Gestisci i gruppi tenant

StorageGRID software

NetApp
July 23, 2026

Sommario

Gestisci i gruppi tenant

Creare gruppi per un tenant S3 in StorageGRID

${post_edited_translations.segment}

Prima di iniziare

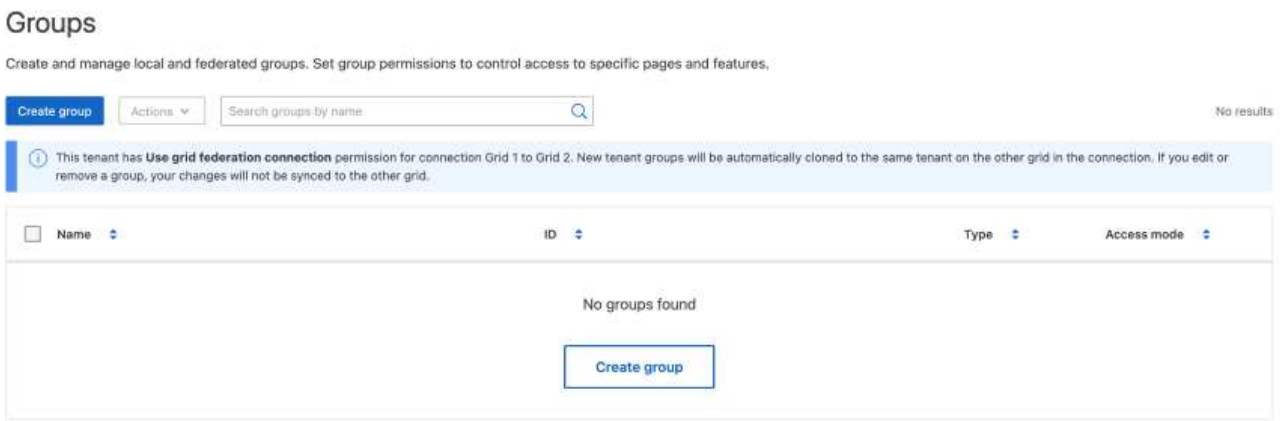
- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Permesso di accesso root".
- Se pianifichi di importare un gruppo federato, hai "${post_edited_translations.segment}" e il gruppo federato esiste già nell'origine dell'identità configurata.
- Se il tuo account tenant dispone dell'autorizzazione **Use grid federation connection**, hai esaminato il workflow e le considerazioni per "${post_edited_translations.segment}" e hai effettuato l'accesso alla grid di origine del tenant.

Accedi alla procedura guidata Crea gruppo

Come primo passo, accedi alla procedura guidata Crea gruppo.

Passaggi

1. ${post_edited_translations.segment}
2. Se il tuo account tenant dispone dell'autorizzazione **Use grid federation connection**, conferma che venga visualizzato un banner blu, a indicare che i nuovi gruppi creati su questa griglia verranno clonati sullo stesso tenant sull'altra griglia della connessione. Se questo banner non viene visualizzato, potresti aver effettuato l'accesso alla griglia di destinazione del tenant.



3. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

Puoi creare un gruppo locale o importare un gruppo federato.

Passaggi

1. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
   - **Gruppo locale**: Inserisci sia un nome visualizzato che un nome univoco. Puoi modificare il nome visualizzato in seguito.

     ${post_edited_translations.segment}

   - **Gruppo federato**: Inserisci il nome univoco. Per Active Directory, il nome univoco è il nome associato all'attributo `sAMAccountName`. Per OpenLDAP, il nome univoco è il nome associato all'attributo `uid`.
3. Seleziona **Continue**.

Gestisci le autorizzazioni di gruppo

${post_edited_translations.segment}

Passaggi

1. Per la **modalità di accesso**, seleziona una delle seguenti opzioni:
   - ${post_edited_translations.segment}
   - **Sola lettura**: gli utenti possono solo visualizzare le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nel Tenant Manager o nella Tenant Management API. Gli utenti locali in 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.

   Vedi "Autorizzazioni per la gestione dei tenant".
3. Seleziona **Continue**.

Imposta i criteri di gruppo S3

Il criterio di gruppo determina quali autorizzazioni di accesso S3 avranno gli utenti.

Passaggi

1. Seleziona il criterio che vuoi usare 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 una bucket policy. Se scegli questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.

Criteri di gruppo	Descrizione
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 selezioni questa opzione, la stringa JSON per un criterio di gruppo di sola lettura appare nella casella di testo. Non puoi modificare questa stringa.
Accesso completo	Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando selezioni questa opzione, la stringa JSON per un criterio di gruppo con accesso completo appare nella casella di testo. Non puoi modificare questa stringa.
Mitigazione del ransomware	Questa policy 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 oggetti dai bucket che hanno il versioning degli oggetti abilitato. Gli utenti di Tenant Manager che dispongono dell'autorizzazione **Gestisci tutti i bucket** possono ignorare questo criterio di gruppo. Limita l'autorizzazione **Gestisci tutti i bucket** agli utenti attendibili e usa l'autenticazione a più fattori (MFA) dove disponibile.
Personalizzato	Agli utenti del gruppo vengono concesse le autorizzazioni che specifichi 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. Devi inserire una stringa in formato JSON valido.

   Per informazioni dettagliate sulle policy di gruppo, inclusa la sintassi del linguaggio e gli esempi, vedi "Esempi di criteri di gruppo".

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)

Puoi salvare il gruppo senza aggiungere utenti oppure, se vuoi, aggiungere eventuali utenti locali già esistenti.

> Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia**, gli utenti che selezioni quando crei un gruppo locale sulla griglia di origine non vengono inclusi quando il gruppo viene clonato sul cluster di destinazione. Per questo motivo, non selezionare utenti quando crei il gruppo. Invece, seleziona il gruppo quando crei gli utenti.

Passaggi

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

Autorizzazioni di gestione del tenant StorageGRID

Prima di creare un gruppo di tenant, considera quali autorizzazioni desideri assegnare a tale gruppo. Le autorizzazioni di gestione del tenant determinano quali attività 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 al Tenant Manager o per utilizzare l'API Tenant Management, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono accedere possono eseguire le seguenti attività:

- Visualizza la dashboard
- ${post_edited_translations.segment}

${post_edited_translations.segment}

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.

Puoi assegnare le seguenti autorizzazioni a un gruppo.

Permesso	Descrizione	Dettagli
Accesso root	Fornisce accesso completo al Tenant Manager e al Tenant Management API.	
Gestisci le tue credenziali S3	${post_edited_translations.segment}	Gli utenti che non dispongono di questa autorizzazione non vedono l'opzione di menu **STORAGE (S3)** > **My S3 access keys**.
Visualizza tutti i bucket	Consente agli utenti di visualizzare tutti i bucket e le configurazioni dei bucket.	Gli utenti che non dispongono dell'autorizzazione "Visualizza tutti i bucket" o "Gestisci tutti i bucket" non vedono l'opzione di menu **Bucket**. Questa autorizzazione è sostituita dall'autorizzazione Manage all buckets. Non influisce sulle policy di gruppo o dei bucket S3 utilizzate dai client S3 o dalla Console S3.

Permesso	Descrizione	Dettagli
${post_edited_translations.segment}	${post_edited_translations.segment}	Gli utenti che non dispongono dell'autorizzazione "Visualizza tutti i bucket" o "Gestisci tutti i bucket" non vedono l'opzione di menu **Bucket**. Questa autorizzazione sostituisce l'autorizzazione Visualizza tutti i bucket. Non influisce sulle policy dei bucket o dei gruppi S3 utilizzate dai client S3 o dalla S3 Console.
Gestisci gli endpoint	Consente agli utenti di utilizzare il Tenant Manager o l'API di gestione dei tenant per creare o modificare gli endpoint dei servizi della piattaforma, che vengono utilizzati come destinazione per i servizi della piattaforma StorageGRID.	Gli utenti che non dispongono di questa autorizzazione non vedono l'opzione di menu **Endpoint dei servizi della piattaforma**.
Usa la scheda Console S3	${post_edited_translations.segment}	

Gestisci i gruppi tenant di StorageGRID

Gestisci i tuoi gruppi di tenant secondo necessità per visualizzare, modificare o duplicare un gruppo e altro ancora.

Prima di iniziare

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

Visualizza o modifica gruppo

Puoi visualizzare e modificare le informazioni e i dettagli di base per ogni gruppo.

Passaggi

1. ${post_edited_translations.segment}
2. Esamina le informazioni fornite nella pagina Gruppi, che elenca i dati di base di tutti i gruppi locali e federati per questo tenant account.

   ${post_edited_translations.segment}

   - Un messaggio a comparsa 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. Puoi riprovare un clone di gruppo che non sono riusciti.
3. Se vuoi cambiare il nome del gruppo:
   a. ${post_edited_translations.segment}

b. Seleziona **Azioni** > **Modifica nome gruppo**.

c. ${post_edited_translations.segment}

d. Seleziona **Salva modifiche.**

4. Se desideri visualizzare maggiori dettagli o apportare ulteriori modifiche, procedi in uno dei seguenti modi:
   - Seleziona il nome del gruppo.
   - Seleziona la casella di controllo relativa al gruppo e seleziona **Azioni** > **Visualizza dettagli del gruppo**.
5. ${post_edited_translations.segment}
   - Nome da visualizzare
   - Nome unico
   - Tipo
   - Modalità di accesso
   - Autorizzazioni
   - Policy S3
   - Numero di utenti in questo gruppo
   - ${post_edited_translations.segment}
     - ${post_edited_translations.segment}
     - ${post_edited_translations.segment}
6. Modifica le impostazioni del gruppo secondo necessità. Consulta "Crea gruppi per un tenant S3" 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 di gruppo**, aggiorna le autorizzazioni e seleziona **Salva modifiche**.

   c. ${post_edited_translations.segment}

   Facoltativamente, seleziona un criterio di gruppo S3 diverso oppure inserisci la stringa JSON per un criterio personalizzato, se necessario.

7. ${post_edited_translations.segment}

   a. Seleziona la scheda Utenti.

   b. Seleziona **Aggiungi utenti**.

   c. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

8. ${post_edited_translations.segment}
   a. Seleziona la scheda Utenti.
   b. Seleziona **Rimuovi utenti**.
   c. Seleziona gli utenti che desideri rimuovere e seleziona **Rimuovi utenti**.

      ${post_edited_translations.segment}

9. Conferma di aver selezionato **Salva modifiche** per ogni sezione che hai modificato.

${post_edited_translations.segment}

Puoi duplicare un gruppo esistente per creare nuovi gruppi più rapidamente.

${post_edited_translations.segment}

Passaggi

1. ${post_edited_translations.segment}
2. Seleziona la casella di controllo per il gruppo che vuoi duplicare.
3. Seleziona **Azioni** > **Duplica gruppo**.
4. Vedi "Crea gruppi per un tenant S3" per i dettagli su cosa inserire.
5. Seleziona **Crea gruppo**.

Riprova il clone del gruppo

Per riprovare una clonazione non riuscita:

1. ${post_edited_translations.segment}
2. Seleziona **Azioni** > **Clona gruppi**.
3. Visualizza lo stato dell'operazione di clonazione dalla pagina dei dettagli di ogni gruppo che stai clonando.

Per ulteriori informazioni, consulta "${post_edited_translations.segment}".

Elimina uno o più gruppi

Puoi 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 il tuo tenant account ha l'autorizzazione **Use grid federation connection** e elimini un gruppo, StorageGRID non eliminerà il gruppo corrispondente sull'altra grid. Se vuoi mantenere queste informazioni sincronizzate, devi eliminare lo stesso gruppo da entrambe le grid.

Passaggi

1. ${post_edited_translations.segment}
2. Seleziona la casella di controllo per ogni gruppo che vuoi eliminare.
3. ${post_edited_translations.segment}

   Viene visualizzata una finestra di dialogo di conferma.

4. Seleziona **Elimina gruppo** o **Elimina gruppi**.

Configura AssumeRole

Prima di iniziare

Devi essere un amministratore per configurare AssumeRole.

Informazioni su questa attività

Per configurare AssumeRole, crea il gruppo di destinazione da assumere, se il gruppo non esiste già. Modifica la policy S3 del gruppo per specificare le azioni consentite per assumere questo gruppo. Modifica la policy di attendibilità S3 del gruppo per specificare gli utenti attendibili autorizzati ad assumere il gruppo con l'API AssumeRole.

Le credenziali di sicurezza temporanee create assumendo questo gruppo sono valide per una durata limitata. La sessione dura da 15 minuti a 12 ore e la sessione predefinita è di 1 ora. Quando rimuovi l'utente dalla policy di attendibilità S3 del gruppo, l'utente non può più assumere questo gruppo.

Passaggi

1. ${post_edited_translations.segment}
2. Fai clic sul nome del gruppo.
3. Seleziona la scheda **S3 trust policy**.
4. Aggiungi la tua policy di attendibilità S3, incluso un elenco di utenti che possono eseguire AssumeRole.
5. Seleziona **Salva modifiche**.
6. Seleziona la scheda **Criteri di gruppo S3**.
7. Modifica la policy S3 per specificare solo le azioni S3 necessarie per gli utenti attendibili aggiunti alla S3 trust policy di questo gruppo.
8. Seleziona **Salva modifiche**.

Esempio di policy di trust S3 AssumeRole

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

Al termine della configurazione, gli utenti elencati nella policy di attendibilità di S3 possono eseguire

AssumeRole e ricevere le credenziali. Le autorizzazioni finali sono determinate dalla policy di gruppo, dalla policy del bucket e dalla policy di sessione. Per ulteriori informazioni, consulta "Usa le policy di accesso".