTAP-243278 de NetApp Bugs Online"](#).

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

Acerca de esta tarea

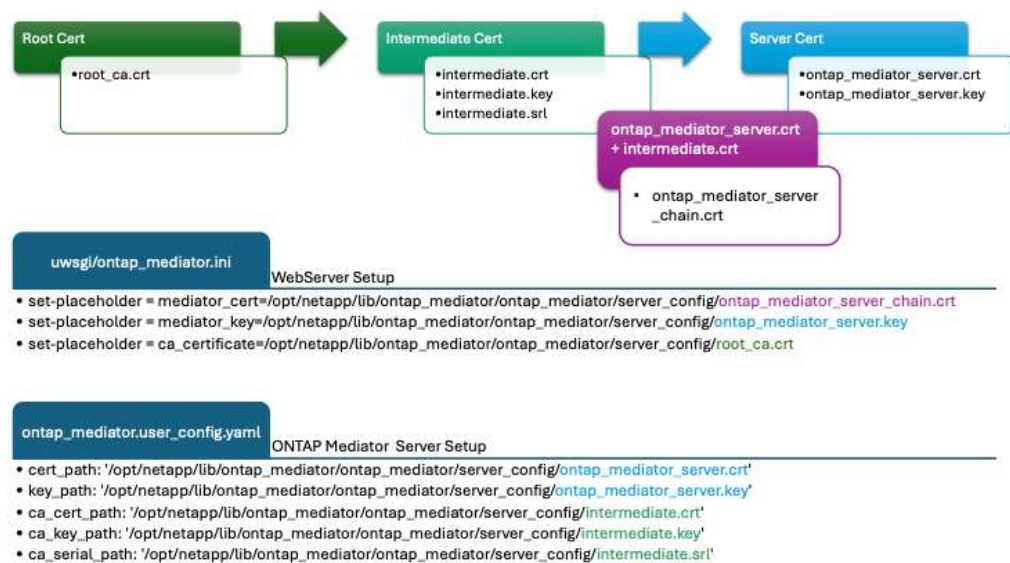
- Realiza esta tarea en el host Linux en el que hayas instalado ONTAP Mediator.
- Puedes realizar esta tarea si es necesario sustituir los certificados autofirmados generados por certificados obtenidos de una autoridad de certificación (CA) subordinada de confianza. Para ello, debes tener acceso a una 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 ~]#
```

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas registradas, patentes y más.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas registradas

NETAPP, el logotipo de NETAPP y las marcas que aparecen en la página de NetApp Trademarks son marcas comerciales de NetApp, Inc. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Una lista actual de patentes propiedad de NetApp se puede encontrar en:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de privacidad

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Código abierto

Los archivos de aviso proporcionan información sobre los derechos de autor y las licencias de terceros utilizadas en el software NetApp.

ONTAP Mediator para MetroCluster IP y la sincronización activa de SnapMirror

- ["Aviso sobre ONTAP Mediator 1.12.1"](#)
- ["Aviso sobre ONTAP Mediator 1.11"](#)
- ["Aviso sobre ONTAP Mediator 1.10"](#)
- ["Aviso sobre ONTAP Mediator 1.9.1"](#)
- ["Aviso sobre ONTAP Mediator 1.8"](#)
- ["Aviso sobre ONTAP Mediator 1.7"](#)
- ["Aviso sobre ONTAP Mediator 1.5"](#)

Información de copyright

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

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

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

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

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

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

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

Información de la marca comercial

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