Amazon Simple Storage Service

Guide de démarrage

Amazon Simple Storage Service: Guide de démarrage

Table of Contents

Ce guide ne fait plus l'objet de mises à jour. Pour obtenir des informations et des instructions actuelles, reportez-vous au nouveau Guide de l'utilisateur Amazon S3.

Mise en route avec Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) est une solution de stockage sur Internet. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web. Vous pouvez accomplir ces tâches en utilisant AWS Management Console, qui est une interface Web simple et intuitive.

Amazon S3 stocke les données en tant qu'objets dans des compartiments. Un objet est un fichier et toutes les métadonnées facultatives qui le décrivent. Pour stocker un fichier dans Amazon S3, chargez-le dans un compartiment. Lorsque vous téléchargez un fichier, vous pouvez définir des autorisations sur l'objet et sur des métadonnées quelconques.

Les compartiments sont les conteneurs des objets. Vous pouvez avoir un ou plusieurs compartiments. Vous pouvez contrôler l'accès à chaque compartiment, en décidant qui peut créer, supprimer et répertorier les objets qu'il contient. Vous pouvez également choisir la région géographique où Amazon S3 stockera le compartiment et son contenu, et afficher les journaux d'accès pour le compartiment et ses objets.

Ce guide vous présente Amazon S3 et explique comment utiliser AWS Management Console pour exécuter les tâches suivantes :

Pour de plus amples informations sur les fonctions Amazon S3, la tarification et les questions fréquentes, veuillez consulter la page produit Amazon S3.

Configuration d'Amazon S3

Lors de votre inscription à AWS, votre compte AWS est automatiquement inscrit à tous les services dans AWS, notamment Amazon S3. Seuls les services que vous utilisez vous sont facturés.

Avec Amazon S3, vous ne payez que les services que vous utilisez. Pour de plus amples informations sur les fonctions et les tarifs d'Amazon S3, veuillez consulter Amazon S3. Si vous êtes un nouveau client Amazon S3, vous pouvez commencer à utiliser Amazon S3 gratuitement. Pour de plus amples informations, veuillez consulter Offre gratuite d'AWS.

Pour commencer à utiliser Amazon S3, procédez comme suit :

Rubriques

Inscrivez-vous à AWS

Si vous n'avez pas de compte AWS, complétez les étapes suivantes pour en créer un.

Pour s'inscrire à un compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

AWS vous envoie un e-mail de confirmation lorsque le processus d'inscription est terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en cliquant sur My Account (Mon compte).

Création d'un utilisateur IAM

Lorsque vous créez un compte Amazon Web Services (AWS) pour la première fois, vous commencez par une identité de connexion unique. Cette identité a un accès complet à tous les services et ressources AWS du compte. Cette identité est appelée l'utilisateur racine du compte AWS. Lorsque vous vous connectez, saisissez l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte.

> **Important**
>
> Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Respectez plutôt la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateur IAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services. Pour connaître les tâches qui nécessitent de se connecter en tant qu'utilisateur racine, veuillez consulter Tâches AWS qui requièrent un utilisateur racine.

Si vous vous êtes inscrit à AWS mais n'avez pas créé d'utilisateur IAM pour vous-même, procédez comme suit.

Pour créer un administrateur pour vous-même et ajouter l'utilisateur à un groupe d'administrateurs (console)

1. Connectez-vous à la IAM console (Console IAM) en tant que propriétaire du compte en choisissant Root user (Utilisateur racine) et en entrant l'adresse e-mail de votre compte AWS. Sur la page suivante, saisissez votre mot de passe.

   Note

   Nous vous recommandons vivement de respecter la bonne pratique qui consiste à avoir recours à l'utilisateur IAM **`Administrator`** ci-dessous et protéger les informations d'identification de l'utilisateur racine. Connectez-vous en tant qu'utilisateur racine pour effectuer certaines tâches de gestion des comptes et des services.
2. Dans le panneau de navigation, choisissez Utilisateurs, puis Add user (Ajouter un utilisateur).
3. Dans User name (Nom d'utilisateur), entrez **`Administrator`**.
4. Activez la case à cocher en regard de l'accès à AWS Management Console. Puis, sélectionnez Custom password (Mot de passe personnalisé, et entrez votre nouveau mot de passe dans la zone de texte.
5. Par défaut, AWS oblige le nouvel utilisateur à créer un nouveau mot de passe lors de sa première connexion. Décochez la case en regard de User must create a new password at next sign-in (L'utilisateur doit créer un nouveau mot de passe à sa prochaine connexion) pour autoriser le nouvel utilisateur à réinitialiser son mot de passe une fois qu'il s'est connecté.
6. Choisissez Next: Permissions (Suivant : Autorisations).
7. Sous Set permissions (Accorder des autorisations), choisissez Add user to group (Ajouter un utilisateur au groupe).
8. Choisissez Create group.
9. Dans la boîte de dialogue Create group (Créer un groupe), pour Group name (Nom du groupe), tapez **`Administrators`**.
10. Choisissez Filter policies (Filtrer les stratégies), puis sélectionnez AWS managed -job function (Fonction professionnelle gérée par AWS) pour filtrer le contenu de la table.
11. Dans la liste des stratégies, cochez la case AdministratorAccess. Choisissez ensuite Create group.

    Note

    Vous devez activer l'accès de l'utilisateur et du rôle IAM à la facturation avant de pouvoir utiliser les autorisations `AdministratorAccess` pour accéder à la console AWS Billing and Cost Management. Pour ce faire, suivez les instructions de l'étape 1 du didacticiel portant sur comment déléguer l'accès à la console de facturation.
12. De retour dans la liste des groupes, activez la case à cocher du nouveau groupe. Choisissez Refresh si nécessaire pour afficher le groupe dans la liste.
13. Choisissez Next: Tags (Suivant : Balises).
14. (Facultatif) Ajoutez des métadonnées à l'utilisateur en associant les balises sous forme de paires clé-valeur. Pour de plus amples informations sur l'utilisation des balises dans IAM, veuillez consulter Balisage des utilisateurs et des rôles IAM dans le Guide de l'utilisateur IAM.
15. Choisissez Next: Review pour afficher la liste des membres du groupe à ajouter au nouvel utilisateur. Une fois que vous êtes prêt à continuer, choisissez Create user.

Vous pouvez utiliser ce même processus pour créer d'autres groupes et utilisateurs et pour accorder l'accès aux ressources de votre compte AWS à vos utilisateurs. Pour en savoir plus sur l'utilisation des stratégies permettant de limiter les autorisations d'accès des utilisateurs à certaines ressources AWS, veuillez consulter Gestion des accès et Exemples de stratégies.

Connectez-vous en tant qu'utilisateur IAM.

Après avoir créé un utilisateur IAM, vous pouvez vous connecter à AWS avec votre nom d'utilisateur et votre mot de passe IAM.

Avant de vous connecter en tant qu'utilisateur IAM, vous pouvez vérifier le lien de connexion pour les utilisateurs IAM dans la console IAM. Dans le tableau de bord IAM, sous IAM users sign-in link (Lien de connexion des utilisateurs IAM), vous pouvez voir le lien de connexion pour votre compte AWS. L'URL de votre lien de connexion contient votre ID de compte AWS sans tirets (-).

Si vous ne souhaitez pas que l'URL de votre lien de connexion contienne votre ID de compte AWS, vous pouvez créer un alias de compte. Pour de plus amples informations, veuillez consulter Création, suppression et affichage d'un alias de compte AWS dans le Guide de l'utilisateur IAM.

Pour se connecter en tant qu'utilisateur AWS

1. Déconnectez-vous d'AWS Management Console.
2. Entrez votre lien de connexion.

   Votre lien de connexion inclut votre ID de compte AWS (sans tirets) ou votre alias de compte AWS :

   ```
   https://aws_account_id_or_alias.signin.aws.amazon.com/console
   ```

3. Saisissez le nom utilisateur et le mot de passe IAM que vous venez de créer.

   Lorsque vous êtes connecté, la barre de navigation affiche « votre_nom_utilisateur @ votre_id_de_compte_aws ».

Créer un compartiment

Maintenant que vous êtes inscrit à AWS, vous êtes prêt à créer un compartiment à l'aide de AWS Management Console. Dans Amazon S3, chaque objet est stocké dans un compartiment. Avant de pouvoir stocker des données dans Amazon S3, vous devez créer un compartiment.

> **Note**
>
> Vous n'êtes pas facturé pour la création d'un compartiment. Seuls le stockage d'objets dans le compartiment et le transfert des objets dans et hors du compartiment vous sont facturés. Les frais que vous encourez en appliquant les exemples suivants de ce manuel sont minimes (moins de 1 USD). Pour de plus amples informations sur les coûts de stockage, veuillez consulter Tarification Amazon S3.

Pour créer un compartiment à l'aide de l'interface de ligne de commande AWS, veuillez consulter create-bucket dans la Référence de l'interface de ligne de commande AWS.

Pour créer un compartiment

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.

   La page Créer un compartiment s'ouvre.
3. Dans Bucket name (Nom du compartiment), saisissez un nom compatible DNS pour votre compartiment.

   Les caractéristiques du nom du compartiment doivent être les suivantes :

   - Il doit être unique sur l'ensemble d'Amazon S3.
   - Il doit comporter entre 3 et 63 caractères.
   - Ne contient pas de majuscules.
   - Il doit commencer par une minuscule ou un chiffre.

   Une fois le compartiment créé, vous ne pouvez pas changer son nom. Pour de plus amples informations sur l'attribution de noms de compartiments, veuillez consulter Règles relatives à l'attribution des noms de compartiments dans le Manuel du développeur Amazon Simple Storage Service.

   > **Important**
   >
   > Évitez d'inclure des informations sensibles, notamment des numéros de compte, dans le nom du compartiment. Le nom de compartiment est visible dans les URL qui pointent vers les objets du compartiment.
4. Dans Region (Région), choisissez la région AWS où vous voulez placer le compartiment.

   Choisissez une région proche de vous afin de limiter la latence et les coûts,et répondre aux exigences légales. Les objets stockés dans une région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre région. Pour obtenir la liste des régions AWS Amazon S3, veuillez consulter Points de terminaison de service AWS dans la Référence générale d'Amazon Web Services.
5. Dans Bucket settings for Block Public Acces (Paramètres de compartiment pour Bloquer l'accès public), conservez les valeurs définies par défaut.

Par défaut, Amazon S3 bloque tout accès public à vos compartiments. Nous vous recommandons de laisser tous les paramètres Bloquer l'accès public activés. Pour de plus amples informations sur le blocage de l'accès public, veuillez consulter Utilisation de la fonctionnalité de blocage de l'accès public Amazon S3 dans le Manuel du développeur Amazon Simple Storage Service.

6. Choisissez Créer un compartiment.

Vous avez créé un compartiment dans Amazon S3.

Pour ajouter un objet à votre compartiment, veuillez consulter Chargement d'un objet dans un compartiment (p. 7).

Chargement d'un objet dans un compartiment

Maintenant que vous avez créé un compartiment, vous êtes prêt à y charger un objet. Un objet peut désigner n'importe quel type de fichier : un fichier texte, une photo, une vidéo, etc.

Pour charger un objet dans un compartiment

1. Dans la liste Buckets (Compartiment), choisissez le nom du compartiment dans lequel vous souhaitez charger votre objet.
2. Sous l'onglet Objects (Objets) de votre compartiment, choisissez Upload (Charger).
3. Sous Files and folders (Fichiers et dossiers), choisissez Add files (Ajouter des fichiers).
4. Choisissez un fichier à charger, puis choisissez Open.
5. Choisissez Upload.

Vous avez réussi à charger un objet dans votre compartiment.

Pour afficher votre objet, veuillez consulter Téléchargement d'un objet (p. 8).

Téléchargement d'un objet

Maintenant que vous avez chargé un objet dans un compartiment, vous pouvez afficher des informations sur votre objet et télécharger l'objet sur votre ordinateur local.

Pour télécharger un objet à partir d'un compartiment

1. Dans la liste Compartiments, choisissez le nom du compartiment que vous avez créé.
2. Dans la liste Objects (Objets), choisissez le nom de l'objet que vous avez chargé.

   La présentation de l'objet s'ouvre.
3. Dans l'onglet Présentation, consultez les informations relatives à votre objet.
4. Pour télécharger l'objet sur votre ordinateur, choisissez Télécharger.

Vous avez téléchargé votre objet avec succès.

Pour copier et coller votre objet dans Amazon S3, veuillez consulter Copie d'un objet dans un dossier (p. 9).

Copie d'un objet dans un dossier

Vous avez déjà ajouté un objet dans un compartiment et téléchargé l'objet. Dans ce didacticiel, vous créez un dossier et copiez votre objet dans celui-ci.

Pour copier un objet dans un dossier

1. Dans la liste Compartiments, choisissez le nom de votre compartiment.
2. Choisissez Create folder (Créer un dossier) et configurez le nouveau dossier :
   a. Entrez un nom de dossier (par exemple, `favorite-pics`).
   b. Pour le paramètre de chiffrement du dossier, choisissez Aucun.
   c. Choisissez Enregistrer.
3. Accédez au compartiment ou au dossier Amazon S3 contenant les objets que vous souhaitez copier.
4. Cochez la case située à gauche des noms des objets que vous souhaitez copier.
5. Choisissez Actions et Copy (Copier) dans la liste des options qui s'affiche.

   Vous pouvez également choisir Copy (Copier) parmi les options en haut à droite.
6. Choisissez le dossier de destination.
   a. Choisissez Browse S3 (Parcourir S3).
   b. Cliquez sur le bouton d'option situé à gauche du nom du dossier.

      Pour naviguer dans un dossier et choisir un sous-dossier comme destination, choisissez le nom du dossier.
   c. Choisissez Choose destination (Choisir une destination).

   Le chemin d'accès au dossier de destination apparaît dans la zone Destination. Dans Destination, vous pouvez alternativement entrer votre chemin de destination, par exemple, s3://*nom-compartiment*/*nom-dossier*/.
7. En bas à droite, choisissez Copy (Copier).

   Amazon S3 déplace vos objets vers le dossier de destination.

Pour supprimer un objet et un compartiment dans Amazon S3, veuillez consulter Suppression d'objets et de compartiments (p. 10).

Suppression d'objets et de compartiments

Lorsque vous n'avez plus besoin d'un objet ou d'un compartiment, nous vous recommandons de les supprimer pour éviter des frais supplémentaires. Si vous avez terminé cette procédure de mise en route en tant qu'exercice d'apprentissage et que vous ne prévoyez pas d'utiliser votre compartiment ou vos objets, nous vous recommandons de supprimer votre compartiment afin que les frais ne s'accumulent plus. Avant de supprimer votre compartiment, vous devez vider celui-ci ou supprimer les objets du compartiment. Une fois que vous avez supprimé vos objets et votre compartiment, ils ne sont plus disponibles.

Si vous souhaitez continuer à utiliser le même nom de compartiment, nous vous recommandons de supprimer les objets ou de vider le compartiment, mais de ne pas supprimer celui-ci. Une fois que vous avez supprimé un compartiment, le nom devient disponible et peut être réutilisé. Toutefois, un autre compte peut créer un compartiment portant le même nom avant que vous n'ayez l'occasion de réutiliser celui-ci.

Rubriques

Vider votre compartiment

Si vous envisagez de supprimer votre compartiment, vous devez d'abord vider celui-ci, ce qui supprimera tous les objets du compartiment.

Pour vider un compartiment :

1. Dans la liste Compartiments, sélectionnez le compartiment à vider, puis choisissez Vider.
2. Pour confirmer que vous souhaitez vider le compartiment et supprimer tous les objets qu'il contient, dans Vider le compartiment, entrez le nom du compartiment.

   Important

   Cette opération ne peut pas être annulée. Les objets ajoutés au compartiment pendant le vidage de celui-ci seront supprimés.
3. Pour vider le compartiment et supprimer tous les objets qu'il contient, choisissez Vider.

   Une page Empty bucket: Status (Vider le compartiment : statut) s'ouvre et vous permet de consulter un résumé des suppressions d'objets qui ont réussi et échoué.
4. Pour revenir à votre liste de compartiments, choisissez Quitter.

Suppression d'un objet

Si vous souhaitez choisir les objets que vous supprimez sans vider tous les objets de votre compartiment, vous pouvez supprimer un objet.

1. Dans la liste Compartiments, choisissez le nom du compartiment à partir duquel vous souhaitez supprimer un objet.

2. Cochez la case située à gauche des noms des objets que vous souhaitez supprimer.
3. Choisissez Actions, puis Delete (Supprimer) dans la liste des options qui s'affiche.

   Vous pouvez également choisir Delete (Supprimer) dans les options situées en haut à droite.
4. Entrez **`delete`** si vous êtes invité à confirmer que vous souhaitez supprimer ces objets.
5. Choisissez Delete objects (Supprimer les objets) en bas à droite et Amazon S3 supprime les objets spécifiés.

Suppression de votre compartiment

Après avoir vidé votre compartiment ou supprimé tous les objets de votre compartiment, vous pouvez supprimer celui-ci.

1. Pour supprimer un compartiment, dans la liste Compartiments, sélectionnez le compartiment.
2. Sélectionnez Delete (Supprimer).
3. Pour confirmer la suppression, dans Supprimer le compartiment, entrez le nom du compartiment.

   Important

   La suppression d'un compartiment ne peut pas être annulée. Les noms de compartiment sont uniques. Si vous supprimez votre compartiment, un autre utilisateur AWS pourra en utiliser le nom. Si vous souhaitez continuer à utiliser le même nom de compartiment, ne supprimez pas le compartiment. Au lieu de cela, videz et conservez le compartiment.
4. Pour supprimer votre compartiment, choisissez Supprimer le compartiment.

Pour de plus amples informations sur l'utilisation d'Amazon S3, veuillez consulter Comment procéder ensuite ? (p. 12)

Comment procéder ensuite ?

Dans les exemples précédents, vous avez appris à réaliser certaines tâches Amazon S3 élémentaires. Pour de plus amples informations détaillées, veuillez consulter l'un des guides Amazon S3 suivants :

- Le Guide de l'utilisateur de la console Amazon Simple Storage Service pour en savoir plus sur l'utilisation de la console Amazon S3.
- Le Manuel du développeur Amazon Simple Storage Service pour obtenir des informations détaillées sur les fonctions d'Amazon S3 et des exemples de code pour prendre en charge ces fonctions.
- La Référence de l'API Amazon Simple Storage Service pour obtenir des détails sur l'API REST Amazon S3.

Les rubriques suivantes expliquent différentes méthodes permettant de mieux comprendre Amazon S3 afin de pouvoir l'implémenter dans vos applications.

Rubriques

Scénarios d'utilisation courants

Le site de solutions AWS répertorie un grand nombre d'utilisations possibles d'Amazon S3. La liste suivante résume certaines de ces utilisations.

- Sauvegarde et stockage – Proposez des services de sauvegarde et de stockage pour le compte d'autres utilisateurs.
- Hébergement d'applications – Proposez des services de déploiement, d'installation et de gestion d'applications web.
- Hébergement de contenus multimédias – Développez une infrastructure redondante, évolutive et hautement disponible qui héberge des chargements et des téléchargements de vidéos, photos ou musique.
- Livraison de logiciels – Hébergez vos applications logicielles afin que vos clients puissent les télécharger.

Pour de plus amples informations, veuillez consulter Solutions AWS.

Pour aller plus loin

Cette section présente les éléments que vous devez prendre en compte avant de lancer votre propre produit Amazon S3.

Rubriques

Compte AWS et informations d'identification

Lorsque vous vous êtes inscrit au service, vous avez créé un compte AWS à l'aide d'une adresse e-mail et d'un mot de passe. Il s'agit des informations d'identification utilisateur racine de votre compte AWS. Comme bonne pratique, vous ne devez pas utiliser les informations d'identification utilisateur racine pour accéder à AWS. Vous ne devez pas non plus fournir vos informations d'identification à quelqu'un d'autre. Créez plutôt des utilisateurs individuels pour toutes les personnes qui ont besoin d'accéder à votre compte AWS. Tout d'abord, créez un utilisateur administrateur AWS Identity and Access Management (IAM) pour vous-même et utilisez-le pour votre travail quotidien. Pour de plus amples informations, veuillez consulter Création de votre premier utilisateur administrateur et groupe IAM dans le Guide de l'utilisateur IAM. Créez ensuite d'autres utilisateurs IAM pour les autres personnes. Pour de plus amples informations, veuillez consulter Création de votre premier groupe et utilisateur délégué IAM dans le Guide de l'utilisateur IAM.

Si vous êtes propriétaire ou administrateur de compte et souhaitez en savoir davantage sur IAM, consultez la description du produit sur https://aws.amazon.com/iam ou dans la documentation technique du Guide de l'utilisateur IAM.

Sécurité

Amazon S3 fournit des mécanismes d'authentification permettant de sécuriser les données stockées dans Amazon S3 en les protégeant contre tout accès non autorisé. Sauf si vous spécifiez le contraire, seul le propriétaire du compte AWS peut accéder aux données chargées vers Amazon S3. Pour de plus amples informations sur la gestion de l'accès aux compartiments et aux objets, veuillez consulter Gestion des identités et des accès dans Amazon S3 dans le Manuel du développeur Amazon Simple Storage Service.

Vous pouvez également chiffrer vos données avant de les charger vers Amazon S3.

Intégration à AWS

Vous pouvez utiliser Amazon S3 seul ou avec d'autres produits Amazon. Voici les produits les plus courants utilisés avec Amazon S3 :

- Amazon EC2
- Amazon EMR
- Amazon SQS
- Amazon CloudFront

Tarification

Découvrez la grille tarifaire du stockage et du transfert de données sur Amazon S3. Pour de plus amples informations, veuillez consulter Tarification Amazon S3.

Fonctionnalités avancées Amazon S3

Les exemples présentés dans ce manuel expliquent comment accomplir les tâches élémentaires telles que la création d'un compartiment, le chargement et le téléchargement de données depuis et vers ce compartiment, ainsi que le déplacement et la suppression de données. Le tableau suivant rassemble certaines des fonctionnalités avancées les plus utilisées parmi celles proposées par Amazon S3 Veuillez

noter que certaines fonctionnalités avancées ne sont pas disponibles dans AWS Management Console et impliquent donc d'utiliser l'API Amazon S3. Toutes les fonctionnalités avancées et des indications concernant leur utilisation sont décrites dans le Manuel du développeur Amazon Simple Storage Service.

Lien	Fonctionnalité
Compartiments de type Paiement par le demandeur	Découvrez comment configurer un compartiment, afin que les clients paient les téléchargements qu'ils effectuent.
Utilisation de BitTorrent avec Amazon S3	Découvrez comment utiliser BitTorrent, un protocole peer-to-peer permettant de distribuer des fichiers.
Contrôle de version	Découvrez les fonctions de gestion des versions Amazon S3
Hébergement de sites Web statiques	Découvrez comment héberger un site web statique sur Amazon S3.
Gestion du cycle de vie des objets	Découvrez comment gérer le cycle de vie des objets de votre compartiment. La gestion du cycle de vie comprend l'expiration des objets et leur archivage (passage des objets à la catégorie de stockage `S3 S3 Glacier`).

Bonnes pratiques en matière de contrôle d'accès

Amazon S3 fournit plusieurs fonctionnalités et outils de sécurité. Les scénarios suivants devraient fournir une orientation sur les outils et paramètres que vous pouvez utiliser lors de l'exécution de certaines tâches ou lors d'opérations dans des environnements spécifiques. Une utilisation adéquate de ces outils peut aider à préserver l'intégrité de vos données et à garantir que vos ressources sont accessibles aux utilisateurs visés.

Rubriques

Création d'un nouveau compartiment

Lorsque vous créez un nouveau compartiment, vous devez appliquer les outils et paramètres suivants pour vous assurer que vos ressources Amazon S3 sont protégées.

Blocage de l'accès public

La fonctionnalité de blocage de l'accès public S3 fournit quatre paramètres pour vous aider à éviter d'exposer vos ressources S3 par inadvertance. Vous pouvez appliquer ces paramètres de manière combinée à des points d'accès individuels, à des compartiments ou à des comptes AWS entiers. Si vous appliquez un paramètre à un compte, il s'applique à tous les compartiments et points d'accès appartenant à ce compte. Par défaut, le paramètre Block all public access (Bloquer tous les accès publics) est appliqué aux nouveaux compartiments créés dans la console Amazon S3.

Pour de plus amples informations, veuillez consultez La signification du mot « public » dans le Manuel du développeur Amazon Simple Storage Service.

Si les paramètres de blocage de l'accès public S3 sont trop restrictifs, vous pouvez utiliser des identités AWS Identity and Access Management (IAM) pour accorder l'accès à des utilisateurs spécifiques plutôt que de désactiver tous les paramètres Block Public Access. L'utilisation de Block Public Access avec des identités IAM permet de s'assurer que toute opération bloquée par un paramètre Block Public Access est rejetée, sauf si l'utilisateur demandeur a reçu une autorisation spécifique.

Pour de plus amples informations, veuillez consulter Paramètres Block Public Access dans le Manuel du développeur Amazon Simple Storage Service.

Accorder l'accès avec des identités IAM

Lors de la configuration de comptes pour les nouveaux membres de l'équipe qui ont besoin d'un accès S3, utilisez des utilisateurs et des rôles IAM pour garantir le principe de moindre privilège. Vous pouvez également mettre en œuvre une forme d'authentification multi-facteur IAM (Multi-Factor Authentication) pour soutenir une base d'identité solide. À l'aide des identités IAM, vous pouvez accorder des autorisations uniques aux utilisateurs et spécifier les ressources auxquelles ils peuvent accéder et les actions qu'ils peuvent effectuer. Les identités IAM offrent des capacités accrues, notamment la possibilité d'exiger des utilisateurs qu'ils saisissent des informations d'identification de connexion avant d'accéder aux ressources partagées et d'appliquer des hiérarchies d'autorisations à différents objets au sein d'un même compartiment.

Pour de plus amples informations, veuillez consulter Exemple 1 : propriétaire d'un compartiment accordant à ses utilisateurs des autorisations sur un compartiment dans le Manuel du développeur Amazon Simple Storage Service.

Stratégies de compartiment

Avec les stratégies de compartiment, vous pouvez personnaliser l'accès au compartiment pour vous assurer que seuls les utilisateurs que vous avez approuvés peuvent accéder aux ressources et effectuer des actions en leur sein. Outre les stratégies de compartiment, vous devez utiliser les paramètres Block Public Access au niveau du compartiment pour limiter davantage l'accès public à vos données.

Pour de plus amples informations, veuillez consulter Stratégies et autorisations dans Amazon S3 dans le Manuel du développeur Amazon Simple Storage Service.

Lors de la création de stratégies, évitez l'utilisation de caractères génériques dans l'élément `Principal`, car cela permet à quiconque d'accéder effectivement à vos ressources Amazon S3. Il est préférable de répertorier explicitement les utilisateurs ou les groupes autorisés à accéder au compartiment. Plutôt que d'inclure un caractère générique pour leurs actions, accordez-leur des autorisations spécifiques le cas échéant.

Pour étendre la pratique des moindres privilèges, les instructions Refuser dans l'élément `Effect` doivent être aussi larges que possible et les instructions Autoriser doivent être aussi restreintes que possible. Les effets des instructions Refuser associés à l'action « `s3:*` » sont un autre bon moyen de mettre en œuvre des bonnes pratiques d'acceptation pour les utilisateurs inclus dans les instructions de condition de stratégie.

Pour de plus amples informations sur la spécification des conditions relatives au moment où une stratégie est en vigueur, veuillez consulter Clés de condition pour Amazon S3 dans le Manuel du développeur Amazon Simple Storage Service.

Compartiments dans une configuration de VPC

Lorsque vous ajoutez des utilisateurs dans une configuration d'entreprise, vous pouvez utiliser un point de terminaison de VPC pour permettre à tous les utilisateurs de votre réseau virtuel d'accéder à vos ressources Amazon S3. Les points de terminaison d'un VPC permettent aux développeurs de fournir un accès et des autorisations spécifiques à des groupes d'utilisateurs en fonction du réseau auquel l'utilisateur

est connecté. Plutôt que d'ajouter chaque utilisateur à un rôle ou un groupe IAM, vous pouvez utiliser des points de terminaison d'un VPC pour refuser l'accès au compartiment, si la demande ne provient pas du point de terminaison spécifié.

Pour de plus amples informations, veuillez consulter Exemple de stratégies de compartiment pour les points de terminaison d'un VPC pour Amazon S3 dans le Manuel du développeur Amazon Simple Storage Service.

Stockage et partage des données

Utilisez les bonnes pratiques et les outils suivants pour stocker et partager vos données Amazon S3.

Gestion des versions et verrouillage d'objet pour l'intégrité des données

Si vous utilisez la console Amazon S3 pour gérer des compartiments et des objets, vous devez implémenter la gestion des versions S3 et le verrouillage des objets S3. Ces fonctionnalités permettent d'éviter des modifications accidentelles des données critiques et vous permettent d'annuler les actions non programmées. Cette fonctionnalité est particulièrement utile lorsqu'il y a plusieurs utilisateurs disposant d'autorisations d'écriture et d'exécution complètes qui accèdent à la console Amazon S3.

Pour de plus amples informations sur la gestion des versions S3, veuillez consulter Utilisation de la gestion des versions dans le Manuel du développeur Amazon Simple Storage Service. Pour de plus amples informations sur le verrouillage d'objets, veuillez consulter Verrouillage d'objets à l'aide de la fonctionnalité de verrouillage des objets Amazon S3 dans le Manuel du développeur Amazon Simple Storage Service.

Gestion du cycle de vie des objets en vue de leur rentabilité

Pour gérer vos objets de manière à ce qu'ils soient stockés à moindre coût tout au long de leur cycle de vie, vous pouvez associer des stratégies de cycle de vie à la gestion des versions d'objets. Les stratégies de cycle de vie définissent les actions que vous souhaitez que S3 prenne au cours de la durée de vie d'un objet. Par exemple, vous pouvez créer une stratégie de cycle de vie qui fera passer les objets vers une autre classe de stockage, les archiver ou les supprimer après une période spécifiée. Vous pouvez définir une stratégie de cycle de vie pour tous les objets ou un sous-ensemble d'objets du compartiment à l'aide d'une balise ou d'un préfixe partagé.

Pour de plus amples informations, veuillez consulter Gestion du cycle de vie des objets dans le Manuel du développeur Amazon Simple Storage Service.

Réplication entre régions pour plusieurs emplacements de bureaux

Lors de la création de compartiments auxquels accèdent différents emplacements de bureau, vous devez envisager la mise en œuvre de la réplication entre régions S3. La réplication entre régions permet de s'assurer que tous les utilisateurs ont accès aux ressources dont ils ont besoin et augmente l'efficacité opérationnelle. La réplication entre régions apporte une disponibilité accrue en copiant des objets entre compartiments S3 dans différentes régions AWS. Cependant, l'utilisation de cet outil augmente les coûts de stockage.

Pour de plus amples informations, veuillez consulter Réplication dans le Manuel du développeur Amazon Simple Storage Service.

Autorisations pour l'hébergement sécurisé de site Web statique

Lorsque vous configurez un compartiment à utiliser comme site web statique accessible publiquement, vous devez désactiver tous les paramètres Bloc Public Access. Il est important de fournir uniquement des action `s3:GetObject` et non des autorisations `ListObject` ou `PutObject` lors de l'écriture de la stratégie de compartiment pour votre site web statique. Cela permet de s'assurer que les utilisateurs ne peuvent pas voir tous les objets de votre compartiment ou ajouter leur propre contenu.

Pour de plus amples informations, veuillez consulter Définition des autorisations pour l'accès au site web dans le Manuel du développeur Amazon Simple Storage Service.

Amazon CloudFront fournit les fonctionnalités nécessaires pour configurer un site web statique sécurisé. Les sites web statiques Amazon S3 prennent uniquement en charge les points de terminaison HTTP. CloudFront utilise le stockage durable d'Amazon S3 tout en fournissant des en-têtes de sécurité supplémentaires, tels que HTTPS. HTTPS accroît la sécurité en chiffrant une requête HTTP normale et en offrant une protection contre les cyberattaques courantes.

Pour de plus amples informations, veuillez consulter Démarrer avec un site web statique sécurisé dans le Manuel du développeur Amazon CloudFront.

Partage de ressources

Il existe plusieurs façons de partager des ressources avec un groupe spécifique d'utilisateurs. Les outils suivants vous permettent de partager un ensemble de documents ou d'autres ressources avec un seul groupe d'utilisateurs, de service ou bureau. Bien qu'ils puissent tous être utilisés pour atteindre le même objectif, certains outils peuvent mieux s'adapter que d'autres à vos paramètres existants.

Stratégies utilisateur

Vous pouvez partager des ressources avec un groupe limité de personnes à l'aide de groupes IAM et de stratégies utilisateur. Lors de la création d'un nouvel utilisateur IAM, vous êtes invité à le créer et à l'ajouter à un groupe. Toutefois, vous pouvez créer et ajouter des utilisateurs à des groupes à tout moment. Si les personnes avec lesquelles vous avez l'intention de partager ces ressources sont déjà configurées dans IAM, vous pouvez les ajouter à un groupe commun et partager le compartiment avec leur groupe dans la stratégie utilisateur. Vous pouvez également utiliser les stratégies utilisateur IAM pour partager des objets individuels dans un compartiment.

Pour de plus amples informations, veuillez consulter Autoriser un accès utilisateur IAM à l'un de vos compartiments dans le Manuel du développeur Amazon Simple Storage Service.

Listes de contrôle d'accès (ACL)

En règle générale, nous vous recommandons d'utiliser des stratégies de compartiment S3 ou des stratégies IAM pour le contrôle d'accès. Les listes de contrôle d'accès (ACL) Amazon S3 sont un mécanisme de contrôle d'accès hérité antérieur à IAM. Si vous utilisez déjà les ACL S3 et que vous les trouvez satisfaisantes, il n'est pas nécessaire de les modifier. Cependant, certains scénarios de contrôle d'accès nécessitent l'utilisation de listes de contrôle d'accès. Par exemple, lorsqu'un propriétaire de compartiment souhaite accorder une autorisation à des objets, mais que tous les objets ne lui appartiennent, le propriétaire de l'objet doit d'abord accorder l'autorisation au propriétaire du compartiment. On utilise pour ce faire un objet ACL.

Pour de plus amples informations, veuillez consulter Exemple 3 : Propriétaire d'un compartiment accordant à ses utilisateurs des autorisations sur des objets qu'il ne possède pas dans le Manuel du développeur Amazon Simple Storage Service.

Préfixes

Lorsque vous tentez de partager des ressources spécifiques à partir d'un compartiment, vous pouvez répliquer des autorisations au niveau du dossier à l'aide de préfixes. La console Amazon S3 prend en charge le concept de dossier comme moyen de regrouper des objets à l'aide d'un préfixe de nom partagé pour les objets. Vous pouvez ensuite spécifier un préfixe dans les conditions d'un stratégie utilisateur IAM pour leur accorder l'autorisation explicite d'accéder aux ressources associées à ce préfixe.

Pour de plus amples informations, veuillez consulter Utilisation de dossiers dans le Guide de l'utilisateur de la console Amazon Simple Storage Service.

Ajout de balises

Si vous utilisez le balisage d'objets pour catégoriser le stockage, vous pouvez partager des objets balisés avec une valeur spécifique avec des utilisateurs spécifiés. Le balisage des ressources vous permet de contrôler l'accès aux objets en fonction des balises associées à la ressource à laquelle un utilisateur tente

d'accéder. Pour ce faire, utilisez la condition `ResourceTag/key-name` dans une stratégie utilisateur IAM pour autoriser l'accès aux ressources balisées.

Pour de plus amples informations, veuillez consulter Contrôle de l'accès aux ressources AWS à l'aide des balises de ressources dans le Guide de l'utilisateur IAM.

Protection des données

Utilisez les outils suivants pour protéger les données en transit et au repos, toutes deux essentielles au maintien de l'intégrité et de l'accessibilité de vos données.

Chiffrement de l'objet

Amazon S3 offre plusieurs options de chiffrement d'objet qui protègent les données en transit et au repos. Le chiffrement côté serveur chiffre vos objets avant de les enregistrer sur les disques des centres de données, puis les déchiffre lorsque vous téléchargez les objets. Tant que vous authentifiez votre demande et que vous avez des autorisations d'accès, il n'y a aucune différence dans la manière dont vous accédez aux objets chiffrés ou déchiffrés. Lorsque vous configurez le chiffrement côté serveur, vous disposez de trois options mutuellement exclusives :

- Clés gérées par Amazon S3 (SSE-S3)
- Clés principales client (CMK) stockées dans AWS Key Management Service (SSE-KMS)
- Clés fournies par le client (SSE-C).

Pour de plus amples informations, veuillez consulter Protection des données à l'aide du chiffrement côté serveur dans le Manuel du développeur Amazon Simple Storage Service.

Le chiffrement côté client consiste à chiffrer des données avant de les envoyer à Amazon S3. Pour de plus amples informations, veuillez consulter Protection des données à l'aide du chiffrement côté client dans le Manuel du développeur Amazon Simple Storage Service.

Méthodes de signature

Signature Version 4 est le processus permettant d'ajouter des informations d'authentification à des demandes AWS par HTTP. Pour des raisons de sécurité, la plupart des demandes à AWS doivent être signées avec une clé d'accès, qui se compose d'un ID de clé d'accès et de la clé d'accès secrète. Ces deux clés sont généralement appelées informations d'identification de sécurité.

Pour plus d'informations, consultez Authentification des demandes (Signature AWS version 4) et Processus de signature Signature Version 4.

Journalisation et surveillance

La surveillance est un élément clé pour assurer la fiabilité, la disponibilité et les performances de vos solutions Amazon S3, pour vous permettre de déboguer plus facilement une défaillance multi-points potentielle. La journalisation peut fournir un aperçu des erreurs que les utilisateurs reçoivent, ainsi que du moment où des demandes sont faites et le type de demande. AWS fournit plusieurs outils pour surveiller vos ressources Amazon S3 :

- Amazon CloudWatch
- AWS CloudTrail
- Journaux d'accès Amazon S3
- AWS Trusted Advisor

Pour de plus amples informations, veuillez consulter Journalisation et surveillance dans Amazon S3 dans le Manuel du développeur Amazon Simple Storage Service.

Amazon S3 est intégré à AWS CloudTrail, service qui enregistre les actions effectuées par un utilisateur, un rôle ou un service AWS dans Amazon S3. Cette fonctionnalité peut être jumelée à Amazon GuardDuty, qui surveille les menaces contre vos ressources Amazon S3 en analysant les événements de gestion CloudTrail et les événements de données CloudTrail S3. Ces sources de données surveillent différents types d'activités. Par exemple, les événements de gestion CloudTrail liés à S3 incluent des opérations qui répertorient ou configurent des projets S3. GuardDuty analyse les événements de données S3 de tous vos compartiments S3 et les surveille pour détecter les activités malveillantes et suspectes.

Pour de plus amples informations, veuillez consulter Protection Amazon S3 dans Amazon GuardDuty dans le Guide de l'utilisateur GuardDuty.

Ressources de développement

Pour vous aider à développer des applications utilisant le langage de votre choix, nous fournissons les ressources suivantes :

- Exemples de code et bibliothèques – Le centre pour développeurs AWS propose des exemples de code et de bibliothèques conçus spécialement pour Amazon S3.

  Vous pouvez utiliser ces exemples de codes afin de mieux comprendre comment mettre en œuvre l'API Amazon S3. Pour de plus amples informations, veuillez consulter le Centre pour développeurs AWS.
- Tutoriels – Notre centre de ressources propose des tutoriels supplémentaires sur Amazon S3.

  Ces tutoriels fournissent une approche concrète de l'utilisation des fonctionnalités Amazon S3. Pour de plus amples informations, veuillez consulter Articles et tutoriels.
- Forum client – Nous vous conseillons de consulter le forum Amazon S3 afin de découvrir comment les autres utilisateurs exploitent ce service et de tirer parti des réponses aux questions qu'ils ont déjà posées.

  Le forum peut vous aider à identifier les actions que vous pouvez effectuer ou non avec Amazon S3. Le forum vous permet également de poser des questions auxquelles d'autres utilisateurs ou responsables AWS pourraient répondre. Vous pouvez utiliser le forum pour signaler des problèmes liés au service ou à l'API. Pour de plus amples informations, veuillez consulter Forums de discussion.

Ressources de référence

La liste suivante présente des ressources supplémentaires que vous pouvez utiliser pour mieux comprendre Amazon S3.

- Le Guide de l'utilisateur de la console Amazon Simple Storage Service décrit toutes les fonctionnalités AWS Management Console liées à Amazon S3.
- Le Manuel du développeur Amazon Simple Storage Service fournit des informations détaillées sur ce service.

  Il inclut une présentation architecturale, des descriptions de concept détaillées et des procédures pour utiliser l'API.
- La Référence de l'API Amazon Simple Storage Service fournit une présentation détaillée des actions et des paramètres dans Amazon S3.
- Le tableau de bord de l'état des services vous indique l'état du service web Amazon S3.

  Le tableau de bord de l'état des services vous indique si Amazon S3 (et tous les autres produits AWS) fonctionne correctement. Pour de plus amples informations, veuillez consulter le Tableau de bord de l'état des services.

A propos de ce manuel

Il s'agit du Guide de démarrage Amazon Simple Storage Service.

Dans ce guide, Amazon Simple Storage Service est souvent désigné sous le nom « Amazon S3 ». Tous les droits d'auteur et protections légales restent applicables.