Gestisci gruppi e utenti

StorageGRID software

NetApp
July 23, 2026

Sommario

Gestisci gruppi e utenti

Usa la federazione delle identità in StorageGRID

L'utilizzo della federazione delle identità rende più veloce la configurazione di gruppi e utenti tenant e permette agli utenti tenant di accedere all'account tenant usando le loro credenziali abituali.

Configura la federazione delle identità per Tenant Manager

Puoi configurare la federazione delle identità per il Tenant Manager se vuoi che i gruppi di tenant e gli utenti siano gestiti in un altro sistema, come Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server.

Prima di iniziare

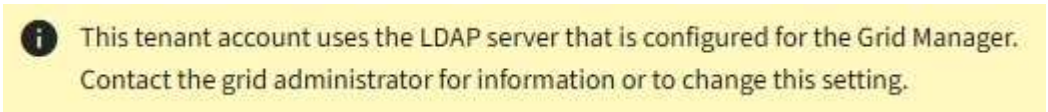
- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Permesso di accesso root".
- Stai utilizzando Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server come provider di identità.

  Se vuoi usare un servizio LDAP v3 che non è presente nell'elenco, contatta il supporto tecnico.

- Se vuoi usare OpenLDAP, devi configurare il server OpenLDAP. Vedi Linee guida per la configurazione del server OpenLDAP.
- Se vuoi utilizzare Transport Layer Security (TLS) per le comunicazioni con il LDAP server, il provider di identità deve usare TLS 1.2 o 1.3. Vedi "Algoritmi di crittografia supportati per le connessioni TLS in uscita".

Informazioni su questa attività

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

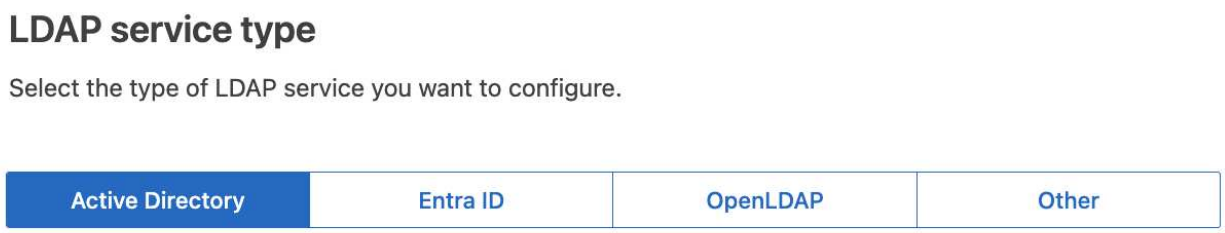


Inserisci la configurazione

Quando configuri la federazione delle identità, fornisci i valori di cui StorageGRID ha bisogno per connettersi a un servizio LDAP.

Passaggi

1. Seleziona **Gestione accessi** > **Federazione delle identità**.
2. Seleziona **Abilita federazione delle identità**.
3. Nella sezione relativa al tipo di servizio LDAP, seleziona il tipo di servizio LDAP che vuoi configurare.



Seleziona **Altro** per configurare i valori per un LDAP server che usa Oracle Directory Server.

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

     La porta predefinita per STARTTLS è 389, e la porta predefinita per LDAPS è 636. Tuttavia, puoi usare qualsiasi porta purché il firewall sia configurato correttamente.

   - **Nome utente**: Il full path del distinguished name (DN) dell'utente che si connetterà al LDAP server.

     Per Active Directory, puoi anche specificare il Down-Level Logon Name o lo User Principal Name.

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

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

- `memberOf` o `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, e `userPrincipalName`
- **Entra ID**: `accountEnabled` e `userPrincipalName`

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

> Se in futuro cambierai la password, dovrai aggiornarla su questa pagina.

◦ **DN di base del gruppo**: il full path del nome distinto (DN) per un sottoalbero LDAP in cui vuoi 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 usati come gruppi federati.

> ${post_edited_translations.segment}

◦ **DN della base utente**: Il full path del nome distinto (DN) di un sottoalbero LDAP in cui vuoi cercare gli utenti.

> I valori del **nome univoco utente** devono essere univoci all'interno del **User Base DN** a cui appartengono.

◦ ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

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

  Inserisci **[USERNAME]** esattamente come è scritto.

6. Nella sezione Transport Layer Security (TLS), seleziona un'impostazione di sicurezza.
   ◦ **Usa STARTTLS**: usa STARTTLS per proteggere le comunicazioni con il LDAP server. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma questa opzione non è supportata per Microsoft Entra ID.
   ◦ **Usa LDAPS**: L'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al LDAP server. Devi selezionare questa opzione per Microsoft Entra ID.
   ◦ **Non utilizzare TLS**: il traffico di rete tra il sistema StorageGRID e il LDAP server non sarà protetto. Questa opzione non è supportata per Microsoft Entra ID.

   > L'utilizzo dell'opzione **Non utilizzare TLS** non è supportato se il tuo server Active Directory impone la firma LDAP. Devi 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 CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.

- **Utilizza un 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 del certificato CA.

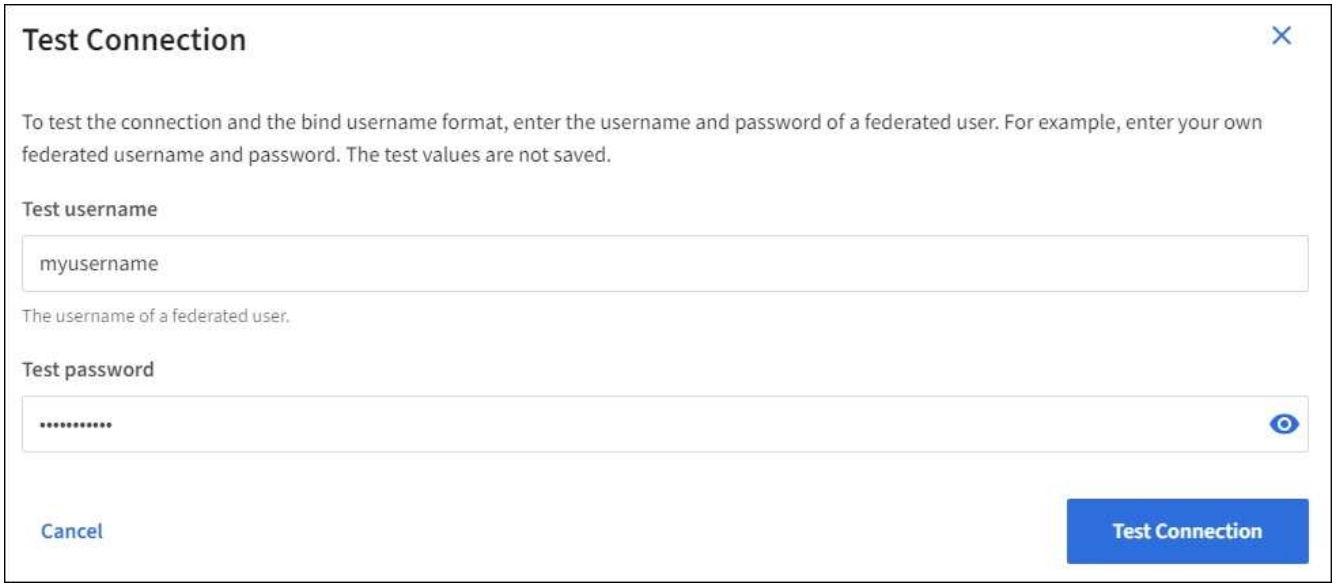
Verifica la connessione e salva la configurazione

Dopo aver inserito tutti i valori, devi testare la connessione prima di poter salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il LDAP server e il formato del nome utente di bind, se ne hai fornito uno.

Passaggi

1. Seleziona **Test connessione**.
2. Se non hai fornito un formato per il nome utente bind:
   - Viene visualizzato il messaggio "Test di connessione riuscito" se le impostazioni di connessione sono valide. Seleziona **Salva** per salvare la configurazione.
   - Viene visualizzato il messaggio "Impossibile stabilire la connessione di prova" se le impostazioni di connessione non sono valide. Seleziona **Chiudi**. Quindi, risolvi eventuali problemi e prova nuovamente la connessione.
3. Se hai specificato un formato di nome utente di bind, 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 /.



   - Viene visualizzato il messaggio "Test di connessione riuscito" se le impostazioni di connessione sono valide. Seleziona **Salva** per salvare la configurazione.
   - Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente di bind o il nome utente e la password di test non sono validi. Risolvi eventuali problemi e prova nuovamente la connessione.

Forza la sincronizzazione con l'origine di identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dalla sorgente di identità. Puoi forzare l'avvio della sincronizzazione se vuoi abilitare o limitare le autorizzazioni degli utenti il più rapidamente possibile.

Passaggi

1. Vai alla pagina di federazione delle identità.
2. ${post_edited_translations.segment}

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

   ${post_edited_translations.segment}

Disabilita la federazione delle identità

Puoi disabilitare 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 delle identità. Tuttavia, tutte le impostazioni che hai configurato vengono mantenute, permettendoti di riattivare facilmente la federazione delle identità in futuro.

Informazioni su questa attività

Prima di disabilitare la federazione delle identità, dovresti tenere presente quanto segue:

- Gli utenti federati non potranno accedere.
- Gli utenti federati attualmente connessi manterranno l'accesso al sistema StorageGRID fino alla scadenza della loro sessione, ma non potranno accedere dopo la scadenza della sessione.
- ${post_edited_translations.segment}
- La casella di controllo **Abilita federazione delle identità** è disabilitata se lo stato del single sign-on (SSO) è **Abilitato** o **Modalità Sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedi "${post_edited_translations.segment}".

Passaggi

1. Vai alla pagina di federazione delle identità.
2. Deseleziona la casella di controllo **Abilita federazione delle identità**.

Linee guida per la configurazione del server OpenLDAP

Se vuoi usare un server OpenLDAP per la federazione delle identità, devi configurare impostazioni specifiche sul server OpenLDAP.

Per le origini di identità diverse da Active Directory o Microsoft Entra ID, StorageGRID non bloccherà automaticamente l'accesso S3 per gli utenti disabilitati esternamente. Per bloccare l'accesso S3, elimina tutte le chiavi S3 dell'utente o rimuovi l'utente da tutti i gruppi.

Sovrapposizioni Memberof e Refint

Le sovrapposizioni memberof e refint devono essere abilitate. Per ulteriori informazioni, consulta le istruzioni per la manutenzione della membership inversa del gruppo nel "Documentazione di OpenLDAP: Guida dell'amministratore versione 2.4".

Indicizzazione

${post_edited_translations.segment}

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Inoltre, assicurati che i campi menzionati nell'aiuto per Nome utente siano indicizzati per prestazioni ottimali.

Vedi le informazioni sulla manutenzione dell'appartenenza inversa ai gruppi nel "Documentazione di OpenLDAP: Guida dell'amministratore versione 2.4".

Gestisci i gruppi tenant

Creare gruppi per un tenant S3 in StorageGRID

${post_edited_translations.segment}

Prima di iniziare

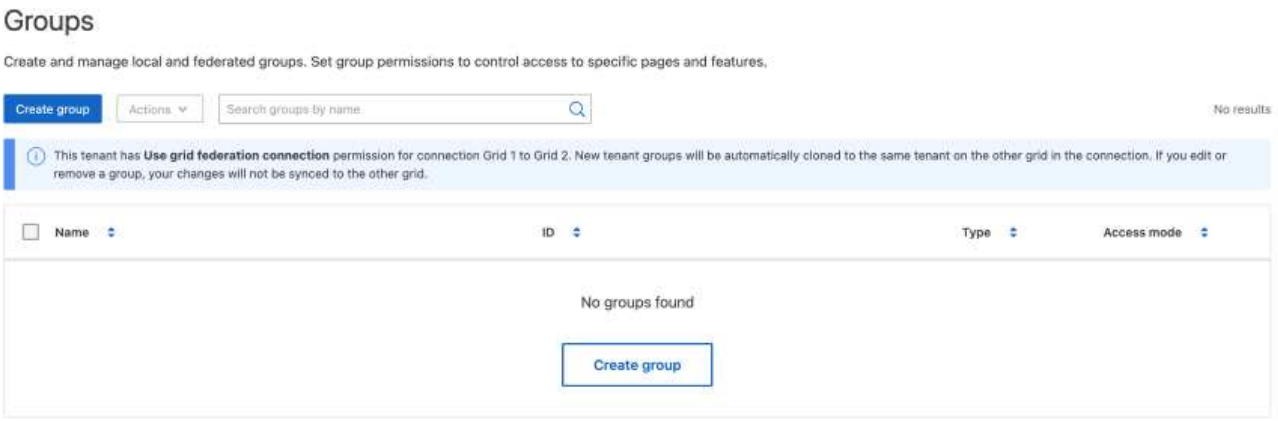
- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Permesso di accesso root".
- Se pianifichi di importare un gruppo federato, hai "${post_edited_translations.segment}" e il gruppo federato esiste già nell'origine dell'identità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

Permesso	Descrizione	Dettagli
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.
${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".

Gestisci utenti tenant di StorageGRID

Puoi creare utenti locali e assegnarli a gruppi locali per determinare a quali funzionalità questi utenti possono accedere. Puoi anche importare utenti federati. Il Tenant Manager include un utente locale predefinito, chiamato "root". Anche se puoi aggiungere e rimuovere utenti locali, non puoi rimuovere l'utente root.

${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 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.

Crea un utente locale

Puoi creare un utente locale e assegnarlo a uno o più gruppi locali per controllare le sue autorizzazioni di accesso.

Gli utenti S3 che non appartengono ad alcun gruppo non dispongono di autorizzazioni di gestione né di criteri di gruppo S3 applicati a loro. Questi utenti potrebbero avere accesso ai bucket S3 concesso tramite un criterio di bucket.

Accedi alla procedura guidata di creazione utente

Passaggi

1. Seleziona **Gestione accessi** > **Utenti**.

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

2. Seleziona **Crea utente**.

${post_edited_translations.segment}

Passaggi

1. ${post_edited_translations.segment}

Campo	Descrizione
Nome e cognome	${post_edited_translations.segment}
Nome utente	Il nome che questo utente utilizzerà per accedere. I nomi utente devono essere univoci e non possono essere cambiati. **Nota**: Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione grid**, si verificherà un errore di clonazione se lo stesso **Username** esiste già per il tenant sulla destinazione grid.
Password e Conferma password	La password che l'utente userà inizialmente per accedere.
Nega l'accesso	Seleziona **Sì** per impedire a questo utente di accedere all'account del tenant, anche se potrebbe ancora appartenere a uno o più gruppi. ${post_edited_translations.segment}

2. Seleziona **Continue**.

Assegna ai gruppi

Passaggi

1. Assegna l'utente a uno o più gruppi locali per determinare quali attività può svolgere.

   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 permessi di gestione. I permessi sono cumulativi. Gli utenti avranno tutti i permessi per tutti i gruppi a cui appartengono. Vedi "Autorizzazioni per la gestione dei tenant".

2. Seleziona **Crea utente**.

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

3. ${post_edited_translations.segment}

${post_edited_translations.segment}

Passaggi

1. Seleziona **Gestione accessi** > **Utenti**.
2. ${post_edited_translations.segment}

   Se il tenant account dispone dell'autorizzazione **Utilizza la connessione di federazione della griglia** e stai visualizzando l'utente sulla griglia di origine del tenant:

   - Un messaggio a comparsa indica che se modifichi o rimuovi un utente, le modifiche non verranno sincronizzate con l'altra grid.
   - Se necessario, un messaggio banner indica se gli utenti non sono stati clonati nel tenant sulla griglia di destinazione. Puoi ${post_edited_translations.segment}.

3. ${post_edited_translations.segment}
   a. Seleziona la casella di controllo per l'utente.
   b. ${post_edited_translations.segment}
   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 utente.
   - ${post_edited_translations.segment}
5. Esamina la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:
   - Nome e cognome
   - Nome utente
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Modalità di accesso

- ${post_edited_translations.segment}
- Campi aggiuntivi se il tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia** e stai visualizzando l'utente sulla griglia di origine del tenant:
  - ${post_edited_translations.segment}
  - Un banner blu indica che, se modifichi questo utente, le modifiche non verranno sincronizzate con l'altra grid.

6. Modifica le impostazioni utente secondo necessità. Consulta ${post_edited_translations.segment} per dettagli su cosa inserire.
   a. Nella sezione Panoramica, modifica il nome completo selezionando il nome o l'icona di modifica .

      ${post_edited_translations.segment}

   b. Nella scheda **Password**, modifica la password dell'utente e seleziona **Salva modifiche**.
   c. ${post_edited_translations.segment}
   d. Nella scheda **Chiavi di accesso**, seleziona **Crea chiave** e segui le istruzioni per "${post_edited_translations.segment}".
   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 che hai modificato.

Importa utenti federati

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

Passaggi

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

   Per inserire più voci, aggiungi ogni UUID o nome utente su una nuova riga.

4. Seleziona **Import**.

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

   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

Duplica utente locale

Puoi duplicare un utente locale per creare un nuovo utente più rapidamente.

> Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia** e duplichi un utente dalla grid di origine del tenant, l'utente duplicato verrà clonato nella grid di destinazione del tenant.

Passaggi

1. Seleziona **Gestione accessi** > **Utenti**.
2. ${post_edited_translations.segment}
3. Seleziona **Azioni** > **Duplica utente**.
4. Vedi ${post_edited_translations.segment} per i dettagli su cosa inserire.
5. Seleziona **Crea utente**.

${post_edited_translations.segment}

Per riprovare una clonazione non riuscita:

1. Seleziona ciascun utente che riporta la dicitura *(Cloning failed)* sotto il nome utente.
2. ${post_edited_translations.segment}
3. Visualizza lo stato dell'operazione di clonazione dalla pagina dei dettagli di ogni utente che stai clonando.

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

Elimina uno o più utenti locali

Puoi eliminare definitivamente uno o più utenti locali che non hanno più bisogno di accedere all'account tenant di StorageGRID.

> Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione grid** e elimini un utente locale, StorageGRID non eliminerà l'utente corrispondente sull'altra grid. Se hai bisogno di mantenere sincronizzate queste informazioni, devi eliminare lo stesso utente da entrambe le grid.

> Devi usare l'origine di identità federata per eliminare gli utenti federati.

Passaggi

1. Seleziona **Gestione accessi** > **Utenti**.
2. ${post_edited_translations.segment}
3. Seleziona **Azioni** > **Elimina utente** oppure **Azioni** > **Elimina utenti**.

   Viene visualizzata una finestra di dialogo di conferma.

4. ${post_edited_translations.segment}