



Usa il blocco oggetto S3

StorageGRID software

NetApp
July 23, 2026

Sommario

- Usa il blocco oggetto S3. 1
 - Come S3 Object Lock protegge gli oggetti in StorageGRID 1
 - Che cos'è S3 Object Lock? 1
 - Confronto tra S3 Object Lock e la Compliance legacy 2
 - Flusso di lavoro S3 Object Lock in StorageGRID 4
 - Requisiti di S3 Object Lock in StorageGRID 5
 - Requisiti per l'utilizzo dell'impostazione globale S3 Object Lock. 5
 - Requisiti per le regole ILM conformi 5
 - Requisiti per le policy ILM 5
 - Requisiti per i bucket con S3 Object Lock abilitato 6
 - Requisiti per gli oggetti nei bucket con S3 Object Lock abilitato 6
 - Ciclo di vita degli oggetti nei bucket con S3 Object Lock abilitato 6
 - Abilita S3 Object Lock a livello globale in StorageGRID 7
 - Risolvi gli errori di coerenza durante l'aggiornamento delle impostazioni di S3 Object Lock o di Compliance legacy in StorageGRID 8

Usa il blocco oggetto S3

Come S3 Object Lock protegge gli oggetti in StorageGRID

Come amministratore della griglia, puoi abilitare S3 Object Lock per il tuo sistema StorageGRID e implementare una policy ILM conforme per assicurarti che gli oggetti in specifici bucket S3 non vengano eliminati o sovrascritti per un periodo di tempo specificato.

Che cos'è S3 Object Lock?

La funzionalità StorageGRID S3 Object Lock è una soluzione di protezione degli oggetti equivalente a S3 Object Lock in Amazon Simple Storage Service (Amazon S3).

Quando l'impostazione globale S3 Object Lock è abilitata per un sistema StorageGRID, un tenant account S3 può creare bucket con o senza S3 Object Lock abilitato. Se un bucket ha S3 Object Lock abilitato, il versioning del bucket è obbligatorio e viene abilitato automaticamente.

Un bucket senza S3 Object Lock può contenere solo oggetti per i quali non sono specificate impostazioni di conservazione. Nessun oggetto ingerito avrà impostazioni di conservazione.

Un bucket con S3 Object Lock può contenere oggetti con o senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con S3 Object Lock e periodo di conservazione predefinito configurato può avere oggetti caricati con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, perché l'impostazione di conservazione non è stata configurata a livello di oggetto.

In pratica, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurato il periodo di conservazione predefinito. Gli oggetti esistenti senza impostazioni di conservazione rimangono invariati.

Modalità di retention

La funzionalità S3 Object Lock di StorageGRID supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità sono equivalenti alle modalità di conservazione di Amazon S3.

- In modalità conformità:
 - L'oggetto non può essere eliminato fino al raggiungimento della sua retain-until-date.
 - La data di conservazione dell'oggetto può essere aumentata, ma non può essere diminuita.
 - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità governance:
 - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare determinate impostazioni di conservazione.
 - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione prevista.
 - Questi utenti possono aumentare, diminuire o rimuovere la retain-until-date di un oggetto.

Impostazioni di conservazione per le versioni degli oggetti

Se crei un bucket con la funzionalità S3 Object Lock abilitata, puoi usare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ogni oggetto aggiunto al bucket:

- **Modalità di conservazione:** conformità o governance.
- **Retain-until-date:** Se la retain-until-date di una versione dell'oggetto è nel futuro, l'oggetto può essere recuperato, ma non può essere eliminato.
- **Blocco legale:** L'applicazione di un blocco legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potresti dover applicare un blocco legale a un oggetto che è collegato a un'indagine o a una controversia legale. Un blocco legale non ha una data di scadenza, ma rimane in vigore finché non viene esplicitamente rimosso. I blocchi legali sono indipendenti dalla retain-until-date.



Se un oggetto è soggetto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla sua modalità di conservazione.

Per i dettagli sulle impostazioni dell'oggetto, vedi ["Utilizza l'API REST S3 per configurare S3 Object Lock"](#).

Impostazione di conservazione predefinita per i bucket

Se crei un bucket con S3 Object Lock abilitato, puoi facoltativamente specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita:** conformità o governance.
- **Periodo di conservazione predefinito:** per quanto tempo le nuove versioni degli oggetti aggiunte a questo bucket devono essere conservate, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non hanno le proprie impostazioni di conservazione. Gli oggetti esistenti nel bucket non vengono influenzati quando aggiungi o modifichi queste impostazioni predefinite.

Vedi ["Crea un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco oggetto S3"](#).

Confronto tra S3 Object Lock e la Compliance legacy

La funzionalità S3 Object Lock sostituisce la funzionalità Compliance che era disponibile nelle versioni precedenti di StorageGRID. Poiché la funzionalità S3 Object Lock è conforme ai requisiti di Amazon S3, depreca la funzionalità proprietaria Compliance di StorageGRID, che ora viene chiamata "legacy Compliance".



L'impostazione globale di conformità è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione S3 Object Lock viene abilitata automaticamente. Puoi continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non puoi creare nuovi bucket conformi. Per dettagli, vedi ["NetApp Knowledge Base: Come gestire i bucket Compliant legacy in StorageGRID 11.5"](#).

Se hai utilizzato la funzione Compliance legacy in una versione precedente di StorageGRID, consulta la tabella seguente per scoprire come si confronta con la funzionalità S3 Object Lock in StorageGRID.

	Blocco oggetto S3	Conformità (legacy)
Come abiliti questa funzionalità a livello globale?	Dal Grid Manager, seleziona Configurazione > Sistema > S3 Object Lock .	Non più supportata.
Come abiliti questa funzionalità per un bucket?	Devi abilitare S3 Object Lock quando crei un nuovo bucket utilizzando il Tenant Manager, l'API di gestione del tenant o l'API REST S3.	Non più supportata.
È supportata la gestione delle versioni dei bucket?	Sì. Il versioning del bucket è obbligatorio e viene abilitato automaticamente quando S3 Object Lock è abilitato per il bucket.	No.
Come imposti la conservazione degli oggetti?	Gli utenti possono impostare una data di conservazione per ogni versione dell'oggetto, oppure possono impostare un periodo di conservazione predefinito per ogni bucket.	Devi impostare un periodo di conservazione per l'intero bucket. Il periodo di conservazione si applica a tutti gli oggetti nel bucket.
È possibile modificare il periodo di conservazione?	• In modalità conformità, la retain-until-date per una versione di un oggetto può essere aumentata, ma mai diminuita. • In modalità governance, gli utenti con autorizzazioni speciali possono ridurre o persino rimuovere le impostazioni di conservazione di un oggetto.	Il periodo di conservazione di un bucket può essere aumentato, ma mai diminuito.
Dove si controlla il legal hold?	Puoi applicare o rimuovere un blocco legale per qualsiasi versione dell'oggetto nel bucket.	Un sequestro legale viene applicato al bucket e riguarda tutti gli oggetti nel bucket.

	Blocco oggetto S3	Conformità (legacy)
Quando puoi eliminare gli oggetti?	• In modalità conformità, una versione di un oggetto può essere eliminata dopo il raggiungimento della retain-until-date, a condizione che l'oggetto non sia soggetto a legal hold. • In modalità governance, gli utenti con autorizzazioni speciali possono eliminare un oggetto prima che venga raggiunta la sua retain-until-date, a condizione che l'oggetto non sia soggetto a legal hold.	Un oggetto può essere eliminato dopo la scadenza del periodo di conservazione, a condizione che il bucket non sia soggetto a blocco legale. Gli oggetti possono essere eliminati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	Sì	No

Flusso di lavoro S3 Object Lock in StorageGRID

Come amministratore della griglia, devi coordinarti strettamente con gli utenti tenant per assicurarti che gli oggetti siano protetti in modo da soddisfare i loro requisiti di conservazione.



L'applicazione delle impostazioni del tenant all'intera griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato dei nodi e delle operazioni di Cassandra.

I seguenti elenchi per gli amministratori della griglia e gli utenti tenant contengono le high-level attività per l'utilizzo della funzionalità S3 Object Lock.

Amministratore della grid

- Abilita l'impostazione globale di S3 Object Lock per l'intero sistema StorageGRID.
- Assicurati che le policy di information lifecycle management (ILM) siano *conformi*; cioè che soddisfino i ["requisiti dei bucket con S3 Object Lock abilitato"](#).
- Se necessario, consenti a un tenant di utilizzare Compliance come modalità di conservazione. Altrimenti, è consentita solo la modalità Governance.
- Se necessario, imposta un periodo massimo di conservazione per un tenant.

Utente tenant

- Esamina le considerazioni relative a bucket e oggetti con S3 Object Lock.
- Se necessario, contatta l'amministratore della grid per abilitare l'impostazione globale S3 Object Lock e impostare le autorizzazioni.
- Crea bucket con S3 Object Lock abilitato.
- Facoltativamente, puoi configurare le impostazioni di conservazione predefinite per un bucket:
 - Modalità di conservazione predefinita: Governance o Compliance, se consentita dall'amministratore

della grid.

- Periodo di conservazione predefinito: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall'amministratore della griglia.
- Utilizza l'applicazione client S3 per aggiungere oggetti e, facoltativamente, impostare la conservazione specifica per ciascun oggetto:
 - Modalità di conservazione. Governance o Compliance, se consentito dall'amministratore del grid.
 - Data di conservazione: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall'amministratore della griglia.

Requisiti di S3 Object Lock in StorageGRID

Devi esaminare i requisiti per abilitare l'impostazione globale S3 Object Lock, i requisiti per creare regole e policy ILM conformi e le restrizioni che StorageGRID impone ai bucket e agli oggetti che utilizzano S3 Object Lock.

Requisiti per l'utilizzo dell'impostazione globale S3 Object Lock

- Devi abilitare l'impostazione globale S3 Object Lock usando il Grid Manager o la Grid Management API prima che qualsiasi tenant possa creare un bucket con S3 Object Lock abilitato.
- L'attivazione dell'impostazione globale S3 Object Lock permette a tutti gli account tenant S3 di creare bucket con S3 Object Lock abilitato.
- Dopo che hai attivato l'impostazione globale S3 Object Lock, non puoi disattivarla.
- Non puoi abilitare il blocco globale degli oggetti S3 a meno che la regola predefinita in tutte le policy ILM attive non sia *conforme* (cioè, la regola predefinita deve essere conforme ai requisiti dei bucket con S3 Object Lock abilitato).
- Quando l'impostazione globale S3 Object Lock è abilitata, non puoi creare una nuova policy ILM o attivare una policy ILM esistente a meno che la regola predefinita nella policy sia conforme. Dopo che l'impostazione globale S3 Object Lock è stata abilitata, le pagine delle regole ILM e delle policy ILM indicano quali regole ILM sono conformi.

Requisiti per le regole ILM conformi

Se vuoi abilitare l'impostazione globale S3 Object Lock, devi assicurarti che la regola predefinita in tutte le policy ILM attive sia conforme. Una regola conforme soddisfa i requisiti sia dei bucket con S3 Object Lock abilitato sia di tutti i bucket esistenti che hanno la Compliance legacy abilitata:

- Devi creare almeno due copie replicate dell'oggetto o una copia con codifica di cancellazione.
- Queste copie devono esistere sui nodi di archiviazione per tutta la durata di ogni riga delle istruzioni di posizionamento.
- Non puoi salvare copie di oggetti in un Cloud Storage Pool.
- Almeno una riga delle istruzioni di posizionamento deve iniziare dal giorno 0, utilizzando **Ingest time** come orario di riferimento.
- Almeno una riga delle istruzioni per il posizionamento deve essere "per sempre".

Requisiti per le policy ILM

Quando l'impostazione globale di S3 Object Lock è abilitata, le policy ILM attive e inattive possono includere

sia regole conformi che non conformi.

- La regola predefinita in una policy ILM attiva o inattiva deve essere conforme.
- Le regole di non conformità si applicano solo agli oggetti nei bucket che non hanno il blocco degli oggetti S3 abilitato o che non hanno la funzionalità di conformità legacy abilitata.
- Le regole di conformità possono essere applicate agli oggetti in qualsiasi bucket; non è necessario abilitare S3 Object Lock o legacy Compliance per il bucket.

["Esempio di una policy ILM conforme per S3 Object Lock"](#)

Requisiti per i bucket con S3 Object Lock abilitato

- Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID, puoi usare il Tenant Manager, la Tenant Management API o la S3 REST API per creare bucket con S3 Object Lock abilitato.
- Se intendi utilizzare S3 Object Lock, devi abilitarlo quando crei il bucket. Non puoi abilitare S3 Object Lock per un bucket esistente.
- Quando il blocco degli oggetti S3 è abilitato per un bucket, StorageGRID abilita automaticamente il versioning per quel bucket. Non puoi disabilitare il blocco degli oggetti S3 o sospendere il versioning per il bucket.
- Facoltativamente, puoi specificare una modalità di conservazione predefinita e un periodo di conservazione per ogni bucket utilizzando il Tenant Manager, la Tenant Management API o la S3 REST API. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non hanno proprie impostazioni di conservazione. Puoi ignorare queste impostazioni predefinite specificando una modalità di conservazione e una retain-until-date per ogni versione dell'oggetto quando viene caricata.
- La configurazione del ciclo di vita dei bucket è supportata per i bucket con S3 Object Lock abilitato.
- CloudMirror replication non è supportata per i bucket con S3 Object Lock abilitato.

Requisiti per gli oggetti nei bucket con S3 Object Lock abilitato

- Per proteggere una versione di un oggetto, puoi specificare le impostazioni di conservazione predefinite per il bucket oppure puoi specificare le impostazioni di conservazione per ogni versione dell'oggetto. Le impostazioni di conservazione a livello di oggetto possono essere specificate usando l'applicazione client S3 o l'S3 REST API.
- Le impostazioni di conservazione si applicano alle singole versioni degli oggetti. Una versione di un oggetto può avere sia una data di conservazione che un'impostazione di legal hold, una sola delle due oppure nessuna delle due. Specificare una data di conservazione o un'impostazione di legal hold per un oggetto protegge solo la versione specificata nella richiesta. Puoi creare nuove versioni dell'oggetto, mentre la versione precedente dell'oggetto rimane bloccata.

Ciclo di vita degli oggetti nei bucket con S3 Object Lock abilitato

Ogni oggetto salvato in un bucket con S3 Object Lock abilitato attraversa queste fasi:

1. Ingestione oggetto

Quando una versione di un oggetto viene aggiunta a un bucket che ha S3 Object Lock abilitato, le impostazioni di conservazione vengono applicate come segue:

- Se per l'oggetto sono specificate delle impostazioni di conservazione, vengono applicate le

impostazioni a livello di oggetto. Le impostazioni predefinite del bucket vengono ignorate.

- Se non vengono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se esistono.
- Se non vengono specificate impostazioni di conservazione per l'oggetto o il bucket, l'oggetto non è protetto da S3 Object Lock.

Se vengono applicate le impostazioni di conservazione, sia l'oggetto che tutti i metadati S3 definiti dall'utente sono protetti.

2. Conservazione ed eliminazione degli oggetti

StorageGRID memorizza più copie di ciascun oggetto protetto per il periodo di conservazione specificato. Il numero e il tipo esatti di copie degli oggetti e le posizioni di archiviazione sono determinati dalle regole conformi nelle policy ILM attive. Se un oggetto protetto può essere eliminato prima che venga raggiunta la sua retain-until-date dipende dalla sua modalità di conservazione.

- Se un oggetto è soggetto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla sua modalità di conservazione.

Informazioni correlate

- ["Crea un bucket S3"](#)
- ["Aggiorna la conservazione predefinita del blocco oggetto S3"](#)
- ["Utilizza l'API REST S3 per configurare S3 Object Lock"](#)
- ["Esempio 7: Criterio ILM conforme per S3 Object Lock"](#)

Abilita S3 Object Lock a livello globale in StorageGRID

Se un tenant S3 deve rispettare i requisiti normativi durante il salvataggio dei dati degli oggetti, devi abilitare S3 Object Lock per l'intero sistema StorageGRID. Abilitando l'impostazione globale S3 Object Lock, qualsiasi utente tenant S3 può creare e gestire bucket e oggetti con S3 Object Lock.

Prima di iniziare

- Hai ["Permesso di accesso root"](#).
- Sei connesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai esaminato il flusso di lavoro S3 Object Lock e ne comprendi le considerazioni.
- Hai confermato che la regola predefinita nella policy ILM attiva è conforme. Consulta ["Crea una regola ILM predefinita"](#) per i dettagli.

Informazioni su questa attività

Un amministratore della griglia deve abilitare l'impostazione globale Blocco oggetti S3 per consentire agli utenti del tenant di creare nuovi bucket con Blocco oggetti S3 abilitato. Una volta abilitata, questa impostazione non può essere disabilitata.

Rivedi le impostazioni di conformità dei tenant esistenti dopo aver abilitato l'impostazione globale S3 Object Lock. Quando abiliti questa impostazione, le impostazioni di S3 Object Lock per singolo tenant dipendono dalla versione di StorageGRID in vigore al momento della creazione del tenant.



L'impostazione globale di conformità è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione S3 Object Lock viene abilitata automaticamente. Puoi continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non puoi creare nuovi bucket conformi. Per dettagli, vedi ["NetApp Knowledge Base: Come gestire i bucket Compliant legacy in StorageGRID 11.5"](#).

Passaggi

1. Seleziona **Configurazione > Sistema > S3 Object Lock**.

Viene visualizzata la pagina delle impostazioni di blocco degli oggetti S3.

2. Seleziona **Abilita S3 Object Lock**.
3. Seleziona **Applica**.

Viene visualizzata una finestra di dialogo di conferma che ti ricorda che non puoi disabilitare S3 Object Lock dopo che è stato abilitato.

4. Se sei sicuro di voler abilitare in modo permanente S3 Object Lock per l'intero sistema, seleziona **OK**.

Quando selezioni **OK**:

- Se la regola predefinita nella policy ILM attiva è conforme, S3 Object Lock è ora abilitato per l'intera griglia e non può essere disabilitato.
- Se la regola predefinita non è conforme, viene visualizzato un errore. Devi creare e attivare una nuova policy ILM che includa una regola conforme come regola predefinita. Seleziona **OK**. Poi crea una nuova policy, simulala e attivala. Vedi ["Crea criteri ILM"](#) per le istruzioni.

Risolvi gli errori di coerenza durante l'aggiornamento delle impostazioni di S3 Object Lock o di Compliance legacy in StorageGRID

Se un sito del data center o più Storage Node in un sito diventano non disponibili, potresti dover aiutare gli utenti tenant S3 ad applicare modifiche alla configurazione di S3 Object Lock o di Compliance legacy.

Gli utenti tenant che dispongono di bucket con S3 Object Lock (o Compliance legacy) abilitato possono modificare determinate impostazioni. Ad esempio, un utente tenant che utilizza S3 Object Lock potrebbe dover mettere una versione di un oggetto sotto blocco legale.

Quando un utente tenant aggiorna le impostazioni di un bucket S3 o di una versione di oggetto, StorageGRID tenta di aggiornare immediatamente i metadati del bucket o dell'oggetto in tutta la grid. Se il sistema non riesce ad aggiornare i metadati perché un sito del data center o più Storage Node non sono disponibili, restituisce un errore:

```
503: Service Unavailable
```

```
Unable to update compliance settings because the settings can't be  
consistently applied on enough storage services. Contact your grid  
administrator for assistance.
```

Per risolvere questo errore, segui questi passaggi:

1. Cerca di rendere nuovamente disponibili tutti i nodi di Storage o i siti il prima possibile.
2. Se non riesci a rendere disponibili un numero sufficiente di Storage Node in ciascun sito, contatta il supporto tecnico, che può aiutarti a recuperare i nodi e a garantire che le modifiche vengano applicate in modo coerente su tutta la grid.
3. Una volta risolto il problema di fondo, ricorda all'utente del tenant di riprovare a modificare la configurazione.

Informazioni correlate

- ["Usa un tenant account"](#)
- ["\\${post_edited_translations.segment}"](#)
- ["Recupera e mantieni"](#)

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.