



# **Sicurezza**

## ONTAP automation

NetApp  
January 18, 2026

This PDF was generated from [https://docs.netapp.com/it-it/ontap-automation/workflows/wf\\_sec\\_list\\_accounts.html](https://docs.netapp.com/it-it/ontap-automation/workflows/wf_sec_list_accounts.html) on January 18, 2026. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Sommario

Sicurezza .....	1
Account .....	1
Elencare gli account utilizzando l'API REST ONTAP .....	1
Certificati e chiavi .....	3
Elencare i certificati installati utilizzando l'API REST ONTAP .....	3
Installare un certificato utilizzando l'API REST ONTAP .....	5
RBAC .....	6
Preparati a utilizzare RBAC usando l'API REST di ONTAP .....	6
Creare ruoli .....	7
Creare un utente con un ruolo utilizzando l'API REST di ONTAP .....	11

# Sicurezza

## Account

### Elencare gli account utilizzando l'API REST ONTAP

È possibile recuperare un elenco degli account. Questa operazione può essere eseguita per valutare l'ambiente di protezione o prima di creare un nuovo account.

#### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/security/accounts

#### Tipo di elaborazione

Sincrono

#### Esempio di arricciamento

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

## Esempio di output JSON

```
{  
  "records": [  
    {  
      "owner": {  
        "uuid": "642573a8-9d14-11ee-9330-005056aed3de",  
        "name": "vs0",  
        "_links": {  
          "self": {  
            "href": "/api/svm/svms/642573a8-9d14-11ee-9330-  
005056aed3de"  
          }  
        }  
      },  
      "name": "vsadmin",  
      "_links": {  
        "self": {  
          "href": "/api/security/accounts/642573a8-9d14-11ee-9330-  
005056aed3de/vsadmin"  
        }  
      }  
    },  
    {  
      "owner": {  
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",  
        "name": "sti214nscluster-1"  
      },  
      "name": "admin",  
      "_links": {  
        "self": {  
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-  
005056aed3de/admin"  
        }  
      }  
    },  
    {  
      "owner": {  
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",  
        "name": "sti214nscluster-1"  
      },  
      "name": "autosupport",  
      "_links": {  
        "self": {  
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-  
005056aed3de/autosupport"  
        }  
      }  
    }  
  ]  
}
```

```

        }
    }
}

],
"num_records": 3,
"_links": {
    "self": {
        "href": "/api/security/accounts"
    }
}
}
}

```

## Certificati e chiavi

### Elencare i certificati installati utilizzando l'API REST ONTAP

È possibile elencare i certificati installati nel cluster ONTAP. È possibile eseguire questa operazione per verificare se un determinato certificato è disponibile o per ottenere l'ID di un certificato specifico.

#### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/sicurezza/certificati

#### Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
max_records	Query	No	Specificare il numero di record che si desidera restituire.

#### Esempio Curl: Restituire tre certificati

```

curl --request GET \
--location "https://$FQDN_IP/api/security/certificates?max_records=3" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"

```

## Esempio di output JSON

```
{  
  "records": [  
    {  
      "uuid": "dad822c2-573c-11ee-a310-005056aecc29",  
      "name": "vs0_17866DB5C933E2EA",  
      "_links": {  
        "self": {  
          "href": "/api/security/certificates/dad822c2-573c-11ee-a310-005056aecc29"  
        }  
      }  
    },  
    {  
      "uuid": "7d8e5570-573c-11ee-a310-005056aecc29",  
      "name": "BuypassClass3RootCA",  
      "_links": {  
        "self": {  
          "href": "/api/security/certificates/7d8e5570-573c-11ee-a310-005056aecc29"  
        }  
      }  
    },  
    {  
      "uuid": "7dbb2191-573c-11ee-a310-005056aecc29",  
      "name": "EntrustRootCertificationAuthority",  
      "_links": {  
        "self": {  
          "href": "/api/security/certificates/7dbb2191-573c-11ee-a310-005056aecc29"  
        }  
      }  
    }  
  ],  
  "num_records": 3,  
  "_links": {  
    "self": {  
      "href": "/api/security/certificates?max_records=3"  
    },  
    "next": {  
      "href": "/api/security/certificates?start.svm_id=sti214nscluster-1&start.uuid=7dbb2191-573c-11ee-a310-005056aecc29&max_records=3"  
    }  
  }  
}
```

## Installare un certificato utilizzando l'API REST ONTAP

Puoi installare un certificato X,509 firmato nel cluster ONTAP. Questa operazione può essere eseguita durante la configurazione di una funzione o di un protocollo ONTAP che richiede un'autenticazione avanzata.

### Prima di iniziare

È necessario disporre del certificato che si desidera installare. Assicurarsi inoltre che tutti i certificati intermedi siano installati secondo necessità.



Prima di utilizzare gli esempi di input JSON riportati di seguito, assicurarsi di aggiornare `public_certificate` con il certificato dell'ambiente.

### Passaggio 1: Installazione del certificato

È possibile eseguire una chiamata API per installare il certificato.

#### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/sicurezza/certificati

#### Esempio Curl: Installare un certificato CA principale a livello di cluster

```
curl --request POST \
--location "https://$FQDN_IP/api/security/certificates" \
--include \
--header "Content-Type: application/json" \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## Esempio di input JSON

```
{  
  "type": "server_ca",  
  "public_certificate":  
  "-----BEGIN CERTIFICATE-----  
MIID0TCCArkCFGYdznvTVvay1VZPNfy4yCCyPph6MA0GCSqGSIB3DQEBCwUAMIGk  
MQswCQYDVQQGEwJVUzELMAkGA1UECAwCTkMxDAAKBgNVBAcMA1JUUDEWMBQGA1UE  
CgwNT05UQVAgRXhhbXBsZTETMBEGA1UECwwKT05UQVAgOS4xNDEcMBoGA1UEAwT  
Ki5vbnRhcC1leGFTcGx1LmNvbTEvMC0GCSqGSIB3DQEJARYgZGF2aWQucGV0ZXJz  
b25Ab250YXAtZXhhbXBsZS5jb20wHhcNMjMxMDA1MTUyOTE4WhcNMjQxMDA0MTUy  
OTE4WjCBpDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQHDANSFAX  
FjAUBgNVBAoMDU9OVEFQIEV4YW1wbGUxEzARBgNVBAsMCK9OVEFQIDkuMTQxHDAa  
BgNVBAMMeYOUb250YXAtZXhhbXBsZS5jb20xLzAtBggkhkiG9w0BCQEwigRhdmlk  
LnBldGVyc29uQG9udGFwLWV4YW1wbGUuY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOC  
AQ8AMIIIBCgKCAQEAxQgy8mhblJhkf0D/MBodpzb0aSp2jGbWJ+Zv2G8BXkp1762  
dPHRkv1hnx9JvwkK4Dba05GiCiD5t3gjH/jUQMSFb+VwDbVmubVFnXjkm/4Q7sea  
tMTA/ZpQdZbQFZ5RKtdWz7dzzPYEl2x8Q1Jc8Kh7NxERNMtgpGWZZn7mfXKYr4O  
N/+vgahIhDibS8YK5rf1w6bfmrik9E2D+PEab9DX/1DL5RX4tZ1H20kyN2UxoBR6  
Fq716n1Hi/5yR0Oi1xStN6s07EPoGak+KS1K41q+EciKRo0bP4mEQp8WMjJuiTkb  
5MmeYoIpWEUgJK7S0M6Tp/3bTh2CST3AWxiNxQIDAQABMA0GCSqGSIB3DQEBCwUA  
A4IBAQABfBqOuROmYxdfrj93OyIiRoDcoMzvo8cHGNUsuhn1BDnL2O3qhWEs97s0  
mIy6zFMGnyNYa0t4i1cFsGDKP/JuljmYHjvv+21HWnxHjTo7AOQCnXmQH5swoDbf  
o1Vjqz8Oxz+PRJ+PA3dF5/8zqaAR6QreAN/iFR++6nUqlsbbM7w03tthBVMgo/h1  
E9I2jVOZsqMFujm2CYfMs4XkZtrYmN6nZA8JcUpDjIWcAVbQYurMnna9r42oS3GB  
WB/FE9n+P+FFJyHJ93KGcCXbH5RF2pi3wLlHilbvVuCjLRrhJ8U20I5mZoiXvABC  
IpYuBcuKXLwAarhDEacXttVjC+Bq  
-----END CERTIFICATE-----"  
}
```

## Passaggio 2: Verificare che il certificato sia stato installato

Eseguire il flusso di lavoro "["Elencare i certificati installati"](#)" e verificare che il certificato sia disponibile.

## RBAC

### Preparati a utilizzare RBAC usando l'API REST di ONTAP

Puoi utilizzare la funzionalità RBAC di ONTAP in diversi modi a seconda dell'ambiente. In questa sezione vengono presentati alcuni scenari comuni come flussi di lavoro. In ogni caso, l'attenzione è rivolta a uno specifico obiettivo amministrativo e di protezione.

Prima di creare ruoli e assegnare un ruolo a un account utente ONTAP, è necessario prepararsi esaminando i principali requisiti e le opzioni di protezione presentati di seguito. Inoltre, verificare i concetti generali del flusso di lavoro all'indirizzo "["Preparati a utilizzare i flussi di lavoro"](#)".

### Quale versione di ONTAP stai utilizzando?

La release ONTAP determina quali endpoint REST e le funzionalità RBAC sono disponibili.

### **Identificare le risorse protette e l'ambito**

È necessario identificare le risorse o i comandi da proteggere e l'ambito (cluster o SVM).

### **Quale accesso deve avere l'utente?**

Dopo aver identificato le risorse e l'ambito, è necessario determinare il livello di accesso da concedere.

### **In che modo gli utenti accedono a ONTAP?**

L'utente può accedere a ONTAP tramite l'API REST o CLI o entrambi.

### **Uno dei ruoli integrati è sufficiente o è necessario un ruolo personalizzato?**

È più conveniente utilizzare un ruolo integrato esistente, ma è possibile creare un nuovo ruolo personalizzato, se necessario.

### **Che tipo di ruolo è necessario?**

In base ai requisiti di sicurezza e all'accesso a ONTAP, è necessario scegliere se creare un ruolo REST o tradizionale.

## **Creare ruoli**

### **Limita l'accesso alle operazioni sul volume delle SVM utilizzando l'API REST ONTAP**

Puoi definire un ruolo per limitare l'amministrazione del volume storage all'interno di una SVM.

#### **Questo flusso di lavoro**

Viene dapprima creato un ruolo tradizionale per consentire inizialmente l'accesso a tutte le principali funzioni di amministrazione dei volumi, ad eccezione del cloning. Il ruolo viene definito con le seguenti caratteristiche:

- È in grado di eseguire tutte le operazioni dei volumi CRUD, tra cui Get, create, Modify ed Delete
- Impossibile creare un clone del volume

È quindi possibile aggiornare il ruolo in base alle esigenze. In questo flusso di lavoro, il ruolo viene modificato nel secondo passaggio per consentire all'utente di creare un clone del volume.

#### **Fase 1: Creare il ruolo**

Puoi emettere una chiamata API per creare il ruolo RBAC.

#### **Metodo HTTP ed endpoint**

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

## Esempio di arricciamento

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## Esempio di input JSON

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    { "path": "volume create", "access": "all" },
    { "path": "volume delete", "access": "all" }
  ]
}
```

## Passaggio 2: Aggiornare il ruolo

È possibile eseguire una chiamata API per aggiornare il ruolo esistente.

### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

### Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
\$SVM_ID	Percorso	Sì	UUID della SVM che contiene la definizione del ruolo.
\$NOME_RUOLO	Percorso	Sì	Nome del ruolo all'interno della SVM da aggiornare.

## Esempio di arricciamento

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## Esempio di input JSON

```
{
  "path": "volume clone",
  "access": "all"
}
```

## Attivare l'amministrazione della protezione dei dati utilizzando l'API REST ONTAP

Puoi fornire a un utente funzionalità di protezione dei dati limitate.

### Questo flusso di lavoro

Il ruolo tradizionale creato viene definito con le seguenti caratteristiche:

- Possibilità di creare ed eliminare snapshot e aggiornare le relazioni di SnapMirror
- Impossibile creare o modificare oggetti di livello superiore come volumi o SVM

### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

## Esempio di arricciamento

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## Esempio di input JSON

```
{  
  "name": "role1",  
  "owner": {  
    "name": "cluster-1",  
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    {"path": "volume snapshot create", "access": "all"},  
    {"path": "volume snapshot delete", "access": "all"},  
    {"path": "volume show", "access": "readonly"},  
    {"path": "vserver show", "access": "readonly"},  
    {"path": "snapmirror show", "access": "readonly"},  
    {"path": "snapmirror update", "access": "all"}  
  ]  
}
```

## Consentire la generazione di report ONTAP utilizzando l'API REST ONTAP

È possibile creare un ruolo REST per fornire agli utenti la possibilità di generare report ONTAP.

### Questo flusso di lavoro

Il ruolo creato viene definito con le seguenti caratteristiche:

- In grado di recuperare tutte le informazioni relative a capacità e performance (ad esempio volume, qtree, LUN, aggregati, nodo, E relazioni SnapMirror)
- Impossibile creare o modificare oggetti di livello superiore (ad esempio volumi o SVM)

### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

## Esempio di arricciamento

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

## Esempio di input JSON

```
{  
  "name": "rest_role1",  
  "owner": {  
    "name": "cluster-1",  
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    {"path": "/api/storage/volumes", "access": "readonly"},  
    {"path": "/api/storage/qtrees", "access": "readonly"},  
    {"path": "/api/storage/luns", "access": "readonly"},  
    {"path": "/api/storage/aggregates", "access": "readonly"},  
    {"path": "/api/cluster/nodes", "access": "readonly"},  
    {"path": "/api/snapmirror/relationships", "access": "readonly"},  
    {"path": "/api/svm/svms", "access": "readonly"}  
  ]  
}
```

## Creare un utente con un ruolo utilizzando l'API REST di ONTAP

È possibile utilizzare questo flusso di lavoro per creare un utente con un ruolo REST associato.

### Questo flusso di lavoro

Questo flusso di lavoro include i passaggi tipici necessari per creare un ruolo REST personalizzato e associarlo a un nuovo account utente. Sia l'utente che il ruolo hanno un ambito SVM e sono associati a un SVM di dati specifico. Alcuni passaggi possono essere opzionali o devono essere modificati a seconda dell'ambiente.

### Fase 1: Elenco delle SVM di dati nel cluster

Eseguire la seguente chiamata API REST per elencare le SVM nel cluster. L'UUID e il nome di ciascuna SVM sono forniti nell'output.

#### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/svm/svm

## Esempio di arricciamento

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

### Al termine

Selezionare la SVM desiderata dall'elenco in cui creare il nuovo utente e il nuovo ruolo.

## Fase 2: Elencare gli utenti definiti nella SVM

Eseguire la seguente chiamata API REST per elencare gli utenti definiti nella SVM selezionata. È possibile identificare la SVM attraverso il parametro owner.

### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/security/accounts

## Esempio di arricciamento

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

### Al termine

In base agli utenti già definiti nella SVM, scegliere un nome univoco per il nuovo utente.

## Fase 3: Elencare i ruoli REST definiti per la SVM

Eseguire la seguente chiamata API REST per elencare i ruoli definiti nella SVM selezionata. È possibile identificare la SVM attraverso il parametro owner.

### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/security/ruoli

## Esempio di arricciamento

```
curl --request GET \
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## Al termine

In base ai ruoli già definiti nella SVM, scegliere un nome univoco per il nuovo ruolo.

## Passaggio 4: Creare un ruolo REST personalizzato

Eseguire la seguente chiamata API REST per creare un ruolo REST personalizzato nella SVM. Il ruolo inizialmente dispone di un solo privilegio che stabilisce un accesso predefinito di **nessuno** in modo che tutti gli accessi siano negati.

### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

## Esempio di arricciamento

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## Esempio di input JSON

```
{
  "name": "dprole1",
  "owner": {
    "name": "dmp",
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "/api", "access": "none"},
  ]
}
```

## Al termine

Eseguire di nuovo il passaggio 3 per visualizzare il nuovo ruolo. È inoltre possibile visualizzare i ruoli nella CLI di ONTAP.

## Passaggio 5: Aggiornare il ruolo aggiungendo ulteriori privilegi

Eseguire la seguente chiamata API REST per modificare il ruolo aggiungendo i privilegi necessari.

### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/roles/{owner.uuid}/{name}/privileges

### Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
\$SVM_ID	Percorso	Sì	L'UUID della SVM che contiene la definizione del ruolo.
\$NOME_RUOLO	Percorso	Sì	Nome del ruolo all'interno della SVM da aggiornare.

## Esempio di arricciamento

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## Esempio di input JSON

```
{
  "path": "/api/storage/volumes",
  "access": "readonly"
}
```

## Al termine

Eseguire di nuovo il passaggio 3 per visualizzare il nuovo ruolo. È inoltre possibile visualizzare i ruoli nella CLI di ONTAP.

## Passaggio 6: Creare un utente

Eseguire la seguente chiamata API REST per creare un account utente. Il ruolo **drole1** creato in precedenza

è associato al nuovo utente.



È possibile creare l'utente senza un ruolo. In questo caso, all'utente viene assegnato un ruolo predefinito (uno dei due admin oppure vsadmin) A seconda che l'utente sia definito con cluster o ambito SVM. Sarà necessario modificare l'utente per assegnare un ruolo diverso.

### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/accounts

### Esempio di arricciamento

```
curl --request POST \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

### Esempio di input JSON

```
{
  "owner": {"uuid": "daf84055-248f-11ed-a23d-005056ac4fe6"} ,
  "name": "david",
  "applications": [
    {"application": "ssh",
     "authentication_methods": ["password"] ,
     "second_authentication_method": "none" }
  ] ,
  "role": "dprole1",
  "password": "<password>"
}
```

### Al termine

È possibile accedere all'interfaccia di gestione SVM utilizzando le credenziali del nuovo utente.

## 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 COMMERCIALITÀ 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.