Gestisci gruppi e utenti

StorageGRID software

NetApp
December 03, 2025

Sommario

Gestisci gruppi e utenti

Utilizzare la federazione delle identità

L'utilizzo della federazione delle identità velocizza 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, Azure Active Directory (Azure AD), OpenLDAP o Oracle Directory Server.

Prima di iniziare

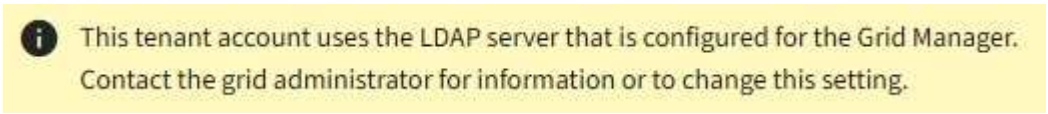
- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Appartieni a un gruppo di utenti che ha il"Permesso di accesso root" .
- Stai utilizzando Active Directory, Azure AD, OpenLDAP o Oracle Directory Server come provider di identità.

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

- Se si prevede di utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere Linee guida per la configurazione del server OpenLDAP .
- Se si prevede di utilizzare Transport Layer Security (TLS) per le comunicazioni con il server LDAP, il provider di identità deve utilizzare TLS 1.2 o 1.3. Vedere "Cifrature supportate per le connessioni TLS in uscita" .

Informazioni su questo compito

La possibilità di configurare un servizio di federazione delle identità per il tenant dipende da come è stato configurato l'account del tenant. Il tenant potrebbe condividere il servizio di federazione delle identità configurato per Grid Manager. Se visualizzi questo messaggio quando accedi alla pagina Federazione delle identità, non puoi configurare un'origine di identità federata separata per questo tenant.

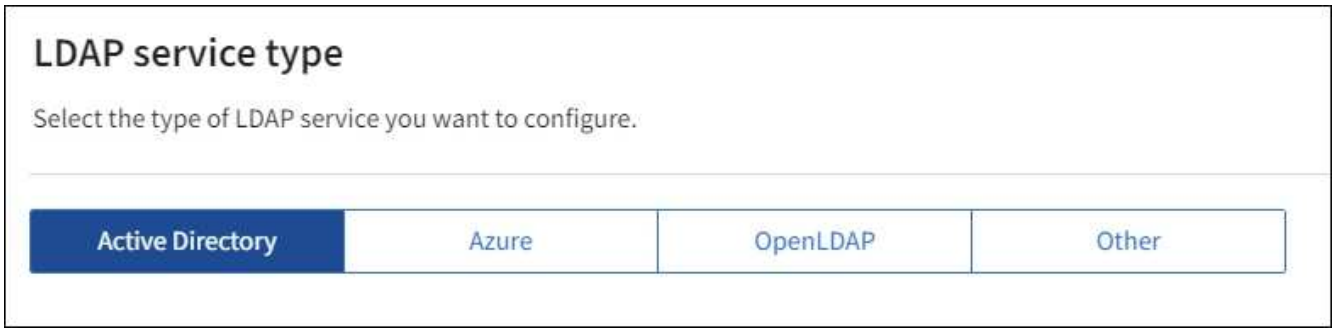


Inserisci la configurazione

Quando si configura la federazione delle identità, si forniscono i valori necessari a StorageGRID per connettersi a un servizio LDAP.

Passi

1. Selezionare **GESTIONE ACCESSI** > **Federazione identità**.
2. Selezionare **Abilita federazione delle identità**.
3. Nella sezione Tipo di servizio LDAP, seleziona il tipo di servizio LDAP che desideri configurare.



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

4. Se hai selezionato **Altro**, compila i campi nella sezione Attributi LDAP. procedere al passaggio successivo.
   - **Nome univoco utente**: il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `uid` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid` .
   - **UUID utente**: il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid` . 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 si sta configurando Oracle Directory Server, immettere `cn` .
   - **UUID gruppo**: il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid` . Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
5. Per tutti i tipi di servizio LDAP, immettere le informazioni richieste sul server LDAP e sulla connessione di rete nella sezione Configura server LDAP.
   - **Nome host**: nome di dominio completo (FQDN) o indirizzo IP del server LDAP.
   - **Porta**: la porta utilizzata per connettersi al server LDAP.

     La porta predefinita per STARTTLS è 389, mentre la porta predefinita per LDAPS è 636. Tuttavia, puoi utilizzare qualsiasi porta, a patto che il firewall sia configurato correttamente.

   - **Nome utente**: percorso completo del nome distinto (DN) dell'utente che si connetterà al server LDAP.

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

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

     - `sAMAccountName`O `uid`
     - `objectGUID`, `entryUUID` , O `nsuniqueid`
     - `cn`

- `memberOf`O `isMemberOf`
- **Directory attiva**: `objectSid` , `primaryGroupID` , `userAccountControl` , E `userPrincipalName`
- **Azzurro**: `accountEnabled` E `userPrincipalName`

◦ **Password**: la password associata al nome utente.

> Se in futuro dovessi cambiare la password, dovrai aggiornarla in questa pagina.

◦ **DN base gruppo**: percorso completo del nome distinto (DN) per un sottoalbero LDAP in cui si desidera cercare i gruppi. Nell'esempio di Active Directory (sotto), 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 **Nome univoco del gruppo** devono essere univoci all'interno del **DN di base del gruppo** a cui appartengono.

◦ **DN base utente**: percorso completo del nome distinto (DN) di un sottoalbero LDAP in cui si desidera cercare gli utenti.

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

◦ **Formato nome utente associato** (facoltativo): il modello di nome utente predefinito che StorageGRID dovrebbe utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il **formato nome utente di associazione** perché può consentire agli utenti di accedere se StorageGRID non è in grado di associarsi all'account di servizio.

Inserisci uno di questi modelli:

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

  Includi **[USERNAME]** esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), seleziona un'impostazione di sicurezza.
   ◦ **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 Azure.
   ◦ **Usa LDAPS**: l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Azure.
   ◦ **Non utilizzare TLS**: il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Azure.

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

7. Se hai selezionato STARTTLS o LDAPS, scegli il certificato utilizzato per proteggere la connessione.

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

  Se selezioni questa impostazione, copia e incolla il certificato di sicurezza personalizzato nella casella di testo Certificato CA.

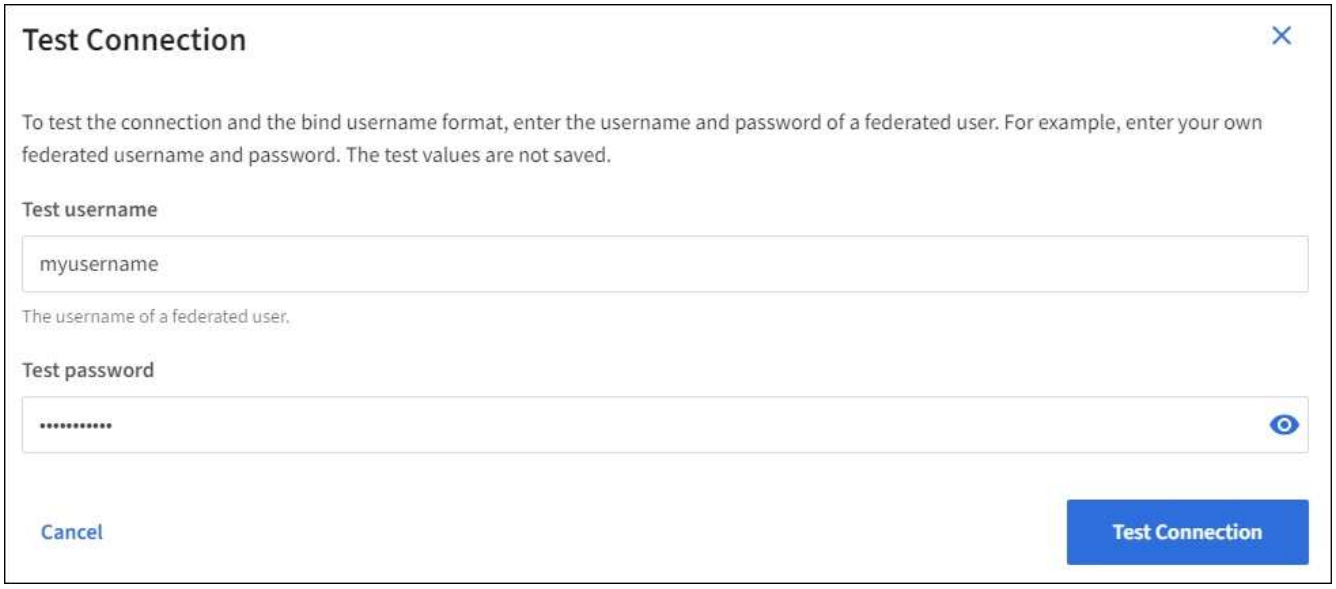
Testare la connessione e salvare la configurazione

Dopo aver immesso tutti i valori, è necessario testare la connessione prima di poter salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente associato, se ne è stato fornito uno.

Passi

1. Selezionare **Test 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 di 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, risolvi eventuali problemi e verifica nuovamente la connessione.
3. Se hai fornito un formato di nome utente vincolato, inserisci il nome utente e la password di un utente federato valido.

   Ad esempio, inserisci il tuo nome utente e la tua password. Non includere caratteri speciali nel nome utente, come @ o /.



   - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di connessione riuscito". Selezionare **Salva** per salvare la configurazione.
   - Se le impostazioni di connessione, il formato del nome utente associato o il nome utente e la password di prova non sono validi, viene visualizzato un messaggio di errore. Risolvi eventuali problemi e verifica nuovamente la connessione.

Forza la sincronizzazione con la fonte dell'identità

Il sistema StorageGRID sincronizza periodicamente i gruppi federati e gli utenti dalla fonte di identità. È possibile forzare l'avvio della sincronizzazione se si desidera abilitare o limitare le autorizzazioni utente il più rapidamente possibile.

Passi

1. Vai alla pagina Federazione delle identità.
2. Seleziona **Sincronizza server** nella parte superiore della pagina.

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

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

Disabilitare 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.

Informazioni su questo compito

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

- Gli utenti federati non potranno effettuare l'accesso.
- Gli utenti federati attualmente connessi manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno effettuare l'accesso 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 l'accesso Single Sign-On (SSO) è impostato su **Abilitato** o **Modalità Sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere "Disabilitare l'accesso singolo" .

Passi

1. Vai alla pagina Federazione delle identità.
2. Deseleziona la casella di controllo **Abilita federazione delle 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 diverse da ActiveDirectory o Azure, 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.

Sovrapposizioni di membri e raffinazione

Le sovrapposizioni memberof e refint dovrebbero essere abilitate. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo inhttp://www.openldap.org/doc/admin24/index.html["Documentazione OpenLDAP: Guida dell'amministratore 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, assicurati che i campi menzionati nella guida per Nome utente siano indicizzati per prestazioni ottimali.

Consultare le informazioni sul mantenimento dell'appartenenza al gruppo inverso inhttp://www.openldap.org/doc/admin24/index.html["Documentazione OpenLDAP: Guida dell'amministratore versione 2.4"^] .

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.

Permesso	Descrizione	Dettagli
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**.
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**.

Permesso	Descrizione	Dettagli
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

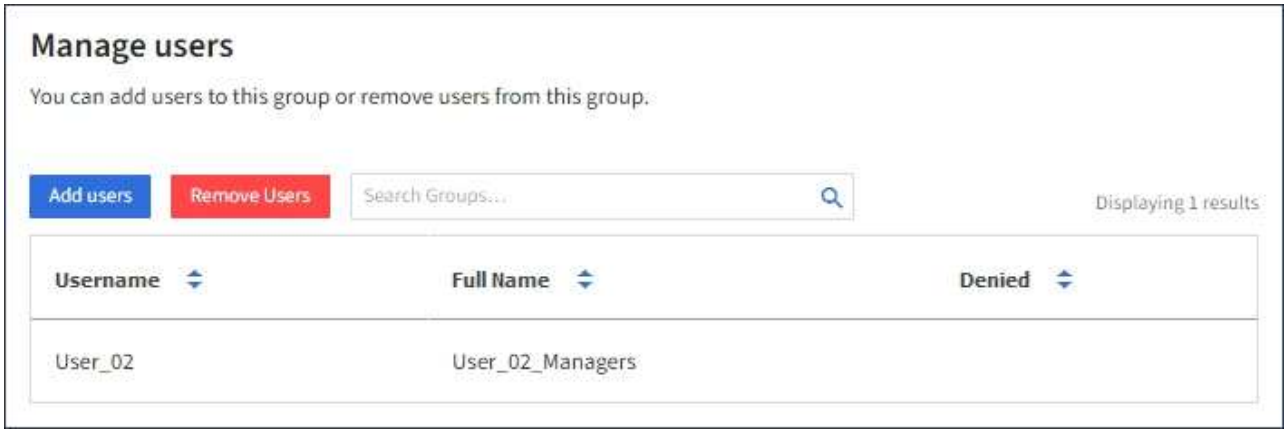
1. Selezionare **GESTIONE ACCESSI** > **Gruppi**.
2. Esaminare le informazioni fornite nella pagina Gruppi, che elenca le informazioni di base per tutti i gruppi locali e federati per questo account tenant.

   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**.

Gestisci gli utenti locali

È possibile creare utenti locali e assegnarli a gruppi locali per determinare a quali funzionalità possono accedere. Il Tenant Manager include un utente locale predefinito, denominato "root". Sebbene sia possibile aggiungere e rimuovere utenti locali, non è possibile rimuovere l'utente root.

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

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 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.

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 ad alcun gruppo non hanno autorizzazioni di gestione né criteri di gruppo S3 applicati. A questi utenti potrebbe essere concesso l'accesso al bucket S3 tramite un criterio bucket.

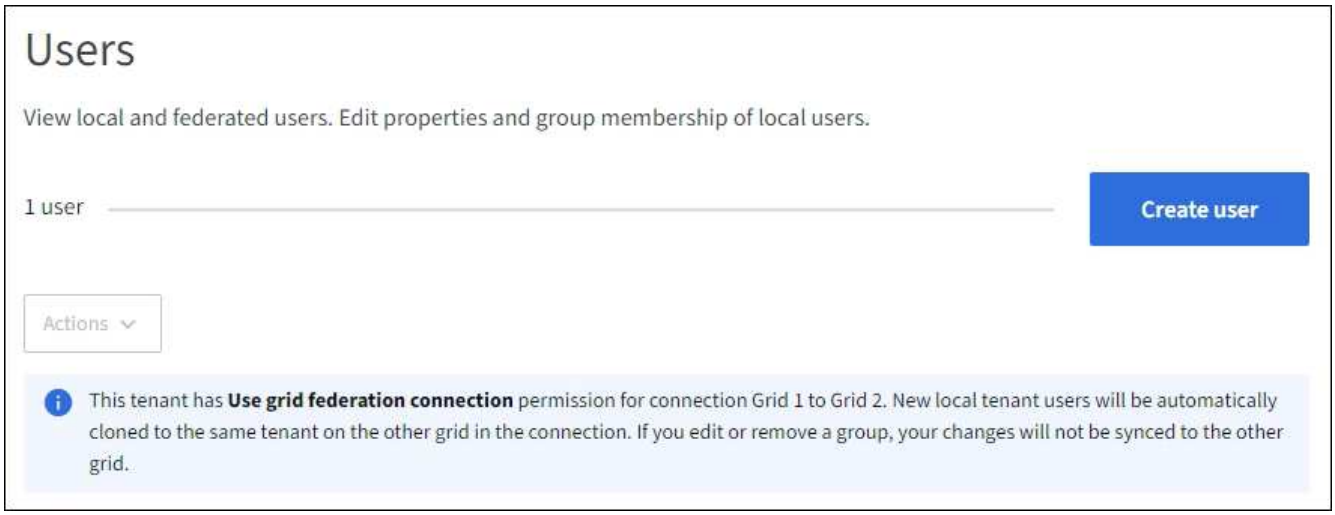
Gli utenti Swift che non appartengono ad alcun gruppo non hanno autorizzazioni di gestione né accesso al contenitore Swift.

Accedi alla procedura guidata Crea utente

Passi

1. Selezionare **GESTIONE ACCESSI** > **Utenti**.

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



2. Seleziona **Crea utente**.

Inserisci le credenziali

Passi

1. Per il passaggio **Inserisci credenziali utente**, compila i seguenti campi.

Campo	Descrizione
Nome e cognome	Il nome completo di questo utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
Nome utente	Il nome che questo utente utilizzerà per accedere. 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 sulla griglia di destinazione.
Password e Conferma password	La password che l'utente utilizzerà inizialmente per effettuare l'accesso.
Nega 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, seleziona **Sì** per sospendere temporaneamente la possibilità di un utente di accedere.

2. Selezionare **Continua**.

Assegna ai gruppi

Passi

1. Assegnare l'utente a uno o più gruppi locali per determinare quali attività può 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 ad alcun gruppo non avranno autorizzazioni di gestione. I permessi sono cumulativi. Gli utenti avranno tutte le autorizzazioni per tutti i gruppi a cui appartengono. Vedere "Autorizzazioni di gestione degli inquilini" .

2. Seleziona **Crea utente**.

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

3. Selezionare **Fine** per tornare alla pagina Utenti.

Visualizza o modifica l'utente locale

Passi

1. Selezionare **GESTIONE ACCESSI** > **Utenti**.
2. Esaminare 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 visualizza l'utente sulla griglia di origine del tenant:

   - Un messaggio banner indica che se modifichi o rimuovi un utente, le modifiche non verranno sincronizzate con l'altra griglia.
   - Se necessario, un messaggio banner indica se gli utenti non sono stati clonati nel tenant sulla griglia di destinazione. È possibile riprova un clone utente che non è riuscito Potrebbe
3. Se vuoi cambiare il nome completo dell'utente:
   a. Selezionare la casella di controllo per l'utente.
   b. Seleziona **Azioni** > **Modifica nome completo**.
   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:
   - Seleziona il nome utente.
   - Selezionare la casella di controllo per l'utente e selezionare **Azioni** > **Visualizza dettagli utente**.
5. Esaminare la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:
   - Nome e cognome
   - 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 si visualizza l'utente sulla griglia di origine del tenant:

- Stato della clonazione, **Riuscito** o **Fallito**
- Un banner blu che indica che se modifichi questo utente, le tue modifiche non verranno sincronizzate con l'altra griglia.

6. Modificare le impostazioni utente secondo necessità. VedereCrea utente locale per i dettagli su cosa inserire.
   a. Nella sezione Panoramica, modifica il nome completo selezionando il nome o l'icona di modifica .

      Non è possibile modificare il nome utente.

   b. Nella scheda **Password**, modifica la password dell'utente e seleziona **Salva modifiche**.
   c. Nella scheda **Accesso**, seleziona **No** per consentire all'utente di accedere oppure seleziona **Sì** per impedirgli di accedere. Quindi, seleziona **Salva modifiche**.
   d. Nella scheda **Chiavi di accesso**, seleziona **Crea chiave** e segui le istruzioni per"creazione delle chiavi di accesso S3 di un altro utente" .
   e. Nella scheda **Gruppi**, seleziona **Modifica gruppi** per aggiungere l'utente ai gruppi o rimuoverlo dai gruppi. Quindi, seleziona **Salva modifiche**.
7. Conferma di aver selezionato **Salva modifiche** per ogni sezione modificata.

Utente locale duplicato

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

> Se l'account del 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.

Passi

1. Selezionare **GESTIONE ACCESSI** > **Utenti**.
2. Seleziona la casella di controllo relativa all'utente che desideri duplicare.
3. Selezionare **Azioni** > **Duplica utente**.
4. VedereCrea utente locale per i dettagli su cosa inserire.
5. Seleziona **Crea utente**.

Riprova la clonazione dell'utente

Per riprovare una clonazione non riuscita:

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

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

Elimina uno o più utenti locali

È possibile eliminare definitivamente 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 sincronizzate queste informazioni, è necessario eliminare lo stesso utente da entrambe le griglie.

> Per eliminare gli utenti federati è necessario utilizzare l'origine dell'identità federata.

Passi

1. Selezionare **GESTIONE ACCESSI** > **Utenti**.
2. Seleziona la casella di controllo per ogni utente che desideri eliminare.
3. Selezionare **Azioni** > **Elimina utente** oppure **Azioni** > **Elimina utenti**.

   Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Elimina utente** o **Elimina utenti**.

Informazioni sul copyright

Informazioni sul marchio commerciale