



Gérer les clés d'accès S3

StorageGRID software

NetApp
July 23, 2026

Sommaire

- Gérer les clés d'accès S3. 1
 - Gérer les clés d'accès S3 dans StorageGRID. 1
 - Créez vos propres clés d'accès S3 dans StorageGRID 1
 - Consultez vos clés d'accès S3 dans StorageGRID 2
 - Supprimez vos propres clés d'accès S3 dans StorageGRID. 3
 - Créez les clés d'accès S3 d'un autre utilisateur dans StorageGRID 4
 - Afficher les clés d'accès S3 d'un autre utilisateur dans StorageGRID. 5
 - Supprimer les clés d'accès S3 d'un autre utilisateur dans StorageGRID 6

Gérer les clés d'accès S3

Gérer les clés d'accès S3 dans StorageGRID

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

Les clés d'accès S3 peuvent être gérées comme suit :

- 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 racine S3 et de tous les autres utilisateurs. Les clés d'accès racine offrent un accès complet à tous les compartiments et objets pour le locataire, sauf si elles sont explicitement désactivées par une stratégie de compartiment.

StorageGRID prend en charge l'authentification Signature Version 2 et Signature Version 4. L'accès inter-comptes n'est pas autorisé, sauf s'il est explicitement activé par une stratégie de compartiment.

Créez vos propres clés d'accès S3 dans StorageGRID

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 Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le `"${post_edited_translations.segment}"`.

À propos de cette tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 qui vous permettent de créer et de gérer des compartiments pour votre compte 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 celles que vous n'utilisez pas. Si vous ne disposez que d'une seule clé et qu'elle est sur le point d'expirer, créez-en une nouvelle avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une date d'expiration spécifique ou ne pas avoir d'expiration. Suivez ces directives concernant la durée d'expiration :

- Définissez un délai d'expiration pour vos clés afin de limiter votre accès à une période donnée. Définir un délai d'expiration court peut aider à réduire les risques si votre ID de clé d'accès et votre clé d'accès secrète sont accidentellement exposés. 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 périodiquement de nouvelles clés, vous n'avez pas besoin de définir de délai d'expiration pour vos clés. Si vous décidez ultérieurement de créer de nouvelles clés, supprimez manuellement les anciennes clés.



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour votre compte dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Effectuez une rotation régulière des clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

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

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

2. Sélectionnez **Créer une clé**.
3. Effectuez l'une des opérations suivantes :
 - Sélectionnez **Ne pas définir de date d'expiration** pour créer une clé qui n'expirera pas. (Par défaut)
 - Sélectionnez **Définir une date d'expiration**, puis indiquez la date et l'heure d'expiration.



La date d'expiration peut être fixée à un maximum de cinq ans à compter de la date actuelle. L'heure d'expiration peut être fixée à un minimum d'une minute à compter de l'heure actuelle.

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

La boîte de dialogue « Download access key » s'affiche, indiquant votre access key ID et votre secret access key.

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



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 les clés après la fermeture de la boîte de dialogue.

6. Sélectionnez **Terminer**.

La nouvelle clé est répertoriée sur la page My access keys.

7. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous pouvez éventuellement utiliser l'API Tenant Management 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](#)".

Consultez vos clés d'accès S3 dans StorageGRID

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 par date d'expiration afin de déterminer quelles clés vont bientôt expirer. Au besoin, vous pouvez "[\\${post_edited_translations.segment}](#)" ou "[\\${post_edited_translations.segment}](#)" que vous n'utilisez plus.



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour votre compte dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Effectuez une rotation régulière des clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède l'autorisation Gérer vos propres informations d'identification S3 `"${post_edited_translations.segment}"`.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.
2. `${post_edited_translations.segment}`
3. `${post_edited_translations.segment}`

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 dans StorageGRID

Si vous utilisez un tenant S3 et que vous disposez des autorisations nécessaires, vous pouvez supprimer vos propres clés d'accès S3. Après la suppression d'une clé d'accès, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du tenant.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Gérez vos propres autorisations d'identifiants S3"](#).



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour votre compte dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Effectuez une rotation régulière des clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.
2. `${post_edited_translations.segment}`
3. Sélectionnez la touche **Delete key**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **Delete key**.

Un message de confirmation apparaît dans le coin supérieur droit de la page.

Créez les clés d'accès S3 d'un autre utilisateur dans StorageGRID

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez créer des clés d'accès S3 pour d'autres utilisateurs, comme des applications qui ont besoin d'accéder aux compartiments et aux objets.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

À propos de cette tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 pour d'autres utilisateurs afin qu'ils puissent créer et gérer des compartiments pour leur compte locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec le nouvel ID de clé d'accès et la nouvelle clé d'accès secrète. Par mesure de sécurité, ne créez pas plus de clés que nécessaire et supprimez celles qui ne sont pas utilisées. Si vous ne possédez qu'une seule clé et qu'elle est sur le point d'expirer, créez-en une nouvelle avant l'expiration de l'ancienne, puis supprimez cette dernière.

Chaque clé peut avoir une date d'expiration spécifique ou ne pas avoir d'expiration. Suivez ces directives concernant la durée d'expiration :

- Définissez une date d'expiration pour les clés afin de limiter l'accès de l'utilisateur à une période donnée. La définition d'une date d'expiration courte peut aider à réduire les risques si l'ID de clé d'accès et la clé d'accès secrète sont accidentellement exposés. 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, il n'est pas nécessaire de définir une date d'expiration pour les clés. Si vous décidez ultérieurement de créer de nouvelles clés, supprimez les anciennes clés manuellement.



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

Étapes

1. `${post_edited_translations.segment}`
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

La page de détails de l'utilisateur s'affiche.

3. Sélectionnez **Access keys**, puis sélectionnez **Create key**.
4. Effectuez l'une des opérations suivantes :
 - Sélectionnez **Ne pas définir de date d'expiration** pour créer une clé qui n'expire pas. (Par défaut)
 - Sélectionnez **Définir une date d'expiration**, puis indiquez la date et l'heure d'expiration.



La date d'expiration peut être fixée à un maximum de cinq ans à compter de la date actuelle. L'heure d'expiration peut être fixée à un minimum d'une minute à compter de l'heure actuelle.

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

`${post_edited_translations.segment}`

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



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 les clés après la fermeture de la boîte de dialogue.

7. Sélectionnez **Terminer**.

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

8. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous pouvez éventuellement utiliser l'API Tenant Management 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 dans StorageGRID

Si vous utilisez un tenant S3 et que vous disposez des autorisations nécessaires, vous pouvez consulter les clés d'accès S3 d'un autre utilisateur. Vous pouvez trier la liste par date d'expiration afin de déterminer quelles clés expireront bientôt. Au besoin, vous pouvez créer de nouvelles clés et supprimer les clés qui ne sont plus utilisées.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous disposez de "[Autorisation d'accès root](#)".



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

Étapes

1. `${post_edited_translations.segment}`
2. Sur la page Utilisateurs, sélectionnez l'utilisateur dont vous souhaitez consulter les clés d'accès S3.
3. `${post_edited_translations.segment}`
4. Triez les clés par **heure d'expiration** ou **ID de clé d'accès**.
5. `${post_edited_translations.segment}`

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 connexes

- ["Créer les clés d'accès S3 d'un autre utilisateur"](#)
- ["\\${post_edited_translations.segment}"](#)

Supprimer les clés d'accès S3 d'un autre utilisateur dans StorageGRID

Si vous utilisez un tenant S3 et que vous disposez des autorisations nécessaires, vous pouvez supprimer les clés d'accès S3 d'un autre utilisateur. Après la suppression d'une clé d'accès, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du tenant.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous disposez de ["Autorisation d'accès root"](#).



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

Étapes

1. ["\\${post_edited_translations.segment}"](#)
2. ["\\${post_edited_translations.segment}"](#)
3. Sur la page Détails de l'utilisateur, sélectionnez **Clés d'accès**, puis cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
4. ["\\${post_edited_translations.segment}"](#)
5. Dans la boîte de dialogue de confirmation, sélectionnez **Delete key**.

Un message de confirmation apparaît dans le coin supérieur droit de la page.

Informations sur le copyright

Copyright © 2026 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 DÉLICTELLE (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.