Gestione delle chiavi di accesso S3

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-115/tenant/creating-your-own-s3-access-keys.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Gestione delle chiavi di accesso S3 . . . 1
Creazione di chiavi di accesso S3 personalizzate . . . 1
Visualizzazione delle chiavi di accesso S3 . . . 3
Eliminazione delle proprie chiavi di accesso S3 . . . 5
Creazione delle chiavi di accesso S3 di un altro utente . . . 6
Visualizzazione delle chiavi di accesso S3 di un altro utente . . . 8
Eliminazione delle chiavi di accesso S3 di un altro utente . . . 10

Gestione delle chiavi di accesso S3

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

A proposito di questa attività

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 **Root Access** possono gestire le chiavi di accesso per l'account root S3 e tutti gli altri utenti. Le chiavi di accesso root forniscono l'accesso completo a tutti i bucket e gli oggetti per il tenant, a meno che non siano esplicitamente disabilitate da una policy bucket.

StorageGRID supporta l'autenticazione Firma versione 2 e Firma versione 4. L'accesso multiaccount non è consentito a meno che non sia esplicitamente abilitato da una policy bucket.

Creazione di chiavi di accesso S3 personalizzate

Se si utilizza un tenant S3 e si dispone dell'autorizzazione appropriata, è possibile creare le proprie chiavi di accesso S3. È necessario disporre di una chiave di accesso per accedere ai bucket e agli oggetti nell'account tenant S3.

Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Gestisci credenziali S3.

A proposito di questa attività

È possibile creare una o più chiavi di accesso S3 che consentono di creare e gestire i bucket per l'account tenant. Dopo aver creato una nuova chiave di accesso, aggiornare 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 ed eliminare le chiavi non utilizzate. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

Ogni chiave può avere un tempo di scadenza specifico o nessuna scadenza. Seguire queste linee guida per la scadenza:

- Impostare una scadenza per le chiavi in modo da limitare l'accesso a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre il rischio in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio di protezione nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare una scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.

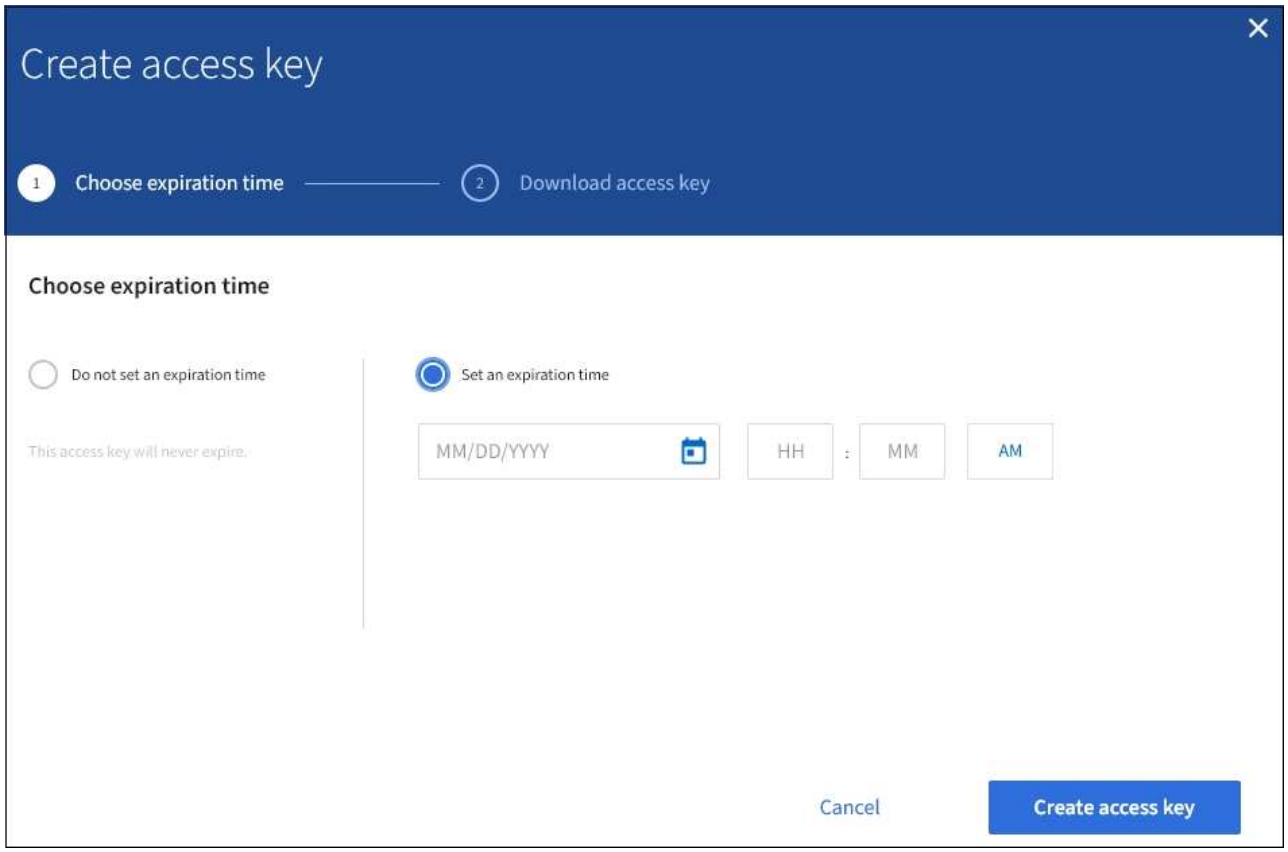
È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **STORAGE (S3)** > **My access key**.

   Viene visualizzata la pagina My access keys (i miei tasti di accesso) che elenca tutti i tasti di accesso esistenti.

2. Selezionare **Crea chiave**.
3. Effettuare una delle seguenti operazioni:
   - Selezionare **non impostare una scadenza** per creare una chiave che non scadrà. (Impostazione predefinita)
   - Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.

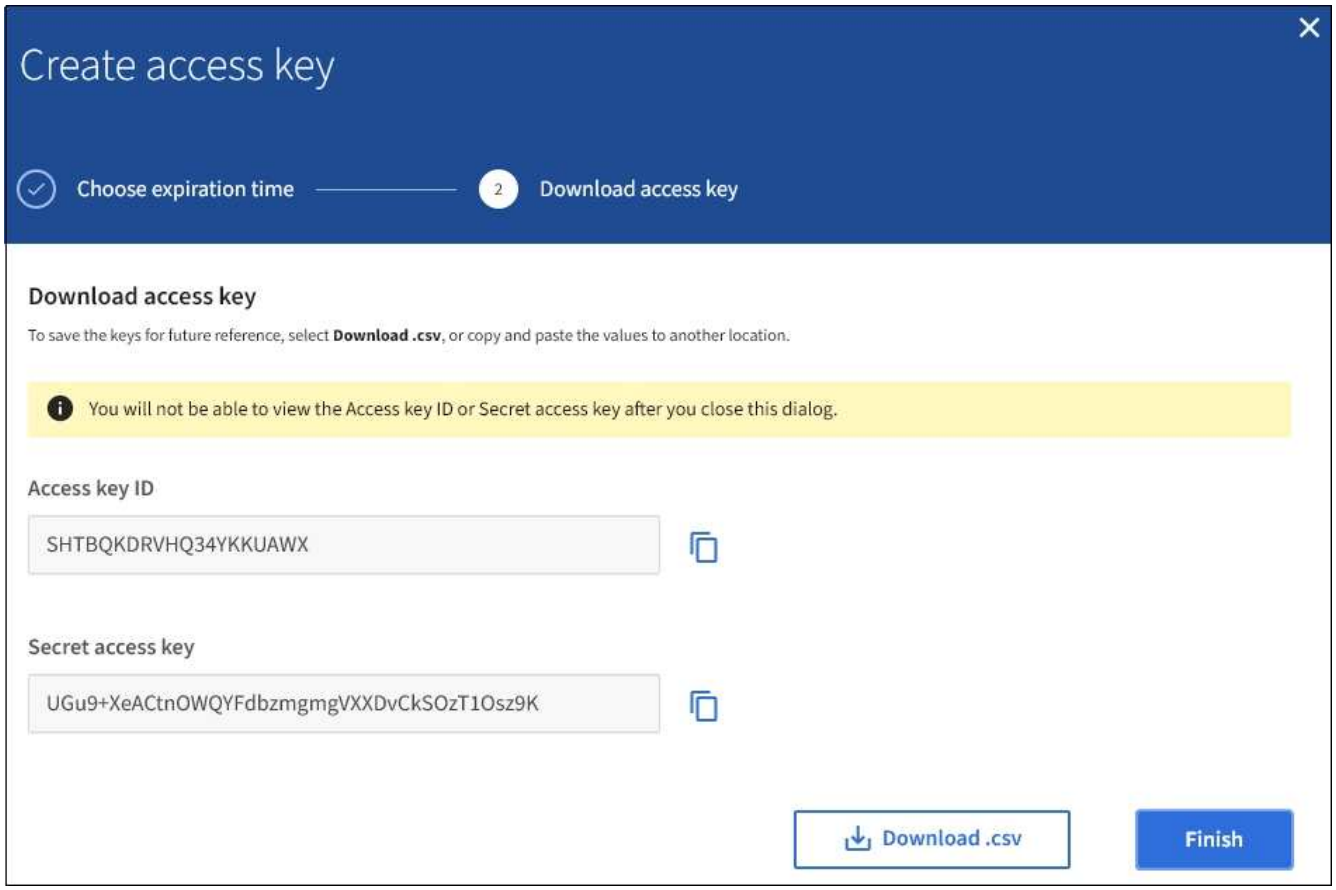


4. Selezionare **Crea chiave di accesso**.

   Viene visualizzata la finestra di dialogo Download access key (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 una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni.



6. Selezionare **fine**.

   La nuova chiave è elencata nella pagina i miei tasti di accesso. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

Informazioni correlate

"Permessi di gestione del tenant"

Visualizzazione delle chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile visualizzare un elenco delle chiavi di accesso S3. È possibile ordinare l'elenco in base alla data di scadenza, in modo da determinare quali chiavi scadranno a breve. In base alle esigenze, è possibile creare nuove chiavi o eliminare chiavi che non vengono più utilizzate.

Di cosa hai bisogno

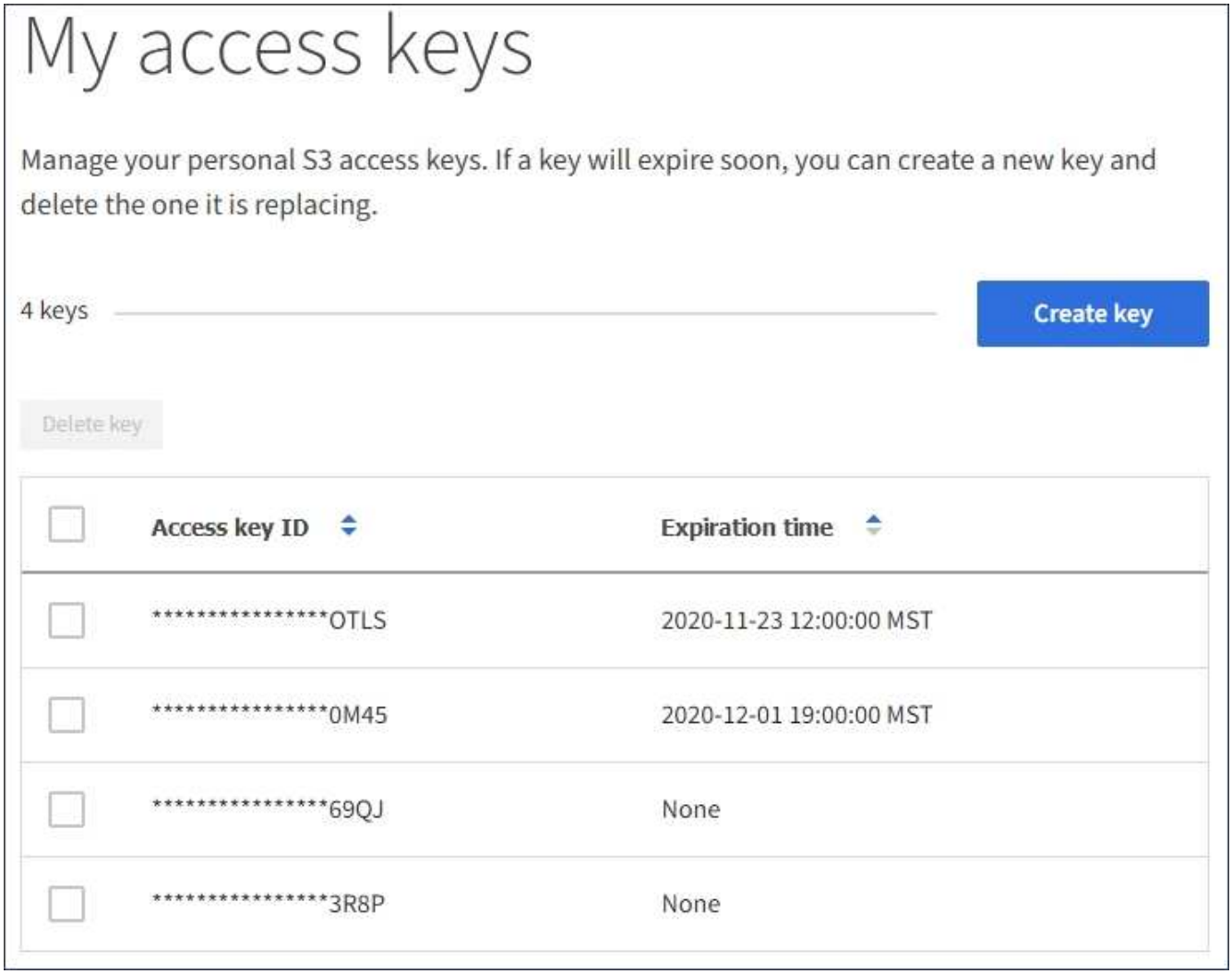
- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Gestisci credenziali S3.

È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **STORAGE (S3)** > **My access key**.

   Viene visualizzata la pagina My access keys (i miei tasti di accesso) che elenca tutti i tasti di accesso esistenti.



2. Ordinare le chiavi in base a **scadenza** o **ID chiave di accesso**.
3. Se necessario, creare nuove chiavi ed eliminarle manualmente che non si stanno più utilizzando.

   Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, è possibile iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

   Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

"Creazione di chiavi di accesso S3 personalizzate"

"Eliminazione delle proprie chiavi di accesso S3"

Eliminazione delle proprie 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. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Gestisci credenziali S3.

> È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

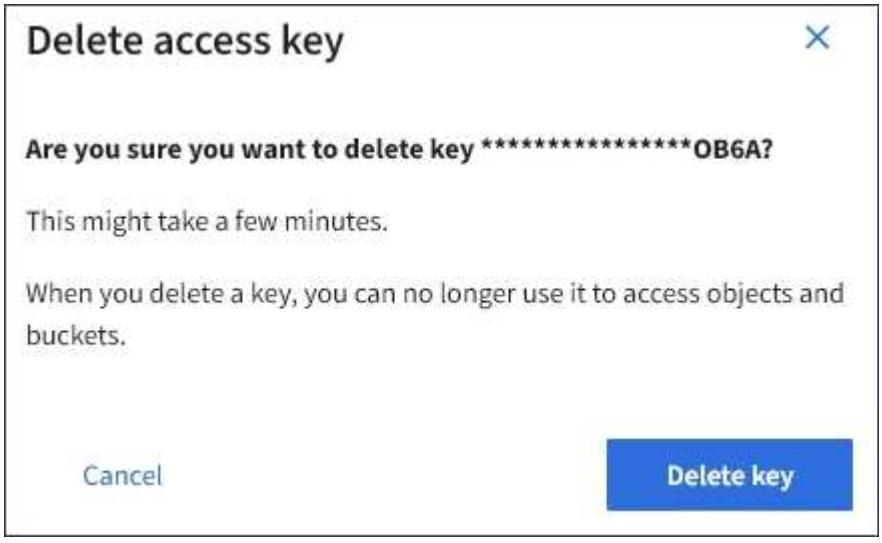
Fasi

1. Selezionare **STORAGE (S3)** > **My access key**.

   Viene visualizzata la pagina My access keys (i miei tasti di accesso) che elenca tutti i tasti di accesso esistenti.

2. Selezionare la casella di controllo per ogni chiave di accesso che si desidera rimuovere.
3. Selezionare **Delete key** (Elimina chiave).

   Viene visualizzata una finestra di dialogo di conferma.



4. Selezionare **Delete key** (Elimina chiave).

   Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

Informazioni correlate

"Permessi di gestione del tenant"

Creazione delle chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone dell'autorizzazione appropriata, è possibile creare chiavi di accesso S3 per altri utenti, ad esempio applicazioni che richiedono l'accesso a bucket e oggetti.

Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

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, aggiornare 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 richieste dall'utente ed eliminare le chiavi non utilizzate. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

Ogni chiave può avere un tempo di scadenza specifico o nessuna scadenza. Seguire queste linee guida per la scadenza:

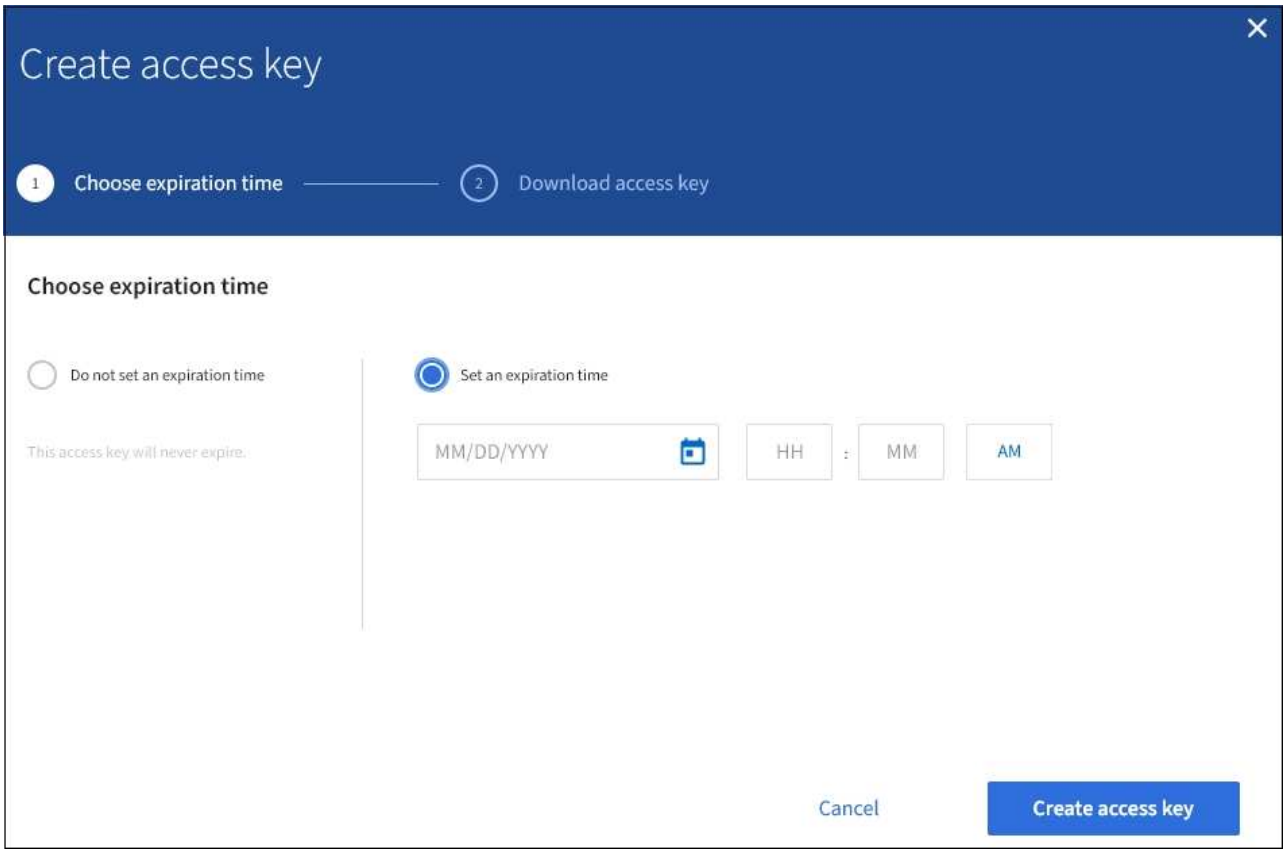
- Impostare una scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre i rischi in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio di protezione nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare una scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.

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

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Users**.
2. Selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.

   Viene visualizzata la pagina User Detail (Dettagli utente).
3. Selezionare **Access keys**, quindi selezionare **Create key**.
4. Effettuare una delle seguenti operazioni:
   - Selezionare **non impostare una scadenza** per creare una chiave che non scade. (Impostazione predefinita)
   - Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.

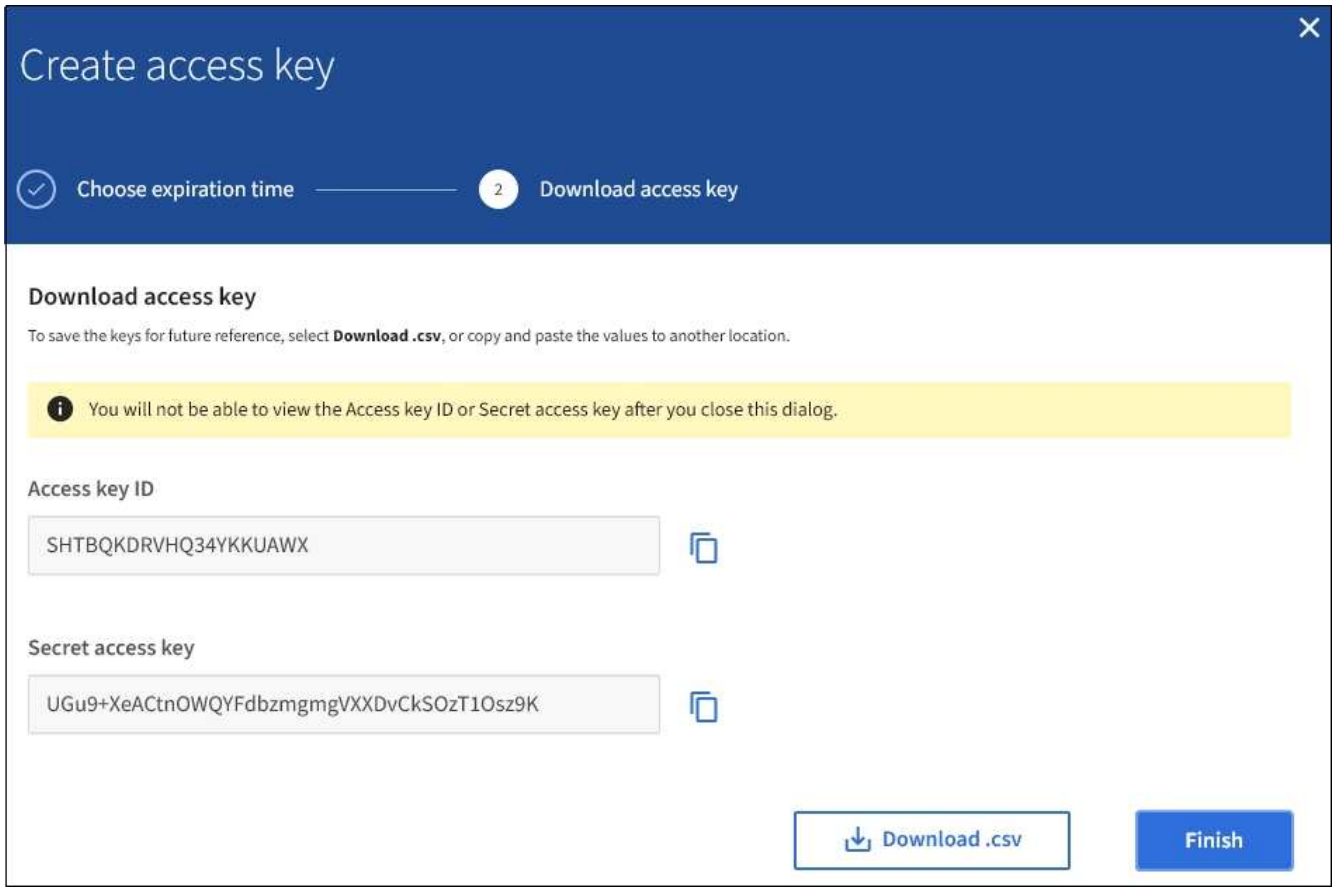


5. Selezionare **Crea chiave di accesso**.

   Viene visualizzata la finestra di dialogo Download access key (Scarica chiave di accesso), che elenca 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 una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni.



7. Selezionare **fine**.

   La nuova chiave è elencata nella scheda Access Keys della pagina User Details (Dettagli utente). Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

Informazioni correlate

"Permessi di gestione del tenant"

Visualizzazione delle 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 all'ora di scadenza, in modo da determinare quali chiavi scadranno a breve. Se necessario, è possibile creare nuove chiavi ed eliminare chiavi che non sono più in uso.

Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

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

Fasi

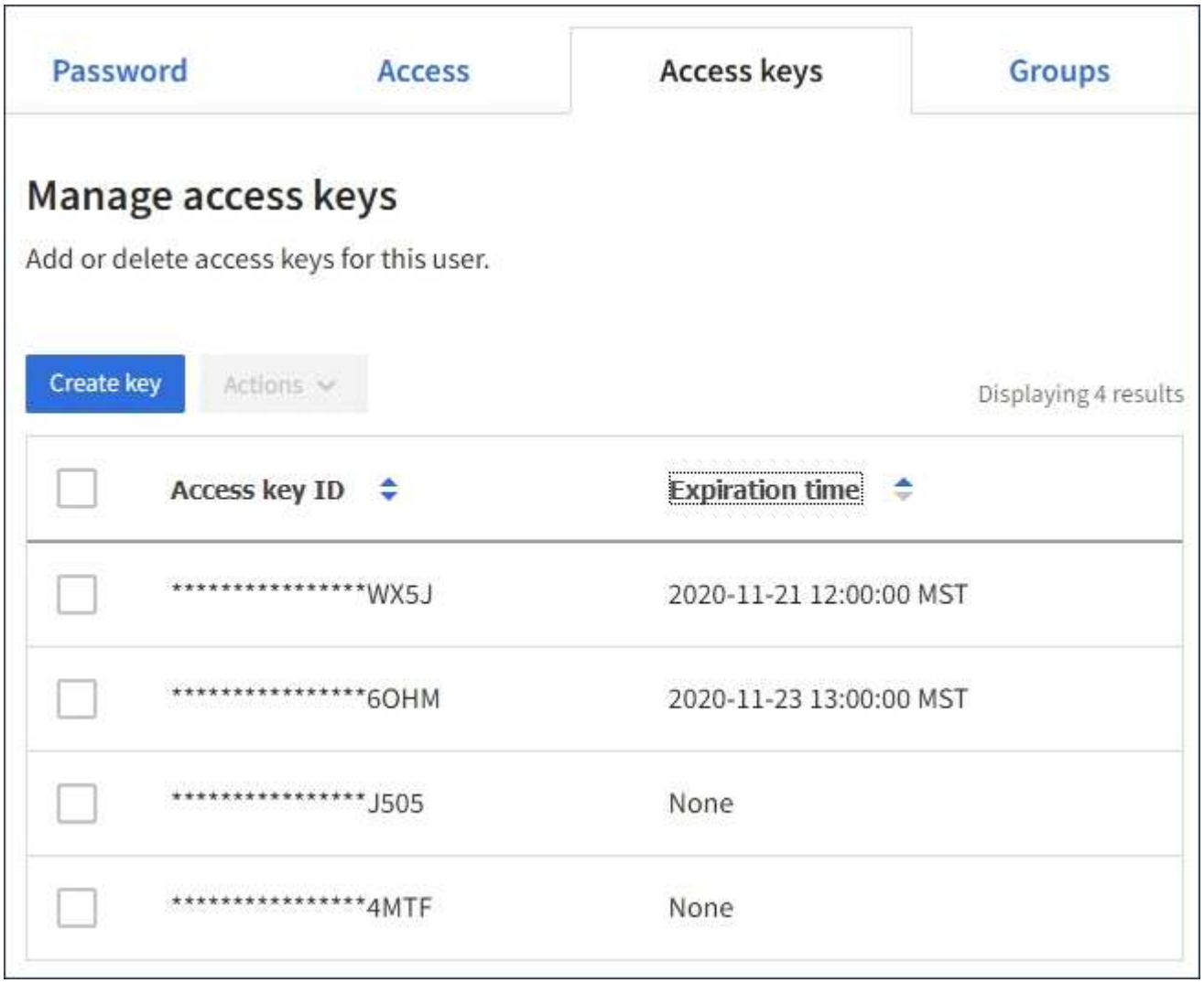
1. Selezionare **ACCESS MANAGEMENT** > **Users**.

   Viene visualizzata la pagina Users (utenti) che elenca gli utenti esistenti.

2. Selezionare l'utente di cui si desidera visualizzare le chiavi di accesso S3.

   Viene visualizzata la pagina User Details (Dettagli utente).

3. Selezionare **Access keys**.



4. Ordinare le chiavi in base a **scadenza** o **ID chiave di accesso**.
5. Se necessario, creare nuove chiavi ed eliminare manualmente le chiavi che non sono più in uso.

   Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, l'utente può iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

   Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

"Creazione delle chiavi di accesso S3 di un altro utente"

"Eliminazione delle chiavi di accesso S3 di un altro utente"

Eliminazione delle 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. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

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

Fasi

1. Selezionare **ACCESS MANAGEMENT** > **Users**.

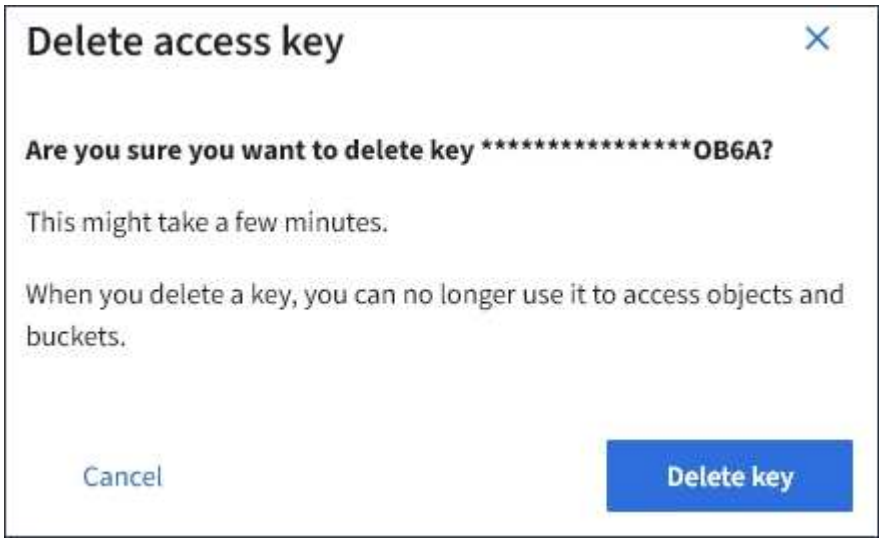
   Viene visualizzata la pagina Users (utenti) che elenca gli utenti esistenti.

2. Selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.

   Viene visualizzata la pagina User Details (Dettagli utente).

3. Selezionare **Access keys**, quindi selezionare la casella di controllo per ogni chiave di accesso che si desidera eliminare.
4. Selezionare **azioni** > **Elimina tasto selezionato**.

   Viene visualizzata una finestra di dialogo di conferma.



5. Selezionare **Delete key** (Elimina chiave).

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

Informazioni correlate

"Permessi di gestione del tenant"

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.