



# **Fornire l'accesso del client S3 ai dati NAS**

## **ONTAP 9**

NetApp  
April 24, 2024

# Sommario

- Fornire l'accesso del client S3 ai dati NAS. . . . . 1
  - Panoramica sul multiprotocollo S3. . . . . 1
  - Requisiti dei dati NAS per l'accesso al client S3 . . . . . 3
  - Abilitare l'accesso del protocollo S3 ai dati NAS . . . . . 4
  - Creare un bucket S3 NAS . . . . . 6
  - Abilitare gli utenti del client S3 . . . . . 7

# Fornire l'accesso del client S3 ai dati NAS

## Panoramica sul multiprotocollo S3

A partire da ONTAP 9.12.1, è possibile consentire ai client che eseguono il protocollo S3 di accedere agli stessi dati forniti ai client che utilizzano i protocolli NFS e SMB senza riformattare. Questa funzionalità consente ai dati NAS di continuare a essere serviti ai client NAS, presentando al contempo i dati a oggetti ai client S3 che eseguono applicazioni S3 (come data mining e intelligenza artificiale).

La funzionalità multiprotocollo S3 consente di gestire due casi di utilizzo:

### 1. Accesso ai dati NAS esistenti mediante client S3

Se i dati esistenti sono stati creati utilizzando client NAS tradizionali (NFS o SMB) e si trovano su volumi NAS (volumi FlexVol o FlexGroup), è ora possibile utilizzare strumenti analitici sui client S3 per accedere a questi dati.

### 2. Storage back-end per client moderni in grado di eseguire i/o utilizzando protocolli NAS e S3

È ora possibile fornire un accesso integrato ad applicazioni come Spark e Kafka in grado di leggere e scrivere gli stessi dati utilizzando i protocolli NAS e S3.

## Funzionamento del multiprotocollo S3

Il multiprotocollo ONTAP consente di presentare lo stesso set di dati come una gerarchia di file o come oggetti in un bucket. A tale scopo, ONTAP crea "bucket S3 NAS" che consentono ai client S3 di creare, leggere, eliminare ed enumerare i file nello storage NAS utilizzando le richieste a oggetti S3. Questa mappatura è conforme alla configurazione di sicurezza NAS, osservando le autorizzazioni di accesso a file e directory e scrivendo nel registro di controllo della sicurezza secondo necessità.

Questa mappatura viene eseguita presentando una gerarchia di directory NAS specificata come bucket S3. Ogni file nella gerarchia di directory è rappresentato come un oggetto S3 il cui nome è relativo dalla directory mappata verso il basso, con i limiti di directory rappresentati dal carattere barra ('/').

Gli utenti S3 definiti da ONTAP normali possono accedere a questo storage, in base alle policy bucket definite per il bucket che esegue la mappatura alla directory NAS. Affinché ciò sia possibile, è necessario definire le mappature tra gli utenti S3 e gli utenti SMB/NFS. Le credenziali dell'utente SMB/NFS verranno utilizzate per il controllo delle autorizzazioni NAS e incluse nei record di audit risultanti da tali accessi.

Quando viene creato da client SMB o NFS, un file viene immediatamente inserito in una directory e quindi visibile ai client, prima che i dati vengano scritti in essa. I client S3 si aspettano semantica diversa, in cui il nuovo oggetto non è visibile nello spazio dei nomi fino a quando non sono stati scritti tutti i dati. Questa mappatura di S3 allo storage NAS crea file utilizzando la semantica S3, mantenendo i file invisibili esternamente fino al completamento del comando di creazione S3.

## Protezione dei dati per i bucket S3 NAS

I "bucket" S3 NAS sono semplicemente mappature di dati NAS per i client S3, non sono bucket S3 standard. Pertanto, non è necessario proteggere i bucket S3 NAS utilizzando la funzionalità SnapMirror di NetApp S3. È invece possibile proteggere volumi contenenti bucket S3 NAS utilizzando la replica del volume asincrona

SnapMirror. Il disaster recovery di SnapMirror Synchronous e SVM non è supportato.

A partire da ONTAP 9.14.1, i bucket S3 NAS sono supportati in aggregati con mirroring e senza mirror per le configurazioni MetroCluster IP e FC.

Scopri di più ["SnapMirror asincrono"](#).

## Audit per i bucket S3 NAS

Poiché i bucket S3 NAS non sono bucket S3 convenzionali, l'audit S3 non può essere configurato per controllare l'accesso su di essi. Scopri di più ["Verifica S3"](#).

Tuttavia, i file e le directory NAS mappati nei bucket S3 NAS possono essere controllati per gli eventi di accesso utilizzando le procedure di audit ONTAP convenzionali. Le operazioni S3 possono quindi attivare eventi di audit NAS, con le seguenti eccezioni:

- Se l'accesso al client S3 viene negato dalla configurazione del criterio S3 (policy di gruppo o bucket), l'audit NAS per l'evento non viene avviato. Questo perché le autorizzazioni S3 vengono controllate prima di poter eseguire i controlli di audit SVM.
- Se il file di destinazione di una richiesta S3 GET è di dimensione 0, il contenuto 0 viene restituito alla richiesta GET e l'accesso in lettura non viene registrato.
- Se il file di destinazione di una richiesta S3 GET si trova in una cartella per la quale l'utente non dispone dell'autorizzazione di attraversamento, il tentativo di accesso non riesce e l'evento non viene registrato.

Scopri di più ["Controllo degli eventi NAS su SVM"](#).

## Interoperabilità S3 e NAS

I bucket NAS ONTAP S3 supportano le funzionalità NAS e S3 standard, ad eccezione di quelle elencate di seguito.

### Funzionalità NAS attualmente non supportata dai bucket S3 NAS

#### Tier di capacità FabricPool

I bucket S3 NAS non possono essere configurati come Tier di capacità per FabricPool.

### La funzionalità S3 non è attualmente supportata dai bucket S3 NAS

#### Metadati utente AWS

- Le coppie di valori chiave ricevute come parte dei metadati utente S3 non vengono memorizzate su disco insieme ai dati oggetto nella release corrente.
- Le intestazioni delle richieste con il prefisso "x-amz-meta" vengono ignorate.

#### Tag AWS

- All'avvio delle richieste PUT object e Multipart, le intestazioni con il prefisso "x-amz-tagging" vengono ignorate.
- Le richieste di aggiornamento dei tag su un file esistente (ad esempio, richieste put, GET ed Delete con la stringa di query ?tagging) vengono rifiutate con un errore.

#### Versione

Non è possibile specificare la versione nella configurazione di mappatura bucket.

- Le richieste che includono specifiche di versione non null (versionID=stringa di query xyz) ricevono risposte di errore.
- Le richieste che influiscono sullo stato di versione di un bucket vengono rifiutate con errori.

### Operazioni multipart

Le seguenti operazioni non sono supportate:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

## Requisiti dei dati NAS per l'accesso al client S3

È importante comprendere che ci sono alcune incompatibilità intrinseche quando si mappano file e directory NAS per l'accesso S3. Potrebbe essere necessario regolare le gerarchie dei file NAS prima di servirle utilizzando i bucket S3 NAS.

Un bucket S3 NAS fornisce l'accesso S3 a una directory NAS mappando tale directory utilizzando la sintassi del bucket S3 e i file nell'albero delle directory vengono visualizzati come oggetti. I nomi degli oggetti sono i percorsi delimitati dalla barra dei file relativi alla directory specificata nella configurazione del bucket S3.

Questa mappatura impone alcuni requisiti quando i file e le directory vengono serviti utilizzando i bucket NAS S3:

- I nomi S3 sono limitati a 1024 byte, pertanto i file con percorsi più lunghi non sono accessibili utilizzando S3.
- I nomi di file e directory sono limitati a 255 caratteri, pertanto il nome di un oggetto non può contenere più di 255 caratteri consecutivi non slash ('/')
- Un nome percorso SMB delimitato da caratteri backslash ('\') viene visualizzato in s3 come nome di oggetto contenente caratteri '/' (barra rovesciata).
- Alcune coppie di nomi di oggetti S3 legali non possono coesistere nell'albero di directory NAS mappato. Ad esempio, i nomi degli oggetti S3 legali "part1/part2" e "part1/part2/part3" corrispondono a file che non possono esistere contemporaneamente nell'albero delle directory NAS, in quanto "part1/part2" è un file nel nome e una directory nell'altro.
  - Se "part1/part2" è un file esistente, la creazione S3 di "part1/part2/part3" non riesce.
  - Se "part1/part2/part3" è un file esistente, la creazione o l'eliminazione S3 di "part1/part2" non avrà esito positivo.
  - La creazione di un oggetto S3 che corrisponde al nome di un oggetto esistente sostituisce l'oggetto pre-esistente (nei bucket senza versione), che contiene in NAS ma richiede una corrispondenza esatta. Gli esempi precedenti non causeranno la rimozione dell'oggetto esistente perché, mentre i nomi si scontrano, non corrispondono.

Sebbene un archivio di oggetti sia progettato per supportare un numero molto elevato di nomi arbitrari, una struttura di directory NAS può riscontrare problemi di performance se un numero molto elevato di nomi viene inserito in una directory. In particolare, i nomi che non contengono caratteri slash ('/') verranno tutti inseriti nella directory principale della mappatura NAS. Le applicazioni che utilizzano in modo esteso nomi non compatibili con NAS potrebbero essere ospitate meglio su un bucket di archivio di oggetti effettivo piuttosto che su una mappatura NAS.

# Abilitare l'accesso del protocollo S3 ai dati NAS

L'abilitazione dell'accesso al protocollo S3 consiste nel garantire che una SVM abilitata NAS soddisfi gli stessi requisiti di un server abilitato S3, tra cui l'aggiunta di un server di archiviazione a oggetti e la verifica dei requisiti di rete e autenticazione.

Per le nuove installazioni ONTAP, si consiglia di abilitare l'accesso al protocollo S3 a una SVM dopo averla configurato per fornire i dati NAS ai client. Per ulteriori informazioni sulla configurazione del protocollo NAS, consultare:

- ["Configurazione NFS"](#)
- ["Configurazione SMB"](#)

## Prima di iniziare

Prima di attivare il protocollo S3, è necessario configurare quanto segue:

- Il protocollo S3 e i protocolli NAS desiderati (NFS, SMB o entrambi) sono concessi in licenza.
- Viene configurata una SVM per i protocolli NAS desiderati.
- Esistono server NFS e/o SMB.
- Il DNS e gli altri servizi richiesti sono configurati.
- I dati NAS vengono esportati o condivisi nei sistemi client.

## A proposito di questa attività


Per abilitare il traffico HTTPS dai client S3 alla SVM abilitata per S3, è necessario un certificato CA (Certificate Authority). È possibile utilizzare certificati CA provenienti da tre origini:

- Un nuovo certificato autofirmato ONTAP sulla SVM.
- Un certificato autofirmato ONTAP esistente su SVM.
- Un certificato di terze parti.

Per il bucket S3/NAS è possibile utilizzare le stesse LIF di dati utilizzate per la fornitura dei dati NAS. Se sono richiesti indirizzi IP specifici, vedere ["Creazione di LIF di dati"](#). Per attivare il traffico dati S3 su LIF è necessaria una policy dei dati del servizio S3; è possibile modificare la policy di servizio esistente di SVM in modo da includere S3.

Quando si crea il server a oggetti S3, si dovrebbe essere pronti a inserire il nome del server S3 come FQDN (Fully Qualified Domain Name), che i client utilizzeranno per l'accesso S3. L'FQDN del server S3 non deve iniziare con un nome bucket.

## System Manager

1. Abilitare S3 su una VM di storage con protocolli NAS configurati.
  - a. Fare clic su **Storage > Storage VM**, selezionare una VM storage pronta per NAS, fare clic su Settings (Impostazioni), quindi fare clic su  Sotto S3.
  - b. Selezionare il tipo di certificato. Se si seleziona un certificato generato dal sistema o uno dei propri, questo sarà necessario per l'accesso del client.
  - c. Inserire le interfacce di rete.
2. Se è stato selezionato il certificato generato dal sistema, le informazioni del certificato vengono visualizzate quando viene confermata la creazione della nuova VM di storage. Fare clic su **Download** e salvarlo per accedere al client.
  - La chiave segreta non viene visualizzata di nuovo.
  - Se sono necessarie nuovamente le informazioni del certificato: Fare clic su **Storage > Storage VMS**, selezionare la VM di storage e fare clic su **Settings** (Impostazioni).

## CLI

1. Verificare che il protocollo S3 sia consentito su SVM:  
`vserver show -fields allowed-protocols`
2. Registrare il certificato della chiave pubblica per questa SVM. + se è necessario un nuovo certificato autofirmato ONTAP, vedere ["Creare e installare un certificato CA sulla SVM"](#).
3. Aggiornare la policy dei dati del servizio
  - a. Visualizzare la policy dei dati di servizio per SVM  
`network interface service-policy show -vserver svm_name`
  - b. Aggiungere il data-core e data-s3-server services se non sono presenti.  
`network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. Verificare che i dati LIF presenti su SVM soddisfino i requisiti:  
`network interface show -vserver svm_name`
5. Creare il server S3:  
`vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

È possibile specificare opzioni aggiuntive durante la creazione del server S3 o in qualsiasi momento successivo.

- HTTPS è attivato per impostazione predefinita sulla porta 443. È possibile modificare il numero di porta con l'opzione `-Secure-listener-port`. + quando HTTPS è attivato, i certificati CA sono necessari per la corretta integrazione con SSL/TLS.
- HTTP è disattivato per impostazione predefinita; se attivato, il server è in attesa sulla porta 80. Puoi abilitarlo con l'opzione `-is-http-enabled` o modificare il numero di porta con l'opzione `-listener-port`. + quando HTTP è attivato, tutte le richieste e le risposte vengono inviate in rete in testo non crittografato.

1. Verificare che S3 sia configurato come desiderato:  
`vserver object-store-server show`

**Esempio** + il seguente comando verifica i valori di configurazione di tutti i server di storage a oggetti:

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1
```

```
Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svml_ca
Comment: Server comment
```

## Creare un bucket S3 NAS

Un bucket S3 NAS è una mappatura tra un nome di bucket S3 e un percorso NAS. I bucket NAS S3 consentono di fornire l'accesso S3 a qualsiasi parte di uno spazio dei nomi SVM con volumi e struttura di directory esistenti.

### Prima di iniziare

- Un server a oggetti S3 è configurato in una SVM contenente dati NAS.
- I dati NAS sono conformi a ["Requisiti per l'accesso al client S3"](#).

### A proposito di questa attività

È possibile configurare i bucket S3 NAS per specificare qualsiasi set di file e directory all'interno della directory root di SVM.

È inoltre possibile impostare policy bucket che consentono o non consentono l'accesso ai dati NAS in base a qualsiasi combinazione di questi parametri:

- File e directory
- Autorizzazioni utente e gruppo
- Operazioni S3

Ad esempio, potrebbero essere necessarie policy di bucket separate che concedano l'accesso ai dati di sola lettura a un gruppo di utenti di grandi dimensioni e un'altra che consenta a un gruppo limitato di eseguire operazioni su un sottoinsieme di tali dati.

Poiché i "bucket" S3 NAS sono mappature e non bucket S3, le seguenti proprietà dei bucket S3 standard non si applicano ai bucket S3 NAS.

- **Aggr-list/aggr-list-multiplicer/storage-service-level/volume/size/exclude-aggr-list/qos-policy-group** + Nessun volume o qtree viene creato durante la configurazione dei bucket S3 NAS.
- **Il ruolo è -protetto/è -Protected-on-ontap/è -Protected-on-cloud** + i bucket NAS S3 non sono protetti o mirrorati utilizzando S3 SnapMirror, ma utilizzeranno invece la protezione SnapMirror regolare disponibile alla granularità del volume.



- **Versioning-state** + i volumi NAS dispongono solitamente della tecnologia Snapshot per salvare versioni diverse. Tuttavia, la versione non è attualmente disponibile nei bucket S3 NAS.
- I comandi del volume consentono di accedere alle statistiche utilizzate in modo logico/object-count\* + equivalenti per i volumi NAS.

### System Manager

Aggiungere un nuovo bucket S3 NAS su una VM di storage abilitata per NAS.

1. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
2. Inserire un nome per il bucket S3 NAS e selezionare la VM di storage, non inserire una dimensione, quindi fare clic su **altre opzioni**.
3. Immettere un nome di percorso valido o fare clic su Browse (Sfoglia) per effettuare una selezione da un elenco di nomi di percorso validi. + quando si immette un nome di percorso valido, le opzioni non rilevanti per la configurazione S3 NAS vengono nascoste.
4. Se gli utenti S3 sono già stati mappati agli utenti NAS e sono stati creati dei gruppi, è possibile configurarne le autorizzazioni, quindi fare clic su **Save** (Salva). + prima di configurare le autorizzazioni in questa fase, è necessario aver già mappato gli utenti S3 agli utenti NAS.

Altrimenti, fare clic su **Save** (Salva) per completare la configurazione del bucket S3 NAS.

### CLI

Creare un bucket S3 NAS in una SVM contenente i filesystem NAS.

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name -type nas -nas-path junction_path [-comment text]
```

Esempio:

```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type
nas -path /vol1
```

## Abilitare gli utenti del client S3

Per consentire agli utenti del client S3 di accedere ai dati NAS, è necessario mappare i nomi utente S3 agli utenti NAS corrispondenti, quindi concedere loro l'autorizzazione ad accedere ai dati NAS utilizzando i criteri di servizio bucket.

### Prima di iniziare

I nomi utente per l'accesso al client (utenti LINUX/UNIX, Windows e S3) devono già esistere.

### A proposito di questa attività

La mappatura di un nome utente S3 a un utente LINUX/UNIX o Windows corrispondente consente di onorare i controlli di autorizzazione sui file NAS quando tali file sono accessibili dai client S3. Le mappature da S3 a NAS vengono specificate fornendo un nome utente S3 *Pattern*, che può essere espresso come un singolo nome o un'espressione regolare POSIX, e un nome utente LINUX/UNIX o Windows *Replacement*.

Se non è presente alcuna mappatura dei nomi, viene utilizzata la mappatura dei nomi predefinita, in cui il nome utente S3 stesso verrà utilizzato come nome utente UNIX e nome utente Windows. È possibile modificare le mappature predefinite dei nomi utente UNIX e Windows con `vserver object-store-server modify` comando.

È supportata solo la configurazione di mappatura dei nomi locali; LDAP non è supportato.

Una volta mappati gli utenti S3 agli utenti NAS, è possibile concedere autorizzazioni agli utenti specificando le risorse (directory e file) a cui hanno accesso e le azioni che possono eseguire o meno.

## System Manager

1. Creare mappature dei nomi locali per client UNIX o Windows (o entrambi).
  - a. Fare clic su **Storage > Bucket**, quindi selezionare la VM di storage abilitata per S3/NAS.
  - b. Selezionare **Impostazioni**, quindi fare clic su ➔ In **Name Mapping** (sotto **host Users and Groups**).
  - c. Nei riquadri **S3 to Windows** o **S3 to UNIX** (o entrambi), fare clic su **Add** (Aggiungi), quindi immettere i nomi utente desiderati **Pattern** (S3) e **Replacement** (NAS).
2. Creare una policy bucket per fornire l'accesso al client.
  - a. Fare clic su **Storage > Bucket**, quindi su ⓘ Accanto al bucket S3 desiderato, quindi fare clic su **Edit** (Modifica).
  - b. Fare clic su **Add** (Aggiungi) e fornire i valori desiderati.
    - **Principal** - specificare i nomi utente S3 o utilizzare il valore predefinito (tutti gli utenti).
    - **Effetto** - selezionare **Consenti** o **Nega**.
    - **Azioni** - inserire azioni per questi utenti e risorse. Le operazioni di risorsa attualmente supportate dal server di archiviazione a oggetti per i bucket NAS S3 sono: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketLocation`, `GetBucketVersioning`, `PutBucketVersioning` e `ListBucketVersions`. I caratteri jolly sono accettati per questo parametro.
    - **Risorse** - inserire i percorsi di cartella o file in cui le azioni sono consentite o rifiutate, oppure utilizzare le impostazioni predefinite (directory principale del bucket).

## CLI

1. Creare mappature dei nomi locali per client UNIX o Windows (o entrambi).

```
vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix}
-position integer -pattern s3_user_name -replacement nas_user_name
```

  - `-position` - numero di priorità per la valutazione della mappatura; inserire 1 o 2.
  - `-pattern` - Un nome utente S3 o un'espressione regolare
  - `-replacement` - un nome utente windows o unix

## Esempi

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1 vserver name-mapping create -direction s3-unix
-position 2 -pattern s3_user_1 -replacement unix_user_1
```

1. Creare una policy bucket per fornire l'accesso al client.

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {deny|allow} -action list_of_actions -principal
list_of_users_or_groups -resource [-sid alphanumeric_text]
```

- `-effect {deny|allow}` - specifica se l'accesso è consentito o negato quando un utente richiede un'azione.
- `-action <Action>, ...` - specifica le operazioni di risorsa consentite o negate. Le operazioni di risorsa attualmente supportate dal server di archiviazione a oggetti per i bucket NAS S3 sono: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketLocation`, `GetBucketVersioning`,

PutBucketVersioning e ListBucketVersions. I caratteri jolly sono accettati per questo parametro.

- ° `-principal <Objectstore Principal>, ...` - convalida l'utente che richiede l'accesso in base agli utenti o ai gruppi del server dell'archivio di oggetti specificati in questo parametro.
  - Per specificare un gruppo di server di archiviazione oggetti, aggiungere un gruppo di prefissi/ al nome del gruppo.
  - `-principal -` (il trattino) consente l'accesso a tutti gli utenti.
- ° `-resource <text>, ...` - specifica il bucket, la cartella o l'oggetto per il quale sono impostate le autorizzazioni allow/deny. I caratteri jolly sono accettati per questo parametro.
- ° `[-sid <SID>]` - specifica un commento di testo facoltativo per l'istruzione del criterio bucket del server archivio oggetti.

### Esempi

```
cluster1::> vservers object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* -sid "FullAccessForUser1"

cluster1::> vservers object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

## Informazioni sul copyright

Copyright © 2024 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.