Gestisci le chiavi di accesso S3

StorageGRID software

NetApp
December 03, 2025

Sommario

Gestisci le chiavi di accesso S3

Gestisci le chiavi di accesso S3

Ogni utente di un account tenant S3 deve disporre di una chiave di accesso per archiviare e recuperare oggetti nel sistema StorageGRID . Una chiave di accesso è composta da un ID chiave di accesso e da una chiave di accesso segreta.

Le chiavi di accesso S3 possono essere gestite come segue:

- Gli utenti che dispongono dell'autorizzazione **Gestisci le tue credenziali S3** possono creare o rimuovere le proprie chiavi di accesso S3.
- Gli utenti che dispongono dell'autorizzazione **Accesso root** possono gestire le chiavi di accesso per l'account root S3 e per tutti gli altri utenti. Le chiavi di accesso root forniscono l'accesso completo a tutti i bucket e oggetti per il tenant, a meno che non siano disabilitate esplicitamente da un criterio di bucket.

StorageGRID supporta l'autenticazione Signature Version 2 e Signature Version 4. L'accesso tra account non è consentito, a meno che non sia esplicitamente abilitato da un criterio bucket.

Crea le tue chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile creare le proprie chiavi di accesso S3. Per accedere ai tuoi bucket e oggetti devi disporre di una chiave di accesso.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Appartieni a un gruppo di utenti che ha il"Gestisci le tue credenziali S3 o l'autorizzazione di accesso Root" .

Informazioni su questo compito

Puoi creare una o più chiavi di accesso S3 che ti consentono di creare e gestire i bucket per il tuo account tenant. Dopo aver creato una nuova chiave di accesso, aggiorna l'applicazione con il tuo nuovo ID chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi del necessario ed elimina quelle che non utilizzi. Se hai una sola chiave e questa sta per scadere, creane una nuova prima che scada quella vecchia, quindi eliminala.

Ogni chiave può avere una scadenza specifica o nessuna scadenza. Per quanto riguarda la scadenza, seguire queste linee guida:

- Imposta una scadenza per le tue chiavi per limitare l'accesso a un determinato periodo di tempo. Impostare un tempo di scadenza breve può aiutare a ridurre il rischio nel caso in cui l'ID della chiave di accesso e la chiave di accesso segreta vengano accidentalmente esposti. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio per la sicurezza nel tuo ambiente è basso e non hai bisogno di creare periodicamente nuove chiavi, non devi impostare una data di scadenza per le tue chiavi. Se in seguito decidi di creare nuove chiavi, elimina manualmente quelle vecchie.

È possibile accedere ai bucket e agli oggetti S3 appartenenti al tuo account utilizzando l'ID chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovi dal tuo account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **ARCHIVIAZIONE (S3)** > **Le mie chiavi di accesso**.

   Viene visualizzata la pagina Le mie chiavi di accesso, in cui sono elencate tutte le chiavi di accesso esistenti.

2. Seleziona **Crea chiave**.
3. Eseguire una delle seguenti operazioni:
   - Seleziona **Non impostare una data di scadenza** per creare una chiave che non scadrà. (Predefinito)
   - Seleziona **Imposta una data di scadenza** e imposta la data e l'ora di scadenza.

     La data di scadenza può essere al massimo di cinque anni dalla data corrente. L'orario di scadenza può essere di almeno un minuto rispetto all'orario corrente.

4. Seleziona **Crea chiave di accesso**.

   Viene visualizzata la finestra di dialogo Scarica chiave di accesso, in cui sono elencati l'ID della chiave di accesso e la chiave di accesso segreta.

5. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   Non chiudere questa finestra di dialogo finché non hai copiato o scaricato queste informazioni. Non è possibile copiare o scaricare le chiavi dopo aver chiuso la finestra di dialogo.

6. Selezionare **Fine**.

   La nuova chiave è elencata nella pagina Le mie chiavi di accesso.

7. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, puoi facoltativamente utilizzare l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedere "Clona le chiavi di accesso S3 utilizzando l'API" .

Visualizza le tue chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone di"autorizzazione appropriata" , puoi visualizzare un elenco delle tue chiavi di accesso S3. È possibile ordinare l'elenco in base alla data di scadenza, in modo da poter determinare quali chiavi scadranno presto. Se necessario, puoi"creare nuove chiavi" O"cancellare i tasti" che non utilizzi più.

È possibile accedere ai bucket e agli oggetti S3 appartenenti al tuo account utilizzando l'ID chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovi dal tuo account quelle non utilizzate e non condividerle mai con altri utenti.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Appartieni a un gruppo di utenti che ha la possibilità di gestire le proprie credenziali S3"permesso" .

Passi

1. Selezionare **ARCHIVIAZIONE (S3)** > **Le mie chiavi di accesso**.
2. Dalla pagina Le mie chiavi di accesso, ordina tutte le chiavi di accesso esistenti in base a **Ora di scadenza** o **ID chiave di accesso**.
3. Se necessario, crea nuove chiavi o elimina quelle che non utilizzi più.

   Se crei nuove chiavi prima che quelle esistenti scadano, puoi iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti nell'account.

   Le chiavi scadute vengono rimosse automaticamente.

Elimina le tue chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le proprie chiavi di accesso S3. Dopo aver eliminato una chiave di accesso, non sarà più possibile utilizzarla per accedere agli oggetti e ai bucket nell'account tenant.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Tu hai il"Gestisci le tue autorizzazioni per le credenziali S3" .

È possibile accedere ai bucket e agli oggetti S3 appartenenti al tuo account utilizzando l'ID chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovi dal tuo account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **ARCHIVIAZIONE (S3)** > **Le mie chiavi di accesso**.
2. Nella pagina Le mie chiavi di accesso, seleziona la casella di controllo per ogni chiave di accesso che desideri rimuovere.
3. Selezionare **Elimina tasto**.
4. Nella finestra di dialogo di conferma, seleziona **Elimina chiave**.

   Nell'angolo in alto a destra della pagina appare un messaggio di conferma.

Crea le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile creare chiavi di accesso S3 per altri utenti, ad esempio applicazioni che necessitano di accedere a bucket e oggetti.

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" .

Informazioni su questo compito

È possibile creare una o più chiavi di accesso S3 per altri utenti, in modo che possano creare e gestire i bucket per il proprio account tenant. Dopo aver creato una nuova chiave di accesso, aggiorna l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quelle necessarie all'utente ed elimina quelle che non vengono utilizzate. Se hai una sola chiave e questa sta per scadere, creane una nuova prima che scada quella vecchia, quindi eliminala.

Ogni chiave può avere una scadenza specifica o nessuna scadenza. Per quanto riguarda la scadenza, seguire queste linee guida:

- Imposta una scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. Impostare un tempo di scadenza breve può aiutare a ridurre il rischio nel caso in cui l'ID della chiave di accesso e la chiave di accesso segreta vengano accidentalmente esposti. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio per la sicurezza nel tuo ambiente è basso e non hai bisogno di creare periodicamente nuove chiavi, non devi impostare una data di scadenza per le chiavi. Se in seguito decidi di creare nuove chiavi, elimina manualmente quelle vecchie.

> È possibile accedere ai bucket e agli oggetti S3 appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per quell'utente in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruotare regolarmente le chiavi di accesso, rimuovere dall'account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **GESTIONE ACCESSI** > **Utenti**.
2. Seleziona l'utente di cui desideri gestire le chiavi di accesso S3.

   Viene visualizzata la pagina dei dettagli dell'utente.
3. Selezionare **Chiavi di accesso**, quindi selezionare **Crea chiave**.
4. Eseguire una delle seguenti operazioni:
   - Seleziona **Non impostare una data di scadenza** per creare una chiave che non scade. (Predefinito)
   - Seleziona **Imposta una data di scadenza** e imposta la data e l'ora di scadenza.

     > La data di scadenza può essere al massimo di cinque anni dalla data corrente. L'orario di scadenza può essere di almeno un minuto rispetto all'orario corrente.
5. Seleziona **Crea chiave di accesso**.

Viene visualizzata la finestra di dialogo Scarica chiave di accesso, in cui sono elencati l'ID della chiave di accesso e la chiave di accesso segreta.

6. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   > Non chiudere questa finestra di dialogo finché non hai copiato o scaricato queste informazioni. Non è possibile copiare o scaricare le chiavi dopo aver chiuso la finestra di dialogo.

7. Selezionare **Fine**.

   La nuova chiave è elencata nella scheda Chiavi di accesso della pagina dei dettagli dell'utente.

8. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, puoi facoltativamente utilizzare l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedere "Clona le chiavi di accesso S3 utilizzando l'API" .

Visualizza le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile visualizzare le chiavi di accesso S3 di un altro utente. È possibile ordinare l'elenco in base alla data di scadenza, in modo da poter determinare quali chiavi scadranno presto. Se necessario, è possibile creare nuove chiavi ed eliminare quelle che non sono più in uso.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Tu hai il"Permesso di accesso root" .

> È possibile accedere ai bucket e agli oggetti S3 appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per quell'utente in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruotare regolarmente le chiavi di accesso, rimuovere dall'account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **GESTIONE ACCESSI** > **Utenti**.
2. Dalla pagina Utenti, seleziona l'utente di cui desideri visualizzare le chiavi di accesso S3.
3. Dalla pagina Dettagli utente, seleziona **Chiavi di accesso**.
4. Ordina le chiavi in base a **Data di scadenza** o **ID chiave di accesso**.
5. Se necessario, crea nuove chiavi ed elimina manualmente quelle che non sono più in uso.

   Se si creano nuove chiavi prima che quelle esistenti scadano, l'utente può iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti nell'account.

   Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

- "Crea le chiavi di accesso S3 di un altro utente"
- "Elimina le chiavi di accesso S3 di un altro utente"

Elimina le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le chiavi di accesso S3 di un altro utente. Dopo aver eliminato una chiave di accesso, non sarà più possibile utilizzarla per accedere agli oggetti e ai bucket nell'account tenant.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Tu hai il"Permesso di accesso root" .

> È possibile accedere ai bucket e agli oggetti S3 appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per quell'utente in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruotare regolarmente le chiavi di accesso, rimuovere dall'account quelle non utilizzate e non condividerle mai con altri utenti.

Passi

1. Selezionare **GESTIONE ACCESSI** > **Utenti**.
2. Dalla pagina Utenti, seleziona l'utente di cui desideri gestire le chiavi di accesso S3.
3. Dalla pagina Dettagli utente, seleziona **Chiavi di accesso**, quindi seleziona la casella di controllo per ogni chiave di accesso che desideri eliminare.
4. Selezionare **Azioni** > **Elimina chiave selezionata**.
5. Nella finestra di dialogo di conferma, seleziona **Elimina chiave**.

   Nell'angolo in alto a destra della pagina appare un messaggio di conferma.

Informazioni sul copyright

Informazioni sul marchio commerciale