



# **Mediatore ONTAP per MetroCluster e SnapMirror ActiveSync**

## **ONTAP 9**

NetApp  
February 12, 2026

This PDF was generated from <https://docs.netapp.com/it-it/ontap/mediator/mediator-overview-concept.html> on February 12, 2026. Always check docs.netapp.com for the latest.

# Sommario

Mediatore ONTAP per MetroCluster e SnapMirror ActiveSync .....	1
Ulteriori informazioni su ONTAP Mediator .....	1
Strumenti forniti all'amministratore di sistema .....	1
Note speciali .....	2
Nuove funzionalità di ONTAP Mediator .....	2
Miglioramenti .....	2
Matrice di supporto del sistema operativo .....	4
Matrice di supporto SCST .....	7
Installare o aggiornare .....	8
Riepilogo del flusso di lavoro di installazione di ONTAP Mediator .....	8
Installa o aggiorna ONTAP Mediator .....	9
Aggiornare il sistema operativo host e ONTAP Mediator .....	14
Fornire l'accesso al repository per l'installazione di ONTAP Mediator .....	19
Scaricare il pacchetto di installazione di ONTAP Mediator .....	26
Verificare la firma del codice del mediatore ONTAP .....	27
Installare il pacchetto di installazione di ONTAP Mediator .....	29
Verificare lo stato dell'installazione di ONTAP Mediator .....	45
Configurazione ONTAP Mediator post-installazione .....	46
Gestione di ONTAP Mediator .....	51
Modificare il nome utente .....	51
Modificare la password .....	52
Stop ONTAP Mediator .....	53
Riattivare ONTAP Mediator .....	53
Verificare che ONTAP Mediator sia integro .....	54
Disinstallare ONTAP Mediator .....	55
Rigenerare un certificato autofirmato temporaneo .....	56
Sostituire i certificati autofirmati con certificati di terze parti attendibili .....	57
Risolvere i problemi relativi ai certificati .....	74
Gestire il sistema operativo host per ONTAP Mediator .....	81
Riavviare l'host .....	81
Aggiornamenti dei pacchetti host .....	81
Aggiornare il kernel del sistema operativo host .....	81
Eseguire la manutenzione dell'host .....	81
L'host modifica il nome host o l'IP .....	84

# Mediatore ONTAP per MetroCluster e SnapMirror ActiveSync

## Ulteriori informazioni su ONTAP Mediator

Questa documentazione si riferisce alla versione on-premise di ONTAP Mediator. Per informazioni su ONTAP Cloud Mediator, disponibile a partire da ONTAP 9.17.1, consultare ["Documentazione sulla sincronizzazione attiva SnapMirror"](#).

ONTAP Mediator fornisce diverse funzioni per le funzionalità ONTAP:

- Fornisce un archivio persistente e recintato per i metadati ha.
- Funge da proxy ping per la vivacità del controller.
- Fornisce una funzionalità di query sincrona sullo stato dei nodi per agevolare la determinazione del quorum.

ONTAP Mediator fornisce due servizi systemctl aggiuntivi:

- **ontap\_mediator.service**

Gestisce il server REST API per la gestione delle relazioni ONTAP.

- **mediator-scst.service**

Controlla l'avvio e lo spegnimento del modulo iSCSI (SCST).

## Strumenti forniti all'amministratore di sistema

Strumenti forniti all'amministratore di sistema:

- **/usr/local/bin/mediator\_change\_password**

Imposta una nuova password API quando vengono forniti il nome utente e la password API correnti.

- **/usr/local/bin/mediator\_change\_user**

Imposta un nuovo nome utente API quando vengono forniti il nome utente e la password API correnti.

- **/usr/local/bin/mediator\_generate\_support\_bundle**

Genera un file tgz locale contenente tutte le informazioni di supporto utili necessarie per la comunicazione con il supporto clienti NetApp. Ciò include la configurazione dell'applicazione, i registri e alcune informazioni di sistema. I bundle vengono generati sul disco locale e possono essere trasferiti manualmente, se necessario. Ubicazione dello storage: /Opt/netapp/data/support\_bundle/

- **/usr/local/bin/uninstall\_ontap\_mediator**

Rimuove il pacchetto ONTAP Mediator e il modulo kernel SCST. Sono inclusi tutti i dati di configurazione, registri e mailbox.

- `/usr/local/bin/mediator_unlock_user`

Rilascia un blocco sull'account utente API se viene raggiunto il limite di tentativi di autenticazione. Questa funzione viene utilizzata per impedire la derivazione della password con forza bruta. Viene richiesto all'utente di inserire il nome utente e la password corretti.

- `/usr/local/bin/mediator_add_user`

(Solo supporto) utilizzato per aggiungere l'utente API al momento dell'installazione.

## Note speciali

ONTAP Mediator si affida a SCST per la fornitura di iSCSI (vedere <http://scst.sourceforge.net/index.html>). Questo pacchetto è un modulo del kernel che viene compilato durante l'installazione specificamente per il kernel. Qualsiasi aggiornamento del kernel potrebbe richiedere la reinstallazione di SCST. In alternativa, disinstallare e reinstallare ONTAP Mediator, quindi riconfigurare la relazione ONTAP.



Qualsiasi aggiornamento del kernel del sistema operativo del server deve essere coordinato con una finestra di manutenzione in ONTAP.

## Nuove funzionalità di ONTAP Mediator

Con ogni versione vengono forniti nuovi miglioramenti a ONTAP Mediator. Ecco le novità.

### Miglioramenti

Per informazioni sulla versione di SCST, vedere [Matrice di supporto SCST](#).

Versione del mediatore ONTAP	Miglioramenti
1,11	<ul style="list-style-type: none"> <li>• Supporto per RHEL: <ul style="list-style-type: none"> <li>◦ Compatibile: 9.5.</li> <li>◦ Consigliati: 10.1, 10.0, 9.7, 9.6, 9.4 e 8.10.</li> </ul> </li> <li>• Supporto per Rocky Linux 10.1, 9.7 e 8,10.</li> <li>• Supporto per Oracle Linux 10.0 e 9.6.</li> <li>• Aggiunge il supporto per IPv6 per le configurazioni IP MetroCluster .</li> <li>• Aggiunge il supporto per fapolicyd.</li> </ul>
1,10	<ul style="list-style-type: none"> <li>• Supporto per RHEL: <ul style="list-style-type: none"> <li>◦ Compatibile: 9.5.</li> <li>◦ Consigliati: 10.0, 9.6, 9.4 e 8,10.</li> </ul> </li> <li>• Supporto per Rocky Linux 10.0, 9.6 e 8,10.</li> <li>• Aggiorna la versione base di Python da Python 3.9 a Python 3.12.</li> </ul>

1.9.1	<ul style="list-style-type: none"> <li>• Supporto per RHEL: <ul style="list-style-type: none"> <li>◦ Compatibile: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 e 8.4.</li> <li>◦ Consigliati: 9.5, 9.4, 9.2, 9.0, 8.10 e 8.8.</li> </ul> </li> <li>• Supporto per Rocky Linux 9.5 e 8.10.</li> <li>• Aggiunge nuovi certificati per la verifica della firma del codice.</li> <li>• Aggiunto supporto per saltare i controlli della firma del codice utilizzando <code>-skip-code-signature-check</code> bandiera.</li> <li>• Il programma di installazione visualizza avvisi quando rileva certificati di firma del codice scaduti.</li> </ul>
1,9	<ul style="list-style-type: none"> <li>• Supporto per RHEL: <ul style="list-style-type: none"> <li>◦ Compatibile: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 e 8.4.</li> <li>◦ Consigliati: 9.5, 9.4, 9.2, 9.0, 8.10 e 8.8.</li> </ul> </li> <li>• Supporto per Rocky Linux 9.5 e 8.10.</li> <li>• Supporto FIPS per RHEL e Rocky Linux.</li> <li>• Aggiunti miglioramenti delle performance per una maggiore scalabilità.</li> <li>• Nomi file migliorati per semplificare la configurazione dei certificati firmati PKI.</li> </ul>
1,8	<ul style="list-style-type: none"> <li>• Supporto per RHEL: <ul style="list-style-type: none"> <li>◦ Compatibile: 8.7, 8.6, 8.5 e 8.4.</li> <li>◦ Consigliati: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 e 8.8.</li> </ul> </li> <li>• Supporto per Rocky Linux 9.4 e 8.10.</li> </ul>
1,7	<ul style="list-style-type: none"> <li>• Supporto per RHEL: <ul style="list-style-type: none"> <li>◦ Compatibile: 8.7, 8.6, 8.5 e 8.4.</li> <li>◦ Consigliati: 9.3, 9.2, 9.1, 9.0, 8.9 e 8.8.</li> </ul> </li> <li>• Supporto per Rocky Linux 9.3 e 8.9.</li> <li>• Supporto per i dati SAN (Subject alternative Name) con certificati autofirmati e certificati firmati da terzi.</li> </ul>
1.6	<ul style="list-style-type: none"> <li>• Aggiornamenti di Python 3.9.</li> <li>• Supporto per RHEL: <ul style="list-style-type: none"> <li>◦ Compatibile: 8.7, 8.6, 8.5 e 8.4.</li> <li>◦ Consigliati: 9.2, 9.1, 9.0 e 8.8.</li> </ul> </li> <li>• Supporto per Rocky Linux 9.2 e 8.8.</li> <li>• Supporto interrotto per tutte le release di RHEL 7.x / CentOS.</li> </ul>

1.5	<ul style="list-style-type: none"> <li>• Supporto per RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 e 7.6.</li> <li>• Supporto per CentOS 7.9, 7.8, 7.7 e 7.6.</li> <li>• Include avvisi di deprecazione per RHEL 7.x / CentOS 7.x.</li> <li>• Ottimizza la velocità per sistemi di sincronizzazione attiva SnapMirror su larga scala.</li> <li>• È stata aggiunta una firma crittografica al programma di installazione.</li> </ul>
1.4	<ul style="list-style-type: none"> <li>• Supporto per RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 e 7.6.</li> <li>• Supporto per CentOS 7.9, 7.8, 7.7 e 7.6.</li> <li>• Aggiunto supporto per Secure Boot (SB) del firmware basato su UEFI.</li> </ul>
1.3	<ul style="list-style-type: none"> <li>• Supporto per RHEL 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 e 7.6.</li> <li>• Supporto per CentOS 7.9, 7.8, 7.7 e 7.6.</li> </ul>
1.2	<ul style="list-style-type: none"> <li>• Supporto per RHEL 8.1, 8.0, 7.9, 7.8, 7.7 e 7.6.</li> <li>• Supporto per CentOS 7.9, 7.8, 7.7 e 7.6.</li> <li>• Supporto per le cassette postali HTTPS.</li> <li>• Da utilizzare con ONTAP 9,8+ MCC-IP AURO e con ZRTO Active Sync di SnapMirror.</li> </ul>
1.1	<ul style="list-style-type: none"> <li>• Supporto per RHEL 8.0 e 7.6.</li> <li>• Supporto per CentOS 7,6.</li> <li>• Elimina le dipendenze Perl.</li> </ul>
1.0	<ul style="list-style-type: none"> <li>• Supporto per cassette postali iSCSI.</li> <li>• Per l'utilizzo con ONTAP 9.7+ MCC-IP AURO.</li> <li>• Supporto per RHEL/CentOS 7.6.</li> </ul>

## Matrice di supporto del sistema operativo

So per mediat ore ONTA P	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 10.1	Sì	No	No	No	No	No	No	No	No	No	No	No	No
RHEL 10.0	Sì	Sì	Sì	No	No	No	No	No	No	No	No	No	No

RHEL 9.7	Sì	No	No	No	No	No	No	No	No	No	No	No	No
RHEL 9.6	Sì	Sì	Sì	No	No	No	No	No	No	No	No	No	No
RHEL 9,5	Comp atibile	Comp atibile	Sì	Sì	No	No	No	No	No	No	No	No	No
RHEL 9,4	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No	No	No
RHEL 9,3	No	No	Comp atibile	Comp atibile	Sì	Sì	No	No	No	No	No	No	No
RHEL 9.2	No	No	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No
RHEL 9.1	No	No	Comp atibile	Comp atibile	Sì	Sì	Sì	No	No	No	No	No	No
RHEL 9.0	No	No	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No
RHEL 8,10	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No	No	No
RHEL 8,9	No	No	Comp atibile	Comp atibile	Sì	Sì	No	No	No	No	No	No	No
RHEL 8.8	No	No	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No
RHEL 8.7	No	No	Comp atibile	Comp atibile	Sì	Sì	Sì	No	No	No	No	No	No
RHEL 8.6	No	No	Comp atibile	Comp atibile	Sì	Sì	Sì	No	No	No	No	No	No
RHEL 8.5	No	No	Comp atibile	Comp atibile	Sì	Sì	Sì	Sì	Sì	No	No	No	No
RHEL 8.4	No	No	Comp atibile	Comp atibile	Sì	Sì	Sì	Sì	Sì	No	No	No	No
RHEL 8.3	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Sì	Sì	Sì	No	No	No

RHEL 8.2	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Sì	Sì	Sì	No	No	No
RHEL 8.1	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Sì	Sì	Sì	Sì	No	No
RHEL 8.0	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Sì	Sì	Sì	Sì	Sì	No
RHEL e CentOS 7.9	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Sì	Sì	Sì	Comp atibile	No	No
RHEL e CentOS 7.8	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Sì	Sì	Sì	Sì	No	No
RHEL e CentOS 7.7	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Sì	Sì	Sì	Sì	No	No
RHEL e CentOS 7.6	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Obsol eto	Sì	Sì	Sì	Sì	Sì	Sì (solo RHEL )
CentOS 8 e streaming	No	No	No	No	No	No	No	No	No	No	N/A.	N/A.	N/A.
Rocky Linux 10,0	Sì	Sì	No	No	No	No	No	No	No	No	No	No	No
Rocky Linux 9	Sì	Sì	Sì	Sì	Sì	Sì	Sì	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.
Rocky Linux 8	Sì	Sì	Sì	Sì	Sì	Sì	Sì	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.



Oracle Linux 10,0	Sì	No	No	No	No	No	No	No	No	No	No	No	No
Oracle Linux 9	Sì	No	No	No	No	No	No	No	No	No	No	No	No

- "Sì" significa che il sistema operativo è consigliato per l'installazione di ONTAP Mediator ed è completamente compatibile e supportato.
- "No" significa che il sistema operativo e il mediatore ONTAP non sono compatibili.
- "Compatibile" significa che Red Hat non supporta più queste versioni di RHEL, ma ONTAP Mediator può ancora essere installato su di esse.
- ONTAP Mediator 1.6 aggiunge il supporto per Rocky Linux 9 e 8.
- ONTAP Mediator 1.5 è stata l'ultima release supportata per i sistemi operativi delle filiali RHEL 7.x.
- CentOS 8 è stato rimosso per tutte le release a causa della sua riramificazione. CentOS Stream non è stato considerato un sistema operativo di destinazione adatto per la produzione. Non è previsto alcun supporto.

## Matrice di supporto SCST

La tabella seguente mostra la versione SCST supportata per ciascuna versione di ONTAP Mediator.

Versione del mediatore ONTAP	Versione di SCST supportata
Mediatore ONTAP 1.11	scst-3.9.tar.gz
Mediatore ONTAP 1.10	scst-3.9.tar.gz
Mediatore ONTAP 1.9.1	scst-3,8.0.tar.bz2
ONTAP mediatore 1,9	scst-3,8.0.tar.bz2
ONTAP mediatore 1,8	scst-3,8.0.tar.bz2
ONTAP mediatore 1,7	scst-3.7.0.tar.bz2
Mediatore ONTAP 1.6	scst-3.7.0.tar.bz2
Mediatore ONTAP 1.5	scst-3.6.0.tar.bz2
Mediatore ONTAP 1.4	scst-3.6.0.tar.bz2
Mediatore ONTAP 1.3	scst-3.5.0.tar.bz2
ONTAP mediatore 1,2	scst-3.4.0.tar.bz2
Mediatore ONTAP 1.1	scst-3.4.0.tar.bz2
Mediatore ONTAP 1.0	scst-3.3.0.tar.bz2

# Installare o aggiornare

## Riepilogo del flusso di lavoro di installazione di ONTAP Mediator

L'installazione di ONTAP Mediator include la preparazione dell'installazione, la fornitura dell'accesso ai repository, il download del pacchetto di installazione, la verifica della firma del codice, l'installazione del pacchetto ONTAP Mediator e l'esecuzione di attività di configurazione post-installazione.

1

### "Prepararsi all'installazione o all'aggiornamento di ONTAP Mediator"

Per installare o aggiornare ONTAP Mediator, è necessario assicurarsi che tutti i prerequisiti siano soddisfatti.

2

### "Aggiornare il sistema operativo host e Mediator"

Se stai aggiornando una versione esistente di ONTAP Mediator, devi prima disinstallare la versione precedente e poi installare la nuova versione. Se stai installando ONTAP Mediator per la prima volta, puoi saltare questo passaggio.

3

### "Fornire l'accesso al repository"

È necessario abilitare l'accesso ai repository in modo che ONTAP Mediator possa accedere ai pacchetti richiesti durante il processo di installazione.

4

### "Scaricare il pacchetto di installazione di ONTAP Mediator"

Scaricare il pacchetto di installazione di ONTAP Mediator dalla pagina di download di ONTAP Mediator.

5

### "Verificare la firma del codice del pacchetto di installazione di ONTAP Mediator"

NetApp consiglia di verificare la firma del codice di ONTAP Mediator prima di installare il pacchetto di installazione di ONTAP Mediator.

6

### "Installa ONTAP Mediator"

Per installare ONTAP Mediator, è necessario ottenere il pacchetto di installazione ed eseguire il programma di installazione sull'host.

7

### "Verificare l'installazione di ONTAP Mediator"

Dopo aver installato ONTAP Mediator, verificare che funzioni correttamente.

8

### "Eseguire attività di configurazione post-installazione"

Dopo aver installato e avviato ONTAP Mediator, è necessario eseguire ulteriori attività di configurazione per utilizzare le funzionalità di ONTAP Mediator.

## Installa o aggiorna ONTAP Mediator

Per installare o aggiornare ONTAP Mediator, è necessario soddisfare tutti i prerequisiti, scaricare il pacchetto di installazione ed eseguire il programma di installazione sull'host.

- A partire da ONTAP 9,8, è possibile utilizzare qualsiasi versione di ONTAP Mediator per monitorare una relazione di sincronizzazione attiva di SnapMirror.
- È possibile utilizzare qualsiasi versione di ONTAP Mediator per monitorare una configurazione IP MetroCluster .

### Considerazioni sull'installazione e l'aggiornamento

Prima di aggiornare o installare ONTAP Mediator, rivedere questi punti.



ONTAP Mediator 1.8 e versioni precedenti non sono compatibili con la modalità FIPS di Red Hat Enterprise Linux (RHEL) e ne impediscono l'installazione corretta. È possibile verificare se la modalità FIPS è abilitata utilizzando `fips-mode-setup --check` comando. È possibile disattivare la modalità FIPS utilizzando `fips-modesetup --disable` comando. Riavviare dopo aver disabilitato la modalità FIPS per installare correttamente ONTAP Mediator 1.8 o versioni precedenti.

- Dovresti aggiornare ONTAP Mediator all'ultima versione. Le versioni precedenti funzionano ancora con tutte le release ONTAP , ma le versioni più recenti includono patch di sicurezza per componenti di terze parti.
- Quando si esegue l'aggiornamento a una nuova versione di ONTAP Mediator, il programma di installazione esegue automaticamente l'aggiornamento alla versione SCST consigliata, a meno che non sia disponibile una versione successiva. Per istruzioni sull'installazione manuale di una versione SCST superiore, vedere ["Gestione di ONTAP Mediator"](#). Per le versioni supportate, vedere ["Matrice di supporto SCST"](#).



- Se l'installazione non riesce, potrebbe essere necessario eseguire l'aggiornamento a una versione più recente di ONTAP Mediator.
- Dal 15 giugno 2025 non sarà più possibile installare o aggiornare ONTAP Mediator 1.9 e 1.8 perché i relativi certificati di firma del codice sono scaduti. Se l'installazione o l'aggiornamento non riesce, utilizzare invece la versione patch ONTAP Mediator 1.9.1.

- Se si installa `yum-utils` è possibile utilizzare `needs-restarting` comando.
- A partire da ONTAP Mediator 1.11, IPv6 è supportato per le configurazioni IP MetroCluster .

### Requisiti dell'host

Attenersi a questi requisiti durante l'installazione di RHEL o Rocky Linux e la configurazione dei repository associati.



Se si modifica il processo di installazione o configurazione, potrebbe essere necessario eseguire ulteriori operazioni.

### Requisiti di distribuzione Linux

- Installare RHEL o Rocky Linux secondo le best practice di Red Hat. Poiché CentOS 8.x ha raggiunto la fine del suo ciclo di vita, non si consigliano versioni compatibili di CentOS 8.x.
- Durante l'installazione di ONTAP Mediator, assicurarsi che il sistema abbia accesso al repository richiesto

in modo che il programma di installazione possa recuperare e installare tutte le dipendenze software richieste.

- Per consentire al programma di installazione yum di trovare software dipendente nei repository RHEL, registrare il sistema durante l'installazione o successivamente utilizzando un abbonamento Red Hat valido.



Per ulteriori informazioni, consultate la documentazione di Red Hat Subscription Manager.

## Requisiti di rete

Assicurarsi che le seguenti porte siano disponibili e inutilizzate per ONTAP Mediator:

Porta/servizi	Origine	Direzione	Destinazione	Scopo
22/tcp	Host di gestione	In entrata	Mediatore ONTAP	(Facoltativo) Gestione SSH / ONTAP Mediator
31784/tcp	LIF di gestione del cluster	In entrata	Server web di ONTAP Mediator	(OBBLIGATORIO) API REST (HTTPS)
3260/tcp <sup>1</sup>	LIF dati nodo o LIF di gestione nodi	Bidirezionale	Target iSCSI del mediatore ONTAP	(Necessario per le configurazioni IP MetroCluster ) Connessione dati iSCSI per le cassette postali

Per i clienti SMBC, ONTAP non richiede l'attivazione o la connessione della porta 3260.

- Se si utilizza un firewall di terze parti, vedere "[Requisiti del firewall per ONTAP Mediator](#)".
- Per gli host Linux senza accesso a Internet, assicurarsi che i pacchetti richiesti siano disponibili in un repository locale.

Se si utilizza il protocollo LACP (link Aggregation Control Protocol) in ambiente Linux, configurare il kernel e impostare `sysctl net.ipv4.conf.all.arp_ignore` su 2.

## Requisiti del sistema operativo

Il sistema operativo deve soddisfare i seguenti requisiti:

- installazione fisica a 64 bit o macchina virtuale
- 8 GB DI RAM
- 1 GB di spazio su disco (utilizzato per l'installazione delle applicazioni, i log dei server e il database)
- Utente: Accesso root

La tabella seguente mostra i sistemi operativi supportati per ciascuna versione di ONTAP Mediator.

Versione del mediatore ONTAP	Versioni Linux supportate
------------------------------	---------------------------

1,11	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux <ul style="list-style-type: none"> <li>◦ Compatibile: 9.5 <sup>1</sup></li> <li>◦ Consigliati: 10.1, 10.0, 9.7, 9.6, 9.4 e 8.10</li> </ul> </li> <li>• Rocky Linux 10,1, 9.7 e 8,10</li> <li>• Oracle Linux 10.0 e 9.6</li> </ul>
1,10	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux <ul style="list-style-type: none"> <li>◦ Compatibile: 9.5 <sup>1</sup></li> <li>◦ Consigliati: 10.0, 9.6, 9.4 e 8,10</li> </ul> </li> <li>• Rocky Linux 10,0, 9.6 e 8,10</li> </ul>
1.9.1	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux <ul style="list-style-type: none"> <li>◦ Compatibile: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 e 8.4 <sup>1</sup></li> <li>◦ Consigliati: 9.5, 9.4, 9.2, 9.0, 8.10 e 8.8</li> </ul> </li> <li>• Rocky Linux 9.5 e 8.10</li> </ul>
1,9	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux <ul style="list-style-type: none"> <li>◦ Compatibile: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 e 8.4 <sup>1</sup></li> <li>◦ Consigliati: 9.5, 9.4, 9.2, 9.0, 8.10 e 8.8</li> </ul> </li> <li>• Rocky Linux 9.5 e 8.10</li> </ul>
1,8	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: <ul style="list-style-type: none"> <li>◦ Compatibile: 8.7, 8.6, 8.5 e 8.4 <sup>1</sup></li> <li>◦ Consigliati: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 e 8.8</li> </ul> </li> <li>• Rocky Linux 9.4 e 8.10</li> </ul>
1,7	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: <ul style="list-style-type: none"> <li>◦ Compatibile: 8.7, 8.6, 8.5 e 8.4 <sup>1</sup></li> <li>◦ Consigliati: 9.3, 9.2, 9.1, 9.0, 8.9 e 8.8</li> </ul> </li> <li>• Rocky Linux 9.3 e 8.9</li> </ul>
1.6	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: <ul style="list-style-type: none"> <li>◦ Compatibile: 8.7, 8.6, 8.5 e 8.4 <sup>1</sup></li> <li>◦ Consigliati: 9.2, 9.1, 9.0 e 8,8</li> </ul> </li> <li>• Rocky Linux 9.2 e 8.8</li> </ul>
1.5	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 e 7.6</li> <li>• CentOS: 7.9, 7.8, 7.7 e 7.6</li> </ul>

1.4	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 e 7.6</li> <li>• CentOS: 7.9, 7.8, 7.7 e 7.6</li> </ul>
1.3	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 e 7.6</li> <li>• CentOS: 7.9, 7.8, 7.7 e 7.6</li> </ul>
1.2	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 e 7.6</li> <li>• CentOS: 7.9, 7.8, 7.7 e 7.6</li> </ul>

1. Compatibile significa che Red Hat non supporta più queste versioni di RHEL, ma ONTAP Mediator può ancora essere installato su di esse.

### OS pacchetti richiesti

ONTAP Mediator richiede i seguenti pacchetti:



I pacchetti vengono preinstallati o installati automaticamente dal programma di installazione di ONTAP Mediator.

Tutte le versioni RHEL/CentOS	Pacchetti aggiuntivi per RHEL 10.x / Rocky Linux 10	Pacchetti aggiuntivi per RHEL 9.x / Rocky Linux 9	Pacchetti aggiuntivi per RHEL 8.x / Rocky Linux 8
<ul style="list-style-type: none"> <li>• openssl</li> <li>• openssl-devel</li> <li>• kernel-devel- (uname -r)</li> <li>• gcc</li> <li>• fare</li> <li>• libselinux-utils</li> <li>• patch</li> <li>• bzip2</li> <li>• perl-Data-Dumper</li> <li>• perl-ExtUtils-MakeMaker</li> <li>• efibootmgr</li> <li>• mokutil</li> </ul>	<ul style="list-style-type: none"> <li>• python3.12</li> <li>• python3.12-devel</li> </ul>	<ul style="list-style-type: none"> <li>• elfutils-libelf-devel</li> <li>• policycoreutils-python-utils</li> <li>• python3</li> <li>• python3-devel</li> </ul>	<ul style="list-style-type: none"> <li>• elfutils-libelf-devel</li> <li>• policycoreutils-python-utils</li> <li>• redhat-lsb-core</li> <li>• python39</li> <li>• python39-devel</li> </ul>

Il pacchetto di installazione di Mediator è un file tar compresso autoestraente che include:

- Un file RPM contenente tutte le dipendenze che non è possibile ottenere dal repository della release supportata.
- Uno script di installazione.

Si consiglia un certificato SSL valido.

## Considerazioni sull'aggiornamento del sistema operativo e sulla compatibilità del kernel

- È possibile aggiornare tutti i pacchetti di librerie, ad eccezione del kernel, ma potrebbe essere necessario riavviare il sistema per applicare le modifiche in ONTAP Mediator. Pianificare un periodo di inattività se è necessario riavviare.
- Dovresti mantenere aggiornato il kernel del sistema operativo. Aggiorna il kernel core a una versione supportata elencata in "[Matrice della versione di ONTAP Mediator](#)". È necessario riavviare il sistema, quindi pianificare una finestra di manutenzione per l'interruzione.
  - Disinstallare il modulo kernel SCST prima di riavviare, quindi reinstallarlo in seguito.
  - Preparare una versione supportata di SCST da reinstallare prima di avviare l'aggiornamento del sistema operativo del kernel.



- La versione del kernel deve corrispondere alla versione del sistema operativo.
- Non aggiornare il kernel oltre la versione del sistema operativo supportata per la versione di ONTAP Mediator in quanto il modulo SCST testato probabilmente non funzionerà.

## Installare ONTAP Mediator quando l'avvio protetto UEFI è attivato

ONTAP Mediator può essere installato su un sistema con o senza UEFI Secure Boot abilitato.

### A proposito di questa attività

È possibile scegliere di disattivare l'avvio protetto UEFI prima di installare ONTAP Mediator se non è necessario o se si stanno risolvendo i problemi di installazione di ONTAP Mediator. Disattivare l'opzione UEFI Secure Boot dalle impostazioni del computer.



Per istruzioni dettagliate sulla disattivazione di UEFI Secure Boot, consultare la documentazione relativa al sistema operativo host.

Per installare ONTAP Mediator con UEFI Secure Boot abilitato, è necessario registrare una chiave di sicurezza prima che il servizio possa essere avviato. La chiave viene generata durante la fase di compilazione dell'installazione di SCST e salvata come coppia di chiavi private-public sul computer. Utilizzare l'`mokutil` utilità per aggiungere la chiave pubblica come chiave del proprietario della macchina (MOK) al firmware UEFI, consentendo al sistema di considerare attendibile e caricare il modulo firmato. Salvare la `mokutil` passphrase in un luogo sicuro, in quanto ciò è necessario quando si riavvia il sistema per attivare il MOK.

### Fasi

1. verificare se l'avvio protetto UEFI è attivato sul sistema:

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

I risultati indicano se l'avvio protetto UEFI è abilitato su questo sistema.

Se...	Vai a...
L'avvio protetto UEFI è attivato	
L'avvio protetto UEFI è disattivato	<a href="#">"Aggiornare il sistema operativo host e quindi ONTAP Mediator"</a>



- Viene richiesto di creare una passphrase che deve essere memorizzata in una posizione protetta. Questa passphrase è necessaria per attivare la chiave in UEFI Boot Manager.
- ONTAP Mediator 1.2.0 e le versioni precedenti non supportano questa modalità.

2. se l'`mokutil` utilità non è installata, eseguire il comando seguente:

```
yum install mokutil
```

## Aggiornare il sistema operativo host e ONTAP Mediator

Per aggiornare il sistema operativo host per ONTAP Mediator a una versione successiva, è necessario prima disinstallare ONTAP Mediator.

### A proposito di questa attività

Prima di aggiornare il sistema operativo host per ONTAP Mediator con lo strumento leapp-upgrade, disinstallare ONTAP Mediator. Lo strumento verifica la presenza di nuove versioni RPM nei repository registrati.

Il programma di installazione ONTAP Mediator installa un file .rpm, che lo strumento leapp-upgrade include nella ricerca. Poiché il programma di installazione decompone il file anziché scaricarlo da un repository registrato, lo strumento non riesce a trovare un aggiornamento. Per disinstallare il pacchetto è necessario utilizzare lo strumento leapp-upgrade.

### Fasi

1. Eseguire il backup dei file di 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. Eseguire l'aggiornamento con lo strumento leapp-upgrade:



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

### 3. Reinstallare ONTAP Mediator:



Eseguire il resto della procedura immediatamente dopo la reinstallazione di ONTAP Media per evitare la perdita dei file di log.

```
[rootmediator-host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

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

### 4. Arresta ontap\_mediator:

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

### 5. Sostituisci i file di registro:

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

### 6. Avvia ontap\_mediator:

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

### 7. Ricollegare tutti i cluster ONTAP al mediatore ONTAP aggiornato:

## MetroCluster su 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-nod1    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-nod1    true          true
                siteB-node2    true          true
                siteB-node2    true          true

siteA::>
```

## Sincronizzazione attiva di SnapMirror

Per SnapMirror ActiveSync, non è necessario reinstallare i certificati TLS archiviati all'esterno di /opt/netapp. Eseguire il backup e il ripristino dei certificati archiviati in /opt/netapp.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
172.31.49.237    peer2              unreachable      true

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

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

peer1::> job show -id 39
Job ID Name                      Owning
Vserver      Node                      State
-----
39      mediator remove      peer1      peer1-node1      Success
Description: Removing entry in mediator

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

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

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

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

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

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

The certificate's generated name for reference: ONTAPMediatorCA

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

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

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

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

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

```
peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer  
-cluster peer2 -username mediatoradmin
```

Notice: Enter the mediator password.

Enter the password:

Enter the password again:

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

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

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

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

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

```
peer1::>
```

## Informazioni correlate

- ["eliminazione del certificato di sicurezza"](#)
- ["installazione del certificato di sicurezza"](#)
- ["mostra certificato di sicurezza"](#)
- ["aggiunta del mediatore SnapMirror"](#)
- ["rimozione del mediatore SnapMirror"](#)
- ["mostra di avvio iscsi di archiviazione"](#)

## Fornire l'accesso al repository per l'installazione di ONTAP Mediator

È necessario abilitare l'accesso ai repository in modo che ONTAP Mediator possa accedere ai pacchetti richiesti durante il processo di installazione.

### Fasi

1. Determinare quali repository devono essere utilizzati, come mostrato nella tabella seguente:

Se il sistema operativo in uso è...	È necessario fornire l'accesso a questi repository...
RHEL 10.x	<ul style="list-style-type: none"><li>• rhel-10-per-x86_64-baseos-rpms</li><li>• rhel-10-for-x86_64-appstream-rpms</li></ul>
RHEL 9.x	<ul style="list-style-type: none"><li>• rhel-9-for-x86_64-baseos-rpms</li><li>• rhel-9-for-x86_64-appstream-rpms</li></ul>
RHEL 8.x	<ul style="list-style-type: none"><li>• rhel-8-for-x86_64-baseos-rpms</li><li>• rhel-8-for-x86_64-appstream-rpms</li></ul>
RHEL 7.x	<ul style="list-style-type: none"><li>• rhel-7-server-optional-rpms</li></ul>
CentOS 7.x	<ul style="list-style-type: none"><li>• C7.6.1810 - repository di base</li></ul>
Rocky Linux 10	<ul style="list-style-type: none"><li>• appstream</li><li>• baseos</li></ul>
Rocky Linux 9	<ul style="list-style-type: none"><li>• appstream</li><li>• baseos</li></ul>
Rocky Linux 8	<ul style="list-style-type: none"><li>• appstream</li><li>• baseos</li></ul>

2. Utilizzare una delle seguenti procedure per abilitare l'accesso ai repository elencati in precedenza, in modo che ONTAP Media possa accedere ai pacchetti richiesti durante il processo di installazione.



Se ONTAP Mediator ha dipendenze dai moduli Python presenti nei repository "extra" e "opzionali", potrebbe dover accedere a `rhel-X-for-x86_64-extras-rpms` E `rhel-X-for-x86_64-optional-rpms` file.

## Procedura per il sistema operativo RHEL 10.x

Utilizzare questa procedura se il sistema operativo è **RHEL 10.x** per abilitare l'accesso ai repository:

### Fasi

1. Iscriviti al repository richiesto:

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

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

Nell'esempio seguente viene illustrata l'esecuzione di questo 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.
```

2. Eseguire `yum repolist` comando.

I repository appena sottoscritti dovrebbero apparire nell'elenco.

## Procedura per il sistema operativo RHEL 9.x.

Utilizzare questa procedura se il sistema operativo in uso è **RHEL 9.x** per consentire l'accesso ai repository:

### Fasi

1. Iscriviti al repository richiesto:

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

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

Nell'esempio seguente viene illustrata l'esecuzione di questo 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.
```

2. Eseguire `yum repolist` comando.

I repository appena sottoscritti dovrebbero apparire nell'elenco.

## Procedura per il sistema operativo RHEL 8.x.

Utilizzare questa procedura se il sistema operativo in uso è **RHEL 8.x** per abilitare l'accesso ai repository:

### Fasi

1. Iscriviti al repository richiesto:

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

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

Nell'esempio seguente viene illustrata l'esecuzione di questo 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.
```

2. Eseguire `yum repolist` comando.

I repository appena sottoscritti dovrebbero apparire nell'elenco.



## Procedura per il sistema operativo RHEL 7.x.

Utilizzare questa procedura se il sistema operativo in uso è **RHEL 7.x** per consentire l'accesso ai repository:

### Fasi

1. Iscriviti al repository richiesto:

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

Nell'esempio seguente viene illustrata l'esecuzione di questo comando:

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

2. Eseguire `yum repolist` comando.

Nell'esempio riportato di seguito viene illustrata l'esecuzione di questo comando. Il repository "rhel-7-server-optional-rpms" dovrebbe apparire nell'elenco.

```
[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 ~]#
```

## Procedura per il sistema operativo CentOS 7.x.

Utilizzare questa procedura se il sistema operativo in uso è **CentOS 7.x** per consentire l'accesso ai repository:



I seguenti esempi mostrano un repository per CentOS 7.6 e potrebbero non funzionare per altre versioni di CentOS. Utilizza il repository di base per la tua versione di CentOS.

### Fasi

1. Aggiungere il repository di base C7.6.1810. Il repository dei vault di base di C7.6.1810 contiene il pacchetto "kernel-devel" necessario per il mediatore ONTAP.
2. Aggiungere le seguenti righe 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
```

3. Eseguire `yum repolist` comando.

Nell'esempio riportato di seguito viene illustrata l'esecuzione di questo comando. Il repository CentOS-7.6.1810 - base dovrebbe apparire nell'elenco.

```
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 ~]#
```

## Procedura per i sistemi operativi Rocky Linux 10, 9 o 8

Utilizzare questa procedura se il sistema operativo è **Rocky Linux 10**, **Rocky Linux 9** o **Rocky Linux 8** per abilitare l'accesso ai repository:

### Fasi

1. Iscriviti ai repository richiesti:

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

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

2. Eseguire una clean funzionamento:

```
dnf clean all
```

3. Verificare l'elenco dei repository:

```
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 ~]#
```

## Scaricare il pacchetto di installazione di ONTAP Mediator

Scaricare il pacchetto di installazione ONTAP Mediator e installarlo.

### Fasi

1. Scaricare il pacchetto di installazione di ONTAP Mediator dalla pagina di download di ONTAP Mediator.

["Pagina di download del mediatore ONTAP"](#)

2. Assicurarsi di aver posizionato il pacchetto di installazione di Mediator nella directory di lavoro corrente:

```
[root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.11.0.tgz
```



Per le versioni 1.4 e precedenti di ONTAP Mediator, il programma di installazione è denominato `ontap-mediator`.

Se il sistema non ha accesso a Internet, assicurarsi che il programma di installazione possa accedere ai pacchetti richiesti.

3. Se necessario, spostare il pacchetto di installazione di Mediator nella directory di installazione.
4. Decomprimere il pacchetto di installazione:

```
tar xvfz ontap-mediator-1.11.0.tgz
```

```
ontap-mediator-1.11.0/  
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem  
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem  
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem  
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem  
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub  
ontap-mediator-1.11.0/ontap-mediator-1.11.0  
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr  
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr  
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
```

## Verificare la firma del codice del mediatore ONTAP

NetApp consiglia di verificare la firma del codice ONTAP Mediator prima dell'installazione. Questo passaggio è facoltativo.

### Prima di iniziare

Prima di verificare la firma del codice ONTAP Mediator, accertarsi che il sistema soddisfi queste esigenze.



- Dal 15 giugno 2025, non sarà più possibile installare o aggiornare ONTAP Mediator 1.9 e 1.8 perché i certificati di verifica della firma digitale sono scaduti. In alternativa, installare o aggiornare ONTAP Mediator alla versione 1.11 o 1.10.
- Se il sistema non soddisfa i requisiti indicati di seguito, il processo di verifica non è necessario e si può andare direttamente a ["Installare il pacchetto di installazione di ONTAP Mediator"](#).

- openssl versioni da 1.0.2 a 3.0 per la verifica di base
- openssl versione 1.1.0 o successiva per le operazioni TSA (Time Stamping Authority)
- Accesso a Internet pubblico per la verifica OCSP

Il pacchetto di download include i seguenti file:

File	Descrizione
ONTAP-Mediator-production.pub	Chiave pubblica utilizzata per verificare la firma
csc-prod-chain-ONTAP-Mediator.pem	Catena di trust della CA per la certificazione pubblica
csc-prod-ONTAP-Mediator.pem	Il certificato utilizzato per generare la chiave
ontap-mediator-1.11.0	L'eseguibile di installazione del prodotto per la versione 1.11

ontap-mediator-1.11.0.sig	SHA-256 ha eseguito l'hashing, quindi ha firmato RSA utilizzando la chiave csc-PROD, firma per l'installatore
ontap-mediator-1.11.0.sig.tsr	La richiesta di revoca per l'utilizzo da parte di OCSCP per la firma dell'installatore
ontap-mediator-1.11.0.tsr	File di richiesta firma timestamp
tsc-prod-ONTAP-Mediator.pem	Il certificato pubblico per il TSR
tsc-prod-chain-ONTAP-Mediator.pem	La catena CA del certificato pubblico per il TSR

## Fasi

1. Eseguire il controllo della revoca su `csc-prod-ONTAP-Mediator.pem` Utilizzando il protocollo OCSP (Online Certificate Status Protocol).

- a. Trova l'URL OCSP per il certificato. I certificati degli sviluppatori potrebbero non fornire un URI:

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

- b. Generare una richiesta OCSP per il certificato.

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

- c. Connettersi a OCSP Manager per inviare la richiesta OCSP:

```
openssl ocsp -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. Verificare la catena di attendibilità del CSC e le date di scadenza rispetto all'host locale:

```
openssl verify
```



Il `openssl` La versione dal PERCORSO deve avere un valido `cert.pem` (non autofirmato).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath  
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem # Failure action: The Code-  
Signature-Check certificate has expired or is invalid. Download a newer  
version of the ONTAP Mediator.  
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath  
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem # Failure action: The Time-  
Stamp certificate has expired or is invalid. Download a newer version of  
the ONTAP Mediator.
```

3. Verificare il `ontap-mediator-1.11.0.sig.tsr` E `ontap-mediator-1.11.0.tsr` file utilizzando i certificati associati:

#### OpenSSL 3.x

```
openssl ts -verify -data ontap-mediator-1.11.0.sig -in ontap-mediator-  
1.11.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-  
prod-ONTAP-Mediator.pem
```

#### OpenSSL 1.x

```
openssl ts -verify -data ontap-mediator-1.11.0 -in ontap-mediator-  
1.11.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```



.tsr`I file contengono la risposta con timestamp associata al programma di installazione e la firma del codice. L'elaborazione conferma che il timestamp ha una firma valida da parte della TSA e che il file di input non è stato modificato. La macchina esegue la verifica localmente. Non è necessario accedere ai server TSA.

4. Verificare le firme rispetto alla chiave:

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature  
ontap-mediator-1.11.0.sig ontap-mediator-1.11.0
```

## Installare il pacchetto di installazione di ONTAP Mediator

Per installare ONTAP Mediator, è necessario ottenere il pacchetto di installazione ed eseguire il programma di installazione sull'host.

### Fasi

1. Eseguire il programma di installazione e rispondere alle richieste come richiesto:

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```



Per saltare il controllo della firma durante l'installazione, utilizzare questo comando:

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y --skip-code  
-signature-check
```

Il programma di installazione crea gli account richiesti e installa i pacchetti richiesti. Se Mediator è già installato, ti verrà chiesto di aggiornarlo.



## Esempio di installazione di ONTAP Mediator (uscita console)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.11.0.tgz
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
[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
  Error querying OCSP responder
  80BBA032607F0000:error:1E800080:HTTP
  routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
  data:crypto/http/http_client.c:549:
  80BBA032607F0000:error:1E800067:HTTP
  routines:OSSL_HTTP_REQ_CTX_exchange:error
  receiving:crypto/http/http_client.c:901: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)? yes/no: yes

SKIPPING: Code signature check, manual override due to lack of OCSP response

```
+ 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). 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

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.

Updating Subscription Management repositories.

Unable to read consumer identity

This system is not registered with an entitlement server. You can use  
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025  
01:28:32 AM EDT.

Package openssl-1:3.2.2-16.el10.x86\_64 is already installed.

Package libselinux-utils-3.8-1.el10.x86\_64 is already installed.

Package perl-Data-Dumper-2.189-512.el10.x86\_64 is already installed.

Package bzip2-1.0.8-25.el10.x86\_64 is already installed.

Package efibootmgr-18-8.el10.x86\_64 is already installed.

Package mokutil-2:0.6.0-11.el10.x86\_64 is already installed.

Package polycycoreutils-python-utils-3.8-1.el10.noarch is already  
installed.

Package python3-3.12.9-1.el10.x86\_64 is already installed.

Dependencies resolved.

=====  
=====  
=====  
=====

Package	Version
Architecture	Size
Repository	
=====	
=====	
=====	
=====	

Installing:

elfutils-libelf-devel	
x86_64	0.192-5.el10

AppStream	50 k
gcc	
x86_64	14.2.1-7.el10
AppStream	37 M
kernel-devel	
x86_64	6.12.0-55.9.1.el10_0
AppStream	22 M
make	
x86_64	1:4.4.1-9.el10
BaseOS	591 k
openssl-devel	
x86_64	1:3.2.2-16.el10
AppStream	3.9 M
patch	
x86_64	2.7.6-26.el10
AppStream	134 k
perl-ExtUtils-MakeMaker	
noarch	2:7.70-513.el10
AppStream	297 k
python3-devel	
x86_64	3.12.9-1.el10
AppStream	
334 k	
python3-pip	
noarch	23.3.2-7.el10
AppStream	3.2 M
Installing dependencies:	
annobin-docs	
noarch	12.92-1.el10
AppStream	94 k
annobin-plugin-gcc	
x86_64	12.92-1.el10
AppStream	985 k
bison	
x86_64	3.8.2-9.el10
AppStream	1.0 M
cmake-filesystem	
x86_64	3.30.5-2.el10
AppStream	29 k
cpp	
x86_64	14.2.1-7.el10
AppStream	12 M
dwz	
x86_64	0.15-7.el10
AppStream	139 k
efi-srpm-macros	

noarch	6-6.el10
AppStream	25 k
flex	
x86_64	2.6.4-19.el10
AppStream	303 k
fonts-srpm-macros	
noarch	1:2.0.5-18.el10
AppStream	29 k
forge-srpm-macros	
noarch	0.4.0-6.el10
AppStream	23 k
gcc-plugin-annobin	
x86_64	14.2.1-7.el10
AppStream	62 k
glibc-devel	
x86_64	2.39-37.el10
AppStream	641 k
go-srpm-macros	
noarch	3.6.0-4.el10
AppStream	29 k
kernel-headers	
x86_64	6.12.0-55.9.1.el10_0
AppStream	2.3 M
kernel-srpm-macros	
noarch	1.0-25.el10
AppStream	11 k
libxcrypt-devel	
x86_64	4.4.36-10.el10
AppStream	33 k
libzstd-devel	
x86_64	1.5.5-9.el10
AppStream	
53 k	
lua-srpm-macros	
noarch	1-15.el10
AppStream	10 k
m4	
x86_64	1.4.19-11.el10
AppStream	309 k
ocaml-srpm-macros	
noarch	10-4.el10
AppStream	10 k
openblas-srpm-macros	
noarch	2-19.el10
AppStream	9.0 k
package-notes-srpm-macros	

noarch	0.5-13.e110
AppStream	11 k
perl-AutoSplit	
noarch	5.74-512.e110
AppStream	23 k
perl-Benchmark	
noarch	1.25-512.e110
AppStream	28 k
perl-CPAN-Meta-Requirements	
noarch	2.143-11.e110
AppStream	39 k
perl-CPAN-Meta-YAML	
noarch	0.018-512.e110
AppStream	29 k
perl-Devel-PPPort	
x86_64	3.72-512.e110
AppStream	223 k
perl-ExtUtils-Command	
noarch	2:7.70-513.e110
AppStream	16 k
perl-ExtUtils-Constant	
noarch	0.25-512.e110
AppStream	47 k
perl-ExtUtils-Install	
noarch	2.22-511.e110
AppStream	47 k
perl-ExtUtils-Manifest	
noarch	1:1.75-511.e110
AppStream	37 k
perl-ExtUtils-ParseXS	
noarch	1:3.51-512.e110
AppStream	190 k
perl-File-Compare	
noarch	1.100.800-512.e110
AppStream	15 k
perl-File-Copy	
noarch	2.41-512.e110
AppStream	22 k
perl-I18N-Langinfo	
x86_64	0.24-512.e110
AppStream	28 k
perl-JSON-PP	
noarch	1:4.16-512.e110
AppStream	69 k
perl-Test-Harness	
noarch	1:3.48-512.e110

```

AppStream 288 k
perl-lib
x86_64 0.65-512.el10
AppStream 16 k
perl-srpm-macros
noarch 1-57.el10
AppStream 9.7 k
perl-version
x86_64 8:0.99.32-4.el10
AppStream 68 k
pyproject-srpm-macros
noarch 1.16.2-1.el10
AppStream 16 k
python-srpm-macros
noarch 3.12-9.1.el10
AppStream 26 k
python3-pyparsing
noarch 3.1.1-7.el10
BaseOS 273 k
qt6-srpm-macros
noarch 6.8.1-3.el10
AppStream
11 k
redhat-rpm-config
noarch 288-1.el10
AppStream 83 k
rust-toolset-srpm-macros
noarch 1.84.1-1.el10
AppStream 13 k
systemtap-sdt-devel
x86_64 5.2-2.el10
AppStream 78 k
systemtap-sdt-dtrace
x86_64 5.2-2.el10
AppStream 72 k
zlib-ng-compat-devel
x86_64 2.2.3-1.el10
AppStream 41 k
Installing weak dependencies:
perl-CPAN-Meta
noarch 2.150010-511.el10
AppStream 202 k
perl-Encode-Locale
noarch 1.05-31.el10
AppStream 21 k
perl-Time-HiRes

```

```

x86_64                                4:1.9777-511.el10
AppStream                             62 k
perl-devel
x86_64                                4:5.40.1-512.el10
AppStream                             772 k
perl-doc
noarch                                5.40.1-512.el10
AppStream                             4.9 M

```

#### Transaction Summary

```

=====
=====
=====
=====

```

Install 63 Packages

Total size: 94 M

Installed size: 282 M

Downloading Packages:

BaseOS Packages Red Hat Enterprise Linux 10

439 kB/s | 3.7 kB 00:00

Importing GPG key 0xFD431D51:

Userid : "Red Hat, Inc. (release key 2) <security@redhat.com>"

Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51

From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

Key imported successfully

Importing GPG key 0x5A6340B3:

Userid : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"

Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3

From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

Key imported successfully

Running transaction check

Transaction check succeeded.

Running transaction test

Transaction test succeeded.

Running transaction

Preparing :

1/1

Installing : perl-version-8:0.99.32-4.el10.x86\_64

1/63

Installing : perl-File-Copy-2.41-512.el10.noarch

2/63

Installing : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch

3/63

Installing : perl-Time-HiRes-4:1.9777-511.el10.x86\_64

4/63

```
Installing      : perl-JSON-PP-1:4.16-512.el10.noarch
5/63
Installing      : perl-File-Compare-1.100.800-512.el10.noarch
6/63
Installing      : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
Installing      : m4-1.4.19-11.el10.x86_64
8/63
Installing      : make-1:4.4.1-9.el10.x86_64
9/63
Installing      : bison-3.8.2-9.el10.x86_64
10/63
Installing      : flex-2.6.4-19.el10.x86_64
11/63
Installing      : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
Installing      : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
Installing      : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
Installing      : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
Installing      : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
Installing      : python3-pip-23.3.2-7.el10.noarch
17/63
Installing      : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
Installing      : perl-srpm-macros-1-57.el10.noarch
19/63
Installing      : perl-lib-0.65-512.el10.x86_64
20/63
Installing      : perl-doc-5.40.1-512.el10.noarch
21/63
Installing      : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
Installing      : perl-Encode-Locale-1.05-31.el10.noarch
23/63
Installing      : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
Installing      : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
Installing      : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
Installing      : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
```



```
Installing      : perl-Benchmark-1.25-512.el10.noarch
28/63
Installing      : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
Installing      : perl-AutoSplit-5.74-512.el10.noarch
30/63
Installing      : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
Installing      : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
Installing      : openblas-srpm-macros-2-19.el10.noarch
33/63
Installing      : ocaml-srpm-macros-10-4.el10.noarch
34/63
Installing      : lua-srpm-macros-1-15.el10.noarch
35/63
Installing      : libzstd-devel-1.5.5-9.el10.x86_64
36/63
Installing      : kernel-srpm-macros-1.0-25.el10.noarch
37/63
Installing      : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
Installing      : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
Installing      : glibc-devel-2.39-37.el10.x86_64
40/63
Installing      : efi-srpm-macros-6-6.el10.noarch
41/63
Installing      : dwz-0.15-7.el10.x86_64
42/63
Installing      : cpp-14.2.1-7.el10.x86_64
43/63
Installing      : gcc-14.2.1-7.el10.x86_64
44/63
Installing      : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
Installing      : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
Installing      : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
Installing      : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
Installing      : annobin-docs-12.92-1.el10.noarch
49/63
Installing      : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
```

```

Installing      : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/63
Installing      : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
Installing      : go-srpm-macros-3.6.0-4.el10.noarch
53/63
Installing      : python-srpm-macros-3.12-9.1.el10.noarch
54/63
Installing      : redhat-rpm-config-288-1.el10.noarch
55/63
Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
Installing      : python3-pyparsing-3.1.1-7.el10.noarch
56/63
Installing      : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
Installing      : perl-devel-4:5.40.1-512.el10.x86_64
58/63
Installing      : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
Installing      : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
Installing      : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
Installing      : python3-devel-3.12.9-1.el10.x86_64
62/63
Installing      : patch-2.7.6-26.el10.x86_64
63/63
Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch          annobin-plugin-gcc-
12.92-1.el10.x86_64          bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64      cpp-14.2.1-
7.el10.x86_64
dwz-0.15-7.el10.x86_64          efi-srpm-macros-6-
6.el10.noarch          elfutils-libelf-devel-0.192-
5.el10.x86_64  flex-2.6.4-19.el10.x86_64          fonts-
srpm-macros-1:2.0.5-18.el10.noarch
forge-srpm-macros-0.4.0-6.el10.noarch      gcc-14.2.1-
7.el10.x86_64          gcc-plugin-annobin-14.2.1-
7.el10.x86_64          glibc-devel-2.39-37.el10.x86_64          go-

```

```

srpm-macros-3.6.0-4.el10.noarch
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64      kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64      libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch      m4-1.4.19-
11.el10.x86_64      make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch      openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64      package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch      perl-Benchmark-1.25-
512.el10.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.el10.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.el10.noarch      perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.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-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch      perl-lib-0.65-
512.el10.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-3.12-9.1.el10.noarch      python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch      python3-pyparsing-
3.1.1-7.el10.noarch      qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch      rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64      systemtap-sdt-dtrace-
5.2-2.el10.x86_64      zlib-ng-compat-devel-2.2.3-1.el10.x86_64

```

Complete!

OS package installations finished

+ Installing ONTAP Mediator. (Log: /root/ontap\_mediator.vdizgQ/ontap-mediator-1.11.0/ontap-mediator-1.11.0/install\_20250715160240.log)

This step takes several minutes. View progress in the log file.

Sudoer config verified

```

    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.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.modu
le-signing
    to sign the SCST kernel module. Note that a reboot is
needed.
    SCST does 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:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
    Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
    Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
    Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
    Main PID: 28759 (python)
    Tasks: 1 (limit: 22990)
    Memory: 66.8M (peak: 68.8M)
    CPU: 2.865s

```

```

CGroup: /system.slice/ontap_mediator.service
└─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
   enabled; preset: disabled)
   Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
  15s ago
     Invocation: f1d3be6calf9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
    CGroup: /system.slice/mediator-scst.service
           └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#

```

## Registra la chiave di sicurezza per UEFI Secure Boot

A partire da ONTAP Mediator 1.4, il meccanismo Secure Boot è abilitato sui sistemi UEFI. Se è abilitato l'avvio protetto, è necessario eseguire ulteriori passaggi per registrare la chiave di sicurezza dopo l'installazione.

### Fasi

1. Seguire le istruzioni nel file README per firmare il modulo kernel SCST:

```

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

```

## 2. Individuare le chiavi richieste:

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



Dopo l'installazione, l'output di sistema fornisce i file README e la posizione della chiave.

## 3. Aggiungere la chiave pubblica all'elenco MOK:

```
mokutil --import  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de  
r
```



È possibile lasciare la chiave privata nella sua posizione predefinita oppure spostarla in una posizione sicura. È necessario conservare la chiave pubblica nella sua posizione attuale affinché Boot Manager possa utilizzarla. Per ulteriori informazioni, consultare il file 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. Riavvia l'host e utilizza UEFI Boot Manager del tuo dispositivo per approvare il nuovo MOK. Avrai bisogno della passphrase fornita per mokutil utilità in ["Installare ONTAP Mediator quando l'avvio protetto UEFI è attivato"](#).

### Firma dei moduli del kernel SCST

Dopo l'installazione ONTAP Mediator, se lo stato `systemctl mediator-scst` viene visualizzato come non riuscito (inattivo), seguire questi passaggi per firmare il modulo kernel SCST.

#### Fasi

1. Durante il processo di compilazione viene generata una coppia di chiavi pubblica/privata nel `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/` directory, utilizzando il seguente comando:

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

2. Avviare il processo di importazione della chiave pubblica nel repository delle chiavi UEFI eseguendo i seguenti comandi:

```
[root@mediator-host ~]# mokutil --import  
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de  
r  
input password: input password again:
```

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

3. Il software mokutil richiede una password temporanea da utilizzare per questa chiave durante il processo di importazione.
4. Verificare se il processo di importazione è iniziato con `mokutil --list-new` e quindi riavviare il sistema. Il bootloader avvia il gestore EFI MOK.

5. Utilizzare i menu sullo schermo per attivare il tasto del modulo kernel SCST. Dopo l'avvio, eseguire `systemctl status mediator-scst`. Una volta avviato il servizio, i moduli del kernel SCST vengono firmati.

## Verificare lo stato dell'installazione di ONTAP Mediator

Dopo aver installato ONTAP Mediator, verificare che funzioni correttamente.

### Fasi

1. Visualizza lo stato del mediatore ONTAP:

a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# 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@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# 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@scspr1915530002 ~]#
```

## 2. Conferma le porte utilizzate da ONTAP Mediator:

netstat

```
[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
```

## Configurazione ONTAP Mediator post-installazione

Dopo aver installato e avviato ONTAP Mediator, è necessario eseguire ulteriori attività di configurazione nel sistema di archiviazione ONTAP per utilizzare le funzionalità di ONTAP Mediator:

- Per utilizzare ONTAP Mediator in una configurazione IP MetroCluster, vedere ["Configurare ONTAP Mediator da una configurazione IP MetroCluster"](#).
- Per utilizzare la sincronizzazione attiva di SnapMirror, vedere ["Installa ONTAP Mediator e conferma la configurazione del cluster ONTAP"](#).

### Configurare i criteri di sicurezza di ONTAP Mediator

ONTAP Mediator supporta diverse impostazioni di sicurezza configurabili. I valori predefiniti per tutte le impostazioni vengono forniti in un `low_space_threshold_mib`: 10 file di sola lettura:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_c
onfig.yaml
```



Tutti i valori inseriti in `ontap_mediator.user_config.yaml` Sovrascrive i valori predefiniti e viene mantenuto in tutti gli aggiornamenti di ONTAP Mediator.

Dopo aver modificato `ontap_mediator.user_config.yaml` , riavviare ONTAP Mediator:

```
systemctl restart ontap_mediator
```

## Modificare gli attributi del mediatore ONTAP

Gli attributi del mediatore ONTAP descritti in questa sezione possono essere modificati se necessario.



Gli altri valori predefiniti in `ontap_mediator.config.yaml` non devono essere modificati in quanto i valori modificati non vengono mantenuti durante gli aggiornamenti di ONTAP Mediator.

È possibile modificare gli attributi di ONTAP Mediator copiando le variabili richieste nel `ontap_mediator.user_config.yaml` file per sovrascrivere le impostazioni predefinite.

### Installare certificati SSL di terze parti

Se è necessario sostituire i certificati autofirmati predefiniti con certificati SSL di terze parti, modificare alcuni attributi nei seguenti file:

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

Le variabili in questi file vengono utilizzate per controllare i file di certificato utilizzati da ONTAP Mediator.

## ONTAP Mediator 1,9 e versioni successive

Le variabili predefinite elencate nella tabella seguente sono incluse nel

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml file.

Variabile	Percorso
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- cert\_valid\_days viene utilizzato per impostare la scadenza dei certificati client. Il valore massimo è di tre anni (1095 giorni).
- x509\_passin\_pwd è la passphrase per il certificato client firmato.

Le variabili predefinite elencate nella tabella seguente sono incluse nel

/opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini file.

Variabile	Percorso
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt

## ONTAP Mediator 1,8 e precedenti

Le variabili predefinite elencate nella tabella seguente sono incluse nel

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/server\_config/ontap\_mediator.config.yaml file.

Variabile	Percorso
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_valid_days	1095
x509_passin_pwd	pass:ontap

- cert\_valid\_days viene utilizzato per impostare la scadenza dei certificati client. Il valore massimo è di tre anni (1095 giorni).
- x509\_passin\_pwd è la passphrase per il certificato client firmato.

Le variabili predefinite elencate nella tabella seguente sono incluse nel /opt/netapp/lib/ontap\_mediator/uwsgi/ontap\_mediator.ini file.

Variabile	Percorso
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

Se si modificano questi attributi, riavviare ONTAP Mediator per applicare le modifiche. Per istruzioni dettagliate su come sostituire i certificati predefiniti con quelli di terze parti, fare riferimento a ["Sostituire i certificati autofirmati con certificati di terze parti attendibili"](#).

#### Protezione da attacchi tramite password

Le seguenti impostazioni forniscono protezione contro gli attacchi di tipo "brute force" che inducono le password.

Per attivare la funzione, impostare un valore per window\_seconds e retry\_limit.

Esempi:

- Fornire una finestra di 5 minuti per le ipotesi, quindi ripristinare il conteggio a zero errori:

```
authentication_lock_window_seconds: 300
```

- Bloccare l'account se si verificano cinque guasti entro il periodo di tempo previsto:

```
authentication_retry_limit: 5
```

- Riduci l'impatto degli attacchi di indovinare le password con la forza bruta impostando un ritardo che si verifica prima di rifiutare ogni tentativo, rallentando gli attacchi.

```
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
```

### Regole di complessità delle password

I seguenti campi controllano le regole di complessità delle password dell'account utente API di 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)
```

### Controllo dello spazio libero

Esistono impostazioni che controllano lo spazio libero richiesto sul /opt/netapp/lib/ontap\_mediator disco.

Se lo spazio è inferiore alla soglia impostata, il servizio emetterà un avviso.

```
low_space_threshold_mib: 10
```

## Controllo dello spazio del registro di riserva

RESERVE\_LOG\_SPACE è controllata da impostazioni specifiche. Per impostazione predefinita, l'installazione di ONTAP Mediator crea uno spazio su disco separato per i log. Il programma di installazione crea un nuovo file di dimensioni fisse con un totale di 700 MB di spazio su disco da utilizzare esplicitamente per la registrazione di ONTAP Mediator.

Per disattivare questa funzione e utilizzare lo spazio su disco predefinito, procedere come segue:

1. Modificare il valore di RESERVE\_LOG\_SPACE da 1 a 0 nel seguente file:

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

2. Riavviare Mediator:

- a. 

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

```
RESERVE_LOG_SPACE=0
```

- b. 

```
systemctl restart ontap_mediator
```

Per riattivare la funzione, modificare il valore da 0 a 1 e riavviare Mediator.



L'alternanza tra gli spazi su disco non elimina i registri esistenti. Viene eseguito il backup di tutti i registri precedenti, quindi viene spostato nello spazio su disco corrente dopo l'attivazione e il riavvio di Mediator.

## Gestione di ONTAP Mediator

Gestire ONTAP Mediator, inclusa la modifica delle credenziali utente, l'interruzione e la riattivazione del servizio, la verifica del suo stato e l'installazione o la disinstallazione di SCST per la manutenzione dell'host. È inoltre possibile gestire i certificati, come la rigenerazione di certificati autofirmati, la loro sostituzione con certificati di terze parti attendibili e la risoluzione dei problemi relativi ai certificati.

### Modificare il nome utente

È possibile modificare il nome utente utilizzando la seguente procedura.

#### A proposito di questa attività

Eseguire questa attività sull'host Linux su cui è installato ONTAP Mediator.

Se non si riesce a raggiungere questo comando, potrebbe essere necessario eseguire il comando utilizzando il percorso completo, come illustrato nell'esempio seguente:

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

#### Fasi

Modificare il nome utente scegliendo una delle seguenti opzioni:

- **Opzione (a):** Eseguire il comando `mediator_change_user` e rispondere alle richieste come mostrato nell'esempio seguente:

```
[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 ~]#
```

- **Opzione (b):** Eseguire il seguente 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 ~]#
```

## Modificare la password

È possibile modificare la password utilizzando la seguente procedura.

### A proposito di questa attività

Eseguire questa attività sull'host Linux su cui è installato ONTAP Mediator.

Se non si riesce a raggiungere questo comando, potrebbe essere necessario eseguire il comando utilizzando il percorso completo, come illustrato nell'esempio seguente:

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

### Fasi

Modificare la password scegliendo una delle seguenti opzioni:

- **Opzione (a):** Eseguire `mediator_change_password` e rispondere ai prompt come mostrato nell'esempio seguente:

```
[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 ~]#
```

- **Opzione (b):** Eseguire il seguente comando:

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

L'esempio mostra che la password viene modificata da "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 ~]#
```

## Stop ONTAP Mediator

Per arrestare ONTAP Mediator, procedere come segue:

### Fasi

1. Interrompi il mediatore ONTAP:

```
systemctl stop ontap_mediator
```

2. Arresta SCST:

```
systemctl stop mediator-scst
```

3. Disabilitare ONTAP Mediator e SCST:

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

## Riattivare ONTAP Mediator

Per riattivare ONTAP Mediator, procedere come segue:

### Fasi

1. Abilita ONTAP Mediator e SCST:

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

## 2. Avvia SCST:

```
systemctl start mediator-scst
```

## 3. Avviare ONTAP Mediator:

```
systemctl start ontap_mediator
```

## Verificare che ONTAP Mediator sia integro

Dopo aver installato ONTAP Mediator, verificare che funzioni correttamente.

### Fasi

#### 1. Visualizza lo stato del mediatore ONTAP:

a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# 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@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`



```
[root@scspr1915530002 ~]# 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@scspr1915530002 ~]#
```

## 2. Conferma le porte utilizzate da ONTAP Mediator:

netstat

```
[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
```

## Disinstallare ONTAP Mediator

Se necessario, è possibile rimuovere ONTAP Mediator.

### Prima di iniziare

Prima di rimuoverlo, è necessario scollegare ONTAP Mediator da ONTAP.

### A proposito di questa attività

Eseguire questa attività sull'host Linux su cui è installato ONTAP Mediator.

Se non si riesce a raggiungere questo comando, potrebbe essere necessario eseguire il comando utilizzando il percorso completo, come illustrato nell'esempio seguente:

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

### Fase

#### 1. Disinstallare 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 ~]#
```

## Rigenerare un certificato autofirmato temporaneo

A partire da ONTAP Mediator 1,7, è possibile rigenerare un certificato autofirmato temporaneo utilizzando la seguente procedura.



Questa procedura è supportata solo sui sistemi con ONTAP Mediator 1,7 o versione successiva.

### A proposito di questa attività

- Eseguire questa attività sull'host Linux su cui è installato ONTAP Mediator.
- È possibile eseguire questa attività solo se i certificati autofirmati generati sono diventati obsoleti a causa di modifiche al nome host o all'indirizzo IP dell'host dopo l'installazione di ONTAP Mediator.
- Dopo che il certificato autofirmato temporaneo è stato sostituito da un certificato di terze parti attendibile, *non* utilizzare questa attività per rigenerare un certificato. L'assenza di un certificato autofirmato causerà l'errore di questa procedura.

### Fase

Per rigenerare un nuovo certificato autofirmato temporaneo per l'host corrente, attenersi alla seguente procedura:

1. Riavviare 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
```

## Sostituire i certificati autofirmati con certificati di terze parti attendibili

Se supportati, è possibile sostituire i certificati autofirmati con certificati di terze parti attendibili.

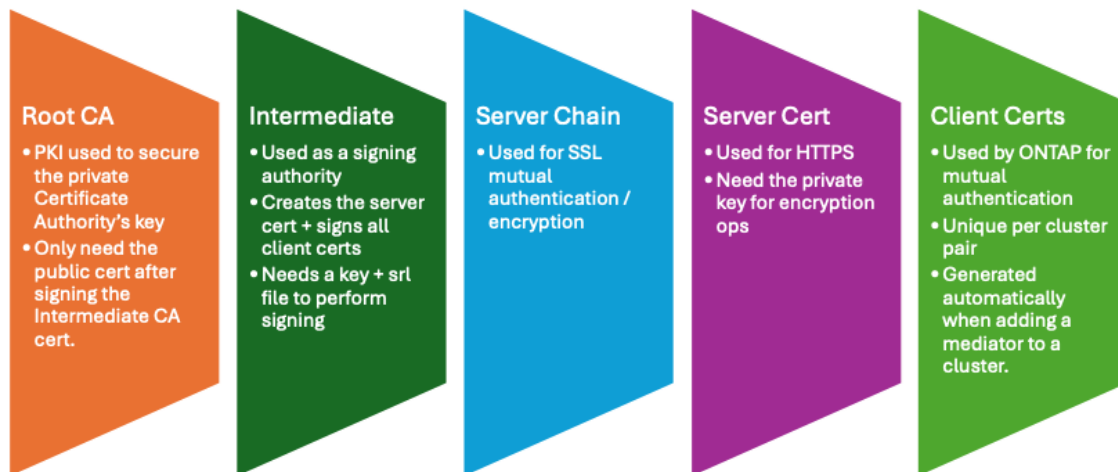


- I certificati di terze parti sono supportati solo a partire da ONTAP 9.16,1 e in alcune versioni precedenti di patch di ONTAP. Vedere ["ID bug online di NetApp CONTAP-243278"](#).
- I certificati di terze parti sono supportati solo sui sistemi che eseguono ONTAP Mediator 1,7 o versioni successive.

### A proposito di questa attività

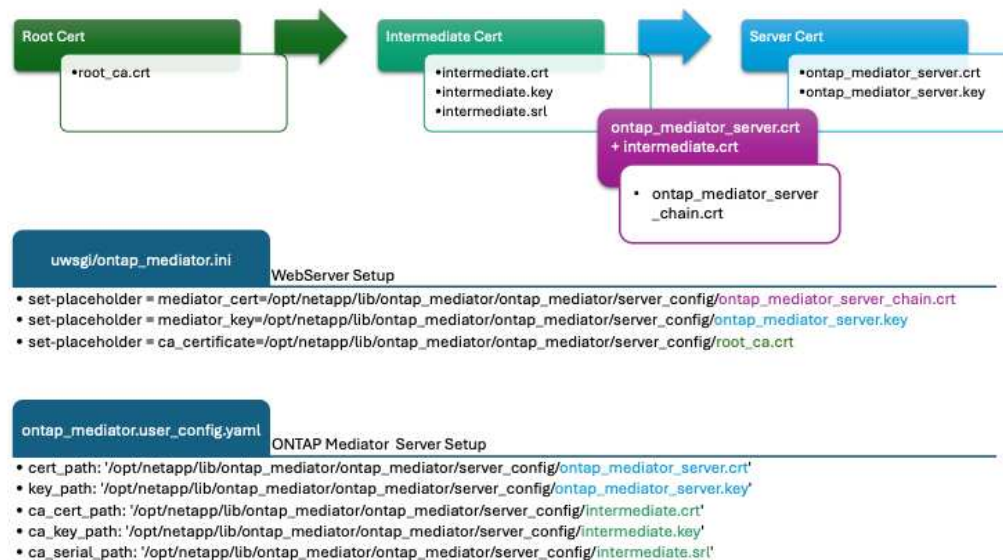
- Eseguire questa attività sull'host Linux su cui è installato ONTAP Mediator.
- È possibile eseguire questa attività se i certificati autofirmati generati devono essere sostituiti da certificati ottenuti da un'autorità di certificazione subordinata attendibile (CA). A tale scopo, è necessario disporre dell'accesso a un'autorità PKI (Public-Key Infrastructure) attendibile.
- L'immagine seguente mostra le finalità di ciascun certificato ONTAP Mediator.

# ONTAP Mediator Certificate Purposes



- L'immagine seguente mostra la configurazione per l'installazione del server Web e l'installazione di ONTAP Mediator.

## ONTAP Mediator Certificates



### Passaggio 1: Ottenere un certificato da una terza parte che emette un certificato CA

È possibile ottenere un certificato da un'autorità PKI utilizzando la seguente procedura.

Nell'esempio seguente viene illustrata la sostituzione degli attori certificati autofirmati con gli attori certificati di

terze parti situati in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`.



L'esempio illustra i criteri necessari per i certificati richiesti per ONTAP Mediator. È possibile ottenere i certificati da un'autorità PKI in modo diverso da questa procedura. Regolare la procedura in base alle esigenze aziendali.

## ONTAP Mediator 1,9 e versioni successive

1. Creare una chiave privata `intermediate.key` e un file di configurazione `openssl_ca.cnf` che verrà utilizzato dall'autorità PKI per generare un certificato.

- a. Generare la chiave privata `intermediate.key`:

### Esempio

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

- a. Il file di configurazione `openssl_ca.cnf` (situato in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definisce le proprietà che il certificato generato deve avere.

2. Utilizzare la chiave privata e il file di configurazione per creare una richiesta di firma del certificato `intermediate.csr`:

### Esempio:

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

```
[root@scs000216655 server_config]# openssl req -key intermediate.key  
-new -config openssl_ca.cnf -out intermediate.csr  
Enter pass phrase for intermediate.key:  
[root@scs000216655 server_config]# cat intermediate.csr  
-----BEGIN CERTIFICATE REQUEST-----  
<certificate_value>  
-----END CERTIFICATE REQUEST-----
```

3. Inviare la richiesta di firma del certificato `intermediate.csr` a un'autorità PKI per la firma.

L'autorità PKI verifica la richiesta e firma la `.csr`, generando il certificato `intermediate.crt`. Inoltre, è necessario ottenere il `root_ca.crt` certificato che ha firmato il `intermediate.crt` certificato dell'autorità PKI.



Per i cluster SnapMirror Business Continuity (SM-BC), è necessario aggiungere `intermediate.crt` e `root_ca.crt` certificati a un cluster ONTAP. Vedere "[Configurare ONTAP Mediator e cluster per SnapMirror ActiveSync](#)".

## ONTAP Mediator 1,8 e precedenti

1. Creare una chiave privata `ca.key` e un file di configurazione `openssl_ca.cnf` che verrà utilizzato dall'autorità PKI per generare un certificato.

- a. Generare la chiave privata `ca.key`:

### Esempio

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

- a. Il file di configurazione `openssl_ca.cnf` (situato in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definisce le proprietà che il certificato generato deve avere.
2. Utilizzare la chiave privata e il file di configurazione per creare una richiesta di firma del certificato `ca.csr`:

**Esempio:**

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

```
[root@scs000216655 server_config]# openssl req -key ca.key -new  
-config openssl_ca.cnf -out ca.csr  
Enter pass phrase for ca.key:  
[root@scs000216655 server_config]# cat ca.csr  
-----BEGIN CERTIFICATE REQUEST-----  
<certificate_value>  
-----END CERTIFICATE REQUEST-----
```

3. Inviare la richiesta di firma del certificato `ca.csr` a un'autorità PKI per la firma.

L'autorità PKI verifica la richiesta e firma il , generando il `.csr` certificato `ca.crt`. Inoltre, è necessario ottenere il `root_ca.crt` that signed the `ca.crt` certificato dall'autorità PKI.



Per i cluster SnapMirror Business Continuity (SM-BC), è necessario aggiungere i `ca.crt` certificati e `root_ca.crt` a un cluster ONTAP. Vedere ["Configurare ONTAP Mediator e cluster per SnapMirror ActiveSync"](#).

## Passaggio 2: Generare un certificato server firmando con una certificazione CA di terze parti

## ONTAP Mediator 1,9 e versioni successive

Un certificato server deve essere firmato dalla chiave privata e dal `intermediate.key` certificato di terzi `intermediate.crt`. Inoltre, il file di configurazione `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contiene alcuni attributi che specificano le proprietà richieste per i certificati server emessi da OpenSSL.

I seguenti comandi possono generare un certificato server.

### Fasi

1. Per generare una richiesta di firma del certificato del server (CSR), eseguire il comando seguente dalla `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` cartella:

```
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. Per generare un certificato server dal CSR, eseguire il seguente comando da `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` cartella:



Questi file sono stati ottenuti da un'autorità PKI. Se si utilizza un nome di certificato diverso, sostituire `intermediate.crt` e `intermediate.key` con i nomi file pertinenti.

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

° L' `-CAcreateserial` opzione viene utilizzata per generare i `intermediate.srl` file.

## ONTAP Mediator 1,8 e precedenti

Un certificato server deve essere firmato dalla chiave privata e dal `ca.key` certificato di terzi `ca.crt`. Inoltre, il file di configurazione `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contiene alcuni attributi che specificano le proprietà richieste per i certificati server emessi da OpenSSL.

I seguenti comandi possono generare un certificato server.

### Fasi

1. Per generare una richiesta di firma del certificato del server (CSR), eseguire il comando seguente dalla `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` cartella:

```
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. Per generare un certificato server dal CSR, eseguire il seguente comando da `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` cartella:





Questi file sono stati ottenuti da un'autorità PKI. Se si utilizza un nome di certificato diverso, sostituire `ca.crt` e `ca.key` con i nomi file pertinenti.

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

◦ L' `-CAcreateserial` opzione viene utilizzata per generare il `ca.srl` file.

### **Passaggio 3: Sostituzione del nuovo certificato CA di terze parti e del certificato server nella configurazione ONTAP Mediator**

## ONTAP Mediator 1.10 e versioni successive

La configurazione del certificato viene fornita a ONTAP Mediator nel file di configurazione situato in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. Il file include i seguenti attributi:

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

- `cert_path` e `key_path` sono variabili di certificato del server.
- `ca_cert_path`, `ca_key_path`, e `ca_serial_path` Sono variabili di certificato CA.

## Fasi

1. Sostituire tutti i `intermediate.*` file con i certificati di terze parti.
2. Creare una catena di certificati da `intermediate.crt` e `ontap_mediator_server.crt` certificati:

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

3. Aggiorna il `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` file.

Aggiorna i valori di `ssl_keyfile`, `ssl_certfile`, E `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
```

- IL `ssl_keyfile` il valore è il percorso chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- IL `ssl_certfile` il valore è il percorso del `ontap_mediator_server_chain.crt` file.
- IL `ssl_ca_certs` il valore è il percorso del `root_ca.crt` file.

4. Verificare che i seguenti attributi dei certificati appena generati siano impostati correttamente:

- Proprietario del gruppo Linux: `netapp:netapp`
- Autorizzazioni Linux: `600`

5. Riavviare ONTAP Mediator:

```
systemctl restart ontap_mediator
```

### ONTAP Mediator 1.9.1 e 1.9

La configurazione del certificato viene fornita a ONTAP Mediator nel file di configurazione situato in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. Il file include i seguenti attributi:

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

- `cert_path` e `key_path` sono variabili di certificato del server.
- `ca_cert_path`, `ca_key_path`, e `ca_serial_path` Sono variabili di certificato CA.

### Fasi

1. Sostituire tutti i `intermediate.*` file con i certificati di terze parti.
2. Creare una catena di certificati da `intermediate.crt` e `ontap_mediator_server.crt` certificati:

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

3. Aggiornare il `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Aggiornare i valori di `mediator_cert`, `mediator_key` e `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
```

- Il `mediator_cert` valore è il percorso del `ontap_mediator_server_chain.crt` file.
- Il `mediator_key` value è il percorso chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- Il `ca_certificate` valore è il percorso del `root_ca.crt` file.

4. Verificare che i seguenti attributi dei certificati appena generati siano impostati correttamente:

- Proprietario del gruppo Linux: `netapp:netapp`
- Autorizzazioni Linux: `600`

5. Riavviare ONTAP Mediator:

```
systemctl restart ontap_mediator
```

### ONTAP Mediator 1,8 e precedenti

La configurazione del certificato viene fornita a ONTAP Mediator nel file di configurazione situato in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. Il file include i seguenti attributi:

```
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/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` e `key_path` sono variabili di certificato del server.
- `ca_cert_path`, `ca_key_path`, e `ca_serial_path` Sono variabili di certificato CA.

## Fasi

1. Sostituire tutti i `ca.*` file con i certificati di terze parti.
2. Creare una catena di certificati da `ca.crt` e `ontap_mediator_server.crt` certificati:

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

3. Aggiornare il `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Aggiornare i valori di `mediator_cert`, `mediator_key` e `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
```

- Il `mediator_cert` valore è il percorso del `ontap_mediator_server_chain.crt` file.
  - Il `mediator_key` value è il percorso chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
  - Il `ca_certificate` valore è il percorso del `root_ca.crt` file.
4. Verificare che i seguenti attributi dei certificati appena generati siano impostati correttamente:
    - Proprietario del gruppo Linux: `netapp:netapp`
    - Autorizzazioni Linux: `600`
  5. Riavviare ONTAP Mediator:

```
systemctl restart ontap_mediator
```

**Passaggio 4: Se si desidera, utilizzare un percorso o un nome diverso per i certificati di terze parti**

## ONTAP Mediator 1.10 e versioni successive

È possibile utilizzare certificati di terze parti con un nome diverso da `intermediate.*` o memorizzare i certificati di terze parti in una posizione diversa.

### Fasi

#### 1. Configurare il

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file in modo che sovrascriva i valori della variabile di default nel `ontap_mediator.config.yaml` file.

Se si è ottenuto `intermediate.crt` da un'autorità PKI e si memorizza la propria chiave privata `intermediate.key` nella posizione

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, il `ontap_mediator.user_config.yaml` file dovrebbe essere simile al seguente esempio:



Se si è utilizzato `intermediate.crt` per firmare il `ontap_mediator_server.crt` certificato, il `intermediate.srl` file viene generato. Per ulteriori informazioni, vedere [Passaggio 2: Generare un certificato server firmando con una certificazione CA di terze parti](#).

```
[root@scs000216655 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. Se si utilizza una struttura di certificato in cui `root_ca.crt` il certificato fornisce un `intermediate.crt` certificato che firma il `ontap_mediator_server.crt` certificato, crea una catena di certificati dal `intermediate.crt` E `ontap_mediator_server.crt` certificati:



I certificati e dovrebbero essere stati ottenuti `intermediate.crt` `ontap_mediator_server.crt` da un'autorità PKI precedentemente nella procedura.

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

- b. Aggiorna il `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` file.

Aggiorna i valori di `ssl_keyfile`, `ssl_certfile`, E `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
```

- IL `ssl_keyfile` il valore è il percorso chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- IL `ssl_certfile` il valore è il percorso del `ontap_mediator_server_chain.crt` file.
- IL `ssl_ca_certs` il valore è il percorso del `root_ca.crt` file.



Per i cluster SnapMirror Business Continuity (SM-BC), è necessario aggiungere `intermediate.crt` E `root_ca.crt` certificati a un cluster ONTAP. Vedere ["Configurare ONTAP Mediator e cluster per SnapMirror ActiveSync"](#).

c. Verificare che i seguenti attributi dei certificati appena generati siano impostati correttamente:

- Proprietario del gruppo Linux: `netapp:netapp`
- Autorizzazioni Linux: `600`

2. Riavviare ONTAP Mediator quando i certificati vengono aggiornati nel file di configurazione:

```
systemctl restart ontap_mediator
```

### ONTAP Mediator 1.9.1 e 1.9

È possibile utilizzare certificati di terze parti con un nome diverso da `intermediate.*` o memorizzare i certificati di terze parti in una posizione diversa.

#### Fasi

1. Configurare il

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file in modo che sovrascriva i valori della variabile di default nel `ontap_mediator.config.yaml` file.

Se si è ottenuto `intermediate.crt` da un'autorità PKI e si memorizza la propria chiave privata `intermediate.key` nella posizione

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, il `ontap_mediator.user_config.yaml` file dovrebbe essere simile al seguente esempio:





Se si è utilizzato `intermediate.crt` per firmare il `ontap_mediator_server.crt` certificato, il `intermediate.srl` file viene generato. Per ulteriori informazioni, vedere [Passaggio 2: Generare un certificato server firmando con una certificazione CA di terze parti](#).

```
[root@scs000216655 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. Se si utilizza una struttura di certificato in cui `root_ca.crt` il certificato fornisce un `intermediate.crt` certificato che firma il `ontap_mediator_server.crt` certificato, crea una catena di certificati dal `intermediate.crt` E `ontap_mediator_server.crt` certificati:



I certificati e dovrebbero essere stati ottenuti `intermediate.crt` `ontap_mediator_server.crt` da un'autorità PKI precedentemente nella procedura.

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

b. Aggiornare il `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Aggiornare i valori di `mediator_cert`, `mediator_key` e `ca_certificate`:

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

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

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

- Il `mediator_cert` valore è il percorso del `ontap_mediator_server_chain.crt` file.
- Il `mediator_key` valore è il percorso chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- Il `ca_certificate` valore è il percorso del `root_ca.crt` file.



Per i cluster SnapMirror Business Continuity (SM-BC), è necessario aggiungere `intermediate.crt` E `root_ca.crt` certificati a un cluster ONTAP . Vedere ["Configurare ONTAP Mediator e cluster per SnapMirror ActiveSync"](#) .

c. Verificare che i seguenti attributi dei certificati appena generati siano impostati correttamente:

- Proprietario del gruppo Linux: `netapp:netapp`
- Autorizzazioni Linux: `600`

2. Riavviare ONTAP Mediator quando i certificati vengono aggiornati nel file di configurazione:

```
systemctl restart ontap_mediator
```

### ONTAP Mediator 1,8 e precedenti

È possibile utilizzare certificati di terze parti con un nome diverso da `ca.*` o memorizzare i certificati di terze parti in una posizione diversa.

#### Fasi

1. Configurare il

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file in modo che sovrascriva i valori della variabile di default nel `ontap_mediator.config.yaml` file.

Se si è ottenuto `ca.crt` da un'autorità PKI e si memorizza la propria chiave privata `ca.key` nella posizione `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, il `ontap_mediator.user_config.yaml` file dovrebbe essere simile al seguente esempio:



Se si è utilizzato `ca.crt` per firmare il `ontap_mediator_server.crt` certificato, il `ca.srl` file viene generato. Per ulteriori informazioni, vedere [Passaggio 2: Generare un certificato server firmando con una certificazione CA di terze parti](#).

```
[root@scs000216655 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. Se si utilizza una struttura di certificato in cui il `root_ca.crt` certificato fornisce un `ca.crt` certificato che firma il `ontap_mediator_server.crt` certificato, creare una catena di certificati da `ca.crt` e `ontap_mediator_server.crt` certificati:



I certificati e dovrebbero essere stati ottenuti `ca.crt` `ontap_mediator_server.crt` da un'autorità PKI precedentemente nella procedura.

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

- b. Aggiornare il `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Aggiornare i valori di `mediator_cert`, `mediator_key` e `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
```

- Il `mediator_cert` valore è il percorso del `ontap_mediator_server_chain.crt` file.
- Il `mediator_key` valore è il percorso chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- Il `ca_certificate` valore è il percorso del `root_ca.crt` file.



Per i cluster SnapMirror Business Continuity (SM-BC), è necessario aggiungere i `ca.crt` certificati e `root_ca.crt` a un cluster ONTAP. Vedere ["Configurare ONTAP Mediator e cluster per SnapMirror ActiveSync"](#).

- c. Verificare che i seguenti attributi dei certificati appena generati siano impostati correttamente:

- Proprietario del gruppo Linux: `netapp:netapp`
- Autorizzazioni Linux: `600`

2. Riavviare ONTAP Mediator quando i certificati vengono aggiornati nel file di configurazione:

```
systemctl restart ontap_mediator
```

## Risolvere i problemi relativi ai certificati

È possibile controllare determinate proprietà dei certificati.

### Verificare la scadenza del certificato

Utilizzare il seguente comando per identificare l'intervallo di validità del certificato.

### ONTAP Mediator 1,9 e versioni successive

```
[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 e precedenti

```
[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
```

### Verificare le estensioni X509v3 nella certificazione CA

Utilizzare il seguente comando per verificare le estensioni X509v3 nella certificazione CA.

### ONTAP Mediator 1,9 e versioni successive

Le proprietà definite **v3\_ca** in `openssl_ca.cnf` vengono visualizzate come X509v3 extensions in `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 e precedenti

Le proprietà definite **v3\_ca** in `openssl_ca.cnf` vengono visualizzate come X509v3 extensions in `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

```

### Verificare le estensioni X509v3 nel certificato del server e nei nomi Alt del soggetto

Il `v3_req` proprietà definite nella `openssl_server.cnf` il file di configurazione viene visualizzato come `X509v3 extensions` nel certificato.

Nell'esempio seguente, è possibile ottenere le variabili in `alt_names` sezioni eseguendo i comandi `hostname -A` e `hostname -I` sulla VM Linux su cui è installato ONTAP Mediator.

Rivolgersi all'amministratore di rete per i valori corretti delle variabili.

## ONTAP Mediator 1,9 e versioni successive

```
[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 e precedenti



```

[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

```

### Verificare che una chiave privata corrisponda a un certificato

È possibile verificare se una particolare chiave privata corrisponde a un certificato.

Utilizzare i seguenti comandi OpenSSL rispettivamente sulla chiave e sul certificato.

### ONTAP Mediator 1,9 e versioni successive

```
[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 e precedenti

```
[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
```

Se il `-modulus` attributo per entrambe le corrispondenze, indica che la chiave privata e la coppia di certificati sono compatibili e possono funzionare l'una con l'altra.

### Verificare che un certificato server sia stato creato da un determinato certificato CA

È possibile utilizzare il comando seguente per verificare che il certificato del server venga creato da un determinato certificato CA.

### ONTAP Mediator 1,9 e versioni successive

```
[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 e precedenti

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

Se viene utilizzata la convalida OSCP (Online Certificate Status Protocol), utilizzare il comando `"openssl-verify"`.

# Gestire il sistema operativo host per ONTAP Mediator

Assicurarsi che il sistema operativo host per ONTAP Mediator venga sottoposto a manutenzione regolare per ottenere prestazioni ottimali.

## Riavviare l'host

Riavviare l'host solo quando i cluster sono integri. I cluster non possono rispondere ai guasti mentre ONTAP Mediator è offline. Impostare un orario per la manutenzione prima del riavvio.

ONTAP Mediator riprende automaticamente durante un riavvio e ripristina le relazioni precedentemente configurate con i cluster ONTAP .

## Aggiornamenti dei pacchetti host

Aggiornare qualsiasi libreria o pacchetto yum, eccetto il kernel. Se necessario, riavviare l'host affinché le modifiche abbiano effetto. Pianificare una finestra di servizio prima di riavviare l'host.

Se si installa `yum-utils` utilizzare il `needs-restarting` comando per rilevare se qualsiasi modifica del pacchetto richiede un riavvio.

Riavviare dopo aver aggiornato le dipendenze di ONTAP Mediator perché le modifiche non hanno effetto immediato.

## Aggiornare il kernel del sistema operativo host

SCST deve essere compilato per il kernel che stai utilizzando. Per aggiornare il sistema operativo, è necessario pianificare un periodo di manutenzione.

### Fasi

Per aggiornare il kernel del sistema operativo host, seguire questi passaggi.



Prima di aggiornare il kernel, verificare che la versione del sistema operativo e ONTAP Mediator siano compatibili. Per le versioni supportate, vedere "[Matrice di supporto del sistema operativo](#)".

1. Arresta il mediatore ONTAP.
2. Disinstallare il pacchetto SCST, vedere [Eseguire la manutenzione dell'host](#) . (SCST non fornisce un meccanismo di aggiornamento.)
3. Aggiornare il sistema operativo e riavviare.
4. Reinstallare il pacchetto SCST.
5. Riattivare ONTAP Mediator.

## Eseguire la manutenzione dell'host

L'aggiornamento del kernel della VM può causare problemi di compatibilità con i moduli SCST. Disinstallare e reinstallare manualmente SCST.

### Passaggio 1: disinstallare SCST

Per disinstallare SCST, utilizzare il pacchetto tar per la versione di ONTAP Mediator in uso.

## Fasi

1. Scaricare il bundle SCST appropriato (come mostrato nella tabella seguente) ed estrarlo.

Per questa versione ...	USA questo bundle tar...
Mediatore ONTAP 1.11	scst-3.9.tar.gz
Mediatore ONTAP 1.10	scst-3.9.tar.gz
Mediatore ONTAP 1.9.1	scst-3,8.0.tar.bz2
ONTAP mediatore 1,9	scst-3,8.0.tar.bz2
ONTAP mediatore 1,8	scst-3,8.0.tar.bz2
ONTAP mediatore 1,7	scst-3.7.0.tar.bz2
Mediatore ONTAP 1.6	scst-3.7.0.tar.bz2
Mediatore ONTAP 1.5	scst-3.6.0.tar.bz2
Mediatore ONTAP 1.4	scst-3.6.0.tar.bz2
Mediatore ONTAP 1.3	scst-3.5.0.tar.bz2
Mediatore ONTAP 1.1	scst-3.4.0.tar.bz2
Mediatore ONTAP 1.0	scst-3.3.0.tar.bz2

- a. Accedi al pacchetto open source da "[Download di SCST Sourceforge](#)".
  - b. Seleziona **Scarica le versioni rilasciate**.
  - c. Estrarre il bundle nella macchina virtuale.
2. Eseguire i seguenti comandi di disinstallazione in `scst` elenco:
    - a. `systemctl stop mediator-scst`
    - b. `make scstadm_uninstall`
    - c. `make iscsi_uninstall`
    - d. `make usr_uninstall`
    - e. `make scst_uninstall`
    - f. `depmod`

## Passaggio 2: installare SCST

Per installare manualmente SCST, è necessario il bundle tar SCST utilizzato per la versione installata di ONTAP Mediator (vedere [Tabella SCST](#) ).



Eseguire questo passaggio prima di installare ONTAP Mediator. Se la versione SCST in uso è più recente della versione fornita con il programma di installazione ONTAP Mediator, il programma di installazione salta questo passaggio.

1. Eseguire i seguenti comandi di installazione in `scst` elenco:

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



Se stai eseguendo una prima installazione e desideri preinstallare ONTAP Mediator, esegui il seguente comando prima di procedere con il passaggio successivo:

```
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`



Se si preinstalla SCST prima di ONTAP Mediator durante la prima installazione, saltare questo passaggio. Il programma di installazione applica le patch SCST pertinenti.

2. Se, in alternativa, Secure Boot è attivato, prima di riavviare il computer, procedere come segue:

- a. Determinare ciascun nome di file per il `scst_vdisk`, `scst`, E `iscsi_scst` moduli:

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

- b. Determinare il rilascio del kernel:

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

- c. Firmare ogni file del modulo con il 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. Installare la chiave UEFI con il firmware.

Le istruzioni per l'installazione della chiave UEFI sono disponibili all'indirizzo:

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

La chiave UEFI generata si trova in:

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

3. Riavviare il sistema:

```
reboot
```

## L'host modifica il nome host o l'IP

### A proposito di questa attività

- Eseguire questa attività sull'host Linux su cui è installato ONTAP Mediator.
- Eseguire questa operazione solo se i certificati autofirmati non sono più validi perché il nome host o l'indirizzo IP cambiano dopo l'installazione ONTAP Mediator.
- Dopo che il certificato autofirmato temporaneo è stato sostituito da un certificato di terze parti attendibile, *non* è possibile utilizzare questa attività per rigenerare un certificato. Se non si dispone di un certificato autofirmato, non è possibile utilizzare questa procedura.

### Fase

Crea un certificato autofirmato temporaneo per l'host corrente:

1. Riavviare 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

```

## Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.