



Gestire gruppi e utenti

StorageGRID software

NetApp

February 12, 2026

Sommario

- Gestire gruppi e utenti 1
 - USA la federazione delle identità 1
 - Configurare la federazione delle identità per Tenant Manager 1
 - Forzare la sincronizzazione con l'origine dell'identità 5
 - Disattiva la federazione delle identità 5
 - Linee guida per la configurazione del server OpenLDAP 5
 - Gestire i gruppi di tenant 6
 - Creare gruppi per un tenant S3 6
 - Permessi di gestione del tenant 9
 - Gestire i gruppi 11
 - Gestire gli utenti 15
 - Crea un utente locale 15
 - Visualizzare o modificare l'utente locale 17
 - Importa utenti federati 18
 - Utente locale duplicato 18
 - Riprova clone utente 18
 - Eliminare uno o più utenti locali 19

Gestire gruppi e utenti

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 Tenant Manager se si desidera che i gruppi e gli utenti dei tenant vengano gestiti in un altro sistema, ad esempio Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).
- Stai utilizzando Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server come provider di identità.



Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare l'assistenza tecnica.

- 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

Quando si configura Identify Federation, vengono forniti i valori necessari a StorageGRID per connettersi a un servizio LDAP.

Fasi

1. Selezionare **Gestione accessi** > **Federazione identità**.
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	Entra ID	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.
 - **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 stai configurando Oracle Directory Server, inserisci `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 stai configurando Oracle Directory Server, inserisci `nsuniqueid`. Il valore di ciascun utente per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
 - **Nome univoco del 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 stai configurando Oracle Directory Server, inserisci `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 stai configurando Oracle Directory Server, inserisci `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui 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` o `uid`
- `objectGUID`, `entryUUID` o `nsuniqueid`

- `cn`
 - `memberOf o. isMemberOf`
 - **Active Directory:** `objectSid, primaryGroupID, userAccountControl E userPrincipalName`
 - **ID di ingresso:** `accountEnabled E userPrincipalName`
- **Password:** La password associata al nome utente.



Se si modifica la password in futuro, è necessario aggiornarla in questa pagina.

- **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 (ID AD e Entra):** `[USERNAME]@example.com`
- **Modello di nome di accesso di livello inferiore (ID AD e Entra):** `example\[USERNAME]`
- **Modello di 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:** usa STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma non è supportata per Microsoft Entra ID.
- **Usa LDAPS:** l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Microsoft Entra ID.
- **Non utilizzare TLS:** il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Microsoft Entra ID.



L'utilizzo dell'opzione **Non utilizzare TLS** non è supportato se il server Active Directory impone 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.

Fasi

1. Selezionare **Test di connessione**.
2. Se non hai fornito un formato di nome utente di associazione:
 - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.
 - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". 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 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 delle identità per gruppi e utenti. Quando la federazione delle identità è disabilitata, non c'è comunicazione tra StorageGRID e l'origine dell'identità. Tuttavia, tutte le impostazioni configurate vengono mantenute, consentendoti di riattivare 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 verrà eseguita e non verranno generati avvisi per gli account che non sono stati sincronizzati.
- La casella di controllo **Abilita federazione delle identità** è disabilitata se lo stato Single Sign-On (SSO) è **Abilitato** o **Modalità sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare 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 identità che non sono Active Directory o Microsoft Entra ID, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare tutte le chiavi S3 dell'utente o rimuovere l'utente da tutti i gruppi.

MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, vedere le istruzioni per la manutenzione dell'appartenenza al gruppo inverso nella ["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.

Vedere le informazioni sulla manutenzione dell'appartenenza al gruppo inverso nella ["Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4"](#).

Gestire i gruppi di tenant

Creare gruppi per un tenant S3

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

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).
- Se si prevede di importare un gruppo federated, si dispone di ["federazione di identità configurata"](#), e il gruppo Federated esiste già nell'origine identità configurata.
- Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è stato esaminato il flusso di lavoro e le considerazioni relative a ["clonazione di utenti e gruppi tenant"](#) e si è effettuato l'accesso alla griglia di origine del tenant.

Accedere alla procedura guidata Crea gruppo

Come prima fase, accedere alla procedura guidata Crea gruppo.

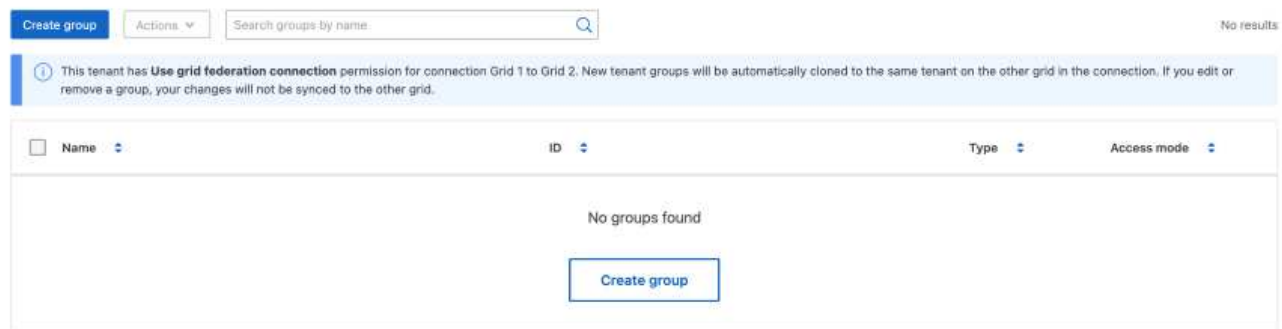
Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, verificare che

venga visualizzato un banner blu che indica che i nuovi gruppi creati in questa griglia verranno clonati nello stesso tenant nell'altra griglia della connessione. Se questo banner non viene visualizzato, potresti aver effettuato l'accesso alla griglia di destinazione del tenant.

Groups

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



3. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federated.

Fasi

1. 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.

2. 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.



Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, si verificherà un errore di clonazione se lo stesso **nome univoco** esiste già per il tenant nella griglia di destinazione.

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

3. Selezionare **continua**.

Gestire le autorizzazioni di gruppo

Le autorizzazioni di gruppo controllano le attività che gli utenti possono eseguire nelle API di gestione tenant e tenant Manager.

Fasi

1. Per la modalità **Access**, selezionare una delle seguenti opzioni:

- **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 tenant Manager o tenant. Gli utenti locali di sola lettura possono modificare le proprie password.



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.

2. Selezionare una o più autorizzazioni per questo gruppo.

Vedere "[Permessi di gestione del tenant](#)".

3. Selezionare **continua**.

Impostare i criteri di gruppo S3

I criteri di gruppo determinano le autorizzazioni di accesso S3 che gli utenti avranno.

Fasi

1. Selezionare il criterio che si desidera utilizzare per questo gruppo.

Policy di gruppo	Descrizione
Nessun accesso S3	Predefinito. 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 in sola lettura	Gli utenti di questo gruppo hanno accesso in 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.

Policy di gruppo	Descrizione
Riduzione del ransomware	<p>Questo criterio di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti.</p> <p>Gli utenti di tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono eseguire l'override di questa policy di gruppo. Limitare l'autorizzazione Manage All bucket (Gestisci tutti i bucket) agli utenti attendibili e utilizzare l'autenticazione multifattore (MFA), se disponibile.</p>
Personalizzato	Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

- 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.

Per informazioni dettagliate sui criteri di gruppo, incluse la sintassi del linguaggio e gli esempi, vedere ["Criteri di gruppo di esempio"](#).

- Se si sta creando un gruppo locale, selezionare **continua**. Se si sta creando un gruppo federated, selezionare **Crea gruppo e fine**.

Aggiunta di utenti (solo gruppi locali)

È possibile salvare il gruppo senza aggiungere utenti oppure aggiungere utenti locali già esistenti.



Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, gli utenti selezionati quando si crea un gruppo locale nella griglia di origine non vengono inclusi quando il gruppo viene clonato nella griglia di destinazione. Per questo motivo, non selezionare gli utenti quando si crea il gruppo. Al momento della creazione degli utenti, selezionare il gruppo.

Fasi

- Facoltativamente, selezionare uno o più utenti locali per questo gruppo.
- Selezionare **Crea gruppo e fine**.

Il gruppo creato viene visualizzato nell'elenco dei gruppi.

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ci si trova nella griglia di origine del tenant, il nuovo gruppo viene clonato nella griglia di destinazione del tenant. **Success** viene visualizzato come **Cloning status** nella sezione Overview della pagina dei dettagli del gruppo.

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 le seguenti autorizzazioni a un gruppo.

Permesso	Descrizione	Dettagli
Accesso root	Fornisce l'accesso completo al tenant Manager e all'API di gestione del tenant.	
Gestisci le tue credenziali 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 STORAGE (S3) > My S3 access keys .
Visualizza tutti i bucket	Consente agli utenti di visualizzare tutti i bucket e le relative configurazioni.	<p>Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu bucket.</p> <p>Questa autorizzazione è sostituita dall'autorizzazione Gestisci tutti i bucket. Non influisce sui bucket S3 o sui criteri di gruppo utilizzati dai client S3 o dalla console S3.</p>
Gestire tutti i bucket	Consente agli utenti di utilizzare Tenant Manager e l'API Tenant Management per creare ed eliminare bucket S3 e gestire le impostazioni per tutti i bucket S3 nell'account tenant, indipendentemente dal bucket S3 o dai criteri di gruppo.	<p>Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu bucket.</p> <p>Questa autorizzazione sostituisce l'autorizzazione Visualizza tutti i bucket. Non influisce sui bucket S3 o sui criteri di gruppo utilizzati dai client S3 o dalla console S3.</p>

Permesso	Descrizione	Dettagli
Gestire gli endpoint	Consente agli utenti di utilizzare il gestore tenant o l'API di gestione tenant per creare o modificare gli endpoint del servizio della piattaforma, che vengono utilizzati come destinazione per i servizi della piattaforma StorageGRID.	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu Platform Services Endpoint .
Utilizzare la scheda Console S3	Se combinato con l'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket, consente agli utenti di visualizzare e gestire gli oggetti dalla scheda Console S3 nella pagina dei dettagli di un bucket.	

Gestire i gruppi

Gestire i gruppi di tenant in base alle esigenze per visualizzare, modificare o duplicare un gruppo e altro ancora.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).

Visualizzare o modificare il gruppo

È possibile visualizzare e modificare le informazioni di base e i dettagli di ciascun gruppo.

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Consultare le informazioni fornite nella pagina gruppi, che elenca le informazioni di base per tutti i gruppi locali e federati per questo account tenant.

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si stanno visualizzando i gruppi nella griglia di origine del tenant:

- Un messaggio banner indica che se si modifica o si rimuove un gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
- Se necessario, un messaggio di intestazione indica se i gruppi non sono stati clonati nel tenant sulla griglia di destinazione. È possibile [riprovare a creare un clone di gruppo](#) che non sia riuscito.


3. Se si desidera modificare il nome del gruppo:
 - a. Selezionare la casella di controllo del gruppo.
 - b. Selezionare **azioni > Modifica nome gruppo**.
 - c. Inserire il nuovo nome.
 - d. Selezionare **Salva modifiche**.
4. Se si desidera visualizzare ulteriori dettagli o apportare modifiche aggiuntive, effettuare una delle seguenti operazioni:

- Selezionare il nome del gruppo.
- Selezionare la casella di controllo relativa al gruppo e selezionare **azioni > Visualizza dettagli gruppo**.

5. Consultare la sezione Panoramica, che mostra le seguenti informazioni per ciascun gruppo:

- Nome visualizzato
- Nome univoco
- Tipo
- Modalità di accesso
- Permessi
- Policy S3
- Numero di utenti in questo gruppo
- Ulteriori campi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando il gruppo nella griglia di origine del tenant:
 - Stato di cloning, **Success** o **Failure**
 - Un banner blu che indica che se modifichi o elimini questo gruppo, le modifiche non verranno sincronizzate con l'altra griglia.

6. Modificare le impostazioni del gruppo secondo necessità. Fare riferimento a "[Creare gruppi per un tenant S3](#)" per i dettagli su cosa inserire.

- Nella sezione Panoramica, modificare il nome visualizzato selezionando il nome o l'icona di modifica .
- Nella scheda **permessi di gruppo**, aggiornare le autorizzazioni e selezionare **Salva modifiche**.
- Nella scheda **Criteri di gruppo**, apportare le modifiche desiderate e selezionare **Salva modifiche**.

Facoltativamente, selezionare un criterio di gruppo S3 diverso o immettere la stringa JSON per un criterio personalizzato, a seconda delle necessità.

7. Per aggiungere uno o più utenti locali al gruppo:

- Selezionare la scheda Users (utenti).

Manage users

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

Displaying one result

Username ⓘ	Full name ⓘ	Denied access ⓘ
User_02	User_02_Managers	No

- Selezionare **Aggiungi utenti**.
- Selezionare gli utenti che si desidera aggiungere e selezionare **Aggiungi utenti**.

In alto a destra viene visualizzato il messaggio Success (operazione riuscita).

8. Per rimuovere utenti locali dal gruppo:

- Selezionare la scheda Users (utenti).

- b. Selezionare **Rimuovi utenti**.
- c. Selezionare gli utenti che si desidera rimuovere e selezionare **Rimuovi utenti**.

In alto a destra viene visualizzato il messaggio Success (operazione riuscita).

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

Gruppo duplicato

È possibile duplicare un gruppo esistente per creare nuovi gruppi più rapidamente.



Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si duplica un gruppo dalla griglia di origine del tenant, il gruppo duplicato verrà clonato nella griglia di destinazione del tenant.

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Selezionare la casella di controllo del gruppo che si desidera duplicare.
3. Selezionare **azioni > Duplica gruppo**.
4. Vedere ["Creare gruppi per un tenant S3"](#) per i dettagli su cosa inserire.
5. Selezionare **Crea gruppo**.

Riprova clone di gruppo

Per riprovare un clone non riuscito:

1. Selezionare ciascun gruppo che indica (*clonazione non riuscita*) sotto il nome del gruppo.
2. Selezionare **azioni > Clona gruppi**.
3. Visualizzare lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun gruppo da clonare.

Per ulteriori informazioni, vedere ["Clonare utenti e gruppi tenant"](#).

Eliminare uno o più gruppi

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



Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si elimina un gruppo, StorageGRID non eliminerà il gruppo corrispondente sull'altra griglia. Se è necessario mantenere queste informazioni sincronizzate, è necessario eliminare lo stesso gruppo da entrambe le griglie.

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Selezionare la casella di controllo per ciascun gruppo che si desidera eliminare.
3. Selezionare **azioni > Elimina gruppo** o **azioni > Elimina gruppi**.

Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Delete group** (Elimina gruppo) o **Delete groups** (Elimina gruppi).

Imposta AssumeRole

Prima di iniziare

Per configurare AssumeRole devi essere un amministratore.

A proposito di questa attività

Per impostare AssumeRole, creare il gruppo di destinazione da assumere, se il gruppo non esiste già. Modificare i criteri S3 del gruppo per specificare le azioni consentite per l'assunzione di questo gruppo. Modificare i criteri di attendibilità S3 del gruppo per specificare gli utenti attendibili autorizzati ad assumere il ruolo del gruppo con l'API AssumeRole.

Credenziali di sicurezza temporanee create presupponendo che questo gruppo sia valido per una durata limitata. La sessione dura tra 15 minuti e 12 ore e la sessione predefinita è di 1 ora. Quando si rimuove l'utente dai criteri di attendibilità S3 del gruppo, l'utente non può più assumere questo gruppo.

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Fare clic sul nome del gruppo.
3. Selezionare la scheda **Criterio di attendibilità S3**.
4. Aggiungi i tuoi criteri di attendibilità S3, incluso un elenco di utenti che possono eseguire AssumeRole.
5. Selezionare **Save Changes** (Salva modifiche).
6. Selezionare la scheda **Criteri di gruppo S3**.
7. Modificare il criterio S3 per specificare solo le azioni S3 richieste per gli utenti attendibili aggiunti nel criterio di attendibilità S3 di questo gruppo.
8. Selezionare **Save Changes** (Salva modifiche).

Esempio di una policy di trust AssumeRole S3

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": [
          "urn:sgws:identity::1234567890:user/user1",
          "arn:aws:iam::1234567890:user/user2"
        ]
      }
    }
  ]
}
```

Una volta completata la configurazione, gli utenti elencati nei criteri di attendibilità S3 possono eseguire

AssumeRole e ricevere le credenziali. Le autorizzazioni finali sono determinate dai criteri di gruppo, dai criteri del bucket e dai criteri di sessione. Per ulteriori informazioni, consultare ["Utilizzare le policy di accesso"](#).

Gestire gli utenti

È possibile creare utenti locali e assegnarli a gruppi locali per determinare a quali funzionalità possono accedere. È anche possibile importare utenti federati. 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.



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

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).
- Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è stato esaminato il flusso di lavoro e le considerazioni relative a ["clonazione di utenti e gruppi tenant"](#) e si è effettuato l'accesso alla griglia di origine del tenant.

Crea un utente locale

È possibile creare un utente locale e assegnarlo 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.

Accedere alla procedura guidata Crea utente

Fasi

1. Selezionare **Gestione accessi > Utenti**.

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, un banner blu indica che si tratta della griglia di origine del tenant. Tutti gli utenti locali creati in questa griglia verranno clonati nell'altra griglia della connessione.

Users

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

Create local user Import federated users Actions Search users by full name or username

Displaying one result

This tenant has Use grid federation connection permission for connection Grid 1 to Grid 2. New local tenant users will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a user, your changes will not be synced to the other grid.

Username	Full name	Denied access	Type
root	Root	No	Local

Previous Next

2. Selezionare **Crea utente**.

Immettere le credenziali

Fasi

1. Per il passo **inserire le credenziali utente**, completare i seguenti campi.

Campo	Descrizione
Nome completo	Il nome completo dell'utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
Nome utente	Il nome utilizzato dall'utente per l'accesso. I nomi utente devono essere univoci e non possono essere modificati. Nota: Se l'account tenant dispone dell'autorizzazione Usa connessione federazione griglia , si verificherà un errore di clonazione se lo stesso Nome utente esiste già per il tenant nella griglia di destinazione.
Password e Conferma password	La password che l'utente utilizzerà inizialmente al momento dell'accesso.
Negare l'accesso	Selezionare Sì per impedire a questo utente di accedere all'account tenant, anche se potrebbe ancora appartenere a uno o più gruppi. Ad esempio, selezionare Sì per sospendere temporaneamente la possibilità di accesso dell'utente.

2. Selezionare **continua**.

Assegnare ai gruppi

Fasi

1. Assegnare l'utente a uno o più gruppi locali per determinare quali attività possono eseguire.

L'assegnazione di un utente ai gruppi è facoltativa. Se preferisci, puoi selezionare gli utenti quando crei o modifichi i gruppi.

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. Vedere ["Permessi di gestione del tenant"](#).

2. Selezionare **Crea utente**.

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ci si trova nella griglia di origine del tenant, il nuovo utente locale viene clonato nella griglia di destinazione del tenant. **Success** viene visualizzato come **Cloning status** nella sezione Overview della pagina dei dettagli dell'utente.


3. Selezionare **fine** per tornare alla pagina utenti.

Visualizzare o modificare l'utente locale

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Consultare le informazioni fornite nella pagina utenti, che elenca le informazioni di base per tutti gli utenti locali e federati per questo account tenant.

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando l'utente nella griglia di origine del tenant:

- Un messaggio banner indica che se si modifica o si rimuove un utente, le modifiche non verranno sincronizzate con l'altra griglia.
 - Se necessario, un messaggio di intestazione indica se gli utenti non sono stati clonati nel tenant sulla griglia di destinazione. È possibile [riprovare un clone utente non riuscito](#).
3. Se si desidera modificare il nome completo dell'utente:
 - a. Selezionare la casella di controllo dell'utente.
 - b. Selezionare **azioni > Modifica nome completo**.
 - c. Inserire il nuovo nome.
 - d. Selezionare **Salva modifiche**.
 4. Se si desidera visualizzare ulteriori dettagli o apportare modifiche aggiuntive, effettuare una delle seguenti operazioni:
 - Selezionare il nome utente.
 - Selezionare la casella di controllo dell'utente e selezionare **azioni > Visualizza dettagli utente**.
 5. Consultare la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:
 - Nome completo
 - Nome utente
 - Tipo di utente
 - Accesso negato
 - Modalità di accesso
 - Appartenenza al gruppo
 - Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e l'utente viene visualizzato nella griglia di origine del tenant:
 - Stato di cloning, **Success** o **Failure**
 - Un banner blu che indica che se modifichi questo utente, le modifiche non verranno sincronizzate con l'altra griglia.
 6. Modificare le impostazioni utente in base alle esigenze. Vedere [Creare un utente locale](#) per i dettagli su cosa immettere.
 - a. Nella sezione Panoramica , modificare il nome completo selezionando il nome o l'icona di modifica .
 - Impossibile modificare il nome utente.
 - b. Nella scheda **Password**, modificare la password dell'utente e selezionare **Salva modifiche**.
 - c. Nella scheda **accesso**, selezionare **No** per consentire all'utente di accedere o selezionare **Sì** per impedire all'utente di accedere. Quindi, selezionare **Salva modifiche**.

- d. Nella scheda **tasti di accesso**, selezionare **Crea tasto** e seguire le istruzioni per "[Creazione delle chiavi di accesso S3 di un altro utente](#)".
- e. Nella scheda **gruppi**, selezionare **Modifica gruppi** per aggiungere l'utente ai gruppi o rimuoverlo dai gruppi. Quindi, selezionare **Save Changes** (Salva modifiche).
7. Confermare di aver selezionato **Save Changes** (Salva modifiche) per ciascuna sezione modificata.

Importa utenti federati

È possibile importare uno o più utenti federati, fino a un massimo di 100 utenti, direttamente nella pagina Utenti.

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Seleziona **Importa utenti federati**.
3. Inserisci l'UUID o il nome utente di uno o più utenti federati.

Per voci multiple, aggiungere ogni UUID o nome utente su una nuova riga.

4. Selezionare **Importa**.

Se l'importazione nel campo Utenti non riesce per uno o più utenti, procedere come segue:

- a. Espandi **Utenti non importati** e seleziona **Copia utenti**.
- b. Riprovare l'importazione selezionando **Precedente** e incollando gli utenti copiati nella finestra di dialogo **Importa utenti federati**.

Dopo aver chiuso la finestra di dialogo **Importa utenti federati**, le informazioni sugli utenti federati vengono visualizzate nella pagina Utenti per gli utenti importati correttamente.

Utente locale duplicato

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



Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si duplica un utente dalla griglia di origine del tenant, l'utente duplicato verrà clonato nella griglia di destinazione del tenant.

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Selezionare la casella di controllo dell'utente che si desidera duplicare.
3. Selezionare **azioni > utente duplicato**.
4. Vedere [Creare un utente locale](#) per i dettagli su cosa immettere.
5. Selezionare **Crea utente**.

Riprova clone utente

Per riprovare un clone non riuscito:

1. Selezionare ogni utente che indica (*clonazione non riuscita*) sotto il nome utente.

2. Selezionare **azioni > Clona utenti**.
3. Visualizzare lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun utente che si sta clonando.

Per ulteriori informazioni, vedere ["Clonare utenti e gruppi tenant"](#).

Eliminare uno o più utenti locali

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



Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si elimina un utente locale, StorageGRID non eliminerà l'utente corrispondente sull'altra griglia. Se è necessario mantenere queste informazioni sincronizzate, è necessario eliminare lo stesso utente da entrambe le griglie.



Per eliminare gli utenti federati, è necessario utilizzare l'origine delle identità federate.

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Selezionare la casella di controllo per ciascun utente che si desidera eliminare.
3. Selezionare **azioni > Elimina utente** o **azioni > Elimina utenti**.

Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Delete user** (Elimina utente) o **Delete users** (Elimina utenti).

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 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.