



Monitorare le performance del cluster con System Manager

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/it-it/ontap/task_cp_monitor_cluster_performance_sm.html on April 24, 2024. Always check docs.netapp.com for the latest.

Sommario

- Monitorare le performance del cluster con System Manager. 1
 - Monitorare le performance del cluster utilizzando System Manager 1
 - Visualizza le performance sulla dashboard del cluster 1
 - Identificare gli hot volumi e altri oggetti 1
 - Modificare QoS. 2
 - Monitorare i rischi. 2
 - Informazioni su System Manager. 4
 - Ottieni informazioni utili per ottimizzare il tuo sistema 9
 - Configurare FPolicy nativo 11

Monitorare le performance del cluster con System Manager

Monitorare le performance del cluster utilizzando System Manager

Gli argomenti di questa sezione mostrano come gestire lo stato e le performance del cluster con Gestione di sistema in ONTAP 9.7 e versioni successive.

È possibile monitorare le prestazioni del cluster visualizzando le informazioni relative al sistema nella dashboard di System Manager. La dashboard visualizza informazioni su avvisi e notifiche importanti, l'efficienza e la capacità dei livelli e dei volumi di storage, i nodi disponibili in un cluster, lo stato dei nodi in una coppia ha, le applicazioni e gli oggetti più attivi, e le metriche delle performance di un cluster o di un nodo.

La dashboard consente di determinare le seguenti informazioni:

- *** Health***: Quanto è sano il cluster?
- **Capacità**: Quale capacità è disponibile sul cluster?
- **Performance**: Quali sono le performance del cluster, in base a latenza, IOPS e throughput?
- **Rete**: Come viene configurata la rete con host e oggetti storage, come porte, interfacce e macchine virtuali di storage?

Nelle panoramiche su salute e capacità, fare clic su [→](#) per visualizzare informazioni aggiuntive ed eseguire attività.

Nella panoramica delle performance, puoi visualizzare le metriche in base all'ora, al giorno, alla settimana, al mese o all'anno.

Nella panoramica della rete viene visualizzato il numero di ciascun oggetto della rete (ad esempio, "8 porte NVMe/FC"). È possibile fare clic sui numeri per visualizzare i dettagli relativi a ciascun oggetto di rete.

Visualizza le performance sulla dashboard del cluster

Utilizza la dashboard per prendere decisioni informate sui carichi di lavoro che potresti voler aggiungere o spostare. Puoi anche considerare i tempi di utilizzo più elevati per pianificare potenziali cambiamenti.

I valori delle performance si aggiornano ogni 3 secondi e il grafico delle performance si aggiorna ogni 15 secondi.

Fasi

1. Fare clic su **Dashboard**.
2. In **Performance**, selezionare l'intervallo.

Identificare gli hot volumi e altri oggetti

Accelera le performance del tuo cluster identificando i volumi con accesso frequente (hot

volumi) e i dati (hot objects).



A partire da ONTAP 9.10.1, è possibile utilizzare la funzione monitoraggio attività di analisi del file system per monitorare gli oggetti hot in un volume.


Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Filtrare le colonne IOPS, latenza e throughput per visualizzare i volumi e i dati utilizzati di frequente.

Modificare QoS

A partire da ONTAP 9,8, per il provisioning dello storage, [Qualità del servizio \(QoS\)](#) è attivato per impostazione predefinita. È possibile disattivare la QoS o scegliere una policy QoS personalizzata durante il processo di provisioning. È inoltre possibile modificare la QoS dopo il provisioning dello storage.

Fasi

1. In Gestione sistema, selezionare **archiviazione**, quindi **volumi**.
2. Accanto al volume per cui si desidera modificare la qualità del servizio, selezionare  Quindi **Modifica**.

Monitorare i rischi

A partire da ONTAP 9.10.0, è possibile utilizzare Gestione di sistema per monitorare i rischi segnalati da Consulente digitale Active IQ. A partire da ONTAP 9.10.1, è possibile utilizzare Gestione di sistema per riconoscere i rischi.

Il consulente digitale NetApp Active IQ segnala le opportunità per ridurre i rischi e migliorare le performance e l'efficienza del tuo ambiente di storage. Con System Manager, puoi conoscere i rischi segnalati da Active IQ e ricevere informazioni utili per amministrare lo storage e ottenere una maggiore disponibilità, una maggiore sicurezza e migliori performance dello storage.

Collegamento all'account Active IQ

Per ricevere informazioni sui rischi da Active IQ, devi prima collegarti al tuo account Active IQ da Gestione sistema.

Fasi

1. In System Manager, fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. In **registrazione Active IQ**, fare clic su **Registra**.
3. Immettere le credenziali per Active IQ.
4. Una volta autenticate le credenziali, fare clic su **Confirm (Conferma) per collegare Active IQ a Gestore di sistema**.

Visualizza il numero di rischi

A partire da ONTAP 9.10.0, è possibile visualizzare dal dashboard di Gestione sistema il numero di rischi segnalati da Active IQ.

Prima di iniziare

È necessario stabilire una connessione da Gestore di sistema all'account Active IQ. Fare riferimento a [Collegamento all'account Active IQ](#).

Fasi

1. In System Manager, fare clic su **Dashboard**.
2. Nella sezione **Health**, visualizzare il numero di rischi segnalati.



È possibile visualizzare informazioni più dettagliate su ciascun rischio facendo clic sul messaggio che indica il numero di rischi. Vedere [Visualizza i dettagli dei rischi](#).

Visualizza i dettagli dei rischi

A partire da ONTAP 9.10.0, è possibile visualizzare da System Manager come i rischi segnalati da Active IQ sono classificati in base alle aree di impatto. È inoltre possibile visualizzare informazioni dettagliate su ciascun rischio segnalato, il suo potenziale impatto sul sistema e le azioni correttive che è possibile intraprendere.

Prima di iniziare

È necessario stabilire una connessione da Gestore di sistema all'account Active IQ. Fare riferimento a [Collegamento all'account Active IQ](#).

Fasi

1. Fare clic su **Eventi > tutti gli eventi**.
2. Nella sezione **Panoramica**, sotto **Active IQ Suggerimenti**, visualizzare il numero di rischi in ciascuna categoria di area di impatto. Le categorie di rischio includono:
 - Performance ed efficienza
 - Disponibilità e protezione
 - Capacità
 - Configurazione
 - Sicurezza
3. Fare clic sulla scheda **Active IQ Suggerimenti** per visualizzare informazioni su ciascun rischio, tra cui:
 - Livello di impatto sul sistema
 - Categoria del rischio
 - Nodi interessati
 - Tipo di mitigazione necessaria
 - Azioni correttive da intraprendere

Riconoscere i rischi

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per riconoscere i rischi aperti.

Fasi

1. In System Manager, visualizzare l'elenco dei rischi eseguendo la procedura descritta in [Visualizza i dettagli dei rischi](#).
2. Fare clic sul nome del rischio di un rischio aperto che si desidera riconoscere.

3. Inserire le informazioni nei seguenti campi:

- Promemoria (data)
- Giustificazione
- Commenti

4. Fare clic su **Conferma**.



Dopo aver riconosciuto un rischio, sono necessari alcuni minuti per riflettere la modifica nell'elenco dei suggerimenti di Active IQ.

Annullare il riconoscimento dei rischi

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per annullare qualsiasi rischio precedentemente riconosciuto.

Fasi

1. In System Manager, visualizzare l'elenco dei rischi eseguendo la procedura descritta in [Visualizza i dettagli dei rischi](#).
2. Fare clic sul nome del rischio riconosciuto che si desidera annullare.
3. Inserire le informazioni nei seguenti campi:
 - Giustificazione
 - Commenti
4. Fare clic su **Annulla riconoscimento**.



Una volta che si annulla la conferma di un rischio, sono necessari alcuni minuti affinché la modifica venga riflessa nell'elenco dei suggerimenti di Active IQ.

Informazioni su System Manager

A partire da ONTAP 9.11.1, System Manager visualizza *informazioni* che consentono di ottimizzare le prestazioni e la sicurezza del sistema.



Per visualizzare, personalizzare e rispondere alle informazioni, fare riferimento a. "[Ottieni informazioni utili per ottimizzare il tuo sistema](#)"

Informazioni sulla capacità

System Manager può visualizzare le seguenti informazioni in risposta alle condizioni di capacità del sistema:

Insight	Severità	Condizione	Correzioni
---------	----------	------------	------------

Gli strati locali sono privi di spazio	Rimediare ai rischi	Uno o più Tier locali sono pieni e in rapida crescita di oltre il 95%. È possibile che i carichi di lavoro esistenti non siano in grado di crescere o, in casi estremi, che i carichi di lavoro esistenti esauriscano lo spazio ed effettuino un errore.	<p>Correzione consigliata: Eseguire una delle seguenti opzioni.</p> <ul style="list-style-type: none"> • Cancellare la coda di ripristino del volume. • Consentire il thin provisioning sui volumi con thick provisioning per liberare lo storage intrappolato. • Sposta i volumi in un altro Tier locale. • Elimina le copie Snapshot non necessarie. • Eliminare le directory o i file non necessari nei volumi. • Consenti a Fabric Pool di eseguire il tiering dei dati nel cloud.
Le applicazioni mancano di spazio	Richiede attenzione	Uno o più volumi sono pieni più del 95%, ma non hanno la funzione di crescita automatica attivata.	<p>Consigliato: Consente di attivare la crescita automatica fino al 150% della capacità di corrente.</p> <p>Altre opzioni:</p> <ul style="list-style-type: none"> • Recupera spazio eliminando le copie Snapshot. • Ridimensionare i volumi. • Eliminare directory o file.
La capacità del volume FlexGroup non è bilanciata	Ottimizzazione dello storage	Le dimensioni dei volumi costituenti di uno o più volumi FlexGroup sono cresciute in modo non uniforme nel tempo, portando a uno squilibrio nell'utilizzo della capacità. Se i volumi costituenti diventano pieni, potrebbero verificarsi errori di scrittura.	<p>Consigliato: Riequilibrare i volumi FlexGroup.</p>

La capacità delle macchine virtuali storage sta per esaurirsi	Ottimizzazione dello storage	Una o più macchine virtuali storage hanno una capacità quasi massima vicina a quella massima. Non sarà quindi possibile eseguire il provisioning di ulteriore spazio per volumi nuovi o esistenti se le Storage VM raggiungono la capacità massima.	Consigliato: Se possibile, aumentare il limite massimo di capacità della VM di storage.
---	------------------------------	---	--

Informazioni sulla sicurezza

System Manager può visualizzare le seguenti informazioni in risposta a condizioni che potrebbero compromettere la sicurezza dei dati o del sistema.

Insight	Severità	Condizione	Correzioni
I volumi sono ancora in modalità di apprendimento anti-ransomware	Richiede attenzione	Uno o più volumi sono in modalità di apprendimento anti-ransomware da 90 giorni.	Consigliato: Abilitare la modalità anti-ransomware attiva per questi volumi.
L'eliminazione automatica delle copie Snapshot è abilitata sui volumi	Richiede attenzione	L'eliminazione automatica dello snapshot è abilitata su uno o più volumi.	Consigliato: Disattiva l'eliminazione automatica delle copie Snapshot. In caso contrario, in caso di attacco ransomware, il recovery di dati per questi volumi potrebbe non essere possibile.
I volumi non dispongono di policy Snapshot	Richiede attenzione	Uno o più volumi non dispongono di una policy Snapshot adeguata.	Consigliato: Allegare un criterio Snapshot ai volumi che non ne hanno uno. In caso contrario, in caso di attacco ransomware, il recovery di dati per questi volumi potrebbe non essere possibile.
FPolicy nativo non è configurato	Best practice	FPolicy nativo non è configurato su una o più macchine virtuali storage NAS.	Consigliato: IMPORTANTE: Il blocco delle estensioni potrebbe causare risultati imprevisti. A partire dal 9.11.1, puoi abilitare FPolicy nativa per le macchine virtuali storage, che blocca oltre 3000 estensioni dei file conosciute per essere utilizzate per gli attacchi ransomware. "Configurare FPolicy nativo" Nelle macchine virtuali storage NAS per controllare le estensioni dei file consentite o non consentite per la scrittura sui volumi nel tuo ambiente.

Telnet è attivato	Best practice	Secure Shell (SSH) deve essere utilizzato per un accesso remoto sicuro.	Consigliato: Disattivare Telnet e utilizzare SSH per un accesso remoto sicuro.
Sono stati configurati troppi server NTP	Best practice	Il numero di server configurati per NTP è inferiore a 3.	Consigliato: Associare al cluster almeno tre server NTP. In caso contrario, possono verificarsi problemi con la sincronizzazione dell'ora del cluster.
Remote Shell (RSH) è attivato	Best practice	Secure Shell (SSH) deve essere utilizzato per un accesso remoto sicuro.	Consigliato: Disabilitare RSH e utilizzare SSH per un accesso remoto sicuro.
Banner di accesso non configurato	Best practice	I messaggi di accesso non sono configurati né per il cluster, né per la VM di storage, né per entrambi.	Consigliato: Configurare i banner di accesso per il cluster e la VM di storage e abilitarne l'utilizzo.
AutoSupport sta utilizzando un protocollo non sicuro	Best practice	AutoSupport non è configurato per comunicare tramite HTTPS.	Consigliato: Si consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per inviare messaggi AutoSupport al supporto tecnico.
L'utente amministratore predefinito non è bloccato	Best practice	Nessuno ha effettuato l'accesso utilizzando un account amministrativo predefinito (admin o diag) e questi account non sono bloccati.	Consigliato: Blocca gli account amministrativi predefiniti quando non vengono utilizzati.
Secure Shell (SSH) sta utilizzando cifrari non sicuri	Best practice	La configurazione corrente utilizza cifrari CBC non protetti.	Raccomandato: Si dovrebbe consentire solo cifrari sicuri sul server web per proteggere la comunicazione sicura con i visitatori. Rimuovere i cifrari con nomi contenenti "cbc", ad esempio "ais128-cbc", "AES192-cbc", "AES256-cbc" e "3DES-cbc".
La compliance FIPS globale 140-2 è disattivata	Best practice	La compliance FIPS globale 140-2 è disabilitata nel cluster.	Consigliato: Per motivi di sicurezza, è necessario abilitare la crittografia globale conforme a FIPS 140-2 per garantire che ONTAP possa comunicare in modo sicuro con client o client server esterni.

I volumi non vengono monitorati alla ricerca di attacchi ransomware	Richiede attenzione	La funzionalità anti-ransomware è disabilitata su uno o più volumi.	Consigliato: Abilitare l'anti-ransomware sui volumi. In caso contrario, potresti non accorgerti quando i volumi sono minacciati o sotto attacco.
Le macchine virtuali storage non sono configurate per anti-ransomware	Best practice	Una o più macchine virtuali storage non sono configurate per la protezione anti-ransomware.	Consigliato: Abilitare l'anti-ransomware sulle macchine virtuali storage. Altrimenti, potresti non notare quando le macchine virtuali storage sono minacciate o sottoposte a attacchi.

Informazioni di configurazione

System Manager può visualizzare le seguenti informazioni in risposta ai problemi relativi alla configurazione del sistema.

Insight	Severità	Condizione	Correzioni
Il cluster non è configurato per le notifiche	Best practice	Email, webhook o trapshot SNMP non sono configurati per consentirti di ricevere notifiche su problemi con il cluster.	Consigliato: Configurare le notifiche per il cluster.
Il cluster non è configurato per gli aggiornamenti automatici.	Best practice	Il cluster non è stato configurato in modo da ricevere aggiornamenti automatici per il pacchetto di qualifica del disco più recente, il firmware del disco, il firmware dello shelf e i file del firmware SP/BMC quando sono disponibili.	Consigliato: Attivare questa funzione.

Il firmware del cluster non è aggiornato	Best practice	Il sistema non dispone dell'ultimo aggiornamento del firmware che potrebbe avere miglioramenti, patch di sicurezza o nuove funzioni che consentono di proteggere il cluster per prestazioni migliori.	Consigliato: Aggiornare il firmware ONTAP.
--	---------------	---	---

Ottieni informazioni utili per ottimizzare il tuo sistema

System Manager consente di visualizzare informazioni utili per ottimizzare il sistema.

A proposito di questa attività

A partire da ONTAP 9.11.0, puoi visualizzare informazioni in System Manager che ti aiutano a ottimizzare la capacità e la conformità alla sicurezza del tuo sistema.

A partire da ONTAP 9.11.1, è possibile visualizzare informazioni aggiuntive che consentono di ottimizzare la capacità, la conformità alla sicurezza e la configurazione del sistema.



Il blocco delle estensioni può causare risultati imprevisti. a partire da ONTAP 9.11.1, è possibile abilitare FPolicy nativo per le VM di archiviazione utilizzando Gestione sistema. Potresti ricevere un messaggio di System Manager Insight che ti consiglia di farlo ["Configurare FPolicy nativo"](#) Per una macchina virtuale di storage.

Con la modalità nativa di FPolicy, è possibile consentire o negare estensioni di file specifiche. System Manager consiglia oltre 3000 estensioni di file non consentite che sono state utilizzate in precedenti attacchi ransomware. Alcune di queste estensioni potrebbero essere utilizzate da file legittimi nell'ambiente in uso e il loro blocco potrebbe causare problemi imprevisti.

Pertanto, si consiglia di modificare l'elenco delle estensioni per soddisfare le esigenze dell'ambiente. Fare riferimento a. ["Come rimuovere un'estensione di file da una configurazione FPolicy nativa creata da System Manager utilizzando System Manager per ricreare il criterio"](#).

Per ulteriori informazioni su FPolicy nativo, vedere ["Tipi di configurazione FPolicy"](#).

In base alle Best practice, queste informazioni vengono visualizzate su una pagina da cui è possibile avviare azioni immediate per ottimizzare il sistema. Per ulteriori informazioni su ciascuna analisi, vedere ["Informazioni su System Manager"](#).





Visualizza informazioni sull'ottimizzazione

Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.

La pagina **Insights** mostra gruppi di informazioni. Ciascun gruppo di informazioni potrebbe contenere uno o più elementi. Vengono visualizzati i seguenti gruppi:

- Ha bisogno della vostra attenzione
 - Rimediare ai rischi
 - Ottimizza il tuo storage
2. (Facoltativo) filtrare le informazioni visualizzate facendo clic sui seguenti pulsanti nell'angolo in alto a destra della pagina:

-  Visualizza le informazioni relative alla sicurezza.
-  Visualizza le informazioni relative alla capacità.
-  Visualizza le informazioni relative alla configurazione.
-  Visualizza tutte le informazioni.

Rispondi alle informazioni per ottimizzare il tuo sistema

In System Manager, puoi rispondere alle informazioni spendendole, esplorando diversi modi per risolvere i problemi o avviando il processo per risolverli.

Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. Passare il mouse su una panoramica per visualizzare i pulsanti per eseguire le seguenti azioni:
 - **Chiudi**: Elimina le informazioni dalla vista. Per “undisperdere” le informazioni, fare riferimento a [\[customize-settings-insights\]](#).
 - **Esplora**: Scopri i vari modi per risolvere il problema menzionato nelle informazioni. Questo pulsante viene visualizzato solo se è presente più di un metodo di correzione.
 - **Fix**: Avviare il processo di risoluzione del problema menzionato nelle informazioni. Verrà richiesto di confermare se si desidera intraprendere l'azione necessaria per applicare la correzione.




Alcune di queste azioni possono essere avviate da altre pagine in System Manager, ma la pagina **Insights** ti aiuta a ottimizzare le attività quotidiane, consentendoti di avviare questa azione da questa pagina.

Personalizzare le impostazioni per ottenere informazioni dettagliate

Puoi personalizzare le informazioni che ti verranno notificate in System Manager.


Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. Nell'angolo superiore destro della pagina, fare clic su , Quindi selezionare **Impostazioni**.
3. Nella pagina **Impostazioni**, verificare che le caselle di controllo accanto alle informazioni di cui si desidera ricevere la notifica siano selezionate. Se in precedenza si è respinto un dato Insight, è possibile “undischissarlo” verificando che sia presente un segno di spunta nella relativa casella di controllo.
4. Fare clic su **Save** (Salva).

Esportare le informazioni come file PDF

Puoi esportare tutte le informazioni pertinenti come file PDF.

Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. Nell'angolo superiore destro della pagina, fare clic su , Quindi selezionare **Esporta**.

Configurare FPolicy nativo

A partire da ONTAP 9.11.1, quando ricevi un System Manager Insight che suggerisce l'implementazione di FPolicy nativo, puoi configurarlo sui volumi e sulle macchine virtuali di storage.

Prima di iniziare

Quando si accede a informazioni su System Manager, in **Applica procedure consigliate**, potrebbe essere visualizzato un messaggio che indica che FPolicy nativo non è configurato.

Per ulteriori informazioni sui tipi di configurazione FPolicy, fare riferimento a. ["Tipi di configurazione FPolicy"](#).

Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. In **Applica Best practice**, individuare **Native FPolicy non è configurato**.
3. Leggere il seguente messaggio prima di intraprendere un'azione:



Il blocco delle estensioni può causare risultati imprevisti. a partire da ONTAP 9.11.1, è possibile abilitare FPolicy nativo per le VM di archiviazione utilizzando Gestione sistema. Con la modalità nativa di FPolicy, è possibile consentire o negare estensioni di file specifiche. System Manager consiglia oltre 3000 estensioni di file non consentite che sono state utilizzate in precedenti attacchi ransomware. Alcune di queste estensioni potrebbero essere utilizzate da file legittimi nell'ambiente in uso e il loro blocco potrebbe causare problemi imprevisti.

Pertanto, si consiglia di modificare l'elenco delle estensioni per soddisfare le esigenze dell'ambiente. Fare riferimento a. ["Come rimuovere un'estensione di file da una configurazione FPolicy nativa creata da System Manager utilizzando System Manager per ricreare il criterio"](#).

4. Fare clic su **Correggi**.
5. Selezionare le macchine virtuali storage a cui si desidera applicare FPolicy native.
6. Per ogni VM di storage, seleziona i volumi che riceveranno FPolicy nativa.
7. Fare clic su **Configura**.

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.