



Gestire ONTAP Mediator

ONTAP Mediator

NetApp
October 19, 2026

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

Sommario

Gestire ONTAP Mediator	1
Aggiorna ONTAP Mediator	1
Aggiorna ONTAP Mediator	1
Aggiorna il sistema operativo host e reinstalla o aggiorna ONTAP Mediator	9
Configura gli attributi di ONTAP Mediator	14
Impostazioni configurabili di ONTAP Mediator	14
Installa certificati SSL di terze parti	15
Configura la protezione dagli attacchi alle password	17
Configura le regole di complessità delle password	17
Configura la soglia di spazio libero	18
Configura lo spazio di log riservato	18
Modifica il nome utente e la password di ONTAP Mediator	19
Cambia il nome utente	19
Cambia la password	20
Avvia e arresta ONTAP Mediator	21
Arresta ONTAP Mediator	21
Avvia ONTAP Mediator	21
Verifica lo stato di salute di ONTAP Mediator	22
Verifica lo stato del servizio	22
Conferma le porte in ascolto	23
Gestisci i certificati	23
Rigenera un certificato temporaneo autofirmato per l'host ONTAP Mediator	23
Sostituisci i certificati autofirmati di ONTAP Mediator con certificati attendibili di terze parti	24
Risolvi i problemi relativi ai certificati di ONTAP Mediator	39
Mantieni il sistema operativo host per ONTAP Mediator	44
Riavvia l'host	44
Aggiornamenti del pacchetto host	44
Aggiorna il kernel del sistema operativo host	44
Esegui la manutenzione dell'host	45
Modifiche dell'host al host name o all'IP	48
Disinstalla ONTAP Mediator	49

Gestire ONTAP Mediator

Aggiorna ONTAP Mediator

Aggiorna ONTAP Mediator

Per aggiornare ONTAP Mediator a una versione più recente senza aggiornare il sistema operativo host, scarica il pacchetto di installazione della nuova versione ed esegui il programma di installazione sull'host in cui ONTAP Mediator è già installato.



Se devi aggiornare il sistema operativo host a una nuova versione e reinstallare o aggiornare ONTAP Mediator nell'ambito di questo processo, consulta invece ["Aggiornare il sistema operativo host e ONTAP Mediator"](#).

Prima di iniziare

- Verifica che il tuo host soddisfi i prerequisiti descritti in ["Preparati a installare ONTAP Mediator"](#), inclusi i requisiti relativi all'host, al firewall e all'OS.
- Scarica il pacchetto di installazione per la nuova versione. Vedi ["Scarica il pacchetto di installazione di ONTAP Mediator"](#).
- NetApp consiglia di verificare la firma del codice del nuovo pacchetto di installazione. Vedi ["Verifica la firma del codice del pacchetto di installazione di ONTAP Mediator"](#).

Informazioni su questa attività

Prima di aggiornare ONTAP Mediator, leggi le seguenti informazioni.

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



- Se l'aggiornamento non riesce, potresti dover provare una versione più recente di ONTAP Mediator.
- Dal 15 giugno 2025, non puoi installare o aggiornare ONTAP Mediator 1.9 e 1.8 perché i relativi certificati di firma del codice sono scaduti. Se l'aggiornamento non riesce, usa invece la versione patch 1.9.1 di ONTAP Mediator.
- A partire da ONTAP 9.19.1 e ONTAP Mediator 1.12, puoi installare ONTAP Mediator con supporto per iSCSI e HTTPS, oppure solo con supporto per HTTPS. Se scegli di installare ONTAP Mediator con supporto solo per HTTPS, il pacchetto SCST non viene installato.
- Se si esegue l'aggiornamento da ONTAP Mediator 1.11 o versioni precedenti con SCST installato e si sceglie l'opzione solo HTTPS durante l'aggiornamento, il pacchetto SCST viene disinstallato e la nuova versione di ONTAP Mediator non contiene il pacchetto SCST.
- Se hai intenzione di usare ONTAP Mediator per monitorare più configurazioni IP di MetroCluster, il supporto dipende dal tipo di Mediator, dalla versione di ONTAP e dal sistema operativo. Per ulteriori

informazioni, consulta ["Utilizza ONTAP Mediator per monitorare più configurazioni IP MetroCluster"](#).

- L'installazione di ONTAP Mediator con supporto solo per HTTPS è supportata nei seguenti casi d'uso:
 - Hai intenzione di utilizzare ONTAP Mediator esclusivamente per monitorare i tuoi SnapMirror cluster di sincronizzazione attivi.
 - Hai intenzione di configurare ONTAP Mediator con HTTPS per monitorare una o più configurazioni IP MetroCluster.
- ONTAP Mediator deve essere installato con il supporto per iSCSI e HTTPS nel seguente scenario:
 - Si prevede di configurare ONTAP Mediator con iSCSI per monitorare una o più configurazioni IP MetroCluster.
- Quando esegui il programma di installazione su un'installazione ONTAP Mediator esistente, il sistema rileva la versione corrente e ti chiede di confermare l'aggiornamento:

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

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

- Nell'ambito dell'aggiornamento, il programma di installazione acquisisce un pacchetto di supporto della configurazione precedente all'aggiornamento e migra il database prima di aggiornare il software ONTAP Mediator.
- Per i casi d'uso di automazione, puoi usare il comando `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 -y` per saltare le richieste dell'installer.

Passaggi

1. Esegui il programma di installazione della nuova versione e rispondi alle richieste come richiesto:

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



Per saltare il controllo della firma durante l'aggiornamento, usa il `./ontap-mediator-1.12.1/ontap-mediator-1.12.1 --skip-code-signature-check` comando

Il programma di installazione rileva l'installazione esistente e ti invita ad aggiornare, quindi installa i pacchetti necessari e migra la tua configurazione.

▼ Esempio di aggiornamento di ONTAP Mediator con supporto HTTPS e iSCSI (output della console)

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

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
  CApath:/etc/pki/tls
+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
```

(netapp), and one for use by ONTAP to the mediator API
(mediatoradmin).

Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

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

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall

+ Installing required packages.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Package polycoreutils-python-utils-3.6-3.el9.noarch is already
installed.

Package python3.12-3.12.12-4.el9_7.2.x86_64 is already installed.

Package python3.12-devel-3.12.12-4.el9_7.2.x86_64 is already
installed.

```

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

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

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

ONTAP Mediator: Self Extracting Installer

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

ONTAP Mediator can be installed with iSCSI and HTTPS support, or
support for HTTPS only.
Do you wish to install ONTAP Mediator with iSCSI and HTTPS support?
Y(es)/n(o): yes

```

```

ONTAP Mediator will be installed with mode: ISCSI_HTTPS
+ Selected install package mode: ISCSI_HTTPS
ONTAP Mediator will be upgraded from version 1.11.0 to 1.12.1.

Do you wish to continue? Y(es)/n(o): yes
Capturing support_bundle to save pre-upgrade configuration. API
Credentials are required.
    Mediator API User Name: mediatoradmin
    Password: Running plugins, please wait...

Creating tar archive...
Support bundle has been generated at
/opt/netapp/data/support_bundles/scs001097036-1_1776711598_BASIC.tgz
Testing the DB can be upgraded
Cloning database...
Cloning successful.
Verifying database is up-to-date...
Database out-of-date.Migrations are necessary:
Current revision: 0d5dcf349b27, Head revision: 758e4873c40d
Performing database migrations against clone...
Migrations successful.
Database upgrade operation complete.
+ Adding python312 specific packages
+ Upgrading ONTAP Mediator. (Log: /root/ontap_mediator.gwaGmU/ontap-
mediator-1.12.1/ontap-mediator-1.12.1/upgrade_20260420145942.log)

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

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

```

▼ Esempio di aggiornamento di ONTAP Mediator con supporto solo per HTTPS (output della console)

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

ONTAP Mediator: Self Extracting Installer

```
+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
```

```
+ Unpacking the ONTAP Mediator installer
```

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

Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

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

```
+ Checking if SELinux is in enforcing mode
```

```
+ Checking for default Linux firewall
```

```
+ Installing required packages.
```

Last metadata expiration check: 0:33:41 ago on Tue 21 Apr 2026 10:48:35 AM EDT.

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

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

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

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

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

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

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

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

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

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

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

```

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

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

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

```

```
ontap-mediator-1.12.1/ONTAP-Mediator-production.pub
ontap-mediator-1.12.1/ontap-mediator-1.12.1
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig
ontap-mediator-1.12.1/ontap-mediator-1.12.1.tsr
ontap-mediator-1.12.1/ontap-mediator-1.12.1.sig.tsr
[root@mediator_host~]#
[root@mediator_host~]# ontap-mediator-1.12.1/ontap-mediator-1.12.1
--https-only
```

ONTAP Mediator: Self Extracting Installer

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

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

Mediator API User Name: mediatoradmin

Password: Running plugins, please wait...

```
Creating tar archive...
Support bundle has been generated at
/opt/netapp/data/support_bundles/scs001097036-1_1776785423_BASIC.tgz
Testing the DB can be upgraded
Cloning database...
Cloning successful.
Verifying database is up-to-date...
Database out-of-date.Migrations are necessary:
Current revision: 0d5dcf349b27, Head revision: 758e4873c40d
Performing database migrations against clone...
Migrations successful.
Database upgrade operation complete.
+ Adding python312 specific packages
+ Upgrading ONTAP Mediator. (Log: /root/ontap_mediator.cRy0mN/ontap-
mediator-1.12.1/ontap-mediator-1.12.1/upgrade_20260421113003.log)
fapolicyd not installed or no rules.d directory found, skipping
```

```
fapolicyd configuration
    ONTAP Mediator rsyslog and logging rotation enabled
+ Upgrade successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/upgrade_20260421113003.log)\n

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

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

[root@mediator_host ~]#
```

Aggiorna il sistema operativo host e reinstalla o aggiorna ONTAP Mediator

Per aggiornare il sistema operativo host di ONTAP Mediator con SCST installato a una versione successiva, è necessario disinstallare ONTAP Mediator. Dopo l'aggiornamento del sistema operativo, è possibile reinstallare la versione corrente di ONTAP Mediator o eseguire l'aggiornamento a una versione più recente.

Informazioni su questa attività

- Questa procedura si applica alle versioni di ONTAP Mediator con SCST installato. Se hai installato ONTAP Mediator 1.12 o versioni successive con supporto solo per HTTPS, il pacchetto SCST non è installato ed è possibile aggiornare il sistema operativo host senza influire su ONTAP Mediator. Consulta la documentazione del fornitore del sistema operativo host per le istruzioni di aggiornamento del sistema operativo.
- Se devi solo aggiornare il kernel del sistema operativo host a una versione supportata senza eseguire l'aggiornamento a una nuova versione del sistema operativo, consulta invece ["Mantieni il sistema operativo host per ONTAP Mediator"](#).
- Prima di aggiornare il sistema operativo host per ONTAP Mediator con lo strumento leapp-upgrade, ["disinstalla ONTAP Mediator"](#). Lo strumento verifica la presenza di nuove versioni RPM nei repository registrati.
- Il programma di installazione di ONTAP Mediator installa un file .rpm, che lo strumento leapp-upgrade include nella ricerca. Poiché il programma di installazione decompime il file anziché scaricarlo da un repository registrato, lo strumento non riesce a trovare un aggiornamento. Devi usare lo strumento leapp-upgrade per disinstallare il pacchetto.

Passaggi

1. Esegui il backup dei file di log:

```
[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. Esegui l'aggiornamento con lo strumento leapp-upgrade:

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

3. Reinstalla ONTAP Mediator:



Esegui i passaggi rimanenti subito dopo aver reinstallato ONTAP Mediator per evitare la perdita dei file di registro.

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

ONTAP Mediator: Self Extracting Installer

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

4. Interrompi ontap_mediator:

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

5. Sostituisci i file di registro:

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

6. Avvia ontap_mediator:

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

7. Riconnetti tutti i cluster ONTAP a ONTAP Mediator aggiornato:

MetroCluster tramite IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
Status           Status
-----
172.31.40.122
31784      siteA-node2      true      false
              siteA-node1      true      false
              siteB-node2      true      false
              siteB-node2      true      false

siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It may
take a few minutes to complete.
```

```

Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

```

```

siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
Status      Status
-----
-----
172.31.40.122
31784      siteA-node2      true      true
           siteA-node1      true      true
           siteB-node2      true      true
           siteB-node2      true      true
siteA::>

```

SnapMirror active sync

Per la sincronizzazione attiva di SnapMirror, non è necessario reinstallare i certificati TLS archiviati al di fuori di /opt/netapp. Esegui il backup e ripristina i 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      Owing
Vserver      Node      State
-----
39      mediator remove      peer1      peer1-node1      Success
Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver      Serial Number      Certificate Name      Type
-----
-----
peer1
4A790360081F41145E14C5D7CE721DC6C210007F

```

ca

Certificate Authority: ONTAP Mediator CA

Expiration Date: Mon Apr 17 10:27:54 2073

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

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

Please enter Certificate: Press <Enter> when done

....

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

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

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

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

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

Please enter Certificate: Press <Enter> when done

....

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

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

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

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

Notice: Enter the mediator password.

Enter the password:

Enter the password again:

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

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

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

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

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

```
peer1::>
```

Informazioni correlate

- ["security certificate delete"](#)
- ["installazione del certificato di sicurezza"](#)
- ["security certificate show"](#)
- ["snapmirror mediator add"](#)
- ["snapmirror mediator remove"](#)
- ["storage iscsi-initiator show"](#)

Configura gli attributi di ONTAP Mediator

Puoi configurare gli attributi lato host di ONTAP Mediator, incluse le impostazioni relative ai certificati e le sovrascritture di configurazione.

Impostazioni configurabili di ONTAP Mediator

ONTAP Mediator supporta diverse impostazioni configurabili. I valori predefiniti per queste impostazioni sono forniti in un `low_space_threshold_mib: 10` file di sola lettura. Il file si trova in:

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

Tutti i valori inseriti nel `ontap_mediator.user_config.yaml` sovrascriveranno i valori predefiniti e verranno mantenuti in tutti gli aggiornamenti di ONTAP Mediator.

Dopo aver apportato le modifiche `ontap_mediator.user_config.yaml`, riavvia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Gli attributi di ONTAP Mediator descritti in questa sezione possono essere modificati se necessario.



Altri valori predefiniti nel `ontap_mediator.config.yaml` non devono essere modificati perché i valori modificati non vengono mantenuti durante gli aggiornamenti di ONTAP Mediator.

Modifichi gli attributi di ONTAP Mediator copiando le variabili necessarie nel `ontap_mediator.user_config.yaml` file per sovrascrivere le impostazioni predefinite.

Installa certificati SSL di terze parti

Puoi sostituire i certificati autofirmati predefiniti con certificati SSL di terze parti modificando i file di configurazione di ONTAP Mediator.

Per sostituire i certificati autofirmati predefiniti con certificati SSL di terze parti, devi 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 servono a controllare i file di certificato usati da ONTAP Mediator.

ONTAP Mediator 1.9 e versioni successive

Le variabili predefinite elencate nella tabella seguente sono incluse nel file `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`.

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

- `cert_valid_days` serve a impostare la data di 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 versioni precedenti

Le variabili predefinite elencate nella tabella seguente sono incluse nel file `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`.

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` serve a impostare la data di 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 modifichi questi attributi, riavvia ONTAP Mediator per applicare le modifiche. Per istruzioni dettagliate su come sostituire i certificati predefiniti con certificati di terze parti, consulta ["Sostituisci i certificati autofirmati con certificati di terze parti attendibili"](#).

Configura la protezione dagli attacchi alle password

Le seguenti impostazioni offrono protezione contro gli attacchi di forza bruta volti a indovinare le password.

Per abilitare la funzione, imposta un valore per `window_seconds` e `retry_limit`.

Esempi:

- Concedi 5 minuti per i tentativi, dopodiché azzera il conteggio degli errori:

```
authentication_lock_window_seconds: 300
```

- Blocca l'account se si verificano cinque errori entro l'intervallo di tempo:

```
authentication_retry_limit: 5
```

- Riduci l'impatto degli attacchi di forza bruta per indovinare le password impostando un ritardo prima di rifiutare ogni tentativo, rallentando così 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
```

Configura le regole di complessità delle password

I seguenti campi controllano le regole di complessità della 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)
```

Configura le impostazioni del disco e dello spazio dei log di ONTAP Mediator, inclusi la soglia di spazio libero e lo spazio riservato per i log.

Configura la soglia di spazio libero

Ci sono impostazioni che controllano lo spazio libero richiesto sul `/opt/netapp/lib/ontap_mediator` disco.

Se lo spazio disponibile è inferiore alla soglia impostata, il servizio genera un evento di avviso.

```
low_space_threshold_mib: 10
```

Configura lo spazio di log riservato

La `RESERVE_LOG_SPACE` funzionalità 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 a dimensione fissa con un totale di 700MB di spazio su disco da utilizzare esplicitamente per la registrazione dei log di ONTAP Mediator.

Per disabilitare questa funzione e utilizzare lo spazio su disco predefinito, segui questi passaggi:

1. Modifica il valore di `RESERVE_LOG_SPACE` da 1 a 0 nel seguente file:

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

- a. Eseguire il seguente comando:

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

```
RESERVE_LOG_SPACE=0
```

b. Riavvia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Per riattivare la funzionalità, modifica il valore da 0 a 1 e riavvia il Mediator.



Il passaggio da uno spazio su disco all'altro non elimina i log esistenti. Viene eseguito il backup di tutti i log precedenti, che vengono poi spostati nello spazio su disco corrente dopo il passaggio e il riavvio di Mediator.

Modifica il nome utente e la password di ONTAP Mediator

Modifica il nome utente o la password di ONTAP Mediator dall'host Linux su cui è installato ONTAP Mediator.

Cambia il nome utente

Puoi modificare il nome utente usando la seguente procedura.

Informazioni su questa attività

Esegui questa operazione sull'host Linux su cui hai installato ONTAP Mediator.

Se non riesci a eseguire questo comando, potresti doverlo eseguire utilizzando il full path, come mostrato nell'esempio seguente:

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

Passaggi

Modifica il nome utente scegliendo una delle seguenti opzioni:

- **Opzione (a):** Esegui il comando `mediator_change_user` e rispondi 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):** Esegui 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 ~]#
```

Cambia la password

Puoi modificare la password seguendo la procedura descritta di seguito.

Informazioni su questa attività

Esegui questa operazione sull'host Linux su cui hai installato ONTAP Mediator.

Se non riesci a eseguire questo comando, potresti doverlo eseguire utilizzando il full path, come mostrato nell'esempio seguente:

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

Passaggi

Modifica la password scegliendo una delle seguenti opzioni:

- **Opzione (a):** Esegui il `mediator_change_password` comando e rispondi alle richieste 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):** Esegui il seguente comando:

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

L'esempio mostra che la password passa 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 ~]#
```

Avvia e arresta ONTAP Mediator

Arresta o riavvia ONTAP Mediator e SCST quando devi eseguire la manutenzione dell'host o riattivare il servizio.

Arresta ONTAP Mediator

Per arrestare ONTAP Mediator, esegui i seguenti passaggi:

Passaggi

1. Arresta ONTAP Mediator:

```
systemctl stop ontap_mediator
```

2. Interrompi SCST:

```
systemctl stop mediator-scst
```

3. Disabilita ONTAP Mediator e SCST:

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

Avvia ONTAP Mediator

Per riattivare ONTAP Mediator, esegui i seguenti passaggi:

Passaggi

1. Abilitare ONTAP Mediator e SCST:

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

2. Avvia SCST:

```
systemctl start mediator-scst
```

3. Avvia ONTAP Mediator:

```
systemctl start ontap_mediator
```

Verifica lo stato di salute di ONTAP Mediator

Verifica che ONTAP Mediator sia in esecuzione normalmente.

Verifica lo stato del servizio

Passaggi

1. Visualizza lo stato di ONTAP Mediator:

a. Eseguire il seguente comando:

```
systemctl status ontap_mediator
```

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

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

[root@mediator_host ~]#
```

b. Visualizza lo stato del servizio SCST:



Se hai installato ONTAP Mediator 1.12 o versioni successive con supporto solo per HTTPS, il pacchetto SCST non è installato e puoi saltare questo passaggio.

```
systemctl status mediator-scst
```

+

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

[root@mediator_host ~]#
```

Conferma le porte in ascolto

1. Conferma le porte utilizzate da ONTAP Mediator:

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

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

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

Gestisci i certificati

Rigenera un certificato temporaneo autofirmato per l'host ONTAP Mediator

Rigenera un certificato temporaneo autofirmato per l'host corrente quando una modifica dell'host name o dell'indirizzo IP invalida il certificato esistente.



Questa procedura è supportata solo sui sistemi che eseguono ONTAP Mediator 1.7 o versioni successive.

Informazioni su questa attività

- Esegui questa operazione sull'host Linux su cui hai installato ONTAP Mediator.
- Puoi eseguire questa operazione solo se i certificati autofirmati generati sono diventati obsoleti a causa di modifiche all'hostname o all'indirizzo IP dell'host dopo aver installato ONTAP Mediator.

- Dopo aver sostituito il certificato temporaneo autofirmato con un certificato di terze parti attendibile, non usare questa procedura per rigenerare un certificato. L'assenza di un certificato autofirmato causerà l'errore di questa procedura.

Passaggio

Per rigenerare un nuovo certificato temporaneo autofirmato per l'host corrente, esegui il seguente passaggio:

1. Riavvia 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
```

Sostituisci i certificati autofirmati di ONTAP Mediator con certificati attendibili di terze parti

Se il tuo ambiente lo consente, sostituisci i certificati autofirmati con certificati attendibili emessi da un'autorità di certificazione.



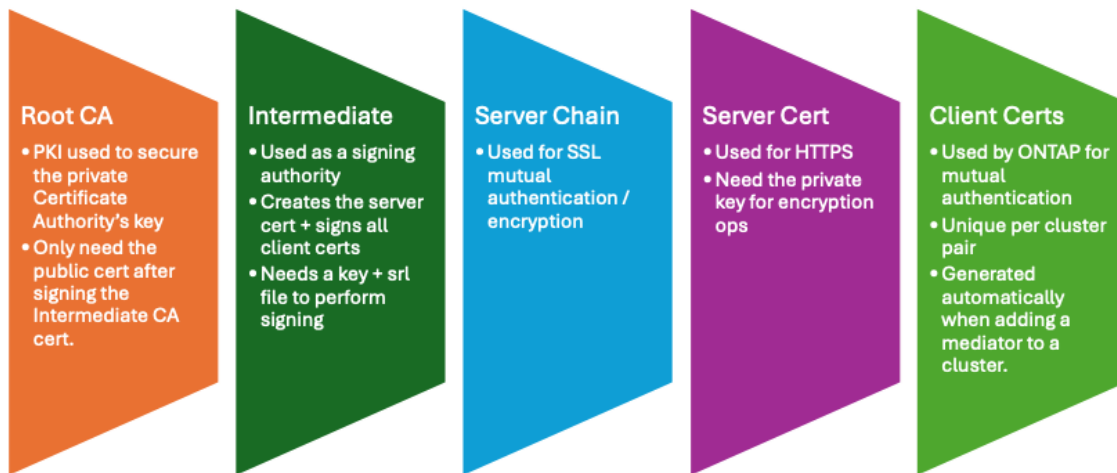
- I certificati di terze parti sono supportati solo a partire da ONTAP 9.16.1 e in alcune release patch precedenti di ONTAP. Consulta ["ID bug Bugs Online NetApp CONTAP-243278"](#).

- I certificati di terze parti sono supportati solo sui sistemi che eseguono ONTAP Mediator 1.7 o versioni successive.

Informazioni su questa attività

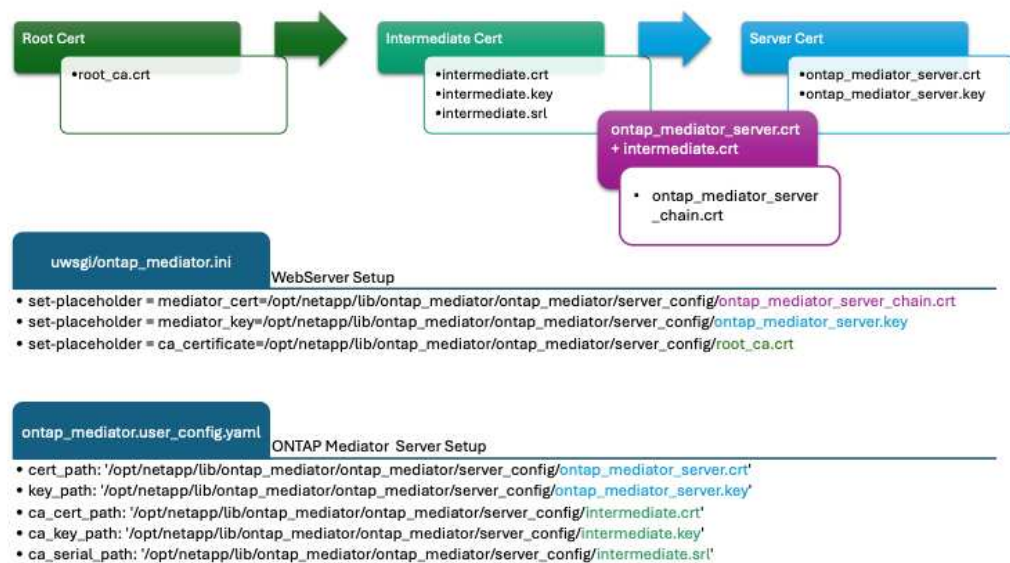
- Esegui questa operazione sull'host Linux su cui hai installato ONTAP Mediator.
- Puoi eseguire questa operazione se i certificati autofirmati generati devono essere sostituiti con certificati ottenuti da un'autorità di certificazione (CA) subordinata attendibile. Per farlo, devi avere accesso a un'autorità attendibile dell'infrastruttura a chiave pubblica (PKI).
- 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 di ONTAP Mediator.

ONTAP Mediator Certificates



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

Puoi ottenere un certificato da un'autorità PKI seguendo la procedura descritta di seguito.

L'esempio seguente mostra come sostituire i componenti del certificato autofirmato con quelli del certificato di terze parti che si trovano in `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`.



L'esempio illustra i criteri necessari per i certificati richiesti per ONTAP Mediator. Puoi ottenere i certificati da un'autorità PKI seguendo una procedura che potrebbe differire da quella descritta. Adatta la procedura alle tue esigenze aziendali.

ONTAP Mediator 1.9 e versioni successive

1. Crea una chiave privata `intermediate.key` e un file di configurazione `openssl_ca.cnf` che verranno utilizzati dall'autorità PKI per generare un certificato.

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

Esempio

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

- b. 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 possedere.

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

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

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



Per i cluster di sincronizzazione attiva di SnapMirror e le configurazioni IP di MetroCluster che utilizzano ONTAP Mediator configurato con HTTPS, devi aggiungere i certificati `intermediate.crt` e `root_ca.crt` a un cluster ONTAP. Vedi ["Configura ONTAP Mediator e i cluster per SnapMirror active sync"](#) e ["Configura il mediatore ONTAP per una configurazione IP MetroCluster"](#).

ONTAP Mediator 1.8 e versioni precedenti

1. Crea una chiave privata `ca.key` e un file di configurazione `openssl_ca.cnf` che l'autorità PKI userà per generare un certificato.
 - a. Genera la chiave privata `ca.key`:

Esempio:

```
openssl genrsa -aes256 -out ca.key 4096
```
 - b. 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 possedere.
2. Usa 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@mediator_host server_config]# openssl req -key ca.key -new
-config openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@mediator_host server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

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

L'autorità PKI verifica la richiesta e firma il documento `.csr`, generando il certificato `ca.crt`. Inoltre, devi ottenere dall'autorità PKI il certificato `root_ca.crt` che ha firmato il certificato `ca.crt`.



Per i cluster con sincronizzazione attiva di SnapMirror, devi aggiungere i `ca.crt` e `root_ca.crt` certificati a un cluster ONTAP. Vedi ["Configura ONTAP Mediator e i cluster per SnapMirror active sync"](#).

Passaggio 2: Genera un certificato server firmandolo con un'autorità di certificazione (CA) di terze parti

ONTAP Mediator 1.9 e versioni successive

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

I seguenti comandi possono generare un certificato del server.

Passaggi

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



Questi file provengono da un'autorità PKI. Se utilizzi un nome di certificato diverso, sostituisci `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'opzione `-CAcreateserial` viene utilizzata per generare i file `intermediate.srl`.

ONTAP Mediator 1.8 e versioni precedenti

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

I seguenti comandi possono generare un certificato del server.

Passaggi

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



Hai ottenuto questi file da un'autorità PKI. Se usi un nome di certificato diverso, sostituisci `ca.crt` e `ca.key` con i nomi di 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 serve a generare il `ca.srl` file.

Passaggio 3: sostituisci il nuovo certificato CA di terze parti e il certificato del server nella configurazione di 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_medi  
ator_server.crt'  
key_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi  
ator_server.key'  
ca_cert_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.crt'  
ca_key_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.key'  
ca_serial_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.srl'
```

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

Passaggi

1. Sostituisci tutti `intermediate.*` i file con i certificati di terze parti.
2. Crea una catena di certificati dai `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` valore è il percorso della chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
 - Il `ssl_certfile` valore corrisponde al percorso del `ontap_mediator_server_chain.crt` file.
 - Il `ssl_ca_certs` valore corrisponde al percorso del `root_ca.crt` file.
4. Verifica che i seguenti attributi dei certificati appena generati siano impostati correttamente:
 - Proprietario del gruppo Linux: `netapp:netapp`
 - Permessi Linux: `600`
 5. Riavvia 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_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
```

```
te.crt'  
ca_key_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.key'  
ca_serial_path:  
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia  
te.srl'
```

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

Passaggi

1. Sostituisci tutti `intermediate.*` i file con i certificati di terze parti.
2. Crea una catena di certificati dai `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/uwsgi/ontap_mediator.ini` file.

Aggiorna 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 corrisponde al 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. Verifica che i seguenti attributi dei certificati appena generati siano impostati correttamente:
 - Proprietario del gruppo Linux: `netapp:netapp`
 - Permessi Linux: `600`
 5. Riavvia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 e versioni 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_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

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

Passaggi

1. Sostituisci tutti `ca.*` i file con i certificati di terze parti.
2. Crea una catena di certificati dai certificati `ca.crt` e `ontap_mediator_server.crt`:

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

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

Aggiorna 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 corrisponde al 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. Verifica che i seguenti attributi dei certificati appena generati siano impostati correttamente:

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

5. Riavvia ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Passaggio 4: Facoltativamente, usa un percorso o un nome diverso per i certificati di terze parti

ONTAP Mediator 1.10 e versioni successive

Puoi utilizzare certificati di terze parti con un nome diverso da `intermediate.*` oppure archiviare i certificati di terze parti in una posizione diversa.

Passaggi

1. Configura il

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file per sovrascrivere i valori predefiniti delle variabili nel `ontap_mediator.config.yaml` file.

Se hai ottenuto `intermediate.crt` da un'autorità PKI e memorizzi la sua 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 hai usato `intermediate.crt` per firmare il `ontap_mediator_server.crt` certificato, viene generato il file `intermediate.srl`. Consulta [Passaggio 2: Genera un certificato server firmandolo con un'autorità di certificazione \(CA\) di terze parti](#) per ulteriori informazioni.

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

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
```

```
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_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'
```

- a. Se utilizzi una struttura di certificati in cui il `root_ca.crt` certificato fornisce un `intermediate.crt` certificato che firma il `ontap_mediator_server.crt` certificato, crea una catena di certificati dai certificati `intermediate.crt` e `ontap_mediator_server.crt`:



Avresti dovuto ottenere i `intermediate.crt` e `ontap_mediator_server.crt` certificati da un'autorità PKI in una fase precedente della 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` valore è il percorso della chiave nel `ontap_mediator_server.crt` file, che è `ontap_mediator_server.key`.
- Il `ssl_certfile` valore corrisponde al percorso del

ontap_mediator_server_chain.crt file.

- Il `ssl_ca_certs` valore corrisponde al percorso del `root_ca.crt` file.



Per i cluster di sincronizzazione attiva di SnapMirror e le configurazioni IP di MetroCluster che utilizzano ONTAP Mediator configurato con HTTPS, devi aggiungere i certificati `intermediate.crt` e `root_ca.crt` a un cluster ONTAP. Vedi ["Configura ONTAP Mediator e i cluster per SnapMirror active sync"](#) e ["Configura il mediatore ONTAP per una configurazione IP MetroCluster"](#).

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

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

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

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 e 1.9

Puoi utilizzare certificati di terze parti con un nome diverso da `intermediate.*` oppure archiviare i certificati di terze parti in una posizione diversa.

Passaggi

1. Configura il

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file per sovrascrivere i valori predefiniti delle variabili nel `ontap_mediator.config.yaml` file.

Se hai ottenuto `intermediate.crt` da un'autorità PKI e memorizzi la sua 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 hai usato `intermediate.crt` per firmare il `ontap_mediator_server.crt` certificato, viene generato il file `intermediate.srl`. Consulta [Passaggio 2: Genera un certificato server firmandolo con un'autorità di certificazione \(CA\) di terze parti](#) per ulteriori informazioni.

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

```
# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
```

```

ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'

```

- a. Se utilizzi una struttura di certificati in cui il `root_ca.crt` certificato fornisce un `intermediate.crt` certificato che firma il `ontap_mediator_server.crt` certificato, crea una catena di certificati dai certificati `intermediate.crt` e `ontap_mediator_server.crt`:



Avresti dovuto ottenere i `intermediate.crt` e `ontap_mediator_server.crt` certificati da un'autorità PKI in una fase precedente della procedura.

```

cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt

```

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

Aggiorna 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 corrisponde al percorso del `ontap_mediator_server_chain.crt` file.
- Il `mediator_key` valore è il percorso della 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), devi aggiungere i certificati `intermediate.crt` e `root_ca.crt` a un cluster ONTAP. Vedi ["Configura ONTAP Mediator e i cluster per SnapMirror active sync"](#).

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

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

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

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 e versioni precedenti

Puoi utilizzare certificati di terze parti con un nome diverso da `ca.*` oppure archiviare i certificati di terze parti in una posizione diversa.

Passaggi

1. Configura il

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file per sovrascrivere i valori predefiniti delle variabili nel `ontap_mediator.config.yaml` file.

Se hai ottenuto `ca.crt` da un'autorità PKI e memorizzi la relativa 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 hai usato `ca.crt` per firmare il `ontap_mediator_server.crt` certificato, viene generato il file `ca.srl`. Consulta [Passaggio 2: Genera un certificato server firmandolo con un'autorità di certificazione \(CA\) di terze parti](#) per ulteriori informazioni.

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

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
```

```

ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'

```

- a. Se utilizzi una struttura di certificati in cui il `root_ca.crt` certificato fornisce un `ca.crt` certificato che firma il `ontap_mediator_server.crt` certificato, crea una catena di certificati dai `ca.crt` e `ontap_mediator_server.crt` certificati:



Avresti dovuto ottenere i `ca.crt` e `ontap_mediator_server.crt` certificati da un'autorità PKI in una fase precedente della procedura.

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

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

Aggiorna 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 corrisponde al percorso del `ontap_mediator_server_chain.crt` file.
- Il `mediator_key` valore è il percorso della 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), devi aggiungere i certificati `ca.crt` e `root_ca.crt` a un cluster ONTAP. Vedi "[Configura ONTAP Mediator e i cluster per SnapMirror active sync](#)".

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

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

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

```
systemctl restart ontap_mediator
```

Risolvi i problemi relativi ai certificati di ONTAP Mediator

Usa questi controlli per verificare le proprietà del certificato durante la risoluzione dei problemi dei certificati.

Verifica la scadenza del certificato

Usa 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 versioni 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
```

Verifica le estensioni X509v3 nel certificato CA

Usa il seguente comando per verificare le estensioni X509v3 nel certificato della CA.

ONTAP Mediator 1.9 e versioni successive

Le proprietà definite all'interno di **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 versioni precedenti

Le proprietà definite all'interno di **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

```

Verifica le estensioni X509v3 nel certificato del server e nei Subject Alternative Name

Le `v3_req` proprietà definite nel `openssl_server.cnf` file di configurazione sono visualizzate come X509v3 extensions nel certificato.

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

Verifica con il tuo amministratore di rete 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 versioni 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
```

Verifica che la chiave privata corrisponda al certificato

Puoi verificare se una determinata chiave privata corrisponde a un certificato.

Usa 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 versioni 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 l'attributo `-modulus` per entrambi corrisponde, significa che la coppia chiave privata-certificato è compatibile e può funzionare insieme.

Verifica che il certificato del server sia stato creato a partire da un certificato CA specifico

Puoi usare il seguente comando per verificare che il certificato del server sia stato creato da un certificato CA specifico.

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 versioni precedenti

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

Se utilizzi la convalida OCSP (Online Certificate Status Protocol), usa il comando ["openssl-verify"](#).

Mantieni il sistema operativo host per ONTAP Mediator

Assicurati di eseguire regolarmente la manutenzione del sistema operativo host per ONTAP Mediator per ottenere prestazioni ottimali.

Riavvia l'host

Riavvia l'host solo quando i cluster sono integri. I cluster non possono rispondere ai guasti mentre ONTAP Mediator è offline. Imposta un orario per la manutenzione prima di riavviare.

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

Aggiornamenti del pacchetto host

Aggiorna tutte le librerie o i pacchetti yum, ad eccezione del kernel. Riavvia l'host, se necessario, affinché le modifiche abbiano effetto. Pianifica una finestra di servizio prima di riavviare l'host.

Se installi il `yum-utils` pacchetto, usa il `needs-restarting` comando per rilevare se eventuali modifiche ai pacchetti richiedono un riavvio.

Riavvia il sistema dopo aver aggiornato le dipendenze di ONTAP Mediator, perché le modifiche non hanno effetto immediato.

Aggiorna il kernel del sistema operativo host

SCST deve essere compilato per il kernel in uso. Per aggiornare il sistema operativo, devi programmare un intervento di manutenzione.

Prima di iniziare

I seguenti requisiti si applicano quando il pacchetto SCST viene installato con ONTAP Mediator.

- Puoi aggiornare tutti i pacchetti di libreria tranne il kernel, ma potresti dover riavviare il sistema per applicare le modifiche in ONTAP Mediator. Pianifica un periodo di inattività se devi riavviare il sistema.
- Dovresti mantenere aggiornato il kernel del sistema operativo. Aggiorna il kernel core a una versione supportata elencata nel "[Matrice delle versioni di ONTAP Mediator](#)". Devi riavviare il sistema, quindi pianifica una finestra di manutenzione per l'interruzione.
 - Disinstalla il modulo del kernel SCST prima di riavviare il sistema, quindi reinstallalo dopo il riavvio.
 - Prepara una versione supportata di SCST da reinstallare prima di avviare l'aggiornamento del kernel del sistema operativo.



Se hai installato ONTAP Mediator 1.12 o versioni successive con supporto solo per HTTPS, il pacchetto SCST non è installato e il kernel del sistema operativo host può essere aggiornato senza influire su ONTAP Mediator. Consulta la documentazione del sistema operativo host per le istruzioni di aggiornamento.

Passaggi

Segui questi passaggi per aggiornare il kernel del sistema operativo host.



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

1. Arresta ONTAP Mediator.
2. Disinstalla il pacchetto SCST, vedi [Esegui la manutenzione dell'host](#). (SCST non fornisce un meccanismo di aggiornamento.)
3. Aggiorna il sistema operativo e riavvia.
4. Reinstalla il pacchetto SCST.
5. Riattiva ONTAP Mediator.

Esegui la manutenzione dell'host

L'aggiornamento del kernel della macchina virtuale può causare problemi di compatibilità con i moduli SCST. Disinstalla e reinstalla SCST manualmente.



Se hai installato ONTAP Mediator 1.12 o versioni successive con supporto solo per HTTPS, il pacchetto SCST non è installato e puoi saltare questo passaggio.

Passaggio 1: Disinstalla SCST

Per disinstallare SCST, usa il bundle tar per la tua versione di ONTAP Mediator.

Passaggi

1. Scarica il pacchetto SCST appropriato (come mostrato nella tabella seguente) ed estrailo.

Per questa versione ...	Usa questo bundle tar...
ONTAP Mediator 1.12.1	scst-3.10.tar.gz

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

- a. Accedi al pacchetto open source dal "[Download SCST da SourceForge](#)".
 - b. Seleziona **Scarica le versioni rilasciate**.
 - c. Estrai il pacchetto nella tua VM.
2. Esegui i seguenti comandi di disinstallazione nella `scst` directory:
- 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: Installa SCST

Per installare manualmente SCST, ti serve il pacchetto tar di SCST usato per la versione installata di ONTAP Mediator (vedi [Tabella SCST](#)).

Informazioni su questa attività

- Esegui questo passaggio prima di installare ONTAP Mediator. Se la versione di SCST che stai usando è più recente della versione inclusa nel programma di installazione di ONTAP Mediator, il programma di installazione salta questo passaggio.
- In alcuni scenari, l'installazione predefinita di SCST sul sistema operativo aggiornato può non riuscire perché il sistema operativo aggiornato richiede una patch.

A partire da ONTAP Mediator 1.12.1, se l'installazione non riesce, puoi usare lo strumento di riparazione SCST che si trova in `/usr/local/bin/mediator_repair_scst` per riparare l'installazione.

Se il sistema operativo aggiornato richiede una patch, il tool la contiene per la versione di SCST fornita all'interno del pacchetto ONTAP Mediator. Il `mediator_repair_scst` tool è un tool standalone separato

dal programma di installazione principale ed è incluso all'interno del file ONTAP Mediator `tgz`. Non influisce sull'installazione o sui percorsi di aggiornamento di ONTAP Mediator.

Passaggi

1. Esegui i seguenti comandi di installazione nella `scst` directory:

- 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 vuoi 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 preinstalli SCST prima di ONTAP Mediator durante una prima installazione, salta questo passaggio. Il programma di installazione applica le patch SCST necessarie.

2. Facoltativamente, se Secure Boot è abilitato, prima di riavviare il computer, esegui i seguenti passaggi:

a. Determina il nome di ciascun file per i moduli `scst_vdisk`, `scst` e `iscsi_scst`:

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

b. Determina la versione del kernel:

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

c. Firma ciascun 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_module_key.der \
_module-filename_
```

d. Installa la chiave UEFI con il firmware.

Le istruzioni per l'installazione della chiave UEFI si trovano al seguente 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.der
```

3. Riavvia il sistema:

```
reboot
```

Modifiche dell'host al host name o all'IP

Informazioni su questa attività

- Esegui questa operazione sull'host Linux su cui hai installato ONTAP Mediator.
- Esegui questa operazione solo se i certificati autofirmati non sono più validi perché l'host name o l'indirizzo IP sono cambiati dopo aver installato ONTAP Mediator.
- Dopo aver sostituito il certificato temporaneo autofirmato con un certificato di terze parti attendibile, non usare questa procedura per rigenerare un certificato. Se non hai un certificato autofirmato, non puoi usare questa procedura.

Passaggio

Crea un certificato temporaneo autofirmato per l'host corrente:

1. Riavvia 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

```

Disinstalla ONTAP Mediator

Se necessario, disinstalla ONTAP Mediator dopo averlo disconnesso da ONTAP.

Prima di iniziare

Devi disconnettere ONTAP Mediator da ONTAP prima di rimuoverlo.

Informazioni su questa attività

Esegui questa operazione sull'host Linux su cui hai installato ONTAP Mediator.

Se non riesci a eseguire questo comando, potresti doverlo eseguire utilizzando il full path, come mostrato nell'esempio seguente:

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

Passaggio

1. Disinstalla 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 ~]#
```

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.