Gestire gruppi di tenant

StorageGRID software

NetApp
December 03, 2025

Sommario

Gestire gruppi di tenant . . . 1
- Creare gruppi per un tenant S3 . . . 1
  - Accedi alla procedura guidata Crea gruppo . . . 1
  - Scegli un tipo di gruppo . . . 1
  - Gestisci i permessi del gruppo . . . 2
  - Imposta i criteri di gruppo S3 . . . 2
  - Aggiungi utenti (solo gruppi locali) . . . 3
- Creare gruppi per un tenant Swift . . . 4
  - Accedi alla procedura guidata Crea gruppo . . . 4
  - Scegli un tipo di gruppo . . . 4
  - Gestisci i permessi del gruppo . . . 5
  - Imposta i criteri di gruppo Swift . . . 5
  - Aggiungi utenti (solo gruppi locali) . . . 5
- Autorizzazioni di gestione degli inquilini . . . 6
- Gestisci gruppi . . . 7
  - Visualizza o modifica il gruppo . . . 8
  - Gruppo duplicato . . . 9
    - Riprova a clonare il gruppo . . . 10
  - Elimina uno o più gruppi . . . 10

Gestire 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

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Appartieni a un gruppo di utenti che ha il"Permesso di accesso root" .
- Se si prevede di importare un gruppo federato, è necessario"federazione di identità configurata" e il gruppo federato esiste già nell'origine identità configurata.
- Se il tuo account tenant ha l'autorizzazione **Usa connessione federazione griglia**, hai esaminato il flusso di lavoro e le considerazioni per"clonazione di gruppi di tenant e utenti" e hai effettuato l'accesso alla griglia di origine del tenant.

Accedi alla procedura guidata Crea gruppo

Come primo passo, accedi alla procedura guidata Crea gruppo.

Passi

1. Selezionare **GESTIONE ACCESSI** > **Gruppi**.
2. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, verifica che venga visualizzato un banner blu, che indica che i nuovi gruppi creati su questa griglia verranno clonati nello stesso tenant sull'altra griglia nella connessione. Se questo banner non viene visualizzato, è possibile che tu abbia effettuato l'accesso alla griglia di destinazione del tenant.

3. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

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

Passi

1. Selezionare la scheda **Gruppo locale** per creare un gruppo locale oppure selezionare la scheda **Gruppo federato** per importare un gruppo dall'origine identità configurata in precedenza.

   Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), gli utenti appartenenti a gruppi locali non potranno accedere a Tenant Manager, sebbene possano utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni del gruppo.

2. Inserisci il nome del gruppo.
   - **Gruppo locale**: immettere sia un nome visualizzato che un nome univoco. Potrai 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 sulla griglia di destinazione.

   - **Gruppo federato**: 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.
3. Selezionare **Continua**.

Gestisci i permessi del gruppo

Le autorizzazioni di gruppo controllano quali attività gli utenti possono eseguire in Tenant Manager e nell'API Tenant Management.

Passi

1. Per **Modalità di accesso**, seleziona una delle seguenti opzioni:
   - **Lettura-scrittura** (predefinito): gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
   - **Sola lettura**: gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Tenant Manager o Tenant Management API. Gli utenti locali con privilegi di sola lettura possono modificare le proprie password.

     > Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su Sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Seleziona una o più autorizzazioni per questo gruppo.

   Vedere "Autorizzazioni di gestione degli inquilini" .

3. Selezionare **Continua**.

Imposta i criteri di gruppo S3

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

Passi

1. Seleziona il criterio che vuoi utilizzare per questo gruppo.

Criteri di gruppo	Descrizione
Nessun accesso S3	Predefinito. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non venga concesso tramite un criterio bucket. Se si seleziona questa opzione, per impostazione predefinita solo l'utente root avrà accesso alle risorse S3.
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 oggetti e leggere dati, metadati e tag degli oggetti. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Non puoi 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 con accesso completo. Non puoi modificare questa stringa.
Mitigazione del ransomware	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 definitivamente gli oggetti dai bucket in cui è abilitato il controllo delle versioni degli oggetti. Gli utenti Tenant Manager che dispongono dell'autorizzazione **Gestisci tutti i bucket** possono ignorare questo criterio di gruppo. Limitare l'autorizzazione Gestisci tutti i bucket agli utenti attendibili e utilizzare l'autenticazione a più fattori (MFA) laddove disponibile.
Costume	Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

2. Se hai selezionato **Personalizzato**, inserisci i criteri di gruppo. Ogni criterio di gruppo ha un limite di dimensione di 5.120 byte. È necessario immettere una stringa valida in formato JSON.

   Per informazioni dettagliate sui criteri di gruppo, inclusa la sintassi del linguaggio e gli esempi, vedere"Criteri di gruppo di esempio" .

3. Se stai creando un gruppo locale, seleziona **Continua**. Se stai creando un gruppo federato, seleziona **Crea gruppo** e **Fine**.

Aggiungi utenti (solo gruppi locali)

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

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, tutti gli utenti selezionati quando si crea un gruppo locale sulla griglia di origine non verranno inclusi quando il gruppo viene clonato sulla griglia di destinazione. Per questo motivo, non selezionare gli utenti quando crei il gruppo. In alternativa, seleziona il gruppo quando crei gli utenti.

Passi

1. Facoltativamente, seleziona uno o più utenti locali per questo gruppo.
2. Seleziona **Crea gruppo** e **Fine**.

   Il gruppo che hai creato appare nell'elenco dei gruppi.

   Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ti trovi sulla griglia di origine del tenant, il nuovo gruppo viene clonato nella griglia di destinazione del tenant. **Successo** appare come **Stato di clonazione** nella sezione Panoramica della pagina dei dettagli del gruppo.

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 di amministratore Swift, necessaria per gestire i contenitori e gli oggetti per un account tenant Swift.

Il supporto per le applicazioni client Swift è stato deprecato e verrà rimosso in una versione futura.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Appartieni a un gruppo di utenti che ha il"Permesso di accesso root" .
- Se si prevede di importare un gruppo federato, è necessario"federazione di identità configurata" e il gruppo federato esiste già nell'origine identità configurata.

Accedi alla procedura guidata Crea gruppo

Passi

Come primo passo, accedi alla procedura guidata Crea gruppo.

1. Selezionare **GESTIONE ACCESSI** > **Gruppi**.
2. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

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

Passi

1. Selezionare la scheda **Gruppo locale** per creare un gruppo locale oppure selezionare la scheda **Gruppo federato** per importare un gruppo dall'origine identità configurata in precedenza.

   Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), gli utenti appartenenti a gruppi locali non potranno accedere a Tenant Manager, sebbene possano utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni del gruppo.

2. Inserisci il nome del gruppo.

- **Gruppo locale**: immettere sia un nome visualizzato che un nome univoco. Potrai modificare il nome visualizzato in un secondo momento.
- **Gruppo federato**: 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.

3. Selezionare **Continua**.

Gestisci i permessi del gruppo

Le autorizzazioni di gruppo controllano quali attività gli utenti possono eseguire in Tenant Manager e nell'API Tenant Management.

Passi

1. Per **Modalità di accesso**, seleziona una delle seguenti opzioni:
   - **Lettura-scrittura** (predefinito): gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
   - **Sola lettura**: gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Tenant Manager o Tenant Management API. Gli utenti locali con privilegi di sola lettura possono modificare le proprie password.

   > Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su Sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Selezionare la casella di controllo **Accesso root** se gli utenti del gruppo devono accedere a Tenant Manager o all'API Tenant Management.
3. Selezionare **Continua**.

Imposta i criteri di gruppo Swift

Gli utenti Swift necessitano dell'autorizzazione di amministratore per autenticarsi nella Swift REST API per creare contenitori e acquisire oggetti.

1. Selezionare la casella di controllo **Amministratore Swift** se gli utenti del gruppo devono utilizzare l'API REST Swift per gestire contenitori e oggetti.
2. Se stai creando un gruppo locale, seleziona **Continua**. Se stai creando un gruppo federato, seleziona **Crea gruppo** e **Fine**.

Aggiungi utenti (solo gruppi locali)

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

Passi

1. Facoltativamente, seleziona uno o più utenti locali per questo gruppo.

   Se non hai ancora creato utenti locali, puoi aggiungere questo gruppo all'utente nella pagina Utenti. Vedere "Gestisci gli utenti locali" .

2. Seleziona **Crea gruppo** e **Fine**.

Il gruppo che hai creato appare nell'elenco dei gruppi.

Autorizzazioni di gestione degli inquilini

Prima di creare un gruppo di tenant, valuta quali autorizzazioni vuoi assegnare a quel gruppo. Le autorizzazioni di gestione degli inquilini determinano quali attività gli utenti possono eseguire utilizzando Tenant Manager o Tenant Management API. 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 Tenant Management, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono effettuare l'accesso possono eseguire le seguenti attività:

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

Per tutte le autorizzazioni, l'impostazione Modalità di accesso del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni oppure se possono solo visualizzare le impostazioni e le funzionalità correlate.

Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su Sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

È possibile assegnare le seguenti autorizzazioni a un gruppo. Si noti che i tenant S3 e i tenant Swift hanno autorizzazioni di gruppo diverse.

Permesso	Descrizione	Dettagli
Accesso root	Fornisce accesso completo al Tenant Manager e all'API Tenant Management.	Gli utenti Swift devono disporre dell'autorizzazione di accesso Root per accedere all'account tenant.
Amministratore	Solo per inquilini Swift. Fornisce l'accesso completo ai contenitori e agli oggetti Swift per questo account tenant	Gli utenti Swift devono disporre dell'autorizzazione di amministratore Swift per eseguire qualsiasi operazione con la Swift REST API.
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 **ARCHIVIAZIONE (S3)** > **Le mie chiavi di accesso S3**.

Permesso	Descrizione	Dettagli
Visualizza tutti i bucket	**Tenant S3**: consente agli utenti di visualizzare tutti i bucket e le relative configurazioni. **Tenant Swift**: consente agli utenti Swift di visualizzare tutti i container e le configurazioni dei container utilizzando l'API di gestione dei tenant.	Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu **Bucket**. Questa autorizzazione è sostituita dall'autorizzazione Gestisci tutti i bucket. Non influisce sui criteri di gruppo o sui bucket S3 utilizzati dai client S3 o dalla console S3. È possibile assegnare questa autorizzazione solo ai gruppi Swift dall'API di gestione tenant. Non è possibile assegnare questa autorizzazione ai gruppi Swift tramite Tenant Manager.
Gestisci tutti i bucket	**Tenant S3**: 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. **Tenant Swift**: consente agli utenti Swift di controllare la coerenza dei contenitori Swift utilizzando l'API di gestione dei tenant.	Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu **Bucket**. Questa autorizzazione sostituisce l'autorizzazione Visualizza tutti i bucket. Non influisce sui criteri di gruppo o sui bucket S3 utilizzati dai client S3 o dalla console S3. È possibile assegnare questa autorizzazione solo ai gruppi Swift dall'API di gestione tenant. Non è possibile assegnare questa autorizzazione ai gruppi Swift tramite Tenant Manager.
Gestisci gli endpoint	Consente agli utenti di utilizzare Tenant Manager o l'API Tenant Management per creare o modificare gli endpoint dei servizi della piattaforma, utilizzati come destinazione per i servizi della piattaforma StorageGRID .	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu **Endpoint dei servizi della piattaforma**.
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.	

Gestisci gruppi

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

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Appartieni a un gruppo di utenti che ha il"Permesso di accesso root" .

Visualizza o modifica il gruppo

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

Passi

1. Selezionare **GESTIONE ACCESSI** > **Gruppi**.
2. Esaminare 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 sulla griglia di origine del tenant:

   - Un messaggio banner indica che se modifichi o rimuovi un gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
   - Se necessario, un messaggio banner indica se i gruppi non sono stati clonati nel tenant sulla griglia di destinazione. Puoiriprovare un clone di gruppo che ha fallito.
3. Se vuoi cambiare il nome del gruppo:
   a. Selezionare la casella di controllo per il gruppo.
   b. Seleziona **Azioni** > **Modifica nome gruppo**.
   c. Inserisci il nuovo nome.
   d. Seleziona **Salva modifiche.**
4. Se desideri visualizzare maggiori dettagli o apportare modifiche aggiuntive, procedi in uno dei seguenti modi:
   - Selezionare il nome del gruppo.
   - Seleziona la casella di controllo per il gruppo e seleziona **Azioni** > **Visualizza dettagli gruppo**.
5. Esaminare la sezione Panoramica, che mostra le seguenti informazioni per ciascun gruppo:
   - Nome da visualizzare
   - Nome univoco
   - Tipo
   - Modalità di accesso
   - Permessi
   - Politica S3
   - Numero di utenti in questo gruppo
   - Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando il gruppo sulla griglia di origine del tenant:
     - Stato della clonazione, **Riuscito** o **Fallito**
     - Un banner blu che indica che se modifichi o elimini questo gruppo, le tue modifiche non verranno sincronizzate con l'altra griglia.
6. Modificare le impostazioni del gruppo secondo necessità. Vedere"Creare gruppi per un tenant S3"

E"Creare gruppi per un tenant Swift" per i dettagli su cosa inserire.

a. Nella sezione Panoramica, modifica il nome visualizzato selezionando il nome o l'icona di modifica .

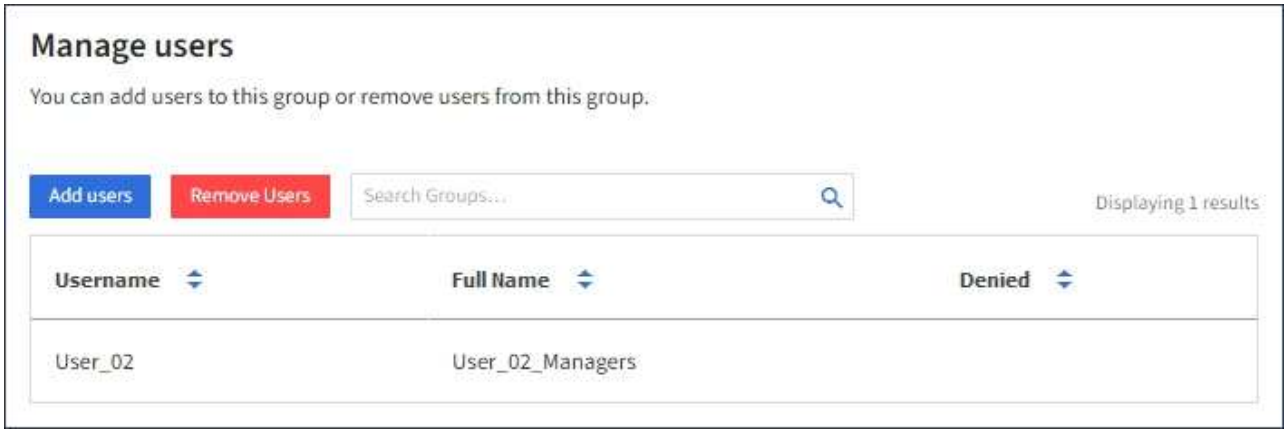
b. Nella scheda **Autorizzazioni gruppo**, aggiorna le autorizzazioni e seleziona **Salva modifiche**.

c. Nella scheda **Criteri di gruppo**, apportare le modifiche desiderate e selezionare **Salva modifiche**.

- Se si sta modificando un gruppo S3, è possibile selezionare facoltativamente un criterio di gruppo S3 diverso oppure immettere la stringa JSON per un criterio personalizzato, a seconda delle necessità.
- Se stai modificando un gruppo Swift, seleziona o deseleziona facoltativamente la casella di controllo **Amministratore Swift**.

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

a. Selezionare la scheda Utenti.



b. Seleziona **Aggiungi utenti**.

c. Seleziona gli utenti esistenti che desideri aggiungere e seleziona **Aggiungi utenti**.

In alto a destra appare un messaggio di conferma.

8. Per rimuovere gli utenti locali dal gruppo:

a. Selezionare la scheda Utenti.

b. Seleziona **Rimuovi utenti**.

c. Seleziona gli utenti che vuoi rimuovere e seleziona **Rimuovi utenti**.

In alto a destra appare un messaggio di conferma.

9. Conferma di aver selezionato **Salva modifiche** per ogni sezione modificata.

Gruppo duplicato

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

Se l'account del 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.

Passi

1. Selezionare **GESTIONE ACCESSI** > **Gruppi**.
2. Seleziona la casella di controllo relativa al gruppo che desideri duplicare.
3. Selezionare **Azioni** > **Duplica gruppo**.
4. Vedere"Creare gruppi per un tenant S3" O"Creare gruppi per un tenant Swift" per i dettagli su cosa inserire.
5. Seleziona **Crea gruppo**.

Riprova a clonare il gruppo

Per riprovare una clonazione non riuscita:

1. Selezionare ciascun gruppo che indica *(Clonazione non riuscita)* sotto il nome del gruppo.
2. Selezionare **Azioni** > **Clona gruppi**.
3. Visualizza lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun gruppo che stai clonando.

Per ulteriori informazioni, vedere"Clona gruppi tenant e utenti" .

Elimina uno o più gruppi

È possibile eliminare uno o più gruppi. Gli utenti che appartengono solo a un gruppo eliminato non potranno più accedere a 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 sincronizzate queste informazioni, è necessario eliminare lo stesso gruppo da entrambe le griglie.

Passi

1. Selezionare **GESTIONE ACCESSI** > **Gruppi**.
2. Seleziona la casella di controllo per ogni gruppo che desideri eliminare.
3. Selezionare **Azioni** > **Elimina gruppo** o **Azioni** > **Elimina gruppi**.

   Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Elimina gruppo** o **Elimina gruppi**.

Informazioni sul copyright

Informazioni sul marchio commerciale