Gestion des clés d'accès S3

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-118/tenant/managing-s3-access-keys.html on November 04, 2025. Always check docs.netapp.com for the latest.

Sommaire

Gestion des clés d’accès S3 1
Présentation de la gestion des clés d’accès S3 1
Créez vos propres clés d’accès S3 1
Affichez vos clés d’accès S3 2
Supprimez vos propres clés d’accès S3 3
Créez les clés d’accès S3 d’un autre utilisateur 4
Afficher les clés d’accès S3 d’un autre utilisateur 5
Supprimez les clés d’accès S3 d’un autre utilisateur 6

Gestion des clés d’accès S3

Présentation de la gestion des clés d’accès S3

Chaque utilisateur d’un compte de locataire S3 doit disposer d’une clé d’accès pour stocker et récupérer des objets dans le système StorageGRID. Une clé d’accès se compose d’un ID de clé d’accès et d’une clé d’accès secrète.

Les clés d’accès S3 peuvent être gérées de la manière suivante :

- Les utilisateurs disposant de l’autorisation **gérer vos propres informations d’identification S3** peuvent créer ou supprimer leurs propres clés d’accès S3.
- Les utilisateurs disposant de l’autorisation **Root Access** peuvent gérer les clés d’accès du compte root S3 et de tous les autres utilisateurs. Les clés d’accès racine offrent un accès complet à toutes les compartiments et objets du locataire, sauf si une règle de compartiment est explicitement désactivée.

StorageGRID prend en charge l’authentification Signature version 2 et Signature version 4. L’accès entre comptes n’est pas autorisé sauf si cette règle est explicitement activée par une règle de compartiment.

Créez vos propres clés d’accès S3

Si vous utilisez un locataire S3 et que vous disposez de l’autorisation appropriée, vous pouvez créer vos propres clés d’accès S3. Vous devez disposer d’une clé d’accès pour accéder à vos compartiments et objets.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l’aide d’un "navigateur web pris en charge".
- Vous appartenez à un groupe d’utilisateurs qui possède le "Gérez vos propres informations d’identification S3 ou autorisations d’accès racine".

Description de la tâche

Vous pouvez créer une ou plusieurs clés d’accès S3 qui vous permettent de créer et de gérer des compartiments pour votre compte de locataire. Après avoir créé une nouvelle clé d’accès, mettez à jour l’application avec votre nouvel ID de clé d’accès et votre clé d’accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que nécessaire et supprimez les clés que vous n’utilisez pas. Si vous n’avez qu’une seule clé et que vous êtes sur le point d’expirer, créez une nouvelle clé avant l’expiration de l’ancienne, puis supprimez l’ancienne.

Chaque clé peut avoir une heure d’expiration spécifique ou pas d’expiration. Suivez les directives ci-dessous pour l’heure d’expiration :

- Définissez une durée d’expiration pour vos clés afin de limiter votre accès à une certaine période. La définition d’un délai d’expiration court peut vous aider à réduire le risque si votre ID de clé d’accès et votre clé secrète sont exposés accidentellement. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n’avez pas besoin de créer régulièrement de nouvelles clés, vous n’avez pas besoin de définir une heure d’expiration pour vos clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.

Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STORAGE (S3)** > **Mes clés d'accès**.

   La page Mes touches d'accès s'affiche et répertorie toutes les clés d'accès existantes.

2. Sélectionnez **Créer clé**.
3. Effectuez l'une des opérations suivantes :
   - Sélectionnez **ne définissez pas d'heure d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
   - Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.

     La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. La durée d'expiration peut être d'au moins une minute à partir de l'heure actuelle.

4. Sélectionnez **Créer une clé d'accès**.

   La boîte de dialogue Télécharger la clé d'accès s'affiche, avec la liste de votre ID de clé d'accès et de votre clé secrète d'accès.

5. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.

   Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger de clés après la fermeture de la boîte de dialogue.

6. Sélectionnez **Terminer**.

   La nouvelle clé apparaît sur la page Mes clés d'accès.

7. Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination. Voir "Cloner les clés d'accès S3 à l'aide de l'API".

Affichez vos clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez de "autorisation appropriée", Vous pouvez afficher la liste de vos clés d'accès S3. Vous pouvez trier la liste en fonction de l'heure d'expiration afin de déterminer quelles clés vont bientôt expirer. Si nécessaire, c'est possible "créer de nouvelles clés" ou "supprimer les clés" que vous n'utilisez plus.

Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs disposant des informations d'identification Manage your own S3 "permission".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Mes clés d'accès**.
2. À partir de la page Mes clés d'accès, triez toutes les clés d'accès existantes par **heure d'expiration** ou **ID de clé d'accès**.
3. Au besoin, créez de nouvelles clés ou supprimez les clés que vous n'utilisez plus.

   Si vous créez de nouvelles clés avant l'expiration des clés existantes, vous pouvez commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

   Les clés expirées sont supprimées automatiquement.

Supprimez vos propres clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer vos propres clés d'accès S3. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Gérez vos propres identifiants S3".

Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STORAGE (S3)** > **Mes clés d'accès**.
2. Sur la page Mes clés d'accès, cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
3. Sélectionnez **Supprimer la touche**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page.

Créez les clés d’accès S3 d’un autre utilisateur

Si vous utilisez un locataire S3 avec l’autorisation appropriée, vous pouvez créer des clés d’accès S3 pour d’autres utilisateurs, comme les applications qui ont besoin d’accéder à des compartiments et des objets.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l’aide d’un "navigateur web pris en charge".
- Vous appartenez à un groupe d’utilisateurs qui possède le "Autorisation d’accès racine".

Description de la tâche

Vous pouvez créer une ou plusieurs clés d’accès S3 pour les autres utilisateurs afin qu’ils puissent créer et gérer des compartiments pour leur compte de locataire. Après avoir créé une nouvelle clé d’accès, mettez à jour l’application avec le nouvel ID de clé d’accès et la clé d’accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que les besoins de l’utilisateur et supprimez les clés qui ne sont pas utilisées. Si vous n’avez qu’une seule clé et que vous êtes sur le point d’expirer, créez une nouvelle clé avant l’expiration de l’ancienne, puis supprimez l’ancienne.

Chaque clé peut avoir une heure d’expiration spécifique ou pas d’expiration. Suivez les directives ci-dessous pour l’heure d’expiration :

- Définissez un délai d’expiration pour les clés afin de limiter l’accès de l’utilisateur à une certaine période. La définition d’un délai d’expiration court peut aider à réduire le risque si l’ID de clé d’accès et la clé secrète sont exposés accidentellement. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n’avez pas besoin de créer régulièrement de nouvelles clés, vous n’avez pas besoin de définir une heure d’expiration pour les clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.

> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l’aide de l’ID de clé d’accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d’accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d’accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d’autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Sélectionnez l’utilisateur dont vous souhaitez gérer les clés d’accès S3.

   La page de détails utilisateur s’affiche.
3. Sélectionnez **touches d’accès**, puis **touche Créer**.
4. Effectuez l’une des opérations suivantes :
   - Sélectionnez **ne pas définir de délai d’expiration** pour créer une clé qui n’expire pas. (Valeur par défaut)
   - Sélectionnez **définissez une heure d’expiration** et définissez la date et l’heure d’expiration.

     > La date d’expiration peut être au maximum de cinq ans à compter de la date actuelle. La durée d’expiration peut être d’au moins une minute à partir de l’heure actuelle.

5. Sélectionnez **Créer une clé d'accès**.

   La boîte de dialogue Télécharger la clé d'accès s'affiche, avec la liste de l'ID de clé d'accès et de la clé secrète.

6. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.

   > Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger de clés après la fermeture de la boîte de dialogue.

7. Sélectionnez **Terminer**.

   La nouvelle clé est répertoriée dans l'onglet touches d'accès de la page des détails de l'utilisateur.

8. Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination. Voir "Cloner les clés d'accès S3 à l'aide de l'API".

Afficher les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez afficher les clés d'accès S3 d'un autre utilisateur. Vous pouvez trier la liste par heure d'expiration pour déterminer quelles clés vont bientôt expirer. Au besoin, vous pouvez créer de nouvelles clés et supprimer des clés qui ne sont plus utilisées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.
3. Dans la page Détails de l'utilisateur, sélectionnez **touches d'accès**.
4. Trier les clés par **heure d'expiration** ou **ID de clé d'accès**.
5. Si nécessaire, créez de nouvelles clés et supprimez manuellement les clés que le n'est plus utilisé.

   Si vous créez de nouvelles clés avant l'expiration des clés existantes, l'utilisateur peut commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

   Les clés expirées sont supprimées automatiquement.

Informations associées

"Créez les clés d'accès S3 d'un autre utilisateur"

"Supprimez les clés d'accès S3 d'un autre utilisateur"

Supprimez les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer les clés d'accès S3 d'un autre utilisateur. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.
3. Sur la page Détails de l'utilisateur, sélectionnez **touches d'accès**, puis cochez la case correspondant à chaque clé d'accès à supprimer.
4. Sélectionnez **actions** > **Supprimer la touche sélectionnée**.
5. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.