# Sicurezza e crittografia dei dati

## Cloud Volumes ONTAP

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/it-it/storage-management-cloud-volumes-ontap/task-encrypting-volumes.html on February 13, 2026. Always check docs.netapp.com for the latest.

# Sommario


Sicurezza e crittografia dei dati . . . 1
- Crittografa i volumi su Cloud Volumes ONTAP con le soluzioni di crittografia NetApp . . . 1
- Gestisci le chiavi di crittografia Cloud Volumes ONTAP con AWS Key Management Service . . . 1
  - Configurazione . . . 1
- Gestisci le chiavi di crittografia Cloud Volumes ONTAP con Azure Key Vault . . . 2
  - Processo di configurazione . . . 3
- Gestisci le chiavi di crittografia Cloud Volumes ONTAP con Google Cloud KMS . . . 10
  - Configurazione . . . 11
  - Risoluzione dei problemi . . . 12
- Abilita le soluzioni di protezione ransomware NetApp per Cloud Volumes ONTAP . . . 12
  - Protezione dalle estensioni di file ransomware più comuni . . . 12
  - Protezione autonoma dal ransomware . . . 14
- Crea copie Snapshot a prova di manomissione dei file WORM su Cloud Volumes ONTAP . . . 15

# Sicurezza e crittografia dei dati

## Crittografa i volumi su Cloud Volumes ONTAP con le soluzioni di crittografia NetApp

Cloud Volumes ONTAP supporta NetApp Volume Encryption (NVE) e NetApp Aggregate Encryption (NAE). NVE e NAE sono soluzioni basate su software che consentono la crittografia dei dati a riposo dei volumi conforme allo standard FIPS 140-2. "Scopri di più su queste soluzioni di crittografia" .

Sia NVE che NAE sono supportati da un gestore di chiavi esterno.

] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[

## Gestisci le chiavi di crittografia Cloud Volumes ONTAP con AWS Key Management Service

Puoi usare"Servizio di gestione delle chiavi (KMS) di AWS" per proteggere le chiavi di crittografia ONTAP in un'applicazione distribuita su AWS.

La gestione delle chiavi con AWS KMS può essere abilitata tramite la CLI o l'API REST ONTAP .

Quando si utilizza il KMS, tenere presente che per impostazione predefinita viene utilizzato il LIF di un SVM di dati per comunicare con l'endpoint di gestione delle chiavi cloud. Per comunicare con i servizi di autenticazione di AWS viene utilizzata una rete di gestione dei nodi. Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

**Prima di iniziare**

- Cloud Volumes ONTAP deve eseguire la versione 9.12.0 o successiva
- È necessario aver installato la licenza Volume Encryption (VE) e
- È necessario aver installato la licenza Multi-tenant Encryption Key Management (MTEKM).
- Devi essere un amministratore del cluster o SVM
- Devi avere un abbonamento AWS attivo

È possibile configurare le chiavi solo per una SVM dati.

### Configurazione

**AWS**

1. Devi creare un"concessione" per la chiave AWS KMS che verrà utilizzata dal ruolo IAM che gestisce la crittografia. Il ruolo IAM deve includere una policy che consenta le seguenti operazioni:
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`Per creare una sovvenzione, fare riferimento a"Documentazione AWS" .

2. "Aggiungere un criterio al ruolo IAM appropriato."La politica dovrebbe sostenere l' `DescribeKey` , `Encrypt` , E `Decrypt` operazioni.

**Cloud Volumes ONTAP**

1. Passa al tuo ambiente Cloud Volumes ONTAP .
2. Passa al livello di privilegio avanzato:
   `set -privilege advanced`
3. Abilitare il gestore delle chiavi AWS:
   `security key-manager external aws enable -vserver` *`data_svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Quando richiesto, immettere la chiave segreta.
5. Verifica che AWS KMS sia stato configurato correttamente:
   `security key-manager external aws show -vserver` *`svm_name`*

# Gestisci le chiavi di crittografia Cloud Volumes ONTAP con Azure Key Vault

È possibile utilizzare Azure Key Vault (AKV) per proteggere le chiavi di crittografia ONTAP in un'applicazione distribuita in Azure. Fare riferimento al"Documentazione Microsoft" .

AKV può essere utilizzato per proteggere le chiavi NetApp Volume Encryption (NVE) solo per le SVM di dati. Per ulteriori informazioni, fare riferimento al "Documentazione ONTAP" .

La gestione delle chiavi con AKV può essere abilitata tramite la CLI o l'API REST ONTAP .

Quando si utilizza AKV, tenere presente che per impostazione predefinita viene utilizzato un LIF SVM dati per comunicare con l'endpoint di gestione delle chiavi cloud. Per comunicare con i servizi di autenticazione del provider cloud (login.microsoftonline.com) viene utilizzata una rete di gestione dei nodi. Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

**Prima di iniziare**

- Cloud Volumes ONTAP deve eseguire la versione 9.10.1 o successiva
- Licenza Volume Encryption (VE) installata (la licenza NetApp Volume Encryption viene installata automaticamente su ogni sistema Cloud Volumes ONTAP registrato presso il supporto NetApp )
- È necessario disporre di una licenza Multi-tenant Encryption Key Management (MT_EK_MGMT)
- Devi essere un amministratore del cluster o SVM
- Un abbonamento Azure attivo

**Limitazioni**

- AKV può essere configurato solo su un SVM dati
- NAE non può essere utilizzato con AKV. NAE richiede un server KMIP supportato esternamente.
- I nodi Cloud Volumes ONTAP interrogano AKV ogni 15 minuti per confermare l'accessibilità e la disponibilità delle chiavi. Questo periodo di polling non è configurabile e, dopo quattro errori consecutivi nel tentativo di polling (per un totale di 1 ora), i volumi vengono messi offline.

## Processo di configurazione

I passaggi descritti descrivono come registrare la configurazione di Cloud Volumes ONTAP con Azure e come creare un Azure Key Vault e le relative chiavi. Se hai già completato questi passaggi, assicurati di avere le impostazioni di configurazione corrette, in particolare inCreare un Azure Key Vault , e poi procedere aConfigurazione Cloud Volumes ONTAP .

- Registrazione dell'applicazione Azure
- Crea il segreto client di Azure
- Creare un Azure Key Vault
- Crea chiave di crittografia
- Creare un endpoint di Azure Active Directory (solo HA)
- Configurazione Cloud Volumes ONTAP

#### Registrazione dell'applicazione Azure

1. Devi prima registrare la tua applicazione nella sottoscrizione di Azure che desideri che Cloud Volumes ONTAP utilizzi per accedere ad Azure Key Vault. Nel portale di Azure, seleziona **Registrazioni app**.
2. Selezionare **Nuova registrazione**.
3. Fornisci un nome per la tua applicazione e seleziona un tipo di applicazione supportato. Per l'utilizzo di Azure Key Vault è sufficiente il tenant singolo predefinito. Seleziona **Registrati**.
4. Nella finestra Panoramica di Azure, seleziona l'applicazione che hai registrato. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)** in una posizione sicura. Saranno richiesti più avanti nel processo di registrazione.

#### Crea il segreto client di Azure

1. Nel portale di Azure per la registrazione dell'app Azure Key Vault, seleziona il riquadro **Certificati e segreti**.
2. Seleziona **Nuovo segreto client**. Inserisci un nome significativo per il tuo segreto client. NetApp consiglia un periodo di scadenza di 24 mesi; tuttavia, le tue specifiche policy di governance del cloud potrebbero richiedere un'impostazione diversa.
3. Fare clic su **Aggiungi** per creare il segreto client. Copiare la stringa segreta elencata nella colonna **Valore** e memorizzarla in un luogo sicuro per un utilizzo successivo inConfigurazione Cloud Volumes ONTAP . Il valore segreto non verrà più visualizzato dopo aver abbandonato la pagina.

#### Creare un Azure Key Vault

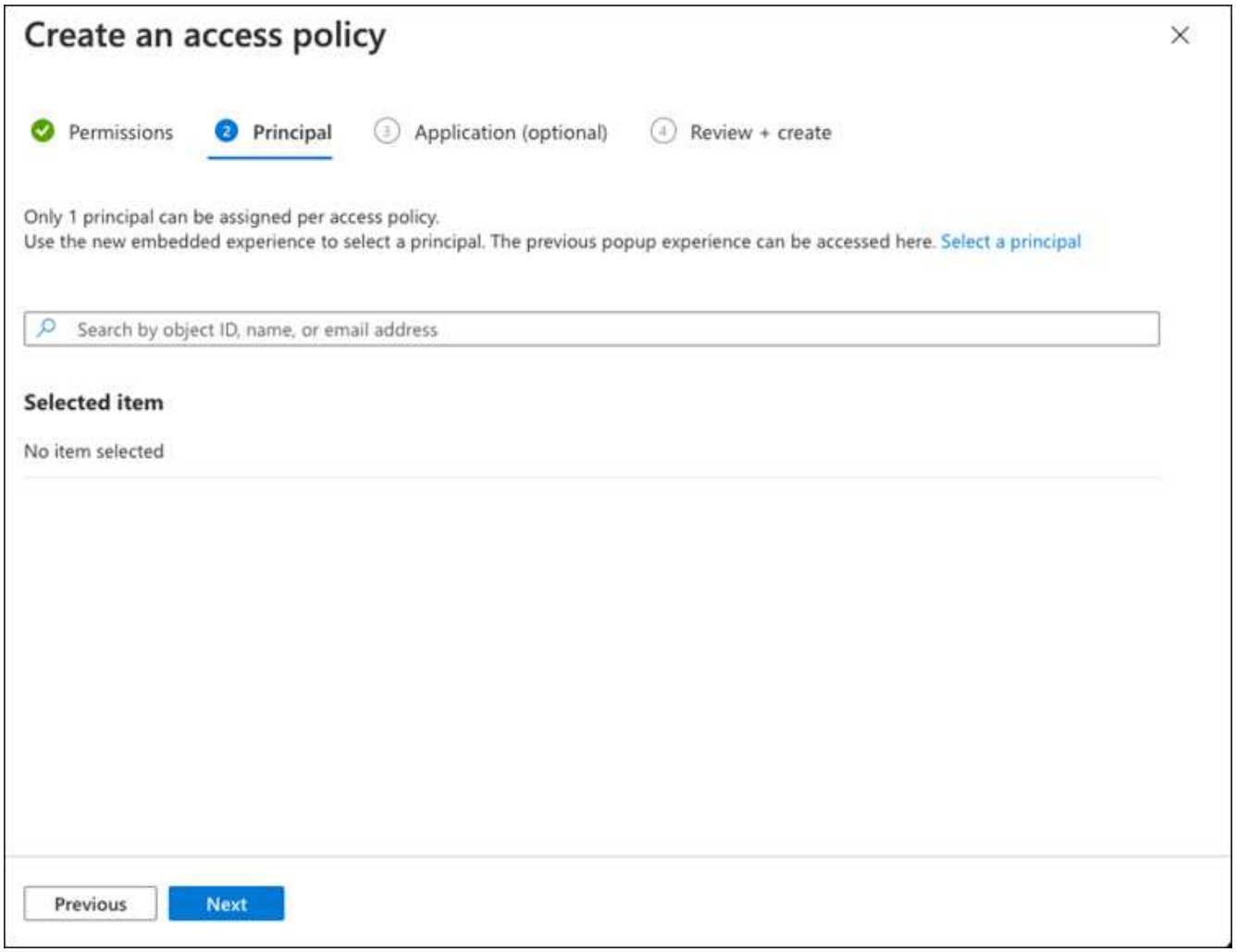
1. Se disponi di un Azure Key Vault esistente, puoi connetterlo alla configurazione Cloud Volumes ONTAP ; tuttavia, devi adattare i criteri di accesso alle impostazioni in questo processo.
2. Nel portale di Azure, passare alla sezione **Key Vault**.
3. Fare clic su **+Crea** e immettere le informazioni richieste, tra cui gruppo di risorse, regione e livello di prezzo. Inoltre, immettere il numero di giorni per cui conservare i vault eliminati e selezionare **Abilita protezione di eliminazione** sul vault delle chiavi.
4. Selezionare **Avanti** per scegliere una policy di accesso.
5. Selezionare le seguenti opzioni:
   a. In **Configurazione di accesso**, seleziona **Criterio di accesso al Vault**.
   b. In **Accesso alle risorse**, seleziona **Azure Disk Encryption per la crittografia del volume**.
6. Selezionare **+Crea** per aggiungere un criterio di accesso.

7. In **Configura da un modello**, fai clic sul menu a discesa e seleziona il modello **Gestione chiavi, segreti e certificati**.
8. Selezionare ciascuno dei menu a discesa delle autorizzazioni (chiave, segreto, certificato), quindi **Seleziona tutto** nella parte superiore dell'elenco del menu per selezionare tutte le autorizzazioni disponibili. Dovresti avere:
    - **Autorizzazioni chiave**: 20 selezionate
    - **Autorizzazioni segrete**: 8 selezionate
    - **Autorizzazioni del certificato**: 16 selezionate

Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. Fare clic su **Avanti** per selezionare l'applicazione Azure registrata **Principale** creata inRegistrazione dell'applicazione Azure . Selezionare **Avanti**.

   È possibile assegnare un solo mandante a ogni polizza.




10. Fare clic due volte su **Avanti** fino ad arrivare a **Revisiona e crea**. Quindi, fai clic su **Crea**.
11. Selezionare **Avanti** per passare alle opzioni di **Rete**.
12. Selezionare il metodo di accesso alla rete appropriato oppure selezionare **Tutte le reti** e **Revisiona + Crea** per creare il vault delle chiavi. (Il metodo di accesso alla rete può essere prescritto da una policy di governance o dal team di sicurezza cloud aziendale.)
13. Registra l'URI del Key Vault: nel Key Vault creato, vai al menu Panoramica e copia l'**URI del Vault** dalla colonna di destra. Ti servirà per un passaggio successivo.

**Crea chiave di crittografia**

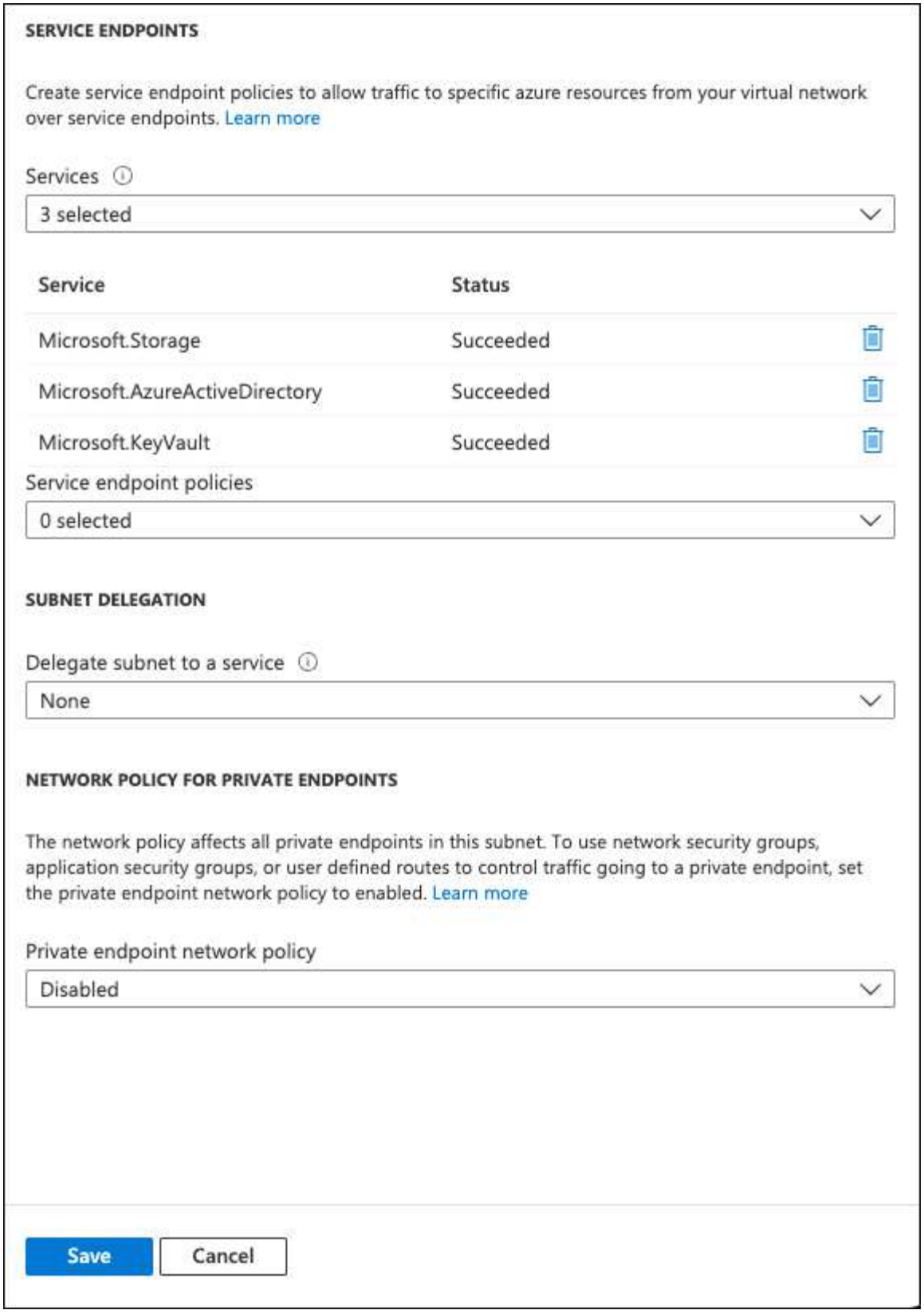
1. Nel menu del Key Vault creato per Cloud Volumes ONTAP, vai all'opzione **Chiavi**.
2. Selezionare **Genera/importa** per creare una nuova chiave.
3. Lasciare l'opzione predefinita impostata su **Genera**.
4. Fornire le seguenti informazioni:
   - Nome della chiave di crittografia

- Tipo di chiave: RSA
- Dimensione chiave RSA: 2048
- Abilitato: Sì

5. Selezionare **Crea** per creare la chiave di crittografia.
6. Torna al menu **Chiavi** e seleziona la chiave appena creata.
7. Selezionare l'ID chiave in **Versione corrente** per visualizzare le proprietà della chiave.
8. Individuare il campo **Identificatore chiave**. Copia l'URI fino alla stringa esadecimale esclusa.

**Creare un endpoint di Azure Active Directory (solo HA)**

1. Questo processo è necessario solo se si sta configurando Azure Key Vault per un sistema HA Cloud Volumes ONTAP .
2. Nel portale di Azure, passare a **Reti virtuali**.
3. Selezionare la rete virtuale in cui è stato distribuito il sistema Cloud Volumes ONTAP e selezionare il menu **Sottoreti** sul lato sinistro della pagina.
4. Seleziona dall'elenco il nome della subnet per la distribuzione Cloud Volumes ONTAP .
5. Passare all'intestazione **Endpoint di servizio**. Nel menu a discesa, seleziona quanto segue:
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage** (facoltativo)




6. Seleziona **Salva** per acquisire le tue impostazioni.

**Configurazione Cloud Volumes ONTAP**

1. Connettiti al LIF di gestione del cluster con il tuo client SSH preferito.
2. Accedi alla modalità privilegio avanzata in ONTAP:

`set advanced -con off`

3. Identificare l'SVM dati desiderato e verificarne la configurazione DNS:
`vserver services name-service dns show`

   a. Se esiste una voce DNS per l'SVM dati desiderato e contiene una voce per il DNS di Azure, non è richiesta alcuna azione. In caso contrario, aggiungere una voce del server DNS per l'SVM dati che punti al DNS di Azure, al DNS privato o al server locale. Dovrebbe corrispondere alla voce per l'SVM di amministrazione del cluster:
   `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. Verificare che il servizio DNS sia stato creato per i dati SVM:
   `vserver services name-service dns show`

4. Abilita Azure Key Vault utilizzando l'ID client e l'ID tenant salvati dopo la registrazione dell'applicazione:
`security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   > IL `_full_key_URI` il valore deve utilizzare il `<https:// <key vault host name>/keys/<key label>` formato.

5. Dopo aver abilitato correttamente Azure Key Vault, immettere `client secret value` quando richiesto.

6. Controllare lo stato del gestore delle chiavi:
`security key-manager external azure check` L'output sarà simile al seguente:

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

Se il `service_reachability` lo stato non è `OK` , l'SVM non riesce a raggiungere il servizio Azure Key Vault con tutta la connettività e le autorizzazioni richieste. Assicurati che i criteri di rete e il routing di Azure non impediscano alla tua rete virtuale privata di raggiungere l'endpoint pubblico di Azure Key Vault. In tal caso, valutare l'utilizzo di un endpoint privato di Azure per accedere al Key Vault dall'interno della rete virtuale. Potrebbe anche essere necessario aggiungere una voce host statica sulla SVM per risolvere

l'indirizzo IP privato per l'endpoint.

IL `kms_wrapped_key_status` riferirà `UNKNOWN` nella configurazione iniziale. Il suo stato cambierà in `OK` dopo che il primo volume è stato crittografato.

7. FACOLTATIVO: creare un volume di prova per verificare la funzionalità di NVE.

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   Se configurato correttamente, Cloud Volumes ONTAP creerà automaticamente il volume e abiliterà la crittografia del volume.

8. Verificare che il volume sia stato creato e crittografato correttamente. Se lo è, il `-is-encrypted` il parametro verrà visualizzato come `true` .
   `vol show -vserver SVM_name -fields is-encrypted`
9. Facoltativo: se si desidera aggiornare le credenziali sul certificato di autenticazione di Azure Key Vault, utilizzare il comando seguente:
   `security key-manager external azure update-credentials -vserver v1 -authentication-method certificate`

**Link correlati**

- "Configurare Cloud Volumes ONTAP per utilizzare una chiave gestita dal cliente in Azure"
- "Documentazione di Microsoft Azure: Informazioni su Azure Key Vault"
- "Guida di riferimento ai comandi ONTAP"

# Gestisci le chiavi di crittografia Cloud Volumes ONTAP con Google Cloud KMS

Puoi usare"Servizio di gestione delle chiavi di Google Cloud Platform (Cloud KMS)" per proteggere le chiavi di crittografia Cloud Volumes ONTAP in un'applicazione distribuita su Google Cloud Platform.

La gestione delle chiavi con Cloud KMS può essere abilitata tramite ONTAP CLI o ONTAP REST API.

Quando si utilizza Cloud KMS, tenere presente che per impostazione predefinita viene utilizzato il LIF di un SVM di dati per comunicare con l'endpoint di gestione delle chiavi cloud. Per comunicare con i servizi di autenticazione del provider cloud (oauth2.googleapis.com) viene utilizzata una rete di gestione dei nodi. Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

**Prima di iniziare**

- Il tuo sistema dovrebbe eseguire Cloud Volumes ONTAP 9.10.1 o versione successiva
- È necessario utilizzare una SVM dati. Cloud KMS può essere configurato solo su una SVM dati.
- Devi essere un amministratore del cluster o SVM
- La licenza Volume Encryption (VE) deve essere installata sull'SVM
- A partire da Cloud Volumes ONTAP 9.12.1 GA, è necessario installare anche la licenza MTEKM (Multi-tenant Encryption Key Management)

- È richiesto un abbonamento attivo a Google Cloud Platform

## Configurazione

### Google Cloud

1. Nel tuo ambiente Google Cloud,"creare un portachiavi GCP simmetrico e una chiave" .
2. Assegna un ruolo personalizzato alla chiave Cloud KMS e all'account di servizio Cloud Volumes ONTAP .
   a. Crea il ruolo personalizzato:

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

   b. Assegna il ruolo personalizzato che hai creato:
   `gcloud kms keys add-iam-policy-binding` *`key_name`* `--keyring` *`key_ring_name`* `--location` *`key_location`* `--member serviceAccount:_service_account_Name_ --role projects/`*`customer_project_id`*`/roles/kmsCustomRole`

> Se utilizzi Cloud Volumes ONTAP 9.13.0 o versione successiva, non è necessario creare un ruolo personalizzato. È possibile assegnare il predefinito[`cloudkms.cryptoKeyEncrypterDecrypter` ^] ruolo.

3. Scarica la chiave JSON dell'account di servizio:
   `gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

### Cloud Volumes ONTAP

1. Connettiti al LIF di gestione del cluster con il tuo client SSH preferito.
2. Passa al livello di privilegio avanzato:
   `set -privilege advanced`
3. Creare un DNS per i dati SVM.
   `dns create -domains c.<`*`project`*`>.internal -name-servers` *`server_address`* `-vserver` *`SVM_name`*
4. Crea voce CMEK:
   `security key-manager external gcp enable -vserver` *`SVM_name`* `-project-id` *`project`* `-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*

5. Quando richiesto, inserisci la chiave JSON dell'account di servizio dal tuo account GCP.
6. Conferma che il processo abilitato è riuscito:
`security key-manager external gcp check -vserver svm_name`
7. FACOLTATIVO: creare un volume per testare la crittografia `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

### Risoluzione dei problemi

Se hai bisogno di risolvere un problema, puoi seguire i log REST API non elaborati negli ultimi due passaggi sopra:

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

# Abilita le soluzioni di protezione ransomware NetApp per Cloud Volumes ONTAP

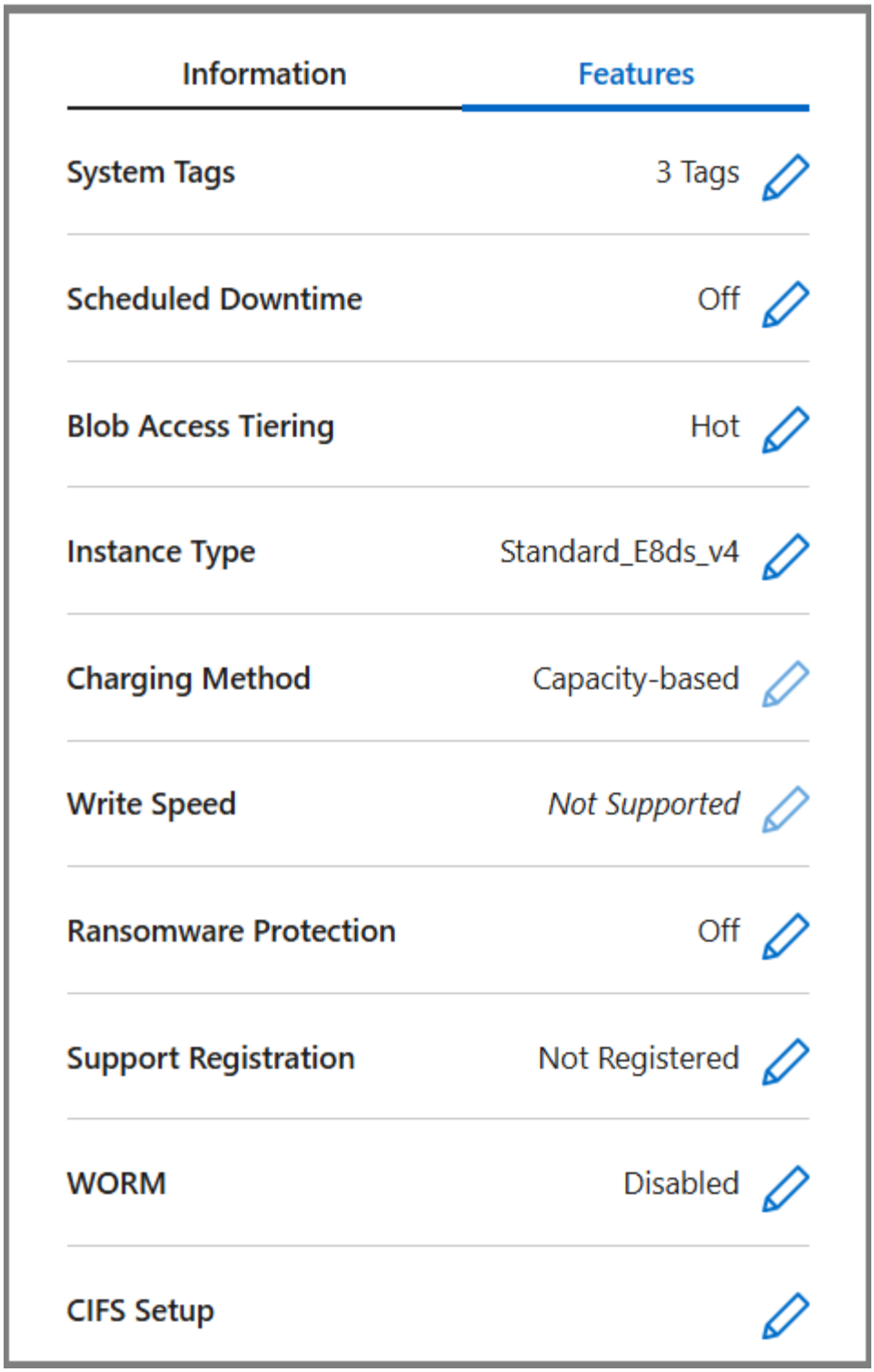
Gli attacchi ransomware possono costare alle aziende tempo, risorse e reputazione. NetApp Console consente di implementare due soluzioni NetApp contro il ransomware: protezione dalle estensioni di file ransomware più comuni e protezione autonoma dal ransomware (ARP). Queste soluzioni forniscono strumenti efficaci per la visibilità, il rilevamento e la correzione.

### Protezione dalle estensioni di file ransomware più comuni

Disponibile sulla Console, l'impostazione Protezione ransomware consente di utilizzare la funzionalità ONTAP FPolicy per proteggersi dai comuni tipi di estensione di file ransomware.

**Passi**

1. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema Cloud Volumes ONTAP configurato per utilizzare la protezione ransomware.
2. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **Protezione ransomware**.




3. Implementare la soluzione NetApp contro il ransomware:

   a. Fare clic su **Attiva criterio snapshot** se si dispone di volumi per i quali non è abilitato un criterio snapshot.

      La tecnologia NetApp Snapshot offre la migliore soluzione del settore per la remediation del ransomware. La chiave per un ripristino riuscito è il ripristino da backup non infetti. Le copie snapshot sono di sola lettura, il che impedisce la corruzione da parte del ransomware. Possono anche fornire la granularità necessaria per creare immagini di una singola copia di file o una soluzione completa di disaster recovery.

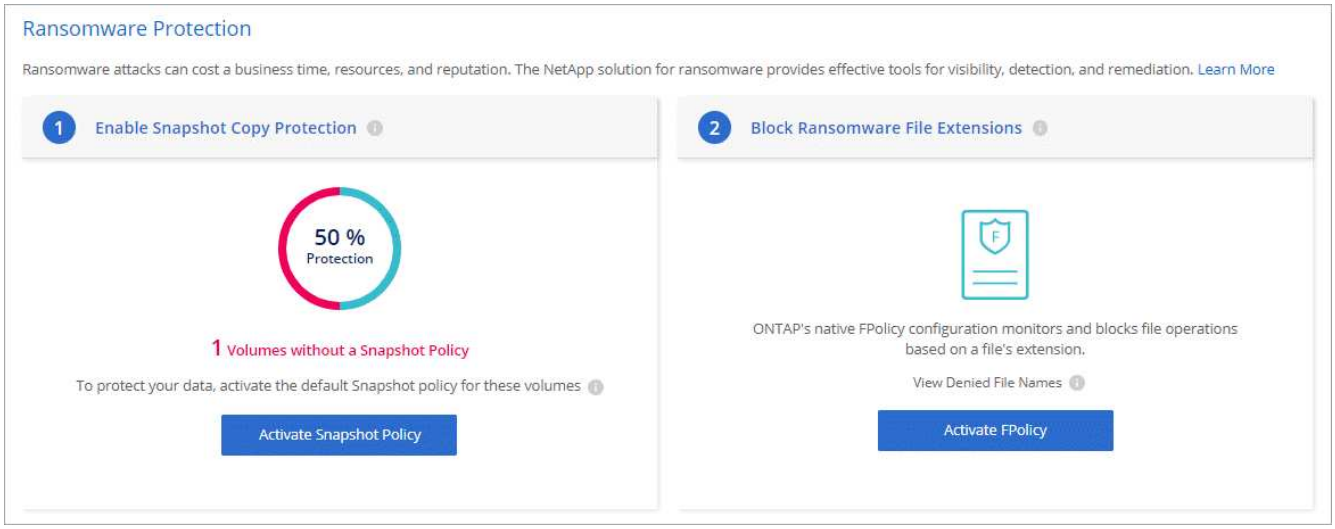
b. Fare clic su **Attiva FPolicy** per abilitare la soluzione FPolicy di ONTAP, che può bloccare le operazioni sui file in base all'estensione del file.

   Questa soluzione preventiva migliora la protezione dagli attacchi ransomware bloccando i tipi di file ransomware più comuni.

   L'ambito FPolicy predefinito blocca i file con le seguenti estensioni:

   micro, crittografato, bloccato, crittografato, criptato, critto, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, buono, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre

   Questo ambito viene creato quando si attiva FPolicy su Cloud Volumes ONTAP. L'elenco si basa sui tipi di file ransomware più comuni. È possibile personalizzare le estensioni dei file bloccati utilizzando i comandi *vserver fpolicy policy scope* dalla CLI di Cloud Volumes ONTAP .




## Protezione autonoma dal ransomware

Cloud Volumes ONTAP supporta la funzionalità Autonomous Ransomware Protection (ARP), che esegue analisi sui carichi di lavoro per rilevare in modo proattivo e avvisare in caso di attività anomale che potrebbero indicare un attacco ransomware.

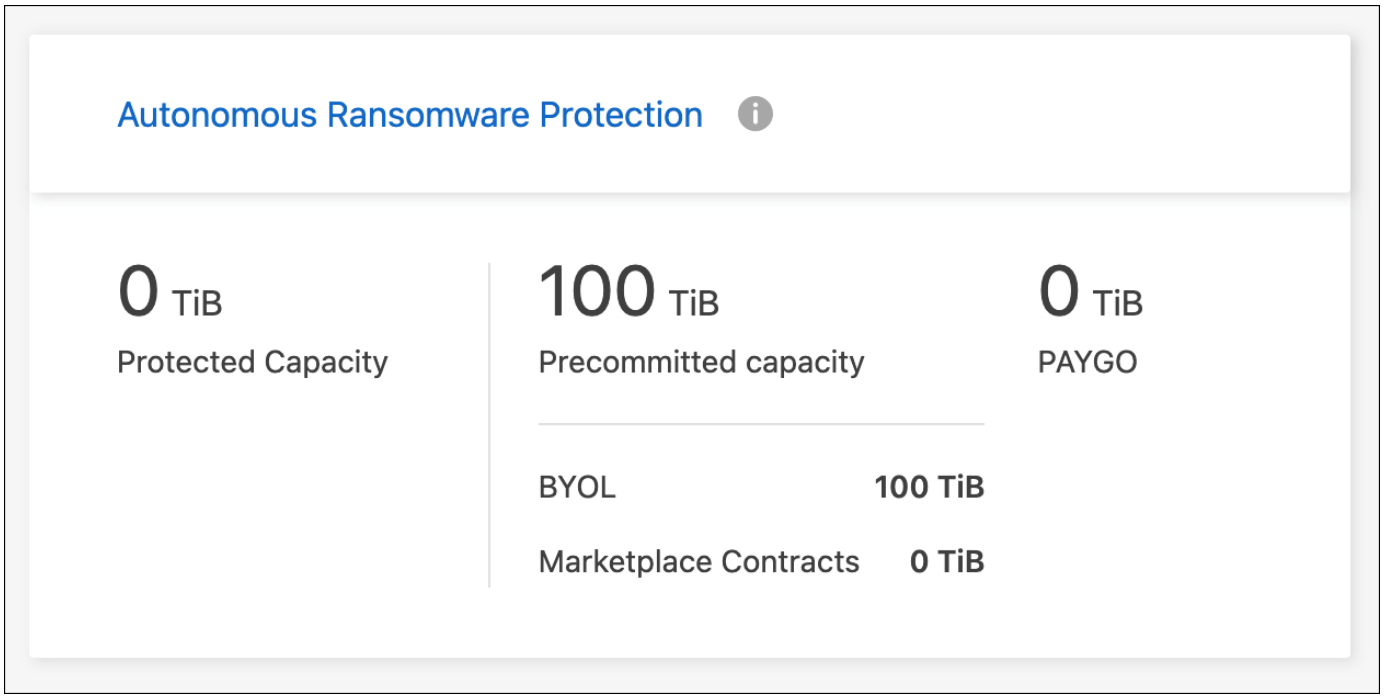
Separato dalle protezioni delle estensioni dei file fornite tramite "impostazione di protezione ransomware" , la funzionalità ARP utilizza l'analisi del carico di lavoro per avvisare l'utente di potenziali attacchi in base alle "attività anomale" rilevate. Per una protezione ransomware completa è possibile utilizzare insieme sia l'impostazione di protezione ransomware sia la funzionalità ARP.

La funzionalità ARP è disponibile per l'uso con la licenza BYOL (Bring Your Own License) e gli abbonamenti Marketplace per le tue licenze senza costi aggiuntivi.

I volumi abilitati per ARP hanno uno stato designato di "Modalità di apprendimento" o "Attivo".

La configurazione di ARP per i volumi viene eseguita tramite ONTAP System Manager e ONTAP CLI.

Per ulteriori informazioni su come abilitare ARP con ONTAP System Manager e ONTAP CLI, fare riferimento a "Documentazione ONTAP : Abilita la protezione autonoma dal ransomware" .




# Crea copie Snapshot a prova di manomissione dei file WORM su Cloud Volumes ONTAP

È possibile creare copie Snapshot a prova di manomissione di file WORM (write once, read many) su un sistema Cloud Volumes ONTAP e conservare gli snapshot in forma non modificata per un periodo di conservazione specifico. Questa funzionalità è basata sulla tecnologia SnapLock e fornisce un ulteriore livello di protezione e conformità dei dati.

**Prima di iniziare**

Assicurarsi che il volume utilizzato per creare copie Snapshot sia un volume SnapLock . Per informazioni sull'abilitazione della protezione SnapLock sui volumi, fare riferimento a "Documentazione ONTAP : Configurare SnapLock" .

**Passi**

1. Crea copie Snapshot dal volume SnapLock . Per informazioni sulla creazione di copie Snapshot tramite CLI o System Manager, fare riferimento a "Documentazione ONTAP : Panoramica sulla gestione delle copie Snapshot locali" .

   Le copie Snapshot ereditano le proprietà WORM del volume, rendendole a prova di manomissione. La tecnologia SnapLock di base garantisce che uno snapshot rimanga protetto da modifiche ed eliminazioni fino alla scadenza del periodo di conservazione specificato.

2. È possibile modificare il periodo di conservazione se è necessario modificare questi snapshot. Per informazioni fare riferimento al "Documentazione ONTAP : Imposta il tempo di conservazione" .

> Anche se una copia Snapshot è protetta per un periodo di conservazione specifico, il volume di origine può essere eliminato da un amministratore del cluster, poiché l'archiviazione WORM in Cloud Volumes ONTAP funziona secondo un modello di "amministratore di archiviazione attendibile". Inoltre, un amministratore cloud fidato può eliminare i dati WORM agendo sulle risorse di archiviazione cloud.

**Link correlati**

- Per ulteriori informazioni su WORM, fare riferimento a"Scopri di più sullo storage WORM su Cloud Volumes ONTAP" .
- Per informazioni sulla ricarica dei volumi SnapLock , fare riferimento a"Licenze e addebiti in Cloud Volumes ONTAP" .

**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.