



Attivare la scansione sulle origini dati

Cloud Manager 3.8

NetApp
March 25, 2024

Sommario

- Attivare la scansione sulle origini dati 1
- Introduzione alla conformità del cloud per Cloud Volumes ONTAP e Azure NetApp Files 1
- Introduzione alla conformità cloud per Amazon S3 5
- Scansione degli schemi del database 13
- Scansione on-premise dei dati ONTAP con conformità al cloud utilizzando SnapMirror 16

Attivare la scansione sulle origini dati

Introduzione alla conformità del cloud per Cloud Volumes ONTAP e Azure NetApp Files

Completa alcuni passaggi per iniziare a utilizzare la conformità cloud per Cloud Volumes ONTAP o Azure NetApp Files.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.



Implementare l'istanza Cloud Compliance

"[Implementazione della conformità al cloud in Cloud Manager](#)" se non è già stata implementata un'istanza.



Abilita la conformità al cloud nei tuoi ambienti di lavoro

Fare clic su **Cloud Compliance**, selezionare la scheda **Configuration** e attivare le scansioni di compliance per ambienti di lavoro specifici.



Garantire l'accesso ai volumi

Ora che la conformità al cloud è abilitata, assicurati che l'IT possa accedere ai volumi.

- L'istanza di conformità cloud richiede una connessione di rete a ciascuna subnet Cloud Volumes ONTAP o subnet Azure NetApp Files.
- I gruppi di sicurezza per Cloud Volumes ONTAP devono consentire connessioni in entrata dall'istanza di conformità cloud.
- Le policy di esportazione dei volumi NFS devono consentire l'accesso dall'istanza Cloud Compliance.
- Cloud Compliance necessita delle credenziali di Active Directory per eseguire la scansione dei volumi CIFS.

Fare clic su **Cloud Compliance > Scan Configuration > Edit CIFS Credentials** e fornire le credenziali. Le credenziali possono essere di sola lettura, ma fornire credenziali di amministratore garantisce che Cloud Compliance possa leggere i dati che richiedono autorizzazioni elevate.



Configurare i volumi da sottoporre a scansione

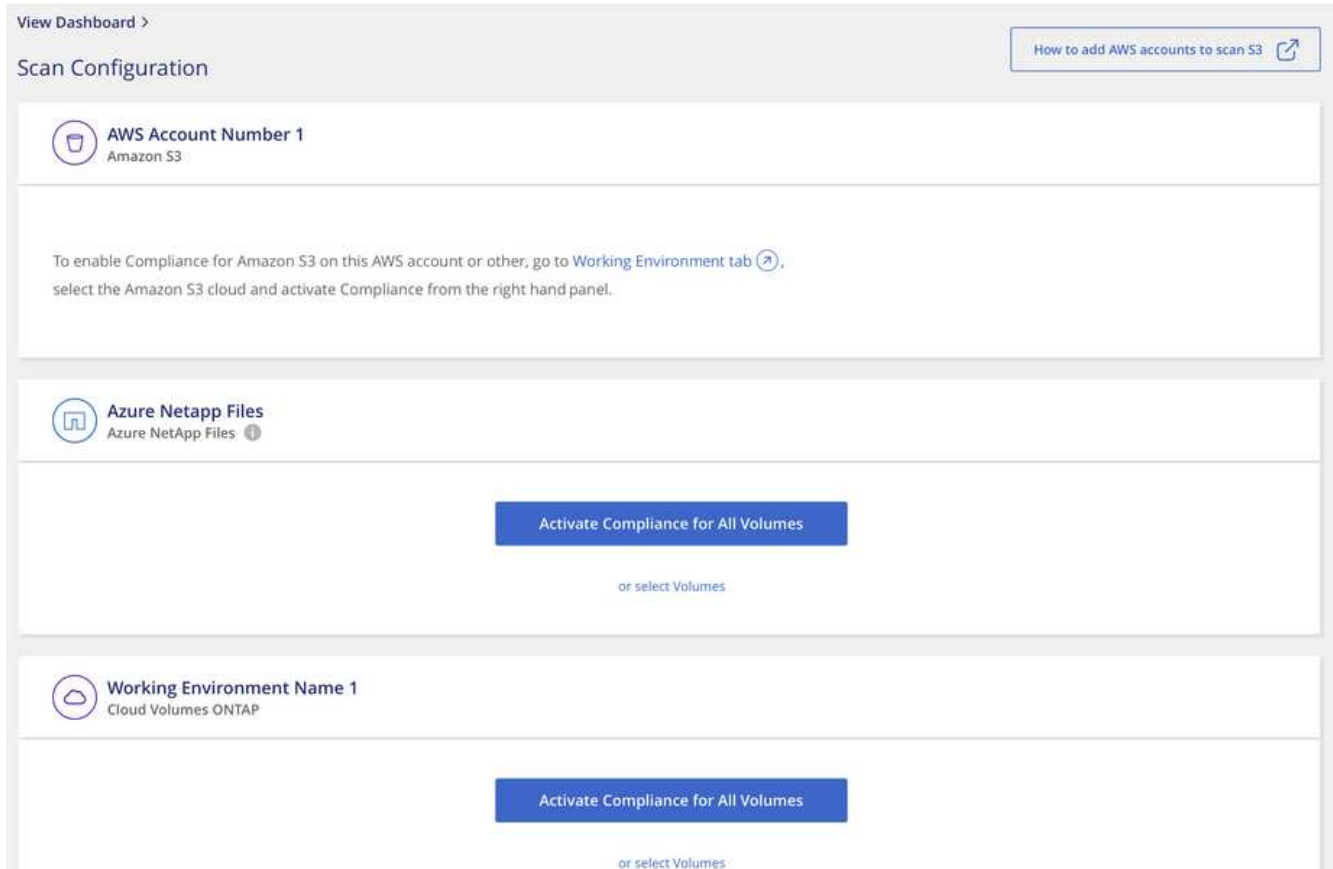
Seleziona i volumi che desideri sottoporre a scansione e la Cloud Compliance inizierà a eseguirne la scansione.

Implementazione dell'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

Abilitare la conformità al cloud nei tuoi ambienti di lavoro

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**, quindi selezionare la scheda **Configuration**.



2. Per eseguire la scansione di tutti i volumi in un ambiente di lavoro, fare clic su **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi).

Per eseguire la scansione solo di determinati volumi in un ambiente di lavoro, fare clic su **o selezionare Volumi** (volumi), quindi scegliere i volumi da sottoporre a scansione.

Vedere [Attivazione e disattivazione delle scansioni di compliance sui volumi](#) per ulteriori informazioni.

Risultato

Cloud Compliance inizia la scansione dei dati in ogni ambiente di lavoro. I risultati saranno disponibili nella dashboard Compliance non appena la Cloud Compliance terminerà le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati, che potrebbe essere di pochi minuti o ore.

Verificare che la conformità del cloud abbia accesso ai volumi

Assicurati che Cloud Compliance possa accedere ai volumi controllando il networking, i gruppi di sicurezza e le policy di esportazione. È necessario fornire le credenziali CIFS per la conformità al cloud in modo che possa accedere ai volumi CIFS.

Fasi

1. Assicurarsi che sia presente una connessione di rete tra l'istanza di conformità cloud e ogni rete che include volumi per Cloud Volumes ONTAP o Azure NetApp Files.



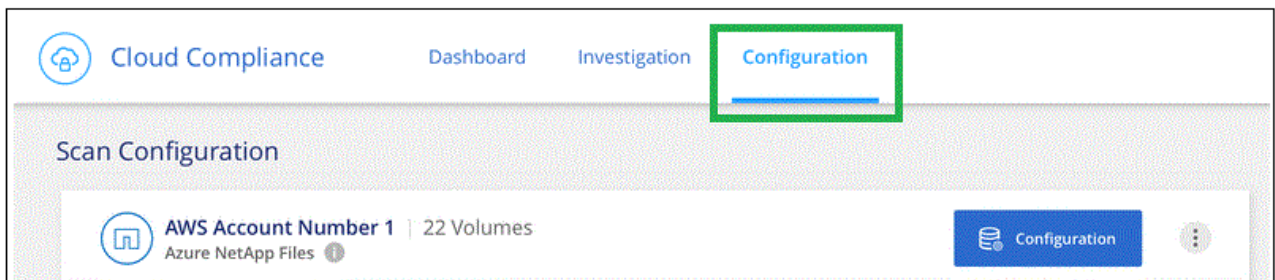
Per Azure NetApp Files, la conformità del cloud può eseguire la scansione solo dei volumi che si trovano nella stessa regione di Cloud Manager.

2. Assicurarsi che il gruppo di sicurezza per Cloud Volumes ONTAP consenta il traffico in entrata dall'istanza di conformità cloud.

È possibile aprire il gruppo di sicurezza per il traffico dall'indirizzo IP dell'istanza Cloud Compliance oppure aprire il gruppo di sicurezza per tutto il traffico dall'interno della rete virtuale.

3. Assicurarsi che le policy di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza Cloud Compliance in modo che possa accedere ai dati di ciascun volume.
4. Se si utilizza CIFS, fornire la conformità cloud con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.

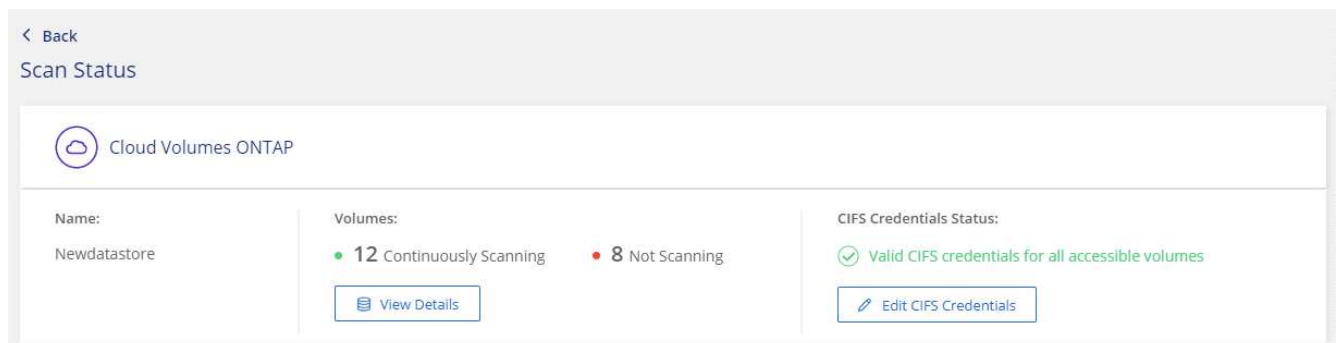
- a. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.
- b. Fare clic sulla scheda **Configurazione**.



- c. Per ciascun ambiente di lavoro, fare clic su **Edit CIFS Credentials** (Modifica credenziali CIFS) e immettere il nome utente e la password necessari per l'accesso ai volumi CIFS nel sistema.

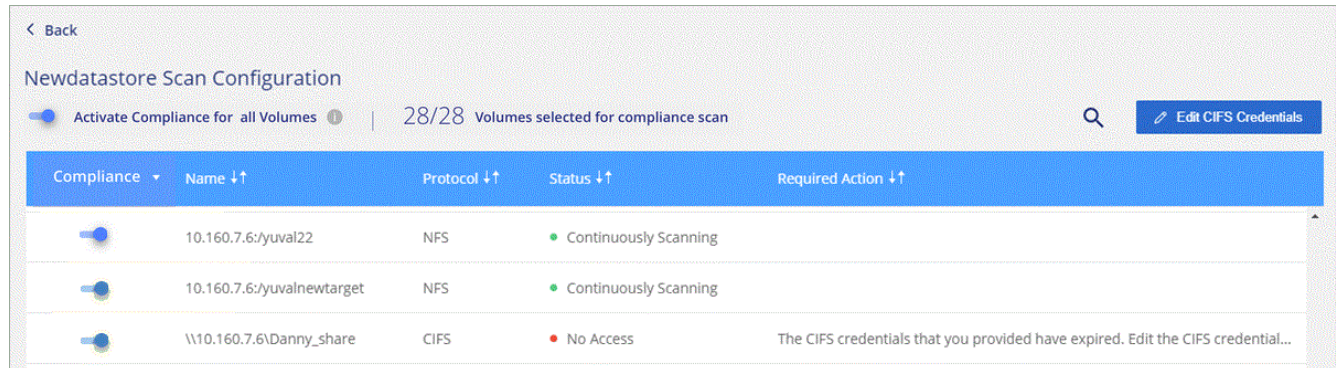
Le credenziali possono essere di sola lettura, ma fornire credenziali di amministratore garantisce che Cloud Compliance possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono memorizzate nell'istanza Cloud Compliance.

Dopo aver immesso le credenziali, viene visualizzato un messaggio che indica che tutti i volumi CIFS sono stati autenticati correttamente.



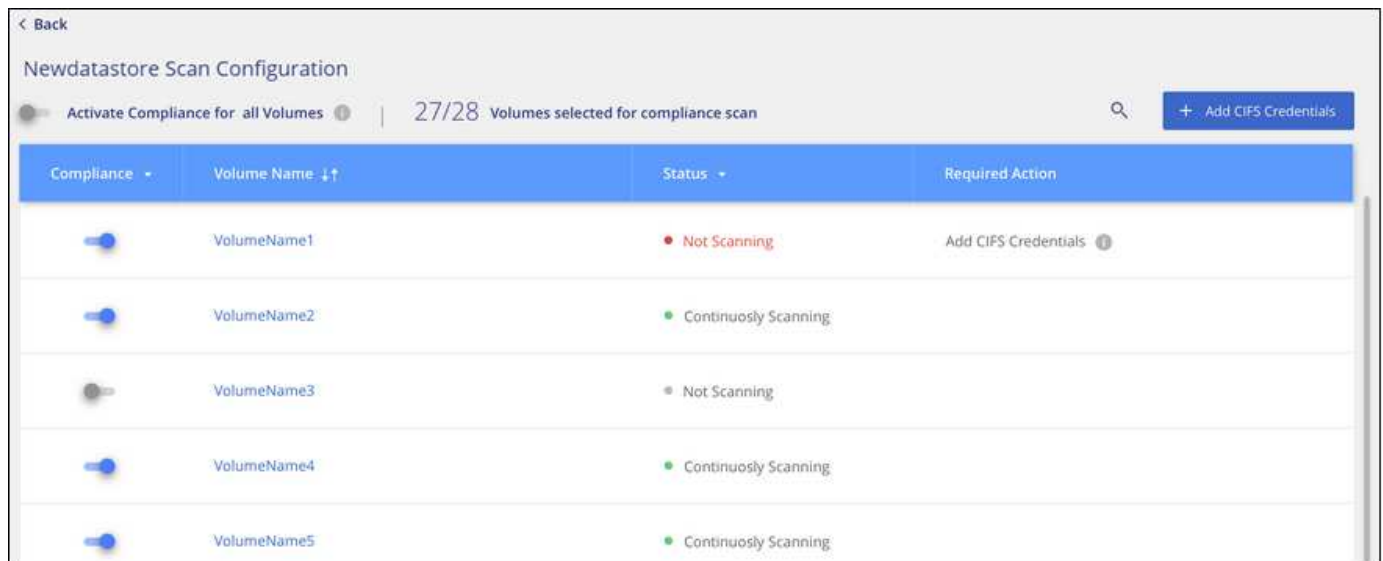
5. Nella pagina *Scan Configuration*, fare clic su **View Details** (Visualizza dettagli) per esaminare lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

Ad esempio, l'immagine seguente mostra tre volumi, uno dei quali non è in grado di eseguire la scansione di Cloud Compliance a causa di problemi di connettività di rete tra l'istanza di Cloud Compliance e il volume.



Attivazione e disattivazione delle scansioni di compliance sui volumi

È possibile interrompere o avviare la scansione dei volumi in un ambiente di lavoro in qualsiasi momento dalla pagina Scan Configuration (Configurazione scansione). Si consiglia di eseguire la scansione di tutti i volumi.



A:	Eseguire questa operazione:
Disattivare la scansione di un volume	Spostare il dispositivo di scorrimento del volume verso sinistra
Disattivare la scansione per tutti i volumi	Spostare il dispositivo di scorrimento Activate Compliance for all Volumes (attiva compliance per tutti i volumi) verso sinistra
Abilitare la scansione per un volume	Spostare il dispositivo di scorrimento del volume verso destra
Abilitare la scansione per tutti i volumi	Spostare il dispositivo di scorrimento Activate Compliance for All Volumes (attiva conformità per tutti i volumi) verso destra



I nuovi volumi aggiunti all'ambiente di lavoro vengono sottoposti automaticamente a scansione solo quando è attivata l'impostazione **attiva conformità per tutti i volumi**. Quando questa impostazione è disattivata, è necessario attivare la scansione su ogni nuovo volume creato nell'ambiente di lavoro.

Scansione dei volumi di protezione dei dati

Per impostazione predefinita, i volumi di protezione dei dati (DP) non vengono sottoposti a scansione perché non sono esposti esternamente e la Cloud Compliance non può accedervi. Questi volumi sono in genere i volumi di destinazione per le operazioni SnapMirror da un cluster ONTAP on-premise.

Inizialmente, l'elenco dei volumi Cloud Compliance identifica questi volumi come *Type DP* con *Status Not Scanning* e *Required Action Enable Access to DP Volumes*.

Compliance	Volume Name	Type	Status	Required Action
<input type="checkbox"/>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes
<input checked="" type="checkbox"/>	VolumeName2	NFS	Continuously Scanning	
<input type="checkbox"/>	VolumeName3	CIFS	Not Scanning	

Fasi

Se si desidera eseguire la scansione di questi volumi di protezione dei dati:

1. Fare clic sul pulsante **Enable Access to DP Volumes** (Abilita accesso ai volumi DP) nella parte superiore della pagina.
2. Attivare ciascun volume DP che si desidera sottoporre a scansione oppure utilizzare il controllo **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi) per abilitare tutti i volumi, inclusi tutti i volumi DP.

Una volta attivata, Cloud Compliance crea una condivisione NFS da ogni volume DP attivato per la conformità, in modo che possa essere scansionato. Le policy di esportazione delle condivisioni consentono l'accesso solo dall'istanza Cloud Compliance.



Solo i volumi creati inizialmente come volumi NFS nel sistema ONTAP di origine vengono visualizzati nell'elenco dei volumi. I volumi di origine creati inizialmente come CIFS non vengono attualmente visualizzati in Cloud Compliance.

Introduzione alla conformità cloud per Amazon S3

Cloud Compliance può eseguire la scansione dei bucket Amazon S3 per identificare i dati personali e sensibili che risiedono nello storage a oggetti S3. Cloud Compliance può eseguire la scansione di qualsiasi bucket dell'account, indipendentemente dal fatto che sia stato creato per una soluzione NetApp.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle sezioni rimanenti per ottenere dettagli completi.



Imposta i requisiti S3 nel tuo ambiente cloud

Assicurati che il tuo ambiente cloud sia in grado di soddisfare i requisiti per la conformità al cloud, tra cui la preparazione di un ruolo IAM e la configurazione della connettività da Cloud Compliance a S3. [Consulta l'elenco completo.](#)



Implementare l'istanza Cloud Compliance

"[Implementazione della conformità al cloud in Cloud Manager](#)" se non è già stata implementata un'istanza.



Attivare la conformità sull'ambiente di lavoro S3

Selezionare l'ambiente di lavoro Amazon S3, fare clic su **Enable Compliance** (attiva conformità) e selezionare un ruolo IAM che includa le autorizzazioni richieste.



Selezionare i bucket da sottoporre a scansione

Seleziona i bucket che desideri sottoporre a scansione e Cloud Compliance inizierà a eseguirne la scansione.

Verifica dei prerequisiti di S3

I seguenti requisiti sono specifici per la scansione dei bucket S3.

Impostare un ruolo IAM per l'istanza Cloud Compliance

Cloud Compliance ha bisogno di autorizzazioni per connettersi ai bucket S3 del tuo account e per eseguirne la scansione. Impostare un ruolo IAM che includa le autorizzazioni elencate di seguito. Cloud Manager ti chiede di selezionare un ruolo IAM quando abiliti Cloud Compliance sull'ambiente di lavoro Amazon S3.


```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}

```

Connettività da Cloud Compliance ad Amazon S3

Cloud Compliance richiede una connessione ad Amazon S3. Il modo migliore per fornire tale connessione è tramite un endpoint VPC al servizio S3. Per istruzioni, vedere ["Documentazione AWS: Creazione di un endpoint gateway"](#).

Quando si crea l'endpoint VPC, assicurarsi di selezionare la regione, il VPC e la tabella di routing che corrispondono all'istanza di Cloud Compliance. È inoltre necessario modificare il gruppo di protezione per aggiungere una regola HTTPS in uscita che abilita il traffico all'endpoint S3. In caso contrario, Cloud Compliance non può connettersi al servizio S3.

In caso di problemi, vedere ["AWS Support Knowledge Center: Perché non è possibile connettersi a un bucket S3 utilizzando un endpoint VPC gateway?"](#)

In alternativa, è possibile stabilire la connessione utilizzando un gateway NAT.



Non puoi utilizzare un proxy per accedere a S3 tramite Internet.

Implementazione dell'istanza Cloud Compliance

["Implementazione della conformità al cloud in Cloud Manager"](#) se non è già stata implementata un'istanza.

È necessario implementare l'istanza in un connettore AWS in modo che Cloud Manager scopra automaticamente i bucket S3 in questo account AWS e li visualizzi in un ambiente di lavoro Amazon S3.

Attivazione della conformità nell'ambiente di lavoro S3

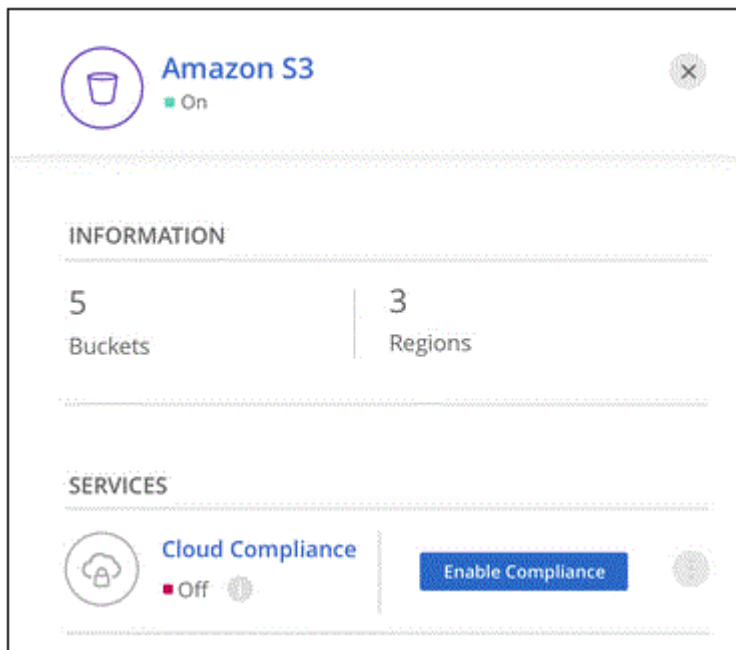
Attiva Cloud Compliance su Amazon S3 dopo aver verificato i prerequisiti.

Fasi

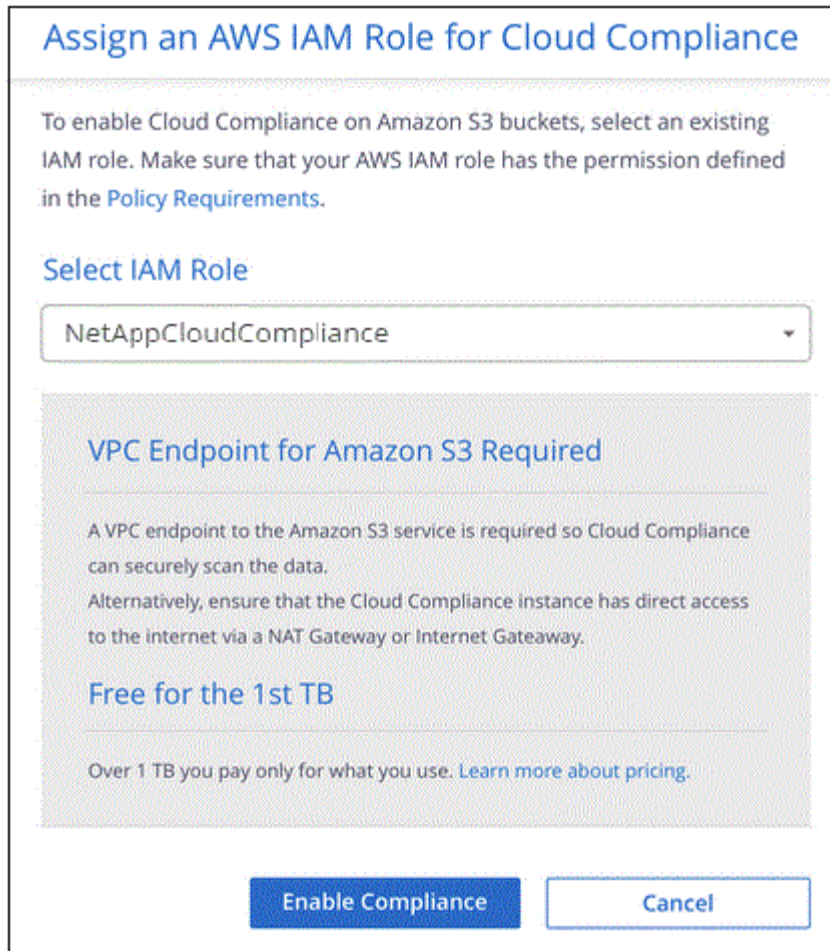
1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare l'ambiente di lavoro Amazon S3.



3. Nel riquadro a destra, fare clic su **Enable Compliance** (attiva conformità).




4. Quando richiesto, assegnare un ruolo IAM all'istanza di Cloud Compliance che ha [le autorizzazioni richieste](#).



5. Fare clic su **Enable Compliance** (attiva conformità)



È inoltre possibile attivare le scansioni di conformità per un ambiente di lavoro dalla pagina

Scan Configuration (Configurazione scansione) facendo clic su  E selezionando **Activate Compliance**.

Risultato

Cloud Manager assegna il ruolo IAM all'istanza.

Attivazione e disattivazione delle scansioni di compliance sui bucket S3

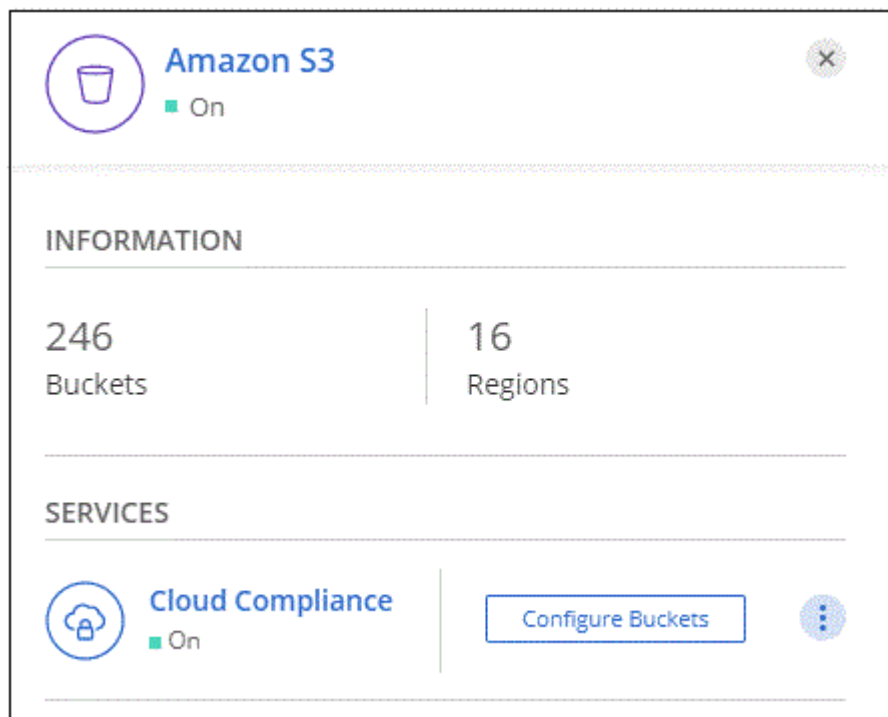
Dopo che Cloud Manager ha attivato Cloud Compliance su Amazon S3, il passaggio successivo consiste nel configurare i bucket che si desidera sottoporre a scansione.

Quando Cloud Manager viene eseguito nell'account AWS che dispone dei bucket S3 che si desidera sottoporre a scansione, rileva tali bucket e li visualizza in un ambiente di lavoro Amazon S3.

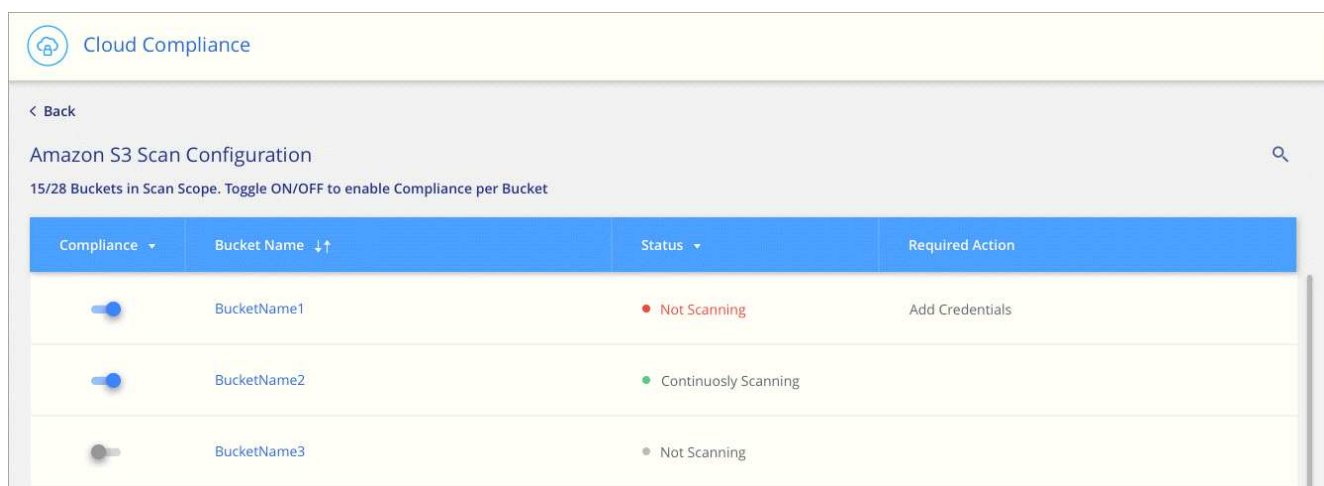
Anche la conformità al cloud può farlo [Eseguire la scansione dei bucket S3 che si trovano in diversi account AWS](#).

Fasi

1. Selezionare l'ambiente di lavoro Amazon S3.
2. Nel riquadro a destra, fare clic su **Configure Bucket** (Configura bucket).



3. Consentire la conformità sui bucket che si desidera sottoporre a scansione.



Risultato

Cloud Compliance inizia la scansione dei bucket S3 abilitati. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

Scansione dei bucket da account AWS aggiuntivi

È possibile eseguire la scansione dei bucket S3 che si trovano sotto un account AWS diverso assegnando un ruolo da tale account per accedere all'istanza esistente di Cloud Compliance.





Fasi

1. Accedere all'account AWS di destinazione in cui si desidera eseguire la scansione dei bucket S3 e creare un ruolo IAM selezionando **un altro account AWS**.

Create role



Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* ⓘ

- Options**
- Require external ID (Best practice when a third party will assume this role)
 - Require MFA ⓘ

Assicurarsi di effettuare le seguenti operazioni:

- Inserire l'ID dell'account in cui risiede l'istanza di Cloud Compliance.
- Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.
- Allega la policy IAM sulla conformità al cloud. Assicurarsi che disponga delle autorizzazioni necessarie.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Accedere all'account AWS di origine in cui risiede l'istanza Cloud Compliance e selezionare il ruolo IAM associato all'istanza.
 - a. Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.
 - b. Fare clic su **Allega policy**, quindi su **Crea policy**.
 - c. Creare una policy che includa l'azione "sts:AssumeRole" e l'ARN del ruolo creato nell'account di destinazione.

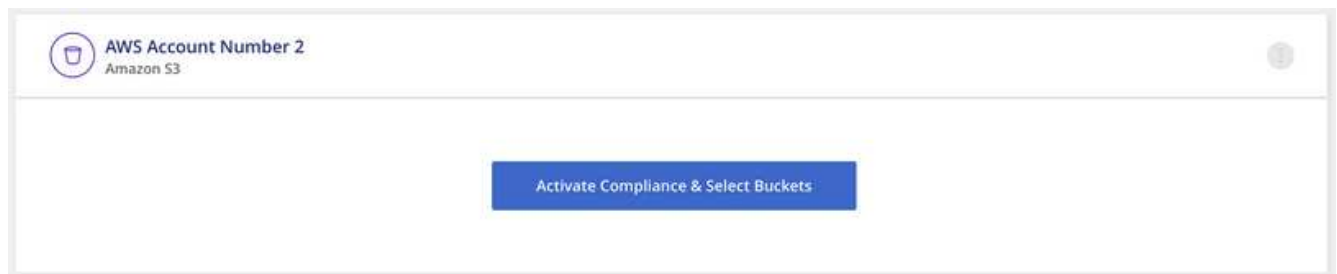
```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}

```

L'account del profilo dell'istanza Cloud Compliance ora ha accesso all'account AWS aggiuntivo.

3. Accedere alla pagina **Amazon S3 Scan Configuration** (Configurazione scansione Amazon S3) per visualizzare il nuovo account AWS. Nota: La sincronizzazione dell'ambiente di lavoro del nuovo account e la visualizzazione di queste informazioni possono richiedere alcuni minuti per la conformità cloud.



4. Fare clic su **Activate Compliance & Select Bucket** (attiva Compliance e seleziona bucket) e selezionare i bucket da sottoporre a scansione.

Risultato

Cloud Compliance inizia la scansione dei nuovi bucket S3 che hai attivato.

Scansione degli schemi del database

Completa alcuni passaggi per iniziare la scansione degli schemi di database con Cloud Compliance.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.



Esaminare i prerequisiti del database

Assicurarsi che il database sia supportato e di disporre delle informazioni necessarie per la connessione al database.



Implementare l'istanza Cloud Compliance

"[Implementazione della conformità al cloud in Cloud Manager](#)" se non è già stata implementata un'istanza.



Aggiungere il server database

Aggiungere il server database a cui si desidera accedere.



Selezionare gli schemi

Selezionare gli schemi da sottoporre a scansione.

Verifica dei prerequisiti

Prima di attivare la conformità al cloud, verificare di disporre di una configurazione supportata.

Database supportati

Cloud Compliance può eseguire la scansione degli schemi dai seguenti database:

- MongoDB
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)



La funzione di raccolta delle statistiche **deve essere abilitata** nel database.

Requisiti del database

È possibile eseguire la scansione di qualsiasi database con connettività all'istanza Cloud Compliance, indipendentemente da dove è ospitato. Per connettersi al database sono necessarie solo le seguenti informazioni:

- Indirizzo IP o nome host
- Porta
- Nome del servizio (solo per l'accesso ai database Oracle)
- Credenziali che consentono l'accesso in lettura agli schemi

Quando si sceglie un nome utente e una password, è importante sceglierne uno che disponga delle autorizzazioni di lettura complete per tutti gli schemi e le tabelle che si desidera sottoporre a scansione. Si consiglia di creare un utente dedicato per il sistema Cloud Compliance con tutte le autorizzazioni necessarie.

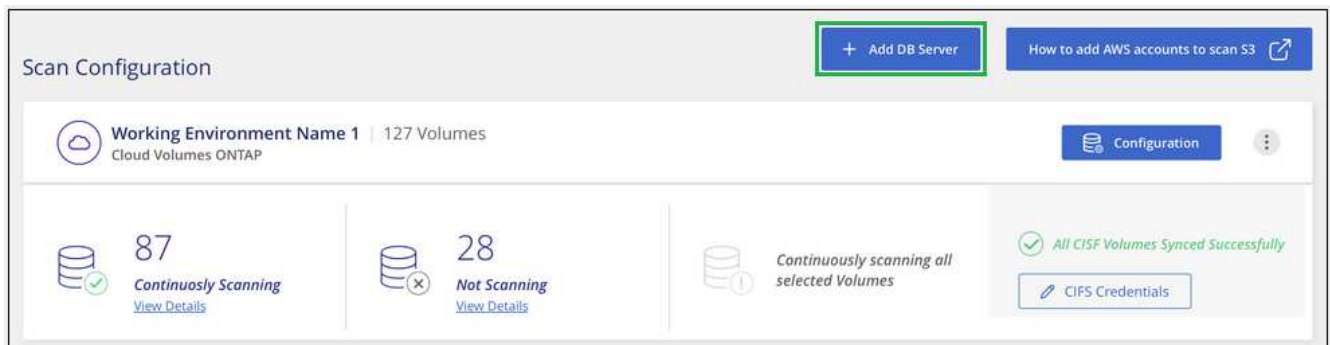
Nota: per MongoDB, è necessario un ruolo Admin di sola lettura.

Aggiunta del server database

Devi avere "[Ha già implementato un'istanza di Cloud Compliance in Cloud Manager](#)".

Aggiungere il server di database in cui risiedono gli schemi.

1. Dalla pagina *Scan Configuration*, fare clic sul pulsante **Add DB Server** (Aggiungi server DB).



2. Inserire le informazioni richieste per identificare il server di database.
 - a. Selezionare il tipo di database.
 - b. Immettere la porta e il nome host o l'indirizzo IP per la connessione al database.
 - c. Per i database Oracle, immettere il nome del servizio.
 - d. Inserire le credenziali in modo che Cloud Compliance possa accedere al server.
 - e. Fare clic su **Add DB Server** (Aggiungi server DB).

Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

Database

Database Type

Host Name or IP Address

Port

Service Name

Credentials

Username

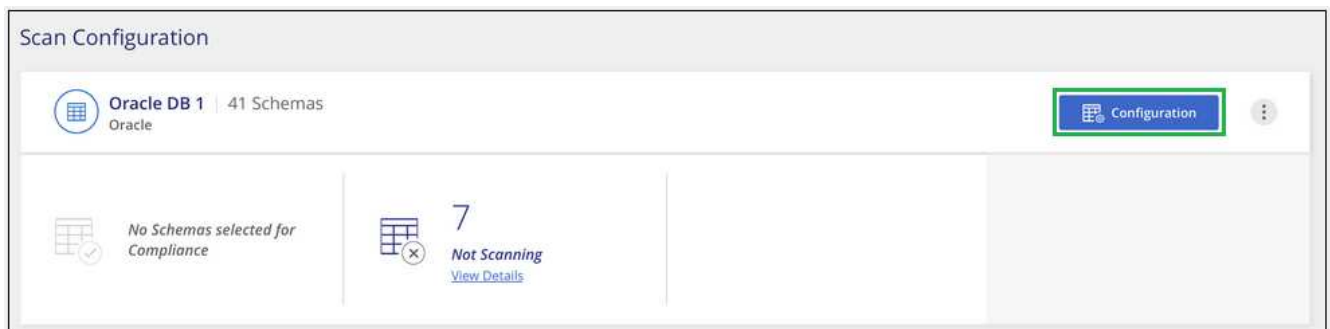
Password

Il database viene aggiunto all'elenco delle directory di lavoro.

Attivazione e disattivazione delle scansioni di compliance sugli schemi di database

È possibile interrompere o avviare la scansione degli schemi in qualsiasi momento.

1. Dalla pagina *Scan Configuration*, fare clic sul pulsante **Configuration** relativo al database che si desidera configurare.



2. Selezionare gli schemi da sottoporre a scansione spostando il dispositivo di scorrimento verso destra.


'Working Environment Name' Scan Configuration			
28/28 Schemas selected for compliance scan			
Compliance	Schema Name	Status	Required Action
<input type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials
<input checked="" type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

Risultato

Cloud Compliance inizia la scansione degli schemi di database abilitati. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

Rimozione di un database da Cloud Manager

Se non si desidera più eseguire la scansione di un determinato database, è possibile eliminarlo dall'interfaccia di Cloud Manager e interrompere tutte le scansioni.

Dalla pagina *Scan Configuration*, fare clic su  Nella riga del database, quindi fare clic su **Remove DB Server** (Rimuovi server DB).



Scansione on-premise dei dati ONTAP con conformità al cloud utilizzando SnapMirror

È possibile eseguire la scansione dei dati ONTAP on-premise con la conformità al cloud replicando i dati NFS o CIFS on-premise in un ambiente di lavoro Cloud Volumes ONTAP e abilitando quindi la conformità. La scansione dei dati direttamente da un ambiente di lavoro ONTAP on-premise non è supportata.

Devi avere "[Ha già implementato un'istanza di Cloud Compliance in Cloud Manager](#)".

Fasi

1. Da Cloud Manager, creare una relazione SnapMirror tra il cluster ONTAP on-premise e Cloud Volumes ONTAP.

- a. ["Scopri il cluster on-premise in Cloud Manager"](#).
 - b. ["Creare una replica SnapMirror tra il cluster ONTAP on-premise e Cloud Volumes ONTAP da Cloud Manager"](#).
2. Per i volumi DP creati dai volumi di origine SMB, dalla CLI ONTAP, configurare i volumi di destinazione SMB per l'accesso ai dati. (Non è necessario per i volumi NFS perché l'accesso ai dati viene attivato automaticamente tramite Cloud Compliance).
- a. ["Creare una condivisione SMB sul volume di destinazione"](#).
 - b. ["Applicare gli ACL appropriati alla condivisione SMB nel volume di destinazione"](#).
3. Da Cloud Manager, attivare la conformità cloud nell'ambiente di lavoro Cloud Volumes ONTAP che contiene i dati SnapMirror:
- a. Fare clic su **ambienti di lavoro**.
 - b. Selezionare l'ambiente di lavoro che contiene i dati SnapMirror e fare clic su **Enable Compliance** (attiva conformità).

["Fai clic qui per ricevere assistenza per abilitare la conformità al cloud su un sistema Cloud Volumes ONTAP"](#).

- c. Fare clic sul pulsante **Enable Access to DP Volumes** (Abilita accesso ai volumi DP) nella parte superiore della pagina *Scan Configuration* (Configurazione scansione).
- d. Attivare ciascun volume DP che si desidera sottoporre a scansione oppure utilizzare il controllo **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi) per abilitare tutti i volumi, inclusi tutti i volumi DP.

Vedere ["Scansione dei volumi di protezione dei dati"](#) Per ulteriori informazioni sulla scansione di volumi DP.

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.