



Keystone in modalità privata

Keystone

NetApp
January 15, 2026

Sommario

Keystone in modalità privata	1
Scopri di più su Keystone (modalità privata)	1
Keystone Collector in modalità privata	1
Prepararsi all'installazione Keystone Collector in modalità privata	3
Requisiti per VMware vSphere	3
Requisiti per Linux	3
Requisiti di rete	4
Installa Keystone Collector in modalità privata	4
Distribuisce su VMware vSphere	4
Installa su Linux	4
Configura Keystone Collector in modalità privata	5
Esporta il report di utilizzo	8
Aggiorna ONTAP	8
Riavvia Keystone Collector	9
Monitora lo stato di salute di Keystone Collector in modalità privata	9
Genera e raccogli pacchetti di supporto	10

Keystone in modalità privata

Scopri di più su Keystone (modalità privata)

Keystone offre una modalità di distribuzione *privata*, nota anche come *dark site*, per soddisfare le tue esigenze aziendali e di sicurezza. Questa modalità è disponibile per le organizzazioni con limitazioni di connettività.

NetApp offre una distribuzione specializzata di Keystone STaaS, pensata appositamente per ambienti con connettività Internet limitata o assente (noti anche come dark site). Si tratta di ambienti sicuri o isolati in cui la comunicazione esterna è limitata per motivi di sicurezza, conformità o requisiti operativi.

Per NetApp Keystone, offrire servizi per i dark site significa fornire il servizio di abbonamento allo storage flessibile Keystone in un modo che rispetti i vincoli di questi ambienti. Ciò comporta:

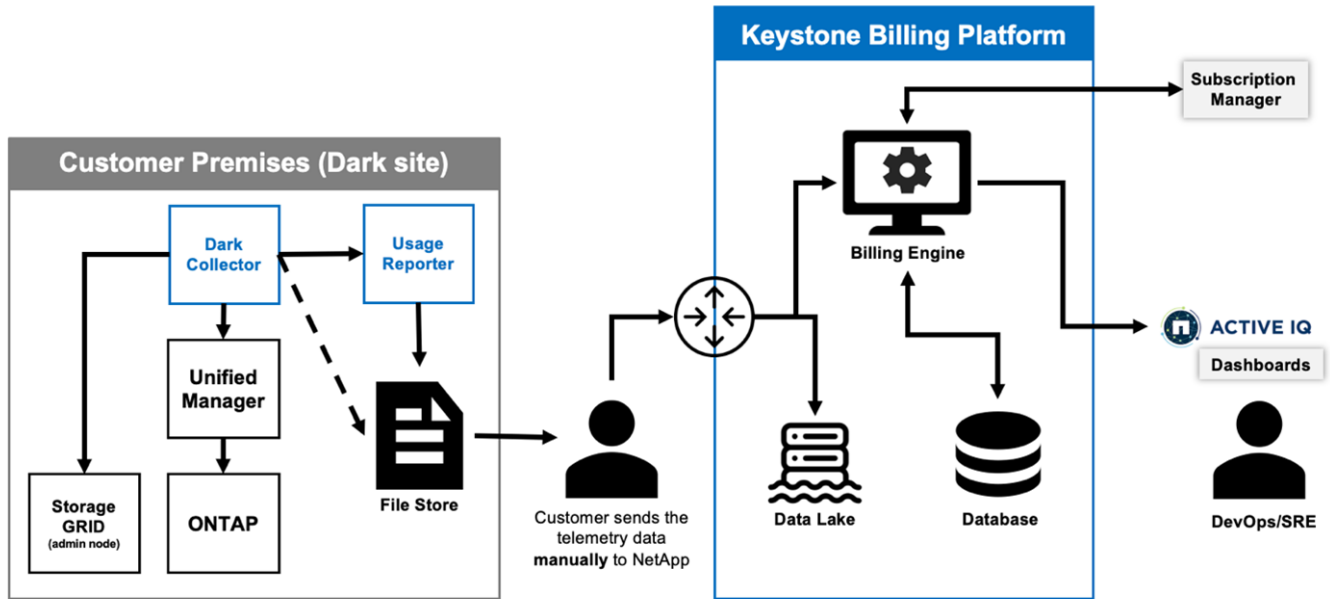
- **Implementazione locale:** Keystone può essere configurato in modo indipendente all'interno di ambienti isolati, senza necessità di connettività Internet o di personale esterno per l'accesso alla configurazione.
- **Operazioni offline:** tutte le funzionalità di gestione dell'archiviazione con controlli di integrità e fatturazione sono disponibili offline per le operazioni.
- **Sicurezza e conformità:** Keystone garantisce che l'implementazione soddisfi i requisiti di sicurezza e conformità dei siti oscuri, che possono includere crittografia avanzata, controlli di accesso sicuri e funzionalità di auditing dettagliate.
- **Assistenza e supporto:** NetApp fornisce supporto globale 24 ore su 24, 7 giorni su 7, con un responsabile Keystone dedicato assegnato a ciascun account per assistenza e risoluzione dei problemi.



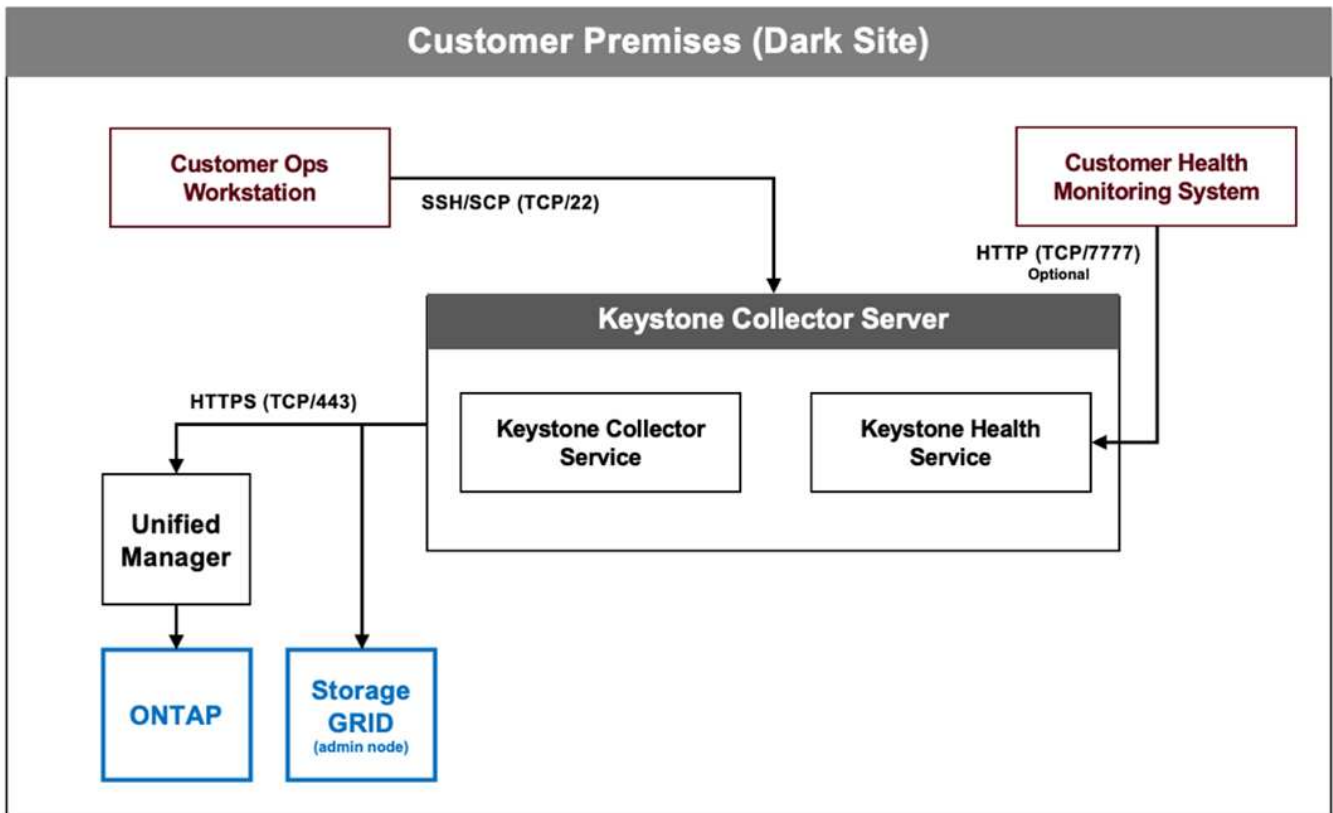
Keystone Collector può essere configurato senza restrizioni di connettività, modalità nota anche come *modalità standard*. Per saperne di più, fare riferimento a "[Scopri di più su Keystone Collector](#)".

Keystone Collector in modalità privata

Keystone Collector è responsabile della raccolta periodica dei dati di utilizzo dai sistemi di archiviazione e dell'esportazione delle metriche in un report di utilizzo offline e in un archivio file locale. I file generati, creati sia in formato crittografato che in formato testo normale, vengono poi inoltrati manualmente a NetApp dall'utente dopo i controlli di convalida. Una volta ricevuti, la piattaforma di fatturazione Keystone di NetApp autentica ed elabora questi file, integrandoli nei sistemi di fatturazione e gestione degli abbonamenti per calcolare gli addebiti mensili.



Il servizio Keystone Collector sul server ha il compito di raccogliere periodicamente i dati di utilizzo, elaborare queste informazioni e generare un file di utilizzo localmente sul server. Il servizio sanitario esegue controlli sullo stato di salute del sistema ed è progettato per interfacciarsi con i sistemi di monitoraggio sanitario utilizzati dal cliente. Questi report sono disponibili per l'accesso offline da parte degli utenti, consentendo la convalida e aiutando nella risoluzione dei problemi.



Prepararsi all'installazione Keystone Collector in modalità privata

Prima di installare Keystone Collector in un ambiente senza accesso a Internet, noto anche come *sito oscuro* o *modalità privata*, assicurati che i tuoi sistemi siano preparati con il software necessario e soddisfino tutti i prerequisiti richiesti.

Requisiti per VMware vSphere

- Sistema operativo: VMware vCenter Server ed ESXi 8.0 o versioni successive
- Nucleo: 1 CPU
- RAM: 2 GB
- Spazio su disco: 20 GB vDisk

Requisiti per Linux

- Sistema operativo (scegline uno):
 - Red Hat Enterprise Linux (RHEL) 8.6 o qualsiasi serie successiva 8.x
 - Red Hat Enterprise Linux 9.0 o versioni successive
 - Debian 12
- Core: 2 CPU
- RAM: 4 GB
- Spazio su disco: 50 GB vDisk
 - Almeno 2 GB liberi in `/var/lib/`
 - Almeno 48 GB liberi in `/opt/netapp`

Sullo stesso server dovrebbero essere installati anche i seguenti pacchetti di terze parti. Se disponibili tramite il repository, questi pacchetti verranno installati automaticamente come prerequisiti:

- RHEL 8.6+ (8.x)
 - `python3 >=v3.6.8, python3 <=v3.9.13`
 - `podman`
 - `sos`
 - `yum-utils`
 - `python3-dnf-plugin-versione-blocco`
- RHEL 9,0+
 - `python3 >= v3.9.0, python3 <= v3.9.13`
 - `podman`
 - `sos`
 - `yum-utils`
 - `python3-dnf-plugin-versione-blocco`

- Debian v12
 - python3 >= v3.9.0, python3 <= v3.12.0
 - podman
 - sosreport

Requisiti di rete

I requisiti di rete per Keystone Collector includono quanto segue:

- Active IQ Unified Manager (Unified Manager) 9.10 o versione successiva, configurato su un server con la funzionalità API Gateway abilitata.
- Il server Unified Manager dovrebbe essere accessibile dal server Keystone Collector sulla porta 443 (HTTPS).
- È necessario configurare un account di servizio con autorizzazioni di utente applicazione per Keystone Collector sul server Unified Manager.
- Non è richiesta la connettività Internet esterna.
- Ogni mese, esporta un file da Keystone Collector e invialo via e-mail al team di supporto NetApp . Per maggiori informazioni su come contattare il team di supporto, fare riferimento a "[Ottieni assistenza con Keystone](#)".

Installa Keystone Collector in modalità privata

Completa alcuni passaggi per installare Keystone Collector in un ambiente senza accesso a Internet, noto anche come *sito oscuro* o *modalità privata*. Questo tipo di installazione è perfetto per i tuoi siti sicuri.

A seconda delle esigenze, è possibile distribuire Keystone Collector sui sistemi VMware vSphere oppure installarlo sui sistemi Linux. Seguire i passaggi di installazione corrispondenti all'opzione selezionata.

Distribuisci su VMware vSphere

Segui questi passaggi:

1. Scarica il file modello OVA da "[Portale web NetApp Keystone](#)" .
2. Per i passaggi per distribuire il raccogliore Keystone con il file OVA, fare riferimento alla sezione "[Distribuzione del modello OVA](#)" .

Installa su Linux

Il software Keystone Collector viene installato sul server Linux utilizzando i file .deb o .rpm forniti, in base alla distribuzione Linux.

Per installare il software sul tuo server Linux, segui questi passaggi:

1. Scarica o trasferisci il file di installazione di Keystone Collector sul server Linux:

```
keystone-collector-<version>.noarch.rpm
```

2. Aprire un terminale sul server ed eseguire i seguenti comandi per avviare l'installazione.

- **Utilizzando il pacchetto Debian**

```
dpkg -i keystone-collector_<version>_all.deb
```

- **Utilizzando il file RPM**

```
yum install keystone-collector-<version>.noarch.rpm
```

O

```
rpm -i keystone-collector-<version>.noarch.rpm
```

3. Entra `y` quando viene richiesto di installare il pacchetto.

Configura Keystone Collector in modalità privata

Completa alcune attività di configurazione per consentire a Keystone Collector di raccogliere dati di utilizzo in un ambiente che non ha accesso a Internet, noto anche come *sito oscuro* o *modalità privata*. Si tratta di un'attività una tantum che serve ad attivare e associare i componenti richiesti al tuo ambiente di archiviazione. Una volta configurato, Keystone Collector monitorerà tutti i cluster ONTAP gestiti da Active IQ Unified Manager.



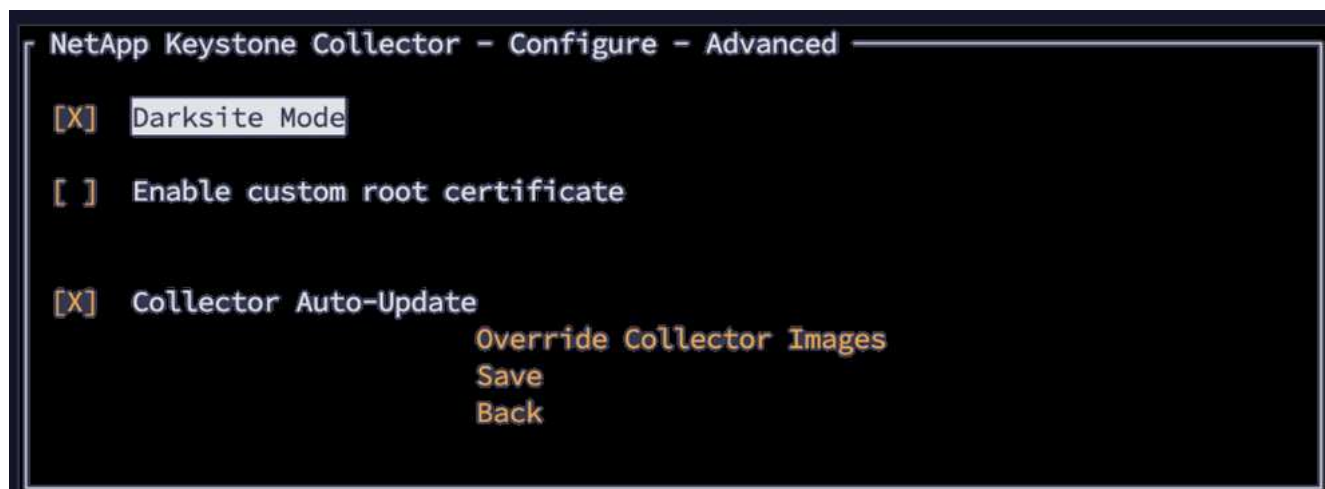
Keystone Collector fornisce l'utilità Keystone Collector Management Terminal User Interface (TUI) per eseguire attività di configurazione e monitoraggio. È possibile utilizzare vari comandi da tastiera, come Invio e i tasti freccia, per selezionare le opzioni e navigare all'interno di questa TUI.

Passi

1. Avviare l'utilità TUI di gestione di Keystone Collector:

```
keystone-collector-tui
```

2. Vai su **Configura > Avanzate**.
3. Attiva l'opzione **Modalità Darksite**.



4. Seleziona **Salva**.
5. Vai su **Configura > KS-Collector** per configurare Keystone Collector.
6. Attivare o disattivare il campo **Avvia KS Collector con il sistema**.
7. Attiva/disattiva il campo ***Raccogli utilizzo ONTAP ***. Aggiungere i dettagli del server Active IQ Unified Manager (Unified Manager) e dell'account utente.
8. **Facoltativo**: attiva il campo **Utilizzo di piani tariffari a livelli** se per l'abbonamento è richiesta la suddivisione in livelli dei dati.
9. In base al tipo di abbonamento acquistato, aggiornare il **Tipo di utilizzo**.



Prima della configurazione, confermare il tipo di utilizzo associato all'abbonamento da NetApp.

```
NetApp Keystone Collector - Configure - KS Collector
[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:
AIQUM Username:
AIQUM Password: -----
[X] Using Tiering Rate plans
Mode Dark
Logging Level info
Usage Type provisioned_v1
Encryption Key Manager
Tunables
Save
Clear Config
Back
```

10. Seleziona **Salva**.
11. Vai su **Configura > KS-Collector** per generare la coppia di chiavi Keystone Collector.
12. Vai a **Encryption Key Manager** e premi Invio.


```
NetApp Keystone Collector - Configure - KS Collector

[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:
AIQUM Username:
AIQUM Password: -----
[ ] Using Tiering Rate plans
Mode Dark
Logging Level info
Usage Type provisioned_v1
Encryption Key Manager
Tunables
Save
Clear Config
Back
```

13. Selezionare **Genera coppia di chiavi del collezionista** e premere Invio.

```
NetApp Keystone Collector - Configure - KS Collector - Key Manager

Generate Collector Keypair
Back
```

14. Per verificare che Keystone Collector sia in buone condizioni, tornare alla schermata principale della TUI e verificare le informazioni sullo **Stato del servizio**. Il sistema dovrebbe mostrare che i servizi sono in uno stato **Complessivo: Integro**. Attendere fino a 10 minuti; se dopo questo periodo lo stato generale rimane non funzionante, rivedere i passaggi di configurazione precedenti e contattare il team di supporto NetApp .

```
Service Status
Overall: Healthy
UM-Dark: Running
ks-billing: Running
ks-collector-dark: Running
Recent collector data: Healthy
ONTAP REST response time: Healthy
DB Disk space: Healthy
DB Disk space 30d: Healthy
DB API responses: Healthy
DB Concurrent flushes: Healthy
DB Slow insert rate: Healthy
```

15. Uscire dall'interfaccia utente terminale di gestione di Keystone Collector selezionando l'opzione **Esci alla shell** nella schermata iniziale.
16. Recupera la chiave pubblica generata:

`~/collector-public.pem`
17. Invia un'e-mail con questo file a ng-keystone-secure-site-upload@netapp.com per siti non USPS sicuri, oppure a ng-keystone-secure-site-usps-upload@netapp.com per siti USPS sicuri.

Esporta il report di utilizzo

Dovresti inviare il report riepilogativo dell'utilizzo mensile a NetApp alla fine di ogni mese. È possibile generare questo report manualmente.

Per generare il report di utilizzo, seguire questi passaggi:

1. Vai su **Esporta utilizzo** nella schermata iniziale di Keystone Collector TUI.
2. Raccogli i file e inviali a ng-keystone-secure-site-upload@netapp.com per i siti non USPS sicuri, oppure a ng-keystone-secure-site-usps-upload@netapp.com per i siti USPS sicuri.

Keystone Collector genera sia un file chiaro che un file crittografato, che devono essere inviati manualmente a NetApp. Il report Clear File contiene i seguenti dettagli che possono essere convalidati dal cliente.

```
node_serial,derived_service_level,usage_tib,start,duration_seconds
123456781,extreme,25.0,2024-05-27T00:00:00,86400
123456782,premium,10.0,2024-05-27T00:00:00,86400
123456783,standard,15.0,2024-05-27T00:00:00,86400

<Signature>
31b3d8eb338ee319ef1

-----BEGIN PUBLIC KEY-----
31b3d8eb338ee319ef1
-----END PUBLIC KEY-----
```

Aggiorna ONTAP

Keystone Collector supporta gli aggiornamenti ONTAP tramite TUI.

Per aggiornare ONTAP, seguire questi passaggi:

1. Vai a ***Manutenzione > Aggiornamento Webserver ONTAP ***.
2. Copiare il file immagine di aggiornamento ONTAP in **/opt/netapp/ontap-upgrade/**, quindi selezionare **Avvia Webserver** per avviare il server Web.



3. Vai a <http://<collector-ip>:8000> utilizzando un browser web per assistenza nell'aggiornamento.

Riavvia Keystone Collector

È possibile riavviare il servizio Keystone Collector tramite TUI. Vai a **Manutenzione > Riavvia Collector Servizi** nella TUI. Questa operazione riavvierà tutti i servizi di raccolta e il loro stato potrà essere monitorato dalla schermata iniziale di TUI.



Monitora lo stato di salute di Keystone Collector in modalità privata

È possibile monitorare lo stato di Keystone Collector utilizzando qualsiasi sistema di monitoraggio che supporti le richieste HTTP.

Per impostazione predefinita, i servizi sanitari Keystone non accettano connessioni da IP diversi da localhost. L'endpoint sanitario Keystone è `/uber/health` e ascolta su tutte le interfacce del server Keystone Collector sulla porta 7777. Alla richiesta, l'endpoint restituisce come risposta un codice di stato della richiesta HTTP con un output JSON, che descrive lo stato del sistema Keystone Collector. Il corpo JSON fornisce uno stato di salute generale per il `is_healthy` attributo, che è un valore booleano; e un elenco dettagliato degli stati per componente per il `component_details` attributo. Ecco un esempio:

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

Vengono restituiti i seguenti codici di stato:

- **200**: indica che tutti i componenti monitorati sono integri
- **503**: indica che uno o più componenti non sono integri
- **403**: indica che il client HTTP che interroga lo stato di integrità non è presente nell'elenco *allow*, ovvero un elenco di CIDR di rete consentiti. Per questo stato non vengono restituite informazioni sanitarie.

L'elenco *allow* utilizza il metodo CIDR di rete per controllare quali dispositivi di rete sono autorizzati a interrogare il sistema sanitario Keystone . Se viene visualizzato l'errore 403, aggiungere il sistema di monitoraggio all'elenco *consentito* da * Keystone Collector management TUI > Configura > Monitoraggio integrità*.

```

NetApp Keystone Collector - Configure - Health Check

Allowed Network CIDR List:
    10.10.10.0/24
    10.10.10.0/24

    Save
    Back

Use CIDR notation to list the external networks allowed to query
the health monitoring endpoint. An empty list denotes that no external addr
are allowed to query the health, while 0.0.0.0/0 allows queries from netwo

```

Genera e raccogli pacchetti di supporto

Per risolvere i problemi con Keystone Collector, puoi rivolgerti al supporto NetApp , che potrebbe richiedere un file *.tar*. È possibile generare questo file tramite l'utilità TUI di gestione Keystone Collector.

Per generare un file *.tar*, seguire questi passaggi:

1. Vai a **Risoluzione dei problemi > Genera pacchetto di supporto**.
2. Seleziona la posizione in cui salvare il pacchetto, quindi fai clic su **Genera pacchetto di supporto**.

```

NetApp Keystone Collector - Troubleshooting - Support Bundle

Bundle Output Directory: /home/esis
[ ] Upload to Keystone Support
    Generate Support Bundle
    Back

```

Questo processo crea un *tar* pacchetto nella posizione indicata che può essere condiviso con NetApp per la risoluzione dei problemi.

3. Una volta scaricato il file, è possibile allegarlo al ticket di supporto Keystone ServiceNow. Per informazioni sull'emissione dei biglietti, vedere "[Generazione di richieste di servizio](#)".

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.