Gestire i gruppi di tenant

StorageGRID software

NetApp
February 12, 2026

Sommario

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

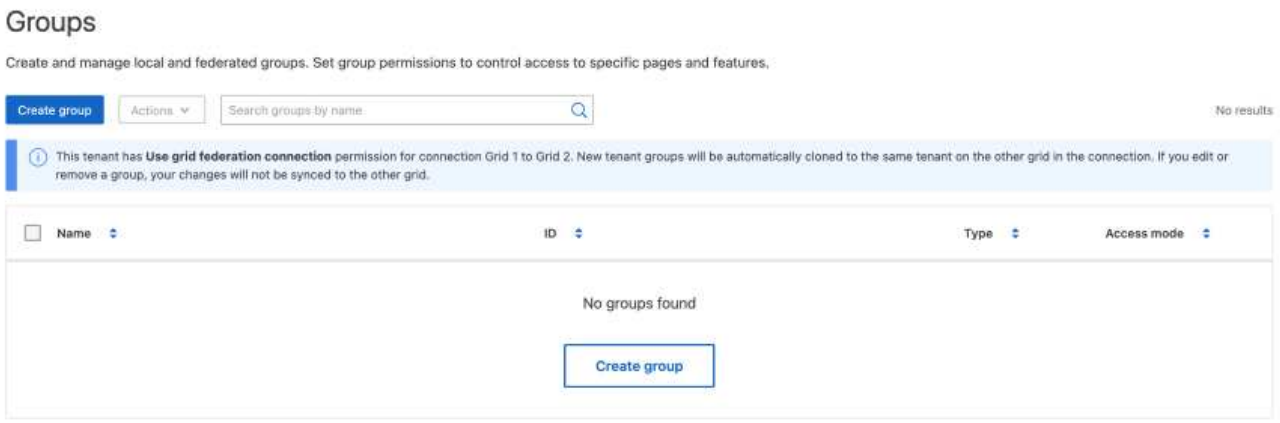
- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".
- Se si prevede di importare un gruppo federated, si dispone di "federazione di identità configurata", e 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.



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.
Riduzione 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 in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti. 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.
Personalizzato	Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

2. 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".

3. 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

1. Facoltativamente, selezionare uno o più utenti locali per questo gruppo.
2. 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**.

Permesso	Descrizione	Dettagli
Visualizza tutti i bucket	Consente agli utenti di visualizzare tutti i bucket e le relative configurazioni.	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 bucket S3 o sui criteri di gruppo utilizzati dai client S3 o dalla console S3.
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.	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 bucket S3 o sui criteri di gruppo utilizzati dai client S3 o dalla console S3.
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.
   a. Nella sezione Panoramica , modificare il nome visualizzato selezionando il nome o l'icona di modifica  .
   b. Nella scheda **permessi di gruppo**, aggiornare le autorizzazioni e selezionare **Salva modifiche**.
   c. 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:
   a. Selezionare la scheda Users (utenti).

   b. Selezionare **Aggiungi utenti**.
   c. 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:
   a. 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" .