Pianificare la configurazione del motore esterno FPolicy

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap/nas-audit/plan-fpolicy-external-engine-config-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Sommario

Pianificare la configurazione del motore esterno FPolicy . . . 1
Configurazioni del motore esterno Plan ONTAP FPolicy . . . 1
Informazioni definite durante la creazione del motore esterno FPolicy . . . 1
Quali sono i parametri esterni di base del motore . . . 2
Quali sono le opzioni avanzate dei motori esterni . . . 5
Ulteriori informazioni sulla configurazione dei motori esterni ONTAP FPolicy per utilizzare connessioni autenticate SSL . . . 8
Autenticazione del server SSL . . . 8
Autenticazione reciproca . . . 8
Installare i certificati per SSL . . . 8
I certificati ONTAP FPolicy non vengono replicati nelle relazioni di ripristino di emergenza SVM con una configurazione senza conservazione dell'ID . . . 8
Limitazioni per i motori esterni ONTAP FPolicy con ambito cluster con configurazioni di disaster recovery MetroCluster e SVM . . . 9
Fogli di lavoro completi per la configurazione del motore esterno ONTAP FPolicy . . . 9
Informazioni per una configurazione di base del motore esterno . . . 10
Informazioni sui parametri esterni avanzati del motore . . . 10

Pianificare la configurazione del motore esterno FPolicy

Configurazioni del motore esterno Plan ONTAP FPolicy

Prima di configurare il motore esterno FPolicy, è necessario comprendere cosa significa creare un motore esterno e quali parametri di configurazione sono disponibili. Queste informazioni consentono di determinare i valori da impostare per ciascun parametro.

Informazioni definite durante la creazione del motore esterno FPolicy

La configurazione del motore esterno definisce le informazioni necessarie a FPolicy per creare e gestire le connessioni ai server FPolicy esterni, tra cui:

- Nome SVM
- Nome del motore
- Gli indirizzi IP dei server FPolicy primario e secondario e il numero di porta TCP da utilizzare per la connessione ai server FPolicy
- Se il tipo di motore è asincrono o sincrono
- Se il formato del motore è `xml` oppure `protobuf`

  A partire da ONTAP 9.15.1, è possibile utilizzare `protobuf` formato motore. Quando è impostato su `protobuf`, I messaggi di notifica sono codificati in forma binaria utilizzando Google Protobuf. Prima di impostare il formato del motore su `protobuf`, Verificare che anche il server FPolicy supporti `protobuf` deserializzazione.

  Poiché il formato protobuf è supportato a partire da ONTAP 9.15.1, è necessario considerare il formato del motore esterno prima di tornare a una versione precedente di ONTAP. Se si torna a una versione precedente rispetto a ONTAP 9.15.1, collaborare con il partner FPolicy per:

  - Modificare ogni formato del motore da `protobuf` a. `xml`
  - Eliminare i motori con un formato motore di `protobuf`
- Come autenticare la connessione tra il nodo e il server FPolicy

  Se si sceglie di configurare l'autenticazione SSL reciproca, è necessario configurare anche i parametri che forniscono le informazioni del certificato SSL.
- Come gestire la connessione utilizzando diverse impostazioni avanzate dei privilegi

  Sono inclusi parametri che definiscono valori di timeout, valori di tentativi, valori di mantenimento, valori di richiesta massimi, valori di dimensione buffer inviati e ricevuti e valori di timeout della sessione.

Il `vserver fpolicy policy external-engine create` Il comando viene utilizzato per creare un motore esterno FPolicy.

Quali sono i parametri esterni di base del motore

È possibile utilizzare la seguente tabella dei parametri di configurazione di base di FPolicy per pianificare la configurazione:

Tipo di informazione	Opzione
SVM Specifica il nome SVM che si desidera associare a questo motore esterno. Ogni configurazione FPolicy viene definita all'interno di una singola SVM. Il motore esterno, l'evento del criterio, l'ambito del criterio e il criterio che si combinano insieme per creare una configurazione del criterio FPolicy devono essere tutti associati alla stessa SVM.	`-vserver vserver_name`
Nome motore Specifica il nome da assegnare alla configurazione esterna del motore. È necessario specificare il nome del motore esterno in un secondo momento quando si crea il criterio FPolicy. In questo modo, il motore esterno viene associato alla policy. Il nome può contenere fino a 256 caratteri. Se si configura il nome del motore esterno in una configurazione di disaster recovery MetroCluster o SVM, il nome deve essere composto da un massimo di 200 caratteri. Il nome può contenere qualsiasi combinazione dei seguenti caratteri ASCII: • `a` attraverso `z` • `A` attraverso `Z` • `0` attraverso `9` • "_", "-", and "``"	`-engine-name engine_name`

Server FPolicy primari Specifica i server FPolicy primari a cui il nodo invia le notifiche per un dato criterio FPolicy. Il valore viene specificato come elenco di indirizzi IP delimitato da virgole. Se viene specificato più di un indirizzo IP del server primario, ogni nodo a cui partecipa SVM crea una connessione di controllo a ogni server FPolicy primario specificato al momento dell'attivazione del criterio. Se si configurano più server FPolicy primari, le notifiche vengono inviate ai server FPolicy in modo round-robin. Se il motore esterno viene utilizzato in una configurazione di disaster recovery MetroCluster o SVM, è necessario specificare gli indirizzi IP dei server FPolicy nel sito di origine come server primari. Gli indirizzi IP dei server FPolicy nel sito di destinazione devono essere specificati come server secondari.	`-primary-servers IP_address,...`
Numero porta Specifica il numero di porta del servizio FPolicy.	`-port integer`
Server FPolicy secondari Specifica i server FPolicy secondari a cui inviare gli eventi di accesso ai file per un determinato criterio FPolicy. Il valore viene specificato come elenco di indirizzi IP delimitato da virgole. I server secondari vengono utilizzati solo quando nessuno dei server primari è raggiungibile. Le connessioni ai server secondari vengono stabilite quando il criterio è attivato, ma le notifiche vengono inviate ai server secondari solo se nessuno dei server primari è raggiungibile. Se si configurano più server secondari, le notifiche vengono inviate ai server FPolicy in modo round-robin.	`-secondary-servers IP_address,...`
Tipo di motore esterno Specifica se il motore esterno funziona in modalità sincrona o asincrona. Per impostazione predefinita, FPolicy opera in modalità sincrona. Quando è impostato su `synchronous`, L'elaborazione della richiesta di file invia una notifica al server FPolicy, ma non continua fino a quando non riceve una risposta dal server FPolicy. A questo punto, il flusso della richiesta continua o l'elaborazione comporta un rifiuto, a seconda che la risposta dal server FPolicy consenta l'azione richiesta. Quando è impostato su `asynchronous`, L'elaborazione della richiesta di file invia una notifica al server FPolicy, quindi continua.	`-extern-engine-type external_engine_type` Il valore di questo parametro può essere uno dei seguenti: • `synchronous` • `asynchronous`

Formato motore esterno Specificare se il formato del motore esterno è xml o protobuf. A partire da ONTAP 9.15.1, è possibile utilizzare il formato del motore protobuf. Quando è impostato su protobuf, i messaggi di notifica vengono codificati in formato binario utilizzando Google Protobuf. Prima di impostare il formato del motore su protobuf, verificare che il server FPolicy supporti anche la deserializzazione di protobuf.	`- extern-engine-format` {`protobuf` oppure `xml`}

Opzione SSL per la comunicazione con il server FPolicy
 	
Specifica l'opzione SSL per la comunicazione con il server FPolicy. Questo è un parametro obbligatorio. È possibile scegliere una delle opzioni in base alle seguenti informazioni:
 	
• Quando è impostato su `no-auth`, non viene eseguita alcuna autenticazione.
 	
Il collegamento di comunicazione viene stabilito tramite TCP.
 	
• Quando è impostato su `server-auth`, SVM autentica il server FPolicy utilizzando l'autenticazione del server SSL.
• Quando è impostato su `mutual-auth`, L'autenticazione reciproca avviene tra SVM e il server FPolicy; SVM autentica il server FPolicy e il server FPolicy autentica SVM.
 	
Se si sceglie di configurare l'autenticazione SSL reciproca, è necessario configurare anche `-certificate-common-name`, `-certificate -serial`, e. `-certifcate-ca` parametri.
	`-ssl-option` {`no-auth`
	
	`server-auth`
	
	`mutual-auth`}

FQDN certificato o nome comune personalizzato Specifica il nome del certificato utilizzato se è configurata l'autenticazione SSL tra SVM e il server FPolicy. È possibile specificare il nome del certificato come FQDN o come nome comune personalizzato. Se si specifica `mutual-auth` per `-ssl-option` specificare un valore per `-certificate-common-name` parametro.	`-certificate-common -name` `text`
Numero di serie del certificato Specifica il numero di serie del certificato utilizzato per l'autenticazione se è configurata l'autenticazione SSL tra SVM e il server FPolicy. Se si specifica `mutual-auth` per `-ssl-option` specificare un valore per `-certificate-serial` parametro.	`-certificate-serial` `text`

Autorità di certificazione Specifica il nome della CA del certificato utilizzato per l'autenticazione se è configurata l'autenticazione SSL tra SVM e il server FPolicy. Se si specifica `mutual-auth` per `-ssl-option` specificare un valore per `-certificate-ca` parametro.	`-certificate-ca text`

Quali sono le opzioni avanzate dei motori esterni

È possibile utilizzare la seguente tabella di parametri di configurazione FPolicy avanzati quando si prevede di personalizzare la configurazione con parametri avanzati. Questi parametri vengono utilizzati per modificare il comportamento delle comunicazioni tra i nodi del cluster e i server FPolicy:

Tipo di informazione	Opzione
Timeout per l'annullamento di una richiesta Specifica l'intervallo di tempo in ore (`h`), minuti (`m`), o secondi (`s`) Che il nodo attende una risposta dal server FPolicy. Se l'intervallo di timeout viene superato, il nodo invia una richiesta di annullamento al server FPolicy. Il nodo invia quindi la notifica a un server FPolicy alternativo. Questo timeout consente di gestire un server FPolicy che non risponde, migliorando la risposta del client SMB/NFS. Inoltre, l'annullamento delle richieste dopo un periodo di timeout può aiutare a rilasciare le risorse di sistema perché la richiesta di notifica viene spostata da un server FPolicy inattivo/non funzionante a un server FPolicy alternativo. L'intervallo per questo valore è `0` attraverso `100`. Se il valore è impostato su `0`, L'opzione è disattivata e i messaggi di richiesta di annullamento non vengono inviati al server FPolicy. L'impostazione predefinita è `20s`.	`-reqs-cancel-timeout integer`[h
m	s]
Timeout per l'interruzione di una richiesta Specifica il timeout in ore (`h`), minuti (`m`), o secondi (`s`) per interrompere una richiesta. L'intervallo per questo valore è `0` attraverso `200`.	`-reqs-abort-timeout ` `integer`[h
m	s]

Intervallo per l'invio delle richieste di stato Specifica l'intervallo in ore (`h`), minuti (`m`), o secondi (`s`) Dopo di che viene inviata una richiesta di stato al server FPolicy. L'intervallo per questo valore è `0` attraverso `50`. Se il valore è impostato su `0`, L'opzione è disattivata e i messaggi di richiesta di stato non vengono inviati al server FPolicy. L'impostazione predefinita è `10s`.	`-status-req-interval integer`[h
m	s]
Numero massimo di richieste in sospeso sul server FPolicy Specifica il numero massimo di richieste in sospeso che è possibile mettere in coda sul server FPolicy. L'intervallo per questo valore è `1` attraverso `10000`. L'impostazione predefinita è `500`.	`-max-server-reqs integer`
Timeout per la disconnessione di un server FPolicy che non risponde Specifica l'intervallo di tempo in ore (`h`), minuti (`m`), o secondi (`s`) Dopo di che la connessione al server FPolicy viene interrotta. La connessione viene interrotta dopo il periodo di timeout solo se la coda del server FPolicy contiene il numero massimo consentito di richieste e non viene ricevuta alcuna risposta entro il periodo di timeout. Il numero massimo consentito di richieste è `50` (impostazione predefinita) o il numero specificato da `max-server-reqs-` parametro. L'intervallo per questo valore è `1` attraverso `100`. L'impostazione predefinita è `60s`.	`-server-progress -timeout integer`[h
m	s]
Intervallo per l'invio di messaggi keep-alive al server FPolicy Specifica l'intervallo di tempo in ore (`h`), minuti (`m`), o secondi (`s`) In cui i messaggi keep-alive vengono inviati al server FPolicy. I messaggi keep-alive rilevano connessioni half-open. L'intervallo per questo valore è `10` attraverso `600`. Se il valore è impostato su `0`, L'opzione è disattivata e non è possibile inviare messaggi keep-alive ai server FPolicy. L'impostazione predefinita è `120s`.	`-keep-alive-interval-integer`[h
m	s]

Numero massimo di tentativi di riconnessione Specifica il numero massimo di tentativi di riconnessione da parte di SVM al server FPolicy dopo l'interruzione della connessione. L'intervallo per questo valore è `0` attraverso `20`. L'impostazione predefinita è `5`.	`-max-connection-retries integer`
Dimensione buffer di ricezione Specifica la dimensione del buffer di ricezione del socket connesso per il server FPolicy. Il valore predefinito è 256 kilobyte (Kb). Quando il valore è impostato su 0, la dimensione del buffer di ricezione viene impostata su un valore definito dal sistema. Ad esempio, se la dimensione predefinita del buffer di ricezione del socket è 65536 byte, impostando il valore sintonizzabile su 0, la dimensione del buffer del socket viene impostata su 65536 byte. È possibile utilizzare qualsiasi valore non predefinito per impostare la dimensione (in byte) del buffer di ricezione.	`-recv-buffer-size integer`
Invia dimensione buffer Specifica la dimensione del buffer di invio del socket connesso per il server FPolicy. Il valore predefinito è 256 kilobyte (Kb). Quando il valore è impostato su 0, la dimensione del buffer di invio viene impostata su un valore definito dal sistema. Ad esempio, se la dimensione predefinita del buffer di invio del socket è impostata su 65536 byte, impostando il valore sintonizzabile su 0, la dimensione del buffer del socket viene impostata su 65536 byte. È possibile utilizzare qualsiasi valore non predefinito per impostare la dimensione (in byte) del buffer di invio.	`-send-buffer-size integer`
Timeout per l'eliminazione di un ID sessione durante la riconnessione Specifica l'intervallo in ore (`h`), minuti (`m`), o secondi (`s`) Dopo di che viene inviato un nuovo ID di sessione al server FPolicy durante i tentativi di riconnessione. Se la connessione tra il controller di storage e il server FPolicy viene interrotta e la riconnessione viene effettuata all'interno di `-session -timeout` Intervallo, il vecchio ID sessione viene inviato al server FPolicy in modo che possa inviare le risposte per le vecchie notifiche. Il valore predefinito è impostato su 10 secondi.	`-session-timeout [.integerh][integerm][integers]`

Ulteriori informazioni sulla configurazione dei motori esterni ONTAP FPolicy per utilizzare connessioni autenticate SSL

Per configurare il motore esterno FPolicy in modo che utilizzi SSL durante la connessione ai server FPolicy, è necessario conoscere alcune informazioni aggiuntive.

Autenticazione del server SSL

Se si sceglie di configurare il motore esterno FPolicy per l'autenticazione del server SSL, prima di creare il motore esterno, è necessario installare il certificato pubblico dell'autorità di certificazione (CA) che ha firmato il certificato del server FPolicy.

Autenticazione reciproca

Se si configurano i motori esterni di FPolicy in modo che utilizzino l'autenticazione reciproca SSL quando si collegano i LIF dei dati delle macchine virtuali di storage (SVM) ai server FPolicy esterni, prima di creare il motore esterno, È necessario installare il certificato pubblico della CA che ha firmato il certificato del server FPolicy insieme al certificato pubblico e al file delle chiavi per l'autenticazione della SVM. Non eliminare questo certificato mentre i criteri FPolicy utilizzano il certificato installato.

Se il certificato viene eliminato mentre FPolicy lo utilizza per l'autenticazione reciproca durante la connessione a un server FPolicy esterno, non è possibile riabilitare un criterio FPolicy disattivato che utilizza tale certificato. Non è possibile riabilitare il criterio FPolicy in questa situazione anche se viene creato e installato un nuovo certificato con le stesse impostazioni sulla SVM.

Se il certificato è stato eliminato, è necessario installare un nuovo certificato, creare nuovi motori esterni FPolicy che utilizzano il nuovo certificato e associare i nuovi motori esterni al criterio FPolicy che si desidera riabilitare modificando il criterio FPolicy.

Installare i certificati per SSL

Il certificato pubblico della CA utilizzato per firmare il certificato del server FPolicy viene installato utilizzando `security certificate install` con il `-type` parametro impostato su `client-ca`. La chiave privata e il certificato pubblico richiesti per l'autenticazione della SVM vengono installati utilizzando `security certificate install` con il `-type` parametro impostato su `server`.

Informazioni correlate

- "installazione del certificato di sicurezza"

I certificati ONTAP FPolicy non vengono replicati nelle relazioni di ripristino di emergenza SVM con una configurazione senza conservazione dell'ID

I certificati di sicurezza utilizzati per l'autenticazione SSL durante le connessioni ai server FPolicy non replicano nelle destinazioni di disaster recovery SVM con configurazioni non ID-preserve. Sebbene la configurazione del motore esterno FPolicy sulla SVM sia replicata, i certificati di sicurezza non vengono replicati. È necessario installare manualmente i certificati di protezione sulla destinazione.

Quando si imposta la relazione di disaster recovery SVM, il valore selezionato per `-identity-preserve` opzione di `snapmirror create` Determina i dettagli di configurazione replicati nella SVM di destinazione.

Se si imposta `-identity-preserve` opzione a. `true` (ID-Preserve), vengono replicati tutti i dettagli di configurazione di FPolicy, incluse le informazioni del certificato di sicurezza. È necessario installare i certificati di protezione sulla destinazione solo se si imposta l'opzione su `false` (Non-ID-Preserve).

Informazioni correlate

- "creazione di snapmirror"

Limitazioni per i motori esterni ONTAP FPolicy con ambito cluster con configurazioni di disaster recovery MetroCluster e SVM

È possibile creare un motore esterno FPolicy con ambito cluster assegnando la SVM (Cluster Storage Virtual Machine) al motore esterno. Tuttavia, quando si crea un motore esterno con ambito cluster in una configurazione di disaster recovery MetroCluster o SVM, esistono alcune restrizioni quando si sceglie il metodo di autenticazione utilizzato da SVM per la comunicazione esterna con il server FPolicy.

Quando si creano server FPolicy esterni, è possibile scegliere tre opzioni di autenticazione: Nessuna autenticazione, autenticazione del server SSL e autenticazione reciproca SSL. Sebbene non vi siano restrizioni quando si sceglie l'opzione di autenticazione se il server FPolicy esterno è assegnato a una SVM di dati, esistono restrizioni quando si crea un motore esterno FPolicy con ambito cluster:

Configurazione	Consentito?
Disaster recovery MetroCluster o SVM e motore esterno FPolicy con ambito cluster senza autenticazione (SSL non configurato)	Sì
Disaster recovery MetroCluster o SVM e motore esterno FPolicy con ambito cluster con server SSL o autenticazione reciproca SSL	No

- Se esiste un motore esterno FPolicy con ambito cluster con autenticazione SSL e si desidera creare una configurazione di disaster recovery MetroCluster o SVM, è necessario modificare questo motore esterno in modo che non utilizzi alcuna autenticazione o rimuovere il motore esterno prima di poter creare la configurazione di disaster recovery MetroCluster o SVM.
- Se la configurazione di disaster recovery MetroCluster o SVM esiste già, ONTAP impedisce di creare un motore esterno FPolicy con ambito cluster e autenticazione SSL.

Fogli di lavoro completi per la configurazione del motore esterno ONTAP FPolicy

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione del motore esterno FPolicy. Se è richiesto un valore di parametro, è necessario determinare quale valore utilizzare per tali parametri prima di configurare il motore esterno.

Informazioni per una configurazione di base del motore esterno

Registrare se si desidera includere ogni impostazione di parametro nella configurazione esterna del motore e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	Sì	
Nome del motore	Sì	Sì	
Server FPolicy primari	Sì	Sì	
Numero di porta	Sì	Sì	
Server FPolicy secondari	No		
Tipo di motore esterno	No		
Opzione SSL per la comunicazione con il server FPolicy esterno	Sì	Sì	
FQDN certificato o nome comune personalizzato	No		
Numero di serie del certificato	No		
Autorità di certificazione	No		

Informazioni sui parametri esterni avanzati del motore

Per configurare un motore esterno con parametri avanzati, è necessario immettere il comando di configurazione in modalità avanzata con privilegi.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Timeout per l'annullamento di una richiesta	No		
Timeout per l'interruzione di una richiesta	No		
Intervallo per l'invio delle richieste di stato	No		
Numero massimo di richieste in sospeso sul server FPolicy	No		
Timeout per la disconnessione di un server FPolicy che non risponde	No		

Intervallo per l'invio di messaggi keep-alive al server FPolicy	No		
Numero massimo di tentativi di riconnessione	No		
Dimensione buffer di ricezione	No		
Dimensione buffer di invio	No		
Timeout per l'eliminazione di un ID sessione durante la riconnessione	No		

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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.