



# **Gestire l'accesso al sistema**

## **StorageGRID**

NetApp  
April 10, 2024

# Sommario

- Gestire l'accesso al sistema ..... 1
  - USA la federazione delle identità ..... 1
- Gestire i gruppi ..... 6
- Gestire gli utenti locali ..... 19

# Gestire l'accesso al sistema

## USA la federazione delle identità

L'utilizzo della federazione delle identità rende più rapida la configurazione di gruppi e utenti tenant e consente agli utenti tenant di accedere all'account tenant utilizzando credenziali familiari.

### Configurare la federazione delle identità per Tenant Manager

È possibile configurare la federazione delle identità per il tenant Manager se si desidera che i gruppi e gli utenti tenant vengano gestiti in un altro sistema, ad esempio Active Directory, Azure Active Directory (Azure ad), OpenLDAP o Oracle Directory Server.

#### Di cosa hai bisogno

- Hai effettuato l'accesso al tenant manager utilizzando un [browser web supportato](#).
- Si dispone di autorizzazioni di accesso specifiche.
- Si utilizza Active Directory, Azure ad, OpenLDAP o Oracle Directory Server come provider di identità.



Se si desidera utilizzare un servizio LDAP v3 non elencato, contattare il supporto tecnico.

- Se si intende utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere [Linee guida per la configurazione del server OpenLDAP](#).
- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità deve utilizzare TLS 1.2 o 1.3. Vedere [Crittografia supportata per le connessioni TLS in uscita](#).

#### A proposito di questa attività

La possibilità di configurare un servizio di federazione delle identità per il tenant dipende dalla configurazione dell'account tenant. Il tenant potrebbe condividere il servizio di federazione delle identità configurato per Grid Manager. Se viene visualizzato questo messaggio quando si accede alla pagina Identity Federation, non è possibile configurare un'origine di identità federata separata per questo tenant.



This tenant account uses the LDAP server that is configured for the Grid Manager.  
Contact the grid administrator for information or to change this setting.

#### Inserire la configurazione

##### Fasi

1. Selezionare **ACCESS MANAGEMENT > Identity Federation**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).
3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.

## LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

Azure

OpenLDAP

Other

Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP. In caso contrario, passare alla fase successiva.
  - **User Unique Name** (Nome univoco utente): Il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a `sAMAccountName` Per Active Directory e `uid` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
  - **UUID utente**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a `objectGUID` Per Active Directory e `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Ogni valore dell'utente per l'attributo specificato deve essere un numero esadecimale a 32 cifre in formato a 16 byte o stringa, dove i trattini vengono ignorati.
  - **Group Unique Name** (Nome univoco gruppo): Il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a `sAMAccountName` Per Active Directory e `cn` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
  - **UUID gruppo**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a `objectGUID` Per Active Directory e `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale a 32 cifre nel formato a 16 byte o stringa, dove i trattini vengono ignorati.
5. Per tutti i tipi di servizio LDAP, inserire le informazioni richieste relative al server LDAP e alla connessione di rete nella sezione Configura server LDAP.
  - **Nome host**: Il nome di dominio completo (FQDN) o l'indirizzo IP del server LDAP.
  - **Port** (porta): Porta utilizzata per la connessione al server LDAP.



La porta predefinita per STARTTLS è 389 e la porta predefinita per LDAPS è 636. Tuttavia, è possibile utilizzare qualsiasi porta purché il firewall sia configurato correttamente.

- **Username**: Percorso completo del nome distinto (DN) per l'utente che si connette al server LDAP.

Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome principale dell'utente.

L'utente specificato deve disporre dell'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

- `sAMAccountName` oppure `uid`
- `objectGUID`, `entryUUID`, o `nsuniqueid`

- `cn`
- `memberOf` oppure `isMemberOf`
- **Active Directory:** `objectSid`, `primaryGroupID`, `userAccountControl`, e. `userPrincipalName`
- **Azure:** `accountEnabled` e. `userPrincipalName`
- **Password:** La password associata al nome utente.
- **DN base gruppo:** Il percorso completo del nome distinto (DN) per una sottostruttura LDAP che si desidera cercare gruppi. Nell'esempio di Active Directory (riportato di seguito), tutti i gruppi il cui nome distinto è relativo al DN di base (`DC=storagegrid,DC=example,DC=com`) possono essere utilizzati come gruppi federati.



I valori **Group unique name** devono essere univoci all'interno del **Group base DN** a cui appartengono.

- **User base DN:** Percorso completo del nome distinto (DN) di una sottostruttura LDAP che si desidera cercare gli utenti.



I valori **Nome univoco utente** devono essere univoci all'interno del **DN base utente** a cui appartengono.

- **Bind username format** (opzionale): Il modello di nome utente predefinito che StorageGRID deve utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il formato **bind username** perché può consentire agli utenti di accedere se StorageGRID non è in grado di collegarsi con l'account del servizio.

Immettere uno di questi modelli:

- **Modello UserPrincipalName (Active Directory e Azure):** `[USERNAME]@example.com`
- **Modello di nome di accesso di livello inferiore (Active Directory e Azure):**  
`example\[USERNAME]`
- **Modello nome distinto:** `CN=[USERNAME],CN=Users,DC=example,DC=com`

Includi **[NOME UTENTE]** esattamente come scritto.

## 6. Nella sezione Transport Layer Security (TLS), selezionare un'impostazione di protezione.

- **Usa STARTTLS:** Utilizza STARTTLS per proteggere le comunicazioni con il server LDAP. Si tratta dell'opzione consigliata per Active Directory, OpenLDAP o altro, ma questa opzione non è supportata per Azure.
- **Usa LDAPS:** L'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. Selezionare questa opzione per Azure.
- **Non utilizzare TLS:** Il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Azure.



L'utilizzo dell'opzione **non utilizzare TLS** non è supportato se il server Active Directory applica la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

7. Se si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.

- **Usa certificato CA del sistema operativo:** Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
- **Usa certificato CA personalizzato:** Utilizza un certificato di protezione personalizzato.

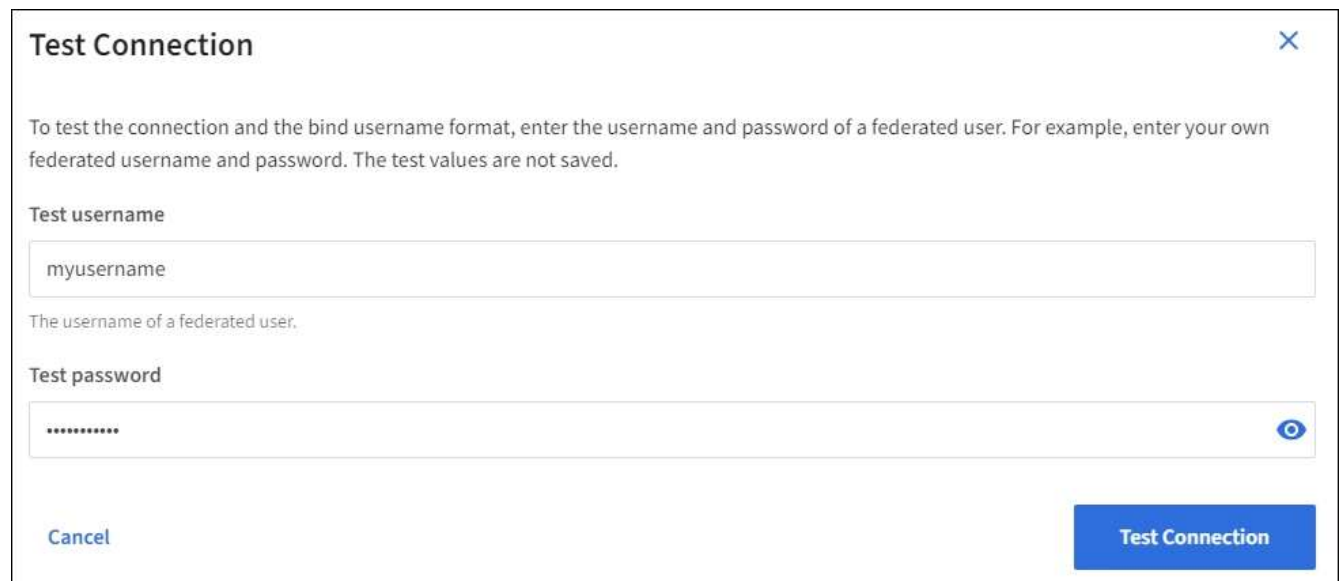
Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

## Verificare la connessione e salvare la configurazione

Dopo aver inserito tutti i valori, è necessario verificare la connessione prima di salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente BIND, se fornito.

1. Selezionare **Test di connessione**.
2. Se non è stato fornito un formato nome utente BIND:
  - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio “Test di connessione riuscito”. Selezionare **Salva** per salvare la configurazione.
  - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio “verifica connessione impossibile”. Selezionare **Chiudi**. Quindi, risolvere eventuali problemi e verificare nuovamente la connessione.
3. Se è stato fornito un formato BIND Username, inserire il nome utente e la password di un utente federato valido.

Ad esempio, inserire il proprio nome utente e la propria password. Non includere caratteri speciali nel nome utente, ad esempio @ o /.



**Test Connection**

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

**Test username**

myusername

The username of a federated user.

**Test password**

\*\*\*\*\*

Cancel Test Connection

- Se le impostazioni di connessione sono valide, viene visualizzato il messaggio “Test di connessione riuscito”. Selezionare **Salva** per salvare la configurazione.
- Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente BIND o il nome utente e la password di prova non sono validi. Risolvere eventuali problemi e verificare nuovamente la connessione.

## Forzare la sincronizzazione con l'origine dell'identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dall'origine dell'identità. È possibile forzare l'avvio della sincronizzazione se si desidera attivare o limitare le autorizzazioni utente il più rapidamente possibile.

### Fasi

1. Vai alla pagina Identity Federation.
2. Selezionare **Sync server** nella parte superiore della pagina.

Il processo di sincronizzazione potrebbe richiedere del tempo a seconda dell'ambiente in uso.



L'avviso **errore di sincronizzazione federazione identità** viene attivato se si verifica un problema durante la sincronizzazione di utenti e gruppi federati dall'origine dell'identità.

## Disattiva la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione di identità per gruppi e utenti. Quando la federazione delle identità è disattivata, non vi è alcuna comunicazione tra StorageGRID e l'origine delle identità. Tuttavia, tutte le impostazioni configurate vengono conservate, consentendo di riabilitare facilmente la federazione delle identità in futuro.

### A proposito di questa attività

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non viene eseguita e non vengono generati avvisi o allarmi per gli account che non sono stati sincronizzati.
- La casella di controllo **Enable Identity Federation** (attiva federazione identità) è disattivata se Single Sign-on (SSO) è impostato su **Enabled** o **Sandbox Mode**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabled** prima di poter disattivare la federazione delle identità. Vedere [Disattiva single sign-on](#).

### Fasi

1. Vai alla pagina Identity Federation.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).

## Linee guida per la configurazione del server OpenLDAP

Se si desidera utilizzare un server OpenLDAP per la federazione delle identità, è necessario configurare impostazioni specifiche sul server OpenLDAP.



Per le origini delle identità che non sono Active Directory o Azure, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare eventuali chiavi S3 per l'utente e rimuovere l'utente da tutti i gruppi.

## MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo in <http://www.openldap.org/doc/admin24/index.html> ["Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4"].

## Indicizzazione

È necessario configurare i seguenti attributi OpenLDAP con le parole chiave di indice specificate:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Inoltre, assicurarsi che i campi indicati nella guida per Nome utente siano indicizzati per ottenere prestazioni ottimali.

Consultare le informazioni relative alla manutenzione dell'appartenenza al gruppo inverso nella sezione <http://www.openldap.org/doc/admin24/index.html> ["Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4"].

# Gestire i gruppi

## Creare gruppi per un tenant S3

È possibile gestire le autorizzazioni per i gruppi di utenti S3 importando gruppi federati o creando gruppi locali.

### Di cosa hai bisogno

- È necessario accedere al tenant manager utilizzando un [browser web supportato](#).
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root. Vedere [Permessi di gestione del tenant](#).
- Se si intende importare un gruppo federated, la federazione delle identità è stata configurata e il gruppo federated esiste già nell'origine delle identità configurata.

Per informazioni su S3, vedere [Utilizzare S3](#).

### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.



# Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beeec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

Previous **1** Next

2. Selezionare **Crea gruppo**.

3. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda **Federated group** (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti appartenenti a gruppi locali non potranno accedere a Gestione tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni di gruppo.

4. Inserire il nome del gruppo.

- **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.
- **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

5. Selezionare **continua**.

6. Selezionare una modalità di accesso. Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

- **Read-write** (valore predefinito): Gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
- **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API di gestione del tenant Manager o del tenant. Gli utenti locali di sola lettura possono modificare le proprie password.

7. Selezionare le autorizzazioni di gruppo per questo gruppo.

Consultare le informazioni sulle autorizzazioni di gestione del tenant.

8. Selezionare **continua**.

9. Selezionare un criterio di gruppo per determinare le autorizzazioni di accesso S3 di cui avranno i membri di questo gruppo.

- **Nessun accesso S3:** Impostazione predefinita. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non sia concesso con una policy bucket. Se si seleziona questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
  - **Accesso di sola lettura:** Gli utenti di questo gruppo hanno accesso di sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile modificare questa stringa.
  - **Accesso completo:** Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo ad accesso completo. Impossibile modificare questa stringa.
  - **Personalizzato:** Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo. Consultare le istruzioni per l'implementazione di un'applicazione client S3 per informazioni dettagliate sui criteri di gruppo, tra cui la sintassi del linguaggio e gli esempi.
10. Se si seleziona **Custom**, inserire il criterio di gruppo. Ogni policy di gruppo ha un limite di dimensione di 5,120 byte. Immettere una stringa valida formattata con JSON.

In questo esempio, i membri del gruppo possono solo elencare e accedere a una cartella corrispondente al proprio nome utente (prefisso della chiave) nel bucket specificato. Tenere presente che le autorizzazioni di accesso da altre policy di gruppo e la policy del bucket devono essere prese in considerazione quando si determina la privacy di queste cartelle.



☐ No S3 Access  
☐ Read Only Access  
☐ Full Access  
☒ Custom  
 (Must be a valid JSON formatted string.)

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
  
```

11. Selezionare il pulsante visualizzato, a seconda che si stia creando un gruppo federated o un gruppo locale:
- Gruppo federato: **Crea gruppo**
  - Gruppo locale: **Continua**

Se si sta creando un gruppo locale, il passaggio 4 (Aggiungi utenti) viene visualizzato dopo aver

selezionato **continua**. Questo passaggio non viene visualizzato per i gruppi federated.

12. Selezionare la casella di controllo per ciascun utente che si desidera aggiungere al gruppo, quindi selezionare **Crea gruppo**.

In alternativa, è possibile salvare il gruppo senza aggiungere utenti. È possibile aggiungere utenti al gruppo in un secondo momento oppure selezionarlo quando si aggiungono nuovi utenti.

13. Selezionare **fine**.

Il gruppo creato viene visualizzato nell'elenco dei gruppi. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Creare gruppi per un tenant Swift

È possibile gestire le autorizzazioni di accesso per un account tenant Swift importando gruppi federati o creando gruppi locali. Almeno un gruppo deve disporre dell'autorizzazione Swift Administrator, necessaria per gestire i container e gli oggetti per un account tenant Swift.

### Di cosa hai bisogno

- È necessario accedere al tenant manager utilizzando un [browser web supportato](#).
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.
- Se si intende importare un gruppo federated, la federazione delle identità è stata configurata e il gruppo federated esiste già nell'origine delle identità configurata.

### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous **1** Next →

2. Selezionare **Crea gruppo**.
3. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda

**Federated group** (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti appartenenti a gruppi locali non potranno accedere a Gestione tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni di gruppo.

4. Inserire il nome del gruppo.

- **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.
- **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

5. Selezionare **continua**.

6. Selezionare una modalità di accesso. Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

- **Read-write** (valore predefinito): Gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
- **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API di gestione del tenant Manager o del tenant. Gli utenti locali di sola lettura possono modificare le proprie password.

7. Impostare l'autorizzazione di gruppo.

- Selezionare la casella di controllo **Root Access** se gli utenti devono accedere all'API di gestione tenant o tenant Manager. (Impostazione predefinita)
- Deselezionare la casella di controllo **Root Access** se gli utenti non hanno bisogno dell'accesso all'API di gestione tenant o tenant. Ad esempio, deselezionare la casella di controllo per le applicazioni che non richiedono l'accesso al tenant. Quindi, assegnare l'autorizzazione **Swift Administrator** per consentire a questi utenti di gestire container e oggetti.

8. Selezionare **continua**.

9. Selezionare la casella di controllo **Swift Administrator** se l'utente deve poter utilizzare l'API SWIFT REST.

Gli utenti Swift devono disporre dell'autorizzazione Root Access per accedere a Tenant Manager. Tuttavia, l'autorizzazione Root Access non consente agli utenti di autenticarsi nell'API SWIFT REST per creare container e acquisire oggetti. Gli utenti devono disporre dell'autorizzazione di amministratore Swift per autenticarsi nell'API DI Swift REST.

10. Selezionare il pulsante visualizzato, a seconda che si stia creando un gruppo federated o un gruppo locale:

- Gruppo federato: **Crea gruppo**
- Gruppo locale: **Continua**

Se si sta creando un gruppo locale, il passaggio 4 (Aggiungi utenti) viene visualizzato dopo aver selezionato **continua**. Questo passaggio non viene visualizzato per i gruppi federated.

11. Selezionare la casella di controllo per ciascun utente che si desidera aggiungere al gruppo, quindi selezionare **Crea gruppo**.

In alternativa, è possibile salvare il gruppo senza aggiungere utenti. È possibile aggiungere utenti al gruppo in un secondo momento oppure selezionarlo quando si creano nuovi utenti.

## 12. Selezionare **fine**.

Il gruppo creato viene visualizzato nell'elenco dei gruppi. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

### Informazioni correlate

[Permessi di gestione del tenant](#)

[USA Swift](#)

## Permessi di gestione del tenant

Prima di creare un gruppo tenant, prendere in considerazione le autorizzazioni che si desidera assegnare a tale gruppo. Le autorizzazioni di gestione del tenant determinano le attività che gli utenti possono eseguire utilizzando il tenant Manager o l'API di gestione del tenant. Un utente può appartenere a uno o più gruppi. Le autorizzazioni sono cumulative se un utente appartiene a più gruppi.

Per accedere a tenant Manager o utilizzare l'API di gestione tenant, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono accedere possono eseguire le seguenti operazioni:

- Visualizza la dashboard
- Modificare la propria password (per gli utenti locali)

Per tutte le autorizzazioni, l'impostazione della modalità di accesso del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni o se possono visualizzare solo le relative impostazioni e funzionalità.



Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

È possibile assegnare a un gruppo le seguenti autorizzazioni. Tenere presente che i tenant S3 e Swift dispongono di permessi di gruppo diversi. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

Permesso	Descrizione
Accesso root	Fornisce l'accesso completo al tenant Manager e all'API di gestione del tenant.  <b>Nota:</b> gli utenti Swift devono disporre dell'autorizzazione di accesso root per accedere all'account tenant.
Amministratore	Solo tenant Swift. Fornisce l'accesso completo ai container e agli oggetti Swift per questo account tenant  <b>Nota:</b> gli utenti di Swift devono disporre dell'autorizzazione di amministratore di Swift per eseguire qualsiasi operazione con l'API DI Swift REST.

Permesso	Descrizione
Gestisci le tue credenziali S3	Solo tenant S3. Consente agli utenti di creare e rimuovere le proprie chiavi di accesso S3. Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu <b>STORAGE (S3) &gt; My S3 access keys</b> .
Gestire tutti i bucket	<ul style="list-style-type: none"> <li>S3 tenant: Consente agli utenti di utilizzare tenant Manager e l'API di gestione tenant per creare ed eliminare i bucket S3 e per gestire le impostazioni di tutti i bucket S3 nell'account tenant, indipendentemente dalle policy di gruppo o bucket S3.</li> </ul> <p>Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu <b>Bucket</b>.</p> <ul style="list-style-type: none"> <li>Tenant Swift: Consente agli utenti Swift di controllare il livello di coerenza per i container Swift utilizzando l'API di gestione tenant.</li> </ul> <p><b>Nota:</b> è possibile assegnare l'autorizzazione Gestisci tutti i bucket solo ai gruppi Swift dall'API di gestione tenant. Non è possibile assegnare questa autorizzazione ai gruppi Swift utilizzando il tenant Manager.</p>
Gestire gli endpoint	<p>Solo tenant S3. Consente agli utenti di utilizzare il gestore tenant o l'API di gestione tenant per creare o modificare gli endpoint, che vengono utilizzati come destinazione per i servizi della piattaforma StorageGRID.</p> <p>Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu <b>Platform Services Endpoint</b>.</p>

#### Informazioni correlate

[Utilizzare S3](#)

[USA Swift](#)

## Visualizzare e modificare i dettagli del gruppo

Quando si visualizzano i dettagli di un gruppo, è possibile modificare il nome visualizzato del gruppo, le autorizzazioni, i criteri e gli utenti che appartengono al gruppo.

#### Di cosa hai bisogno

- È necessario accedere al tenant manager utilizzando un [browser web supportato](#).
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.

#### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.
2. Selezionare il nome del gruppo di cui si desidera visualizzare o modificare i dettagli.

In alternativa, è possibile selezionare **azioni > Visualizza dettagli gruppo**.

Viene visualizzata la pagina dei dettagli del gruppo. L'esempio seguente mostra la pagina dei dettagli del gruppo S3.

## Overview

Display name:	<a href="#">Applications</a> 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

### Group permissions

### S3 group policy

### Users

## Manage group permissions

Select an access mode for this group and select one or more permissions.

### Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

☒ Read-write ☐ Read-only

### Group permissions

Select the tenant account permissions you want to assign to this group.

☒ **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

☒ **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

☒ **Manage Endpoints**

Allows users to configure endpoints for platform services.

☒ **Manage Your Own S3 Credentials**


Allows users to create and delete their own S3 access keys.

Save changes

### 3. Apportare le modifiche necessarie alle impostazioni del gruppo.



Per assicurarsi che le modifiche vengano salvate, selezionare **Save changes** (Salva modifiche) dopo aver apportato le modifiche in ciascuna sezione. Una volta salvate le modifiche, nell'angolo superiore destro della pagina viene visualizzato un messaggio di conferma.

- a. In alternativa, selezionare il nome visualizzato o l'icona di modifica  per aggiornare il nome visualizzato.

Non è possibile modificare il nome univoco di un gruppo. Non è possibile modificare il nome visualizzato per un gruppo federated.

- b. Facoltativamente, aggiornare le autorizzazioni.

- c. Per i criteri di gruppo, apportare le modifiche appropriate al tenant S3 o Swift.

- Se si modifica un gruppo per un tenant S3, selezionare un criterio di gruppo S3 diverso. Se si seleziona un criterio S3 personalizzato, aggiornare la stringa JSON come richiesto.
- Se si modifica un gruppo per un tenant Swift, selezionare o deselezionare la casella di controllo **Swift Administrator**.

Per ulteriori informazioni sull'autorizzazione amministratore Swift, consultare le istruzioni per la creazione di gruppi per un tenant Swift.

- d. Facoltativamente, aggiungere o rimuovere utenti.

### 4. Confermare di aver selezionato **Save Changes** (Salva modifiche) per ciascuna sezione modificata.

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### Informazioni correlate

[Creare gruppi per il tenant S3](#)

[Creare gruppi per il tenant Swift](#)

## Aggiungere utenti a un gruppo locale

È possibile aggiungere utenti a un gruppo locale in base alle esigenze.

#### Di cosa hai bisogno

- È necessario accedere al tenant manager utilizzando un [browser web supportato](#).
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.

#### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.
2. Selezionare il nome del gruppo locale a cui si desidera aggiungere utenti.

In alternativa, è possibile selezionare **azioni > Visualizza dettagli gruppo**.

Viene visualizzata la pagina dei dettagli del gruppo.



## Overview

Display name:	<a href="#">Applications</a> 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

### Group permissions

### S3 group policy

### Users

## Manage group permissions

Select an access mode for this group and select one or more permissions.

### Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

☒ Read-write ☐ Read-only

### Group permissions

Select the tenant account permissions you want to assign to this group.

☒ **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

☒ **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

☒ **Manage Endpoints**

Allows users to configure endpoints for platform services.

☒ **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

Save changes

3. Selezionare **utenti**, quindi selezionare **Aggiungi utenti**.

**Manage users**

You can add users to this group or remove users from this group.

**Add users** **Remove Users** Search Groups... Displaying 1 results

Username	Full Name	Denied
User_02	User_02_Managers	

4. Selezionare gli utenti che si desidera aggiungere al gruppo, quindi selezionare **Aggiungi utenti**.

**Add users**

Select local users to add to the group **Applications**.

Search Groups... Displaying 1 results

<input checked="" type="checkbox"/>	Username	Full Name	Denied
<input checked="" type="checkbox"/>	User_01	User_01_Applications	

Cancel **Add users**

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Modificare il nome del gruppo

È possibile modificare il nome visualizzato di un gruppo. Non è possibile modificare il nome univoco di un gruppo.

### Di cosa hai bisogno

- È necessario accedere al tenant manager utilizzando un [browser web supportato](#).
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root. Vedere [Permessi di gestione del tenant](#).

### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.
2. Selezionare la casella di controllo del gruppo di cui si desidera modificare il nome visualizzato.
3. Selezionare **azioni > Modifica nome gruppo**.

Viene visualizzata la finestra di dialogo Edit group name (Modifica nome gruppo).

**Edit group name** ✕

Specify a new name for the group **Applications**.

Must contain at least 1 and no more than 32 characters

Applications

Cancel Save changes

4. Se si sta modificando un gruppo locale, aggiornare il nome visualizzato in base alle necessità.

Non è possibile modificare il nome univoco di un gruppo. Non è possibile modificare il nome visualizzato per un gruppo federated.

5. Selezionare **Save Changes** (Salva modifiche).

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Gruppo duplicato

È possibile creare nuovi gruppi più rapidamente duplicando un gruppo esistente.

### Di cosa hai bisogno

- È necessario accedere al tenant manager utilizzando un [browser web supportato](#).
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root. Vedere [Permessi di gestione del tenant](#).

### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.
2. Selezionare la casella di controllo relativa al gruppo che si desidera duplicare.
3. Selezionare **Duplica gruppo**. Per ulteriori informazioni sulla creazione di un gruppo, vedere le istruzioni per la creazione di gruppi per [Un tenant S3](#) o per [Tenant Swift](#).
4. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda **Federated group** (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

Se il sistema StorageGRID è abilitato per il Single Sign-on (SSO), gli utenti appartenenti a gruppi locali non potranno accedere al Manager tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, [in base alle autorizzazioni di gruppo](#).

5. Inserire il nome del gruppo.
  - **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.

- **Federated group:** Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

6. Selezionare **continua**.
7. Se necessario, modificare le autorizzazioni per questo gruppo.
8. Selezionare **continua**.
9. Se si desidera duplicare un gruppo per un tenant S3, selezionare un criterio diverso dai pulsanti di opzione **Add S3 policy** (Aggiungi criterio S3). Se è stato selezionato un criterio personalizzato, aggiornare la stringa JSON come richiesto.
10. Selezionare **Crea gruppo**.

## Elimina gruppo

È possibile eliminare un gruppo dal sistema. Gli utenti che appartengono solo a quel gruppo non potranno più accedere al tenant manager o utilizzare l'account tenant.

### Di cosa hai bisogno

- È necessario accedere al tenant manager utilizzando un [browser web supportato](#).
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root. Vedere [Permessi di gestione del tenant](#).

### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous **1** Next →

2. Selezionare le caselle di controllo dei gruppi che si desidera eliminare.
3. Selezionare **azioni > Elimina gruppo**.

Viene visualizzato un messaggio di conferma.

4. Selezionare **Delete group** (Elimina gruppo) per confermare che si desidera eliminare i gruppi indicati nel messaggio di conferma.

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Gestire gli utenti locali

È possibile creare utenti locali e assegnarli a gruppi locali per determinare le funzionalità a cui questi utenti possono accedere. Il tenant Manager include un utente locale predefinito, denominato “root”. Sebbene sia possibile aggiungere e rimuovere utenti locali, non è possibile rimuovere l'utente root.

### Di cosa hai bisogno

- È necessario accedere al tenant manager utilizzando un [browser web supportato](#).
- È necessario appartenere a un gruppo di utenti in lettura/scrittura che disponga dell'autorizzazione di accesso root. Vedere [Permessi di gestione del tenant](#).



Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti locali non potranno accedere al Manager tenant o all'API di gestione tenant, anche se possono utilizzare le applicazioni client S3 o Swift per accedere alle risorse del tenant, in base alle autorizzazioni di gruppo.

### Accedere alla pagina utenti

Selezionare **ACCESS MANAGEMENT > Users**.

# Users

View local and federated users. Edit properties and group membership of local users.

3 users

Create user

Actions

<input type="checkbox"/>	Username	Full Name	Denied	Type
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	User_01	User_01		Local
<input type="checkbox"/>	User_02	User_02		Local

## Creare utenti locali

È possibile creare utenti locali e assegnarli a uno o più gruppi locali per controllarne le autorizzazioni di accesso.

Gli utenti S3 che non appartengono a nessun gruppo non dispongono di autorizzazioni di gestione o criteri di gruppo S3 applicati. Questi utenti potrebbero avere accesso al bucket S3 concesso tramite una policy bucket.

Gli utenti Swift che non appartengono a nessun gruppo non dispongono di autorizzazioni di gestione o di accesso al container Swift.

### Fasi

1. Selezionare **Crea utente**.
2. Compilare i seguenti campi.
  - **Nome completo**: Il nome completo dell'utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
  - **Username**: Il nome che l'utente utilizzerà per accedere. I nomi utente devono essere univoci e non possono essere modificati.
  - **Password**: Una password che viene utilizzata quando l'utente effettua l'accesso.
  - **Conferma password**: Digitare la stessa password immessa nel campo Password.
  - **Nega accesso**: Se si seleziona **Sì**, l'utente non potrà accedere all'account tenant, anche se potrebbe ancora appartenere a uno o più gruppi.

Ad esempio, è possibile utilizzare questa funzione per sospendere temporaneamente la capacità di accesso di un utente.

3. Selezionare **continua**.
4. Assegnare l'utente a uno o più gruppi locali.

Gli utenti che non appartengono a nessun gruppo non disporranno di autorizzazioni di gestione. Le autorizzazioni sono cumulative. Gli utenti disporranno di tutte le autorizzazioni per tutti i gruppi a cui appartengono.

5. Selezionare **Crea utente**.

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.


## Modificare i dettagli dell'utente

Quando si modificano i dettagli di un utente, è possibile modificare il nome completo e la password dell'utente, aggiungerlo a gruppi diversi e impedire all'utente di accedere al tenant.

### Fasi

1. Nell'elenco Users (utenti), selezionare il nome dell'utente di cui si desidera visualizzare o modificare i dettagli.

In alternativa, è possibile selezionare la casella di controllo dell'utente, quindi selezionare **azioni > Visualizza dettagli utente**.

2. Apportare le modifiche necessarie alle impostazioni utente.
  - a. Modificare il nome completo dell'utente in base alle necessità selezionando il nome completo o l'icona di modifica  Nella sezione Panoramica.  
  
Non è possibile modificare il nome utente.
  - b. Nella scheda **Password**, modificare la password dell'utente in base alle necessità.
  - c. Nella scheda **Access**, consentire all'utente di accedere (selezionare **No**) o impedire all'utente di accedere (selezionare **Sì**) in base alle necessità.
  - d. Nella scheda **gruppi**, aggiungere l'utente ai gruppi o rimuoverlo dai gruppi in base alle necessità.
  - e. In base alle esigenze di ciascuna sezione, selezionare **Save Changes** (Salva modifiche).

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Utenti locali duplicati

È possibile duplicare un utente locale per creare un nuovo utente più rapidamente.

### Fasi

1. Nell'elenco Users (utenti), selezionare l'utente che si desidera duplicare.
2. Selezionare **Duplica utente**.
3. Modificare i seguenti campi per il nuovo utente.
  - **Nome completo**: Il nome completo dell'utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
  - **Username**: Il nome che l'utente utilizzerà per accedere. I nomi utente devono essere univoci e non possono essere modificati.

- **Password:** Una password che viene utilizzata quando l'utente effettua l'accesso.
- **Conferma password:** Digitare la stessa password immessa nel campo Password.
- **Nega accesso:** Se si seleziona **Sì**, l'utente non potrà accedere all'account tenant, anche se potrebbe ancora appartenere a uno o più gruppi.

Ad esempio, è possibile utilizzare questa funzione per sospendere temporaneamente la capacità di accesso di un utente.

4. Selezionare **continua**.
5. Selezionare uno o più gruppi locali.

Gli utenti che non appartengono a nessun gruppo non disporranno di autorizzazioni di gestione. Le autorizzazioni sono cumulative. Gli utenti disporranno di tutte le autorizzazioni per tutti i gruppi a cui appartengono.

6. Selezionare **Crea utente**.

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Eliminare gli utenti locali

È possibile eliminare in modo permanente gli utenti locali che non hanno più bisogno di accedere all'account tenant StorageGRID.

Utilizzando Tenant Manager, è possibile eliminare gli utenti locali, ma non quelli federati. Per eliminare gli utenti federati, è necessario utilizzare l'origine delle identità federate.

### Fasi

1. Nell'elenco Users (utenti), selezionare la casella di controllo dell'utente locale che si desidera eliminare.
2. Selezionare **azioni > Elimina utente**.
3. Nella finestra di dialogo di conferma, selezionare **Delete user** (Elimina utente) per confermare che si desidera eliminare l'utente dal sistema.

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.



## 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.