Guide de l’utilisateur

AWS Terminal de transfert de données

AWS Terminal de transfert de données: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'un terminal de transfert de données ?

AWS Le terminal de transfert de données est un emplacement physique prêt à être connecté au réseau sur lequel vous pouvez emporter vos périphériques de stockage de données pour un transfert de données rapide vers et depuis votre service AWS cloud. Téléchargez les données capturées à distance pour faciliter l'accès aux données capturées à distance.

Planifiez une réservation dans l'un de nos terminaux de transfert de données physiques depuis la console de AWS gestion, arrivez à l'heure prévue et téléchargez vos données sur vos services AWS cloud avec vos propres appareils. Une fois que votre réservation est terminée et que vous partez, l'établissement est à nouveau sécurisé et prêt pour la prochaine réservation prévue.

> **Note**
>
> AWS Le terminal de transfert de données n'est actuellement disponible que pour les clients AWS Enterprise.

Pour accéder au terminal de transfert de données :

- AWS Console du terminal de transfert de données : https://console.aws.amazon.com / datatransferterminal
- Installations du terminal de transfert de données : L'emplacement des installations du terminal de transfert de données est indiqué une fois la réservation effectuée dans la console. Pour plus d'informations, voir Effectuer un transfert de données.

Caractéristiques

L'utilisation AWS du terminal de transfert de données facilite l'accès de vos données à votre service AWS Cloud depuis des sites distants. Voici quelques-uns des avantages du terminal de transfert de données pour vos besoins de téléchargement de données à distance :

Sécurisé, privé et exclusif

Chaque terminal de transfert de données est un lieu privé et sécurisé où vous pouvez effectuer des transferts de données importants entre votre périphérique de stockage de données et vos AWS services via une connexion réseau rapide.

Une console de réservation dédiée

Ajoutez du personnel approuvé à votre équipe de transfert et planifiez une réservation de terminal de transfert de données à l'aide de la console du terminal de transfert de AWS données.

Connexions réseau par fibre optique

Chaque terminal de transfert de données comprend deux connexions à fibre optique () de 100 Gigabit (Gbit/s) pour des téléchargements de données rapides et une redondance. LR4

Contrôle de vos dispositifs de stockage de données

Inutile d'expédier votre appareil Snowball et d'attendre que vos données soient téléchargées vers vos services AWS Cloud. Vous contrôlez vos périphériques de stockage de données physiques tout au long du processus de transfert de données, pour acheminer vos données là où elles doivent être acheminées plus rapidement.

Concepts clés

L'utilisation d'un terminal de transfert de AWS données nécessite qu'un responsable du processus planifie une réservation pour qu'un spécialiste du transfert de données puisse accéder à un terminal de transfert de données. Reportez-vous aux sections suivantes pour en savoir plus sur la terminologie des terminaux de transfert de données.

Rubriques

- Équipe de transfert
- Le personnel
- Installations

Équipe de transfert

Une équipe de transfert est un groupe de personnel déterminé par un titulaire de AWS compte qui peut être sélectionné pour effectuer des transferts de données au nom de votre organisation. La mise en place d'une équipe de transfert implique de donner un nom à l'équipe de transfert et de spécifier le personnel de l'équipe. Nous recommandons des groupes de quatre spécialistes du transfert de données ou moins pour une seule réservation.

Pour plus d'informations, voir Planifier la réservation d'un terminal de transfert de données.

Le personnel

Le personnel désigne les personnes qui peuvent soit effectuer et gérer les réservations, soit se rendre aux installations du terminal de transfert de données et les utiliser. Le personnel peut être soit un responsable du processus, soit un spécialiste du transfert de données, soit les deux.

Propriétaire du processus

- Un propriétaire de processus est un propriétaire de AWS compte qui peut ajouter, modifier et supprimer du personnel de son compte de terminal de transfert de AWS données.

Spécialiste du transfert de données

- Un spécialiste du transfert de données est une personne qui peut se rendre dans les installations du terminal de transfert de données pour effectuer des transactions de téléchargement de données. Ce personnel doit être autorisé par le responsable du processus et ajouté à votre compte de terminal de transfert de AWS données. Pour accéder à un terminal de transfert de données, une pièce d'identité émise par le gouvernement sera requise.

Installations

Les terminaux de transfert de données sont des centres de données codétenus et gérés par un ou plusieurs fournisseurs de services. Chaque établissement exige que les spécialistes du transfert de données fournissent une preuve d'identité émise par le gouvernement qui doit correspondre à leurs dossiers de réservation pour accéder à la suite de terminaux de transfert de données.

Considérations concernant la planification

Les réservations peuvent être effectuées dans la console du terminal de transfert de données pour une durée d'une à six heures, tous les jours de la semaine, tout au long de l'année. Les réservations individuelles peuvent être programmées consécutivement, avec un minimum d'une heure d'intervalle entre les réservations. Toutes les réservations doivent être effectuées au moins 24 heures à l'avance.

Le temps nécessaire pour effectuer un transfert de données varie en fonction des vitesses de téléchargement. Lorsque vous planifiez et planifiez la réservation de votre terminal de transfert de données, tenez compte des facteurs suivants qui ont une incidence sur les performances de téléchargement.

Équipement

- Certains équipements peuvent inclure des paramètres susceptibles d'avoir un impact sur les performances de téléchargement. Reportez-vous aux spécifications de votre équipement pour connaître les vitesses de transfert suggérées.

État du réseau

- Les périodes de trafic réseau intense auront un impact sur les vitesses de téléchargement des données et doivent être prises en compte lors du choix de l'heure de votre session de transfert de données. La planification de votre session de transfert de données pendant les heures creuses ou pendant les périodes de faible activité du réseau peut améliorer votre vitesse de téléchargement.

Taille du transfert de données

- La connectivité réseau du terminal de transfert de données est conçue pour les transferts de données importants. Cependant, la taille des données transférées aura un impact sur la durée de la session.

Cas d’utilisation

Bien que tous les clients AWS d'entreprise puissent accéder au système de terminal de transfert de données, certains scénarios d'utilisation peuvent en tirer davantage parti.

Conduite autonome et systèmes avancés d'assistance à la conduite (AD/ADAS) : les fabricants d'équipements automobiles d'origine (OEM) et les fournisseurs génèrent de grands ensembles de données à partir de leurs flottes de véhicules autonomes qui circulent et collectent des données dans de nombreux métros d'Amérique du Nord, d'Europe et de l'ASEAN. Avec le terminal de transfert de données, les données collectées par ces véhicules de flotte peuvent être téléchargées vers le service AWS Cloud et utilisées pour entraîner AD/ADAS des modèles.

Médias et divertissement : les studios et autres créateurs de contenu génèrent souvent des fichiers vidéo et audio numériques (AV) sur des sites distants. Il est important que ces fichiers audiovisuels soient téléchargés sur le cloud en temps opportun afin que les équipes de production et de montage géographiquement dispersées puissent démarrer les flux de travail en parallèle et en temps réel. En utilisant le terminal de transfert de données pour télécharger des données à distance, les délais de production peuvent être raccourcis, ce qui se traduit par une réduction des coûts de production.

Cartes, photogrammétrie et imagerie 3D : les organisations qui utilisent des applications de cartographie ou d'imagerie collectent des données sur des sites distants et doivent télécharger ces

fichiers visuels dans le AWS cloud à des fins d'analyse ou de formation. Le terminal de transfert de données réduit le temps entre la collecte et l'analyse de ces grands ensembles de données, ce qui permet de conserver les données géospatiales up-to-date pour les conducteurs, les agriculteurs et les autres utilisateurs de ces informations.

Services connexes

Les AWS services suivants offrent une expérience optimale lors de l'utilisation du terminal de transfert de données.

AWS service	Description
AWS Snowball Edge	AWS Le terminal de transfert de données complète les produits Snowball en fournissant un emplacement permettant un téléchargement plus rapide vers votre AWS cloud, minimisan t ainsi les temps d'attente pour accéder à vos données.
Amazon S3	Apportez votre propre appareil à un terminal de transfert de données pour télécharger rapidement et en toute sécurité vos données vers votre service Amazon S3.

Exigences techniques relatives à l'utilisation du terminal de transfert de données

Avant de planifier une réservation sur un terminal de transfert de données, vous devez vous assurer que vous disposez de l'équipement et des configurations nécessaires pour vous connecter au réseau. Reportez-vous aux directives suivantes pour une connectivité et une expérience réseau optimales.

Équipement

Vous devez apporter des appareils portables pour la connectivité, notamment des écrans, un clavier, une souris et un ordinateur ou un ordinateur portable, au terminal de transfert de données pour votre réservation prévue.

Votre matériel doit pouvoir fonctionner avec des connexions par fibre optique (L4)

> **Note**
>
> En tant que bonne pratique en matière de sécurité des données, assurez-vous que vos données sont cryptées et sécurisées sur les périphériques de stockage que vous apportez au terminal de transfert de données et que vous appliquez des politiques de cryptage des données lorsque vous utilisez le terminal de transfert de données. Pour plus d'informations, voir Sécurité du terminal de transfert de AWS données

Exigences réseau

Assurez-vous que votre périphérique, serveur ou appliance de téléchargement (ordinateur portable) est prêt à se connecter au réseau et qu'il prend en charge le protocole DHCP. Pour une expérience de téléchargement de données optimale, vous devez disposer des éléments suivants :

- Un émetteur-récepteur QSFP optique 100G QSFP28 LR4 (100GBASE-LR4), compatible avec les connecteurs NIC et LC pour les connexions par câble à fibre optique fournies dans le terminal de transfert de données.
- Configuration automatique des adresses IP (DHCP) activée. Les serveurs DNS sont automatiquement assignés par DHCP.

- Up-to-date logiciels et pilotes de carte réseau.

Optimisation des performances

Pour optimiser le débit lors de l'utilisation du terminal de transfert de AWS données, tenez compte des recommandations suivantes.

- Matériel recommandé :
  - Carte d'interface réseau 100 Gbit/s
  - Processeur 16 cœurs
  - 128 GO DE RAM
  - plusieurs disques SSD NVME dans une matrice RAID
- Utilisez la bibliothèque AWS Common Runtime (AWS CRT) pour les téléchargements à l'aide de l'interface de ligne de AWS commande ou AWS du SDK.

  Optimisez les paramètres de transfert Amazon S3 en configurant les paramètres ci-dessous. Définissez ces valeurs sous la `s3` clé de niveau supérieur dans le fichier de AWS configuration, emplacement par défaut `~/.aws/config`.

  ```
  [default]
  s3 =
      preferred_transfer_client = crt
      target_bandwidth = 100Gb/s
      max_concurrent_requests = 20
      multipart_chunksize = 16MB
  ```

  Notez que toutes les valeurs de configuration Amazon S3 sont indentées et imbriquées sous la clé de niveau `s3` supérieur.

  - Facultatif : vous pouvez définir les valeurs ci-dessus par programmation à l'aide de la `aws configure set` commande. Par exemple, pour définir les valeurs ci-dessus pour le profil par défaut, vous pouvez exécuter les commandes suivantes à la place :

    ```
    aws configure set default.s3.preferred_transfer_client crt
    aws configure set default.s3.target_bandwidth 100Gb/s
    aws configure set default.s3.max_concurrent_requests 20
    aws configure set default.s3.multipart_chunksize 16MB
    ```

- Pour définir ces valeurs par programmation pour un profil autre que le profil par défaut, fournissez l'`--profile`indicateur. Par exemple, pour définir la configuration d'un profil nommé`test-profile`, exécutez une commande comme dans l'exemple ci-dessous.

```
aws configure set s3.max_concurrent_requests 20 --profile test-profile
```

- Activez BBR (Linux) sur l'appareil pour un meilleur débit.

```
sysctl -w net.core.default_qdisc=fq
sysctl -w net.ipv4.tcp_congestion_control=bbr
```

En savoir plus

Pour plus d'informations sur les configurations en ligne de AWS commande Amazon S3 afin d'optimiser la connectivité et les performances de votre réseau, consultez les ressources suivantes.

- AWS Configuration de la CLI Amazon S3 dans la référence des commandes de la AWS CLI
- Utilisez un client Amazon S3 performant : client AWS basé sur CRT dans le SDK Amazon AppStream S3/Amazon pour Java
- Comment optimiser les performances lorsque j'utilise la AWS CLI pour télécharger des fichiers volumineux sur Amazon S3 ? dans le AWS Knowledge Center

Prise en main

Commencez à effectuer des transferts de données à distance vers vos services AWS cloud en effectuant une réservation dans l'un des terminaux de transfert de données. Pour commencer, vous aurez besoin d'un équipement compatible avec le terminal de transfert de données et d'un compte AWS Enterprise.

Consultez la section Exigences techniques relatives à l'utilisation du terminal de transfert de données de ce guide avant de planifier une réservation de terminal de transfert de données afin de vous assurer que vous disposez d'un équipement avec les configurations optimales pour le transfert de données. Tous les périphériques de stockage de données et équipements de connexion réseau ne sont pas compatibles avec les connexions réseau à fibre optique disponibles dans les suites.

Lorsque vous vous inscrivez AWS, votre AWS compte est automatiquement ouvert pour tous les services AWS, y compris le terminal de transfert de données. Seuls les services que vous utilisez vous sont facturés.

Pour configurer le terminal de transfert de données, suivez les étapes décrites dans les sections suivantes.

Lorsque vous vous inscrivez à Data Transfer Terminal AWS et que vous le configurez, vous pouvez éventuellement modifier la langue d'affichage dans la console AWS de gestion. Pour plus d'informations, consultez la section Modification de la langue de la console de AWS gestion dans le guide AWS de démarrage de la console de gestion.

Une fois que vous avez un AWS compte, vous pouvez accéder au terminal de transfert de données. Pour plus d'informations sur la configuration et l'utilisation du terminal de transfert de AWS données, voir Planifier la réservation d'un terminal de transfert de données.

Inscrivez-vous pour un AWS compte

Pour commencer AWS, vous avez besoin d'un AWS compte. Pour plus d'informations sur la création d'un AWS compte, voir Commencer à utiliser un AWS compte dans le Guide de référence sur la gestion des AWS comptes.

Planifier la réservation d'un terminal de transfert de données

Pour commencer à utiliser le terminal de transfert de AWS données, vous devez avoir un AWS compte et vous connecter à la console de votre terminal de transfert de données à l'adresse https://console.aws.amazon.com /datatransferterminal. Une fois connecté à la console de votre terminal de transfert de données, vous pouvez consulter les réservations existantes ou en créer une nouvelle. Pour planifier une réservation, vous devez effectuer les opérations suivantes :

1. Créez une équipe de transfert. Vous devrez créer un groupe d'utilisateurs désigné pour créer une réservation et accéder au terminal de transfert de données pour effectuer un transfert de données. Pour en savoir plus sur ce sujet, voir Création d'une équipe de transfert.
2. Une fois votre équipe constituée, vous devrez y ajouter du personnel. Pour en savoir plus sur l'ajout de personnel à votre équipe de transfert, voir Ajouter du personnel.
3. Le responsable du processus peut planifier le transfert de données avec les équipes associées au compte. Pour plus d'informations sur la planification de la réservation, voir Spécifier les détails de la réservation.
4. Assurez-vous que les détails de la réservation sont corrects avant de soumettre votre demande. Une fois soumise, une demande de réservation ne peut pas être modifiée pendant au moins 24 heures. Pour plus d'informations, voir Vérifier et confirmer votre réservation.

Une fois votre réservation traitée et confirmée, votre équipe de transfert pourra accéder au terminal de transfert de données à l'heure prévue. Pour plus d'informations, voir Effectuer un transfert de données dans le terminal de transfert de données.

Création d'une équipe de transfert

Pour accéder à un terminal de transfert de données, vous devez planifier une réservation dans la console AWS de gestion. Connectez-vous à votre AWS compte pour accéder à la console du terminal de transfert de données et suivez les étapes suivantes pour planifier votre réservation.

1. Sur la page d'accueil du terminal de transfert de données, sélectionnez le bouton Commencer.
2. Si aucune équipe de transfert n'est déjà configurée sur votre compte, le bouton Créer une réservation sera désactivé. Vous devrez créer et nommer une équipe de transfert pour commencer.
   a. Cliquez sur le bouton Créer une équipe de transfert.

b. Donnez un nom à l'équipe.
   - Le nom doit comporter entre 2 et 64 caractères, en commençant par une lettre ou un chiffre.
   - Utilisez uniquement des lettres, des chiffres, des points et des tirets. Les caractères spéciaux ne sont pas reconnus.
   - N'incluez aucune information d'identification sensible.

c. Créez une description de l'équipe de transfert.
   - Fournissez une description qui aide à identifier l'équipe, par exemple en décrivant l'objectif de l'équipe pour une période, une campagne ou un projet spécifique.

d. Cliquez sur le bouton Créer une équipe de transfert.

   Vous serez redirigé vers la page de l'équipe de transfert et votre équipe nouvellement créée apparaîtra dans la section Équipes de transfert.

Mettre à jour les équipes de transfert sur votre compte Data Transfer Terminal

Pour configurer une nouvelle équipe de transfert, reportez-vous à la section Planifier la réservation d'un terminal de transfert de données de ce guide.

Pour modifier ou supprimer une équipe de transfert, procédez comme suit :

1. Sur la page Équipes de transfert, sélectionnez l'équipe de transfert que vous souhaitez modifier.
2. Pour modifier le nom et la description de l'équipe de transfert, cliquez sur le bouton Modifier.
3. Pour ajouter ou supprimer du personnel, sélectionnez l'onglet Personnel et suivez les étapes décrites dans la section Comment modifier, ajouter ou supprimer du personnel de mon compte ? section de cette FAQ.
4. Pour ajouter ou annuler une réservation pour l'équipe de transfert sélectionnée, consultez la section « Mise à jour du personnel de votre compte de terminal de transfert de données » de cette FAQ.

Ajouter du personnel

Ajoutez des responsables du processus et des spécialistes du transfert de données à votre équipe de transfert pour configurer le transfert de données et accéder au terminal de transfert de données. Pour ajouter du personnel à votre équipe de transfert, procédez comme suit :

1. Sur la page Transférer des équipes, sélectionnez la carte d'équipe de transfert souhaitée parmi celles répertoriées dans la section Transférer des équipes. La page récapitulative de l'équipe chargée des transferts s'affichera.
2. Cliquez sur l'onglet Personnel, puis sur le bouton Enregistrer une personne pour ajouter du personnel à l'équipe de transfert.
3. Remplissez les champs avec les informations nécessaires sur la personne que vous ajoutez à l'équipe de transfert sur la page Enregistrer le personnel.
   a. Alias personnel : créez un alias unique pour identifier la personne.
      - L'alias est utilisé pour identifier le personnel tout en protégeant son identité.
      - Il peut comporter jusqu'à 64 caractères et inclure des lettres, des chiffres et des tirets.
      - Les caractères spéciaux ne sont pas autorisés.
   b. Prénom : Indiquez le prénom de la personne tel qu'il apparaît sur sa pièce d'identité émise par le gouvernement.
   c. Nom de famille : Indiquez le nom ou le prénom de la personne tels qu'ils figurent sur sa pièce d'identité émise par le gouvernement.
   d. Adresse e-mail : Indiquez une adresse e-mail valide pour que la personne reçoive les informations de réservation et les instructions pour accéder au terminal de transfert de données.
4. Cliquez sur le bouton Enregistrer une personne pour terminer l'ajout de la personne à votre équipe de transfert.

Informer le personnel de votre compte de terminal de transfert de données

La modification du personnel existant sur votre compte dans la console du terminal de transfert de données n'est actuellement pas prise en charge. AWS Les propriétaires du processus du terminal de transfert de données peuvent uniquement ajouter ou supprimer du personnel pour le moment.

Pour supprimer du personnel de votre compte de terminal de transfert de données, procédez comme suit :

1. Sur la page Équipes de transfert, sélectionnez l'équipe de transfert associée au personnel que vous souhaitez supprimer.
2. Sur la page récapitulative de l'équipe de transfert sélectionnée, sélectionnez l'onglet Personnel.
3. Cliquez sur le bouton radio situé à côté de l'alias que vous souhaitez supprimer. Notez que vous ne pourrez voir l'alias de la personne que lorsque vous supprimerez son profil.

4. Sélectionnez le bouton Supprimer. Un avertissement apparaîtra pour confirmer l'action prévue pour le personnel sélectionné. Cliquez sur le bouton Supprimer pour continuer. Une bannière apparaîtra en haut de la console pour confirmer que le personnel a bien été supprimé.

Spécifiez les détails de la réservation

Les instructions suivantes vous expliquent comment planifier la réservation de votre terminal de transfert de données dans la console AWS de gestion. Pour plus d'informations sur l'utilisation du terminal de transfert de données, voir Effectuer un transfert de données.

1. Sélectionnez le bouton Effectuer une réservation dans l'onglet Réservations à venir.
2. Complétez les champs de la page Spécifier les détails de la réservation.
   a. Sélection de l'équipe de transfert : L'équipe de transfert sélectionnée par défaut apparaît en premier. Si vous souhaitez choisir une autre équipe, cliquez sur la flèche déroulante pour la sélectionner dans la liste des équipes de transfert disponibles.
   b. Responsable du processus : sélectionnez l'alias du personnel que vous souhaitez confier à la gestion de la réservation.
      - Un seul responsable du processus est autorisé à effectuer une réservation et il doit s'agir d'un membre du personnel autorisé sur votre AWS compte.

        Le responsable du processus peut également être inclus comme l'un des spécialistes du transfert de données pour effectuer également l'activité de transfert de données.
   c. Spécialiste du transfert de données : Sélectionnez le personnel auquel vous souhaitez avoir accès au terminal de transfert de données pour effectuer l'activité de transfert de données. Vous pouvez sélectionner plusieurs membres du personnel, selon les besoins.
      - La meilleure pratique consiste à limiter votre équipe de transfert à un maximum de quatre (4) spécialistes du transfert de données.
   d. Informations sur le terminal de transfert de données : Spécifiez l'installation du terminal de transfert de données, la date souhaitée et l'heure précise de la session de transfert de données.
      i. Terminal de transfert de données : Cliquez sur la flèche déroulante pour sélectionner un terminal de transfert de données.

> **Note**
>
> Seules les descriptions des installations seront fournies lors de la réservation. Des informations supplémentaires sur l'emplacement seront fournies dans l'e-mail de confirmation de réservation.

ii. Date et heure du terminal de transfert de données : Cliquez dans le champ Rechercher la date et l'heure de votre réservation pour afficher le calendrier et planifier votre réservation.

- Les réservations doivent être effectuées au moins 24 heures à l'avance et au plus tard six (6) mois à l'avance et ne peuvent durer que six (6) heures au maximum. Une seule réservation peut s'étendre sur plus d'une journée pour tenir compte des scénarios d'une nuit, si nécessaire.
- L'heure est indiquée à l'aide d'une horloge de 24 heures et ne peut être réservée que par tranches d'une heure entière.
- Pour effectuer des réservations consécutives, vous devez créer des réservations distinctes avec au moins une heure entre chaque session de transfert de données.
- Pour plus d'informations, consultez la section Considérations relatives à la planification.

3. Vérifiez que les détails de la réservation sont corrects, puis sélectionnez le bouton Créer pour continuer. Vous serez redirigé vers la page de confirmation, qui fournit un résumé de votre réservation.

Vérifiez et confirmez votre réservation

Après avoir précisé les détails de votre réservation, sélectionnez le bouton Suivant pour continuer à voir la page d'aperçu. Consultez les détails de votre demande de réservation de terminal de transfert de données sur la page Vérifier et créer.

- Si la demande vous convient, cliquez sur le bouton Créer.
- Si vous devez modifier votre réservation, cliquez sur le bouton Précédent.

Une fois la demande de réservation soumise, le responsable du processus recevra un e-mail confirmant que la demande a été reçue et est en cours de traitement. Une fois la demande approuvée, un autre e-mail confirmera la réservation et fournira des instructions pour localiser et

accéder au terminal de transfert de données. Pour plus d'informations sur l'accès au terminal de transfert de données, voir Effectuer un transfert de données.

Apporter des modifications à votre réservation

Il y a un délai de traitement de 24 heures avant que des modifications puissent être apportées à votre demande de réservation de terminal de transfert de données.

Après la période de traitement, pour consulter, modifier ou supprimer votre réservation, accédez à la page Transférer des équipes dans la console.

1. Localisez et sélectionnez la réservation souhaitée sur la carte de l'équipe.
2. Cliquez sur le menu Actions et sélectionnez l'action souhaitée.
   - Afficher : La sélection de l'option d'affichage vous permet de consulter les détails de votre réservation, notamment la date, l'heure, le lieu et le personnel affecté.
   - Modifier : vous pouvez modifier les détails de la réservation, notamment la date, l'heure, le lieu et le personnel affecté. Notez que les modifications doivent être effectuées 24 heures avant la date de réservation souhaitée et que les révisions ne sont pas immédiatement acceptées et appliquées. Le responsable de votre processus recevra une confirmation de la mise à jour de la demande.
   - Supprimer : L'option de suppression vous permet d'annuler votre réservation. La demande d'annulation doit être faite au moins 24 heures avant la date de réservation prévue. Le responsable du processus recevra une confirmation de l'annulation de la réservation lorsque la demande sera approuvée.

Effectuer un transfert de données au terminal de transfert de données

Le terminal de transfert de données est un lieu sécurisé en copropriété qui fournit un accès sécurisé au AWS réseau. Pour accéder au terminal de transfert de données, assurez-vous d'avoir reçu un e-mail de confirmation contenant la description de l'emplacement et les instructions d'accès. Reportez-vous aux rubriques ci-dessous pour plus d'informations sur l'accès et l'utilisation du terminal de transfert de données.

Rubriques

Ce qu'il faut apporter

Les spécialistes du transfert de données doivent apporter les éléments nécessaires pour effectuer un transfert de données, tels qu'un ordinateur portable, des clés USB, des disques SSD (SSDs) et AWS Snowball Edge. Assurez-vous que votre équipement est optimisé pour utiliser les câbles réseau à fibre optique du terminal de transfert de données. Pour plus d'informations sur l'équipement et les configurations optimaux, consultez la section Exigences techniques relatives à l'utilisation du terminal de transfert de données.

Vous êtes responsable de l'installation, de l'utilisation et du retrait de l'équipement et des articles que vous et les spécialistes du transfert de données qui vous accompagnent apportez au terminal de transfert de données. Tout ce qui est apporté dans la suite doit être retiré au moment du départ. AWS Data Transfer Terminal n'est pas responsable des objets oubliés ou perdus.

Adresse physique du terminal de transfert de données

L'adresse physique du terminal de transfert de données ne sera pas fournie. Au lieu de cela, le propriétaire du processus et les spécialistes du transfert de données spécifiés dans la réservation recevront un e-mail contenant le nom public consultable du terminal de transfert de données. AWS

Le terminal de transfert de données utilise le même système d'identification de localisation que AWS Direct Connect. Vous pouvez donc rechercher le nom public sur Internet pour localiser le terminal de transfert de données. Si vous n'avez pas reçu d'e-mail contenant ces informations, vérifiez auprès du responsable de votre compte AWS Data Transfer Terminal que vous faites partie de l'équipe de transfert et que vos informations de courrier électronique sont correctes.

Accès au bâtiment

Pour accéder au terminal de transfert de données, chaque spécialiste du transfert de données doit fournir une preuve d'identité ou une pièce d'identité émise par le gouvernement. Une fois admis dans le bâtiment, les agents de sécurité vous escorteront jusqu'à votre terminal de transfert de données.

Équipement attendu dans la suite Data Transfer Terminal.

Chaque terminal de transfert de données ne doit disposer que de deux (2) câbles à fibres optiques, d'une table ou d'un bureau et de chaises. S'il y a d'autres équipements ou objets dans la pièce, signalez-les immédiatement au Support.

Résolution des problèmes de connexion réseau

Si vous rencontrez des problèmes de connexion au réseau lorsque vous utilisez le terminal de transfert de AWS données, tels que l'impossibilité de vous connecter à Internet ou des vitesses de connexion lentes, tenez compte des conseils de dépannage suivants.

Rubriques

Problèmes de connexion de l'équipement

Si vous éprouvez des difficultés à établir une connexion physique lorsque vous utilisez la suite Data Transfer Terminal, tenez compte des points suivants :

- Chaque terminal de transfert de données sera équipé de deux (2) câbles à fibre LC monomodes. Si l'un de ces câbles ou les deux sont manquants, contactez immédiatement le AWS Support.
- Si un câble à fibre optique ne fonctionne pas, essayez d'abord de le faire rouler. Si vous ne parvenez toujours pas à vous connecter avec le premier câble, essayez d'utiliser l'autre câble.

Si vous ne parvenez toujours pas à utiliser les câbles pour vous connecter, contactez immédiatement le AWS Support.

Dépannage des problèmes de connectivité

Si vous parvenez à connecter votre équipement mais que vous ne parvenez pas à vous connecter au réseau, essayez les suggestions de dépannage suivantes.

- Vérifiez que la configuration de votre équipement répond aux exigences réseau spécifiées. Pour plus d'informations, voir Exigences techniques relatives à l'utilisation du terminal de transfert de données
- Passez à l'autre câble à fibre optique pour vous connecter.
- Redémarrez votre appareil tout en maintenant les câbles à fibres optiques connectés.

- Effectuez des diagnostics réseau de base sur l'appareil afin de garantir les points suivants :
  - DHCP est activé
  - Une adresse IP est attribuée à l'interface réseau connectée
  - Les serveurs DNS sont configurés
  - L'horloge du système est synchronisée avec le protocole NTP

Si vous ne parvenez toujours pas à vous connecter, contactez le AWS Support et fournissez-leur les sorties suivantes en fonction du système d'exploitation (OS) exécuté sur votre appareil.

Linux/Unix

- Obtenez l'adresse IP et les informations de routage dans un terminal ou une interface de ligne de commande (CLI). Vérifiez qu'une adresse IP est attribuée à l'interface réseau et qu'une route par défaut avec une adresse de passerelle par défaut est ajoutée dans la table de routage.

```
ip address show
ip route show
```

  - Sinon, s'il n'`iproute2`est pas installé sur le périphérique et que `ip` les commandes ne sont pas disponibles, utilisez les commandes suivantes :

```
ifconfig
netstat -rn
```

- Collectez les informations du serveur DNS. Cela devrait afficher deux adresses IP commençant par le `nameserver` mot clé.

```
cat /etc/resolv.conf
```

- Collectez les résultats des tests de connectivité de base. Remplacez le `default_gateway_address` par l'adresse IP de la passerelle par défaut attribuée.

```
ping -c 5 <default_gateway_address>
ping -c 5 s3.amazonaws.com
traceroute s3.amazonaws.com
```

- Collectez le résultat du test de connectivité HTTPS. La commande suivante doit afficher une `HTTP 200 OK` réponse d'Amazon S3.

```
curl -i https://s3.amazonaws.com/ping
```

Windows

- Obtenez l'adresse IP, le routage et les informations du serveur DNS dans l'invite de commande. Vérifiez qu'une adresse IP est attribuée à l'interface réseau, que deux serveurs DNS sont assignés et qu'une route par défaut avec une adresse de passerelle par défaut est ajoutée dans la table de routage.

```
ipconfig /all
route print
```

- Collectez les résultats des tests de connectivité de base dans l'invite de commande. Remplacez le `default_gateway_address` par l'adresse IP de la passerelle par défaut attribuée.

```
ping <default_gateway_address>
ping s3.amazonaws.com
tracert s3.amazonaws.com
```

- Collectez le résultat du test de connectivité HTTPS dans PowerShell. La commande suivante doit afficher une `HTTP 200 OK` réponse.

```
Invoke-WebRequest -Uri "https://s3.amazonaws.com/ping"
```

Débit réseau

Le débit du réseau, qui mesure le taux de transfert de données réel dans un réseau, peut être influencé par divers facteurs. Les facteurs suivants peuvent avoir une incidence sur la vitesse de transfert de vos données :

- Matériel : les composants matériels de l'appareil peuvent entraîner une réduction des vitesses de connexion lors du téléchargement de données. Il est possible que le processeur et les disques utilisés dans l'appareil atteignent leurs limites de performance. Envisagez d'utiliser le NVME SSDs dans une matrice RAID. Assurez-vous d'utiliser la bibliothèque AWS CRT pour améliorer les performances et réduire l'utilisation du processeur.

- Surcharge de chiffrement : les transmissions sécurisées, telles que le protocole HTTPS, augmentent le temps de traitement en raison de la surcharge de chiffrement.
- Latence : La latence fait référence au temps nécessaire à un paquet de données pour voyager de la source à la destination. Une latence élevée peut être observée lors du téléchargement vers un compartiment Amazon S3 situé dans une autre région géographique, ce qui peut entraîner des retards dans le transfert des données et une baisse du débit. La meilleure pratique consiste à effectuer des transferts de données au sein d'une même région, dans la mesure du possible.
- Perte de paquets : les paquets perdus nécessitent une retransmission, ce qui ralentit le transfert de données.

Sécurité de AWS Terminal de transfert de données

AWS Le terminal de transfert de données fournit un environnement sécurisé pour effectuer des transferts de données vers et depuis le AWS cloud. Comme toute autre connexion réseau physique par fibre optique, la connexion du terminal de transfert de données ne fournit pas de cryptage par défaut. Par conséquent, vous serez responsable de l'application des meilleures pratiques en matière de chiffrement des données afin de garantir la sécurité de votre transfert de données.

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent au terminal de transfert de AWS données, consultez la section AWS Services concernés par le programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'un terminal de transfert de données. Les rubriques suivantes expliquent comment sécuriser vos données lors de l'utilisation du service Terminal de transfert de données. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre terminal de transfert de données.

Rubriques

- Enregistrement et surveillance dans le terminal de transfert de données
- Sécurité de l'infrastructure dans AWS Terminal de transfert de données

Protection des données dans AWS Terminal de transfert de données

Le modèle de responsabilité AWS partagée s'applique à la protection des AWS données dans le terminal de transfert de données. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble du AWS cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable de la configuration de la sécurité et des tâches de gestion des AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité des données. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de blog sur le RGPD sur le blog AWS de sécurité.

Pour des raisons de protection des données, nous vous recommandons de protéger les informations d'identification des AWS comptes et de configurer des utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein AWS des services.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS.

Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec un terminal de transfert de données ou d'autres AWS services à l'aide de la console, de l'API, de la AWS CLI ou AWS des SDK. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement des données

AWS Le terminal de transfert de données fournit un accès à une connexion réseau haut débit qui vous permet de transférer des données en toute sécurité entre des systèmes de stockage autogérés et des services AWS de stockage. La manière dont vos données de stockage sont cryptées pendant le transfert dépend en partie des politiques activées sur vos appareils et des services vers lesquels vos données sont transférées. La gestion des données et leur cryptage en transit relèvent de la responsabilité de l'utilisateur du terminal de transfert de données.

Chiffrement au repos

AWS Le terminal de transfert de données chiffre toutes les données au repos.

Le terminal de transfert de données ne saisit que les données nécessaires aux réservations, y compris les prénom et nom de famille et les adresses e-mail des personnes spécifiées pour assister et planifier la réservation. Le but de cette collecte de données est de confirmer les détails de la réservation et de garantir l'accès à la chambre pour effectuer le transfert de données. Ces informations transactionnelles ne sont pas sauvegardées plus de 35 jours, mais les informations du AWS compte sont conservées pendant 10 ans.

Chiffrement en transit

AWS Le terminal de transfert de données ne chiffre pas les données en transit. Les données sont cryptées en transit lorsque vous interagissez avec les points de terminaison de l'API du terminal de transfert de données pour configurer les équipes de transfert, ajouter du personnel et planifier

les réservations dans la console. Dans le cadre du modèle de responsabilité AWS partagée, vous pouvez choisir la manière dont vous vous connectez aux AWS services via le terminal de transfert de données. Nous vous recommandons vivement de choisir de vous connecter à AWS des services utilisant un cryptage fort en transit, tels que TLS 1.2 et 1.3.

Par exemple, utilisez uniquement des connexions chiffrées via HTTPS (TLS) en utilisant la SecureTransport condition aws : dans vos politiques de compartiment Amazon S3, comme illustré dans la politique de compartiment ci-dessous.

Pour en savoir plus sur le chiffrement des données en transit avec d'autres AWS services, tels qu'Amazon S3, consultez la section Protection des données par le chiffrement côté serveur dans le guide de l'utilisateur Amazon S3.

Gestion des clés

AWS Le terminal de transfert de données ne prend pas directement en charge les clés gérées par le client. Utilisez le support clé géré par le client disponible pour les AWS services auxquels vous vous connectez lors de la réservation de votre terminal de transfert de données. Pour en savoir plus sur les clés gérées par le client et sur le chiffrement de vos données au repos, consultez la section sur les clés AWS KMS du guide du développeur du service de gestion des AWS clés.

Inter-network confidentialité du trafic

L'accès à la console du terminal de transfert de données s'effectue via des API de service publiées. Les ressources du terminal de transfert de données sont indépendantes du cloud privé virtuel (VPC).

Gestion des identités et des accès pour le terminal de transfert de données

AWS Identity and Access Management (IAM) est un AWS service qui permet à un administrateur de contrôler en toute sécurité l'accès aux ressources. AWS Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources du terminal de transfert de données. IAM est un AWS service que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé

- Authentification par des identités
- Gestion de l'accès à l'aide de politiques
- Comment fonctionne le terminal de transfert de données avec IAM

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Data Transfer Terminal.

Utilisateur du service : si vous utilisez le service Terminal de transfert de données pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités du terminal de transfert de données pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. Si vous comprenez bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité du terminal de transfert de données, consultez la section Résolution AWS des problèmes d'identité et d'accès au terminal de transfert de données.

Administrateur du service — Si vous êtes responsable des ressources du terminal de transfert de données dans votre entreprise, vous avez probablement un accès complet au terminal de transfert de données. Il vous incombe de déterminer les fonctionnalités et les ressources du terminal de transfert de données auxquelles les utilisateurs de vos services doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser l'IAM avec un terminal de transfert de données, consultez Comment le terminal de transfert de données fonctionne avec IAM.

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès au terminal de transfert de données. Pour consulter des exemples de politiques basées sur l'identité d'un terminal de transfert de données que vous pouvez utiliser dans IAM, consultez les exemples de Identity-based politiques du terminal de transfert de AWS données.

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur root du AWS compte, en tant qu'utilisateur IAM ou en assumant un rôle IAM.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS Les utilisateurs de l'IAM Identity Center (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter à la console AWS de gestion ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre AWS compte dans le Guide de AWS Sign-In l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Multi-factor l'authentification dans le guide de l'utilisateur d' AWS IAM Identity Center et l'AWS Multi-factor authentification dans IAM dans le guide de l'utilisateur d'IAM.

AWS Utilisateur racine d'un compte

Lorsque vous créez un AWS compte, vous commencez par utiliser une seule identité de connexion qui donne un accès complet à tous les AWS services et ressources du compte. Cette identité est appelée utilisateur root du AWS compte et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris les utilisateurs nécessitant un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder aux AWS services à l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, le AWS Directory Service, le répertoire Identity Center ou tout utilisateur qui accède AWS aux services à l'aide des informations d'identification fournies par le biais d'une source d'identité. Lorsque des identités fédérées accèdent à AWS des comptes, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion centralisée des accès, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser sur tous vos AWS comptes et applications. Pour plus d'informations sur IAM Identity Center, voir Qu'est-ce qu'IAM Identity Center ? dans le guide de l'utilisateur d' AWS IAM Identity Center.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité de votre AWS compte dotée d'autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des

informations d'identification temporaires. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de votre AWS compte dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans la console de AWS gestion, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API ou de AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les ensembles d'autorisations, consultez la section Ensembles d'autorisations dans le guide de l'utilisateur d' AWS IAM Identity Center.
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Cross-account accès : vous pouvez utiliser un rôle IAM pour autoriser une personne (un principal de confiance) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Cependant, avec certains AWS services, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Cross-service accès — Certains AWS services utilisent des fonctionnalités d'autres AWS services. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service

peut le faire en utilisant les autorisations d'appel du principal, une fonction du service ou un rôle lié au service.

- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. Le FAS utilise les autorisations du principal appelant un AWS service, associées au AWS service demandeur pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres AWS services ou ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.
- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un AWS service dans le Guide de l'utilisateur IAM.
- Service-linked rôle — Un rôle lié à un service est un type de rôle de service lié à un AWS service. Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre AWS compte et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API ou de AWS CLI. AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques

déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur les rôles à partir de la console de AWS gestion, de la AWS CLI ou de l' AWS API.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent également être classées en tant que politiques intégrées ou politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles dans votre AWS compte. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment

Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou AWS des services.

Resource-based les politiques sont des politiques intégrées qui se trouvent dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3, AWS WAF et Amazon VPC sont des exemples de services qui prennent en charge les ACL. Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations qui en résultent sont l'intersection des politiques basées sur l'identité d'une entité et de ses limites d'autorisations. Resource-based les politiques qui spécifient l'utilisateur ou le rôle `Principal` sur le terrain ne sont pas limitées par la limite des autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans

AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée plusieurs AWS comptes détenus par votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités des comptes membres, y compris pour chaque utilisateur root AWS du compte. Pour plus d'informations sur les Organizations et les SCP, consultez les politiques de contrôle des services dans le Guide de l'utilisateur AWS des Organizations.

- Politiques de contrôle des ressources (RCP) : les RCP sont des politiques JSON que vous pouvez utiliser pour définir le nombre maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris l'utilisateur root du AWS compte, qu'il appartienne ou non à votre organisation. Pour plus d'informations sur les Organizations et les RCP, y compris une liste des AWS services compatibles avec les RCP, voir Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur des AWS Organizations.
- Politiques de session : les politiques de session sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la session obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de session. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment fonctionne le terminal de transfert de données avec IAM

Avant d'utiliser IAM pour gérer l'accès au terminal de transfert de données, découvrez quelles fonctionnalités IAM peuvent être utilisées avec le terminal de transfert de données.

Fonctionnalité IAM	Support du terminal de transfert de données
Identity-based politiques	Oui
Resource-based politiques	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Oui
Autorisations de principals	Non
Rôles du service	Non
Service-linked rôles	Non

Pour obtenir une vue d'ensemble du fonctionnement du terminal de transfert de données et AWS des autres services avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le guide de l'utilisateur IAM.

Identity-based politiques relatives au terminal de transfert de données

Prend en charge les politiques basées sur l'identité : oui

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une stratégie basée sur l'identité car il s'applique à l'utilisateur ou au rôle auquel il est attaché. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Identity-based exemples de politiques pour le terminal de transfert de données

Pour consulter des exemples de politiques basées sur l'identité d'un terminal de transfert de données, consultez Identity-based les exemples de politiques du terminal de transfert de AWS données.

Resource-based politiques au sein du terminal de transfert de données

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou AWS des services.

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource se trouvent dans AWS des comptes différents, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour le terminal de transfert de données

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe certaines exceptions, telles que les actions d'autorisation uniquement qui ne correspondent à aucune opération API. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions du terminal de transfert de données, voir Actions définies par le terminal de transfert de AWS données dans la référence d'autorisation de service.

Les actions politiques dans le terminal de transfert de données utilisent le préfixe suivant avant l'action :

```
datatransferterminal
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "datatransferterminal:action1",
      "datatransferterminal:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité d'un terminal de transfert de données, consultez Identity-based les exemples de politiques du terminal de transfert de AWS données.

Ressources relatives aux politiques relatives au terminal de transfert de données

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne prennent pas en charge les autorisations au niveau des ressources, telles que les opérations de listage, utilisez un caractère générique (*) pour indiquer que la déclaration s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources du terminal de transfert de données et de leurs ARN, voir Ressources définies par le terminal de transfert de AWS données dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, voir Actions définies par le terminal de transfert de AWS données.

Pour consulter des exemples de politiques basées sur l'identité d'un terminal de transfert de données, consultez Identity-based les exemples de politiques du terminal de transfert de AWS données.

Clés de conditions de politique pour le terminal de transfert de données

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Condition`élément (ou `Condition` *`block`*`) lets you specify conditions in which a statement is in effect. The `Condition` l'élément) est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations de la déclaration ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition du terminal de transfert de données, voir Clés de condition du terminal de transfert de AWS données dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, voir Actions définies par le terminal de transfert de AWS données.

Pour consulter des exemples de politiques basées sur l'identité d'un terminal de transfert de données, consultez Identity-based les exemples de politiques du terminal de transfert de AWS données.

ACL dans le terminal de transfert de données

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec terminal de transfert de données

Prise en charge d'ABAC (balises dans les politiques) : non

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès en fonction des balises, vous devez fournir des informations de balise dans l'élément de condition d'une politique en utilisant le `aws:ResourceTag/[replaceable]` nom de clé. `, , or aws:TagKeys condition keys.` Si un service prend en charge les trois clés de condition pour chaque type de ressource, la valeur est Oui pour le service. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle. Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec le terminal de transfert de données

Prend en charge les informations d'identification temporaires : oui

Certains AWS services ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les AWS services qui fonctionnent avec des informations d'identification temporaires, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à la console de AWS gestion à l'aide d'une méthode autre que le nom d'utilisateur et le mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de la AWS CLI ou de AWS l'API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Cross-service autorisations principales pour le terminal de transfert de données

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une

action qui initie une autre action dans un autre service. Le FAS utilise les autorisations du principal appelant un AWS service, associées au AWS service demandeur pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres AWS services ou ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transfert des sessions d'accès.

Rôles de service pour le terminal de transfert de données

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un AWS service dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités du terminal de transfert de données. Modifiez les rôles de service uniquement lorsque Data Transfer Terminal fournit des instructions à cet effet.

Service-linked rôles pour le terminal de transfert de données

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle lié à un AWS service. Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre AWS compte et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne des Service-linked rôles. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Identity-based exemples de politiques pour AWS Terminal de transfert de données

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources du terminal de transfert de données. Ils ne peuvent pas non plus effectuer de tâches à l'aide de la console AWS de gestion, de l'interface de ligne de AWS commande (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par, y compris le format des ARN pour chacun des types de ressources, voir Actions dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console du terminal de transfert de données
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer, accéder ou supprimer les ressources du terminal de transfert de données de votre compte. Ces actions peuvent entraîner des frais pour votre AWS compte. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre AWS compte. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre

privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un AWS service spécifique, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root dans AWS votre compte, activez l'authentification MFA pour renforcer la sécurité. Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console du terminal de transfert de données

Pour accéder à la console du terminal de transfert de AWS données, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails relatifs aux ressources du terminal de transfert de données de votre AWS compte. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) dotées de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement la AWS CLI ou l' AWS API. Autorisez plutôt l'accès aux seules actions correspondant à l'opération d'API qu'ils essaient d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console du terminal de transfert de données, associez également le terminal de transfert de données *ConsoleAccess* ou la politique *ReadOnly* AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de la AWS CLI ou AWS de l'API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Résolution des problèmes AWS Identité et accès au terminal de transfert de données

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Data Transfer Terminal et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans le terminal de transfert de données
- Je souhaite autoriser des personnes extérieures à mon AWS compte pour accéder aux ressources de mon terminal de transfert de données

Je ne suis pas autorisé à effectuer une action dans le terminal de transfert de données

Si vous ne parvenez pas à consulter ou à planifier des réservations dans la console du terminal de transfert de AWS données, il se peut que vous ne disposiez pas des autorisations requises. Contactez l'administrateur de votre compte pour configurer une politique d'identité IAM qui vous accorde l'accès et les autorisations appropriées.

Je souhaite autoriser des personnes extérieures à mon AWS compte pour accéder aux ressources de mon terminal de transfert de données

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si le terminal de transfert de données prend en charge ces fonctionnalités, voir Fonctionnement du terminal de transfert de données avec IAM.
- Pour savoir comment fournir un accès à vos ressources sur les AWS comptes que vous possédez, consultez la section Fournir un accès à un utilisateur IAM sur un autre AWS compte que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des AWS comptes tiers, consultez la section Fournir un accès aux AWS comptes détenus par des tiers dans le guide de l'utilisateur IAM.

- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Références de l'API du terminal de transfert de données : actions et ressources

Lorsque vous créez des politiques AWS Identity and Access Management (IAM), cette page peut vous aider à comprendre la relation entre les opérations de l'API du terminal de transfert de AWS données, les actions correspondantes que vous pouvez autoriser à effectuer et les AWS ressources pour lesquelles vous pouvez accorder les autorisations.

En général, voici comment ajouter les autorisations du terminal de transfert de données à votre politique :

- Spécifiez une action dans l'`Action`élément. La valeur inclut un `datatransferterminal:` préfixe et le nom de l'opération d'API. Par exemple, `datatransferterminal:CreateTask`.
- Spécifiez une AWS ressource liée à l'action dans l'`Resource`élément.

Vous pouvez également utiliser des clés de AWS condition dans les politiques de votre terminal de transfert de données. Pour obtenir la liste complète des AWS clés, consultez la section Clés disponibles dans le guide de l'utilisateur IAM.

Opérations de l'API du terminal de transfert de données et actions correspondantes

CreateTransferTeam

- Action : `datatransferterminal:CreateTransferTeam`

  Ressource : `None`

GetTransferTeam

- Action : `datatransferterminal:GetTransferTeam`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

UpdateTransferTeam

- Action : `datatransferterminal:UpdateTransferTeam`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

DeleteTransferTeam

- Action : `datatransferterminal:DeleteTransferTeam`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

ListTransferTeams

- Action : `datatransferterminal:ListTransferTeams`

  Ressource : None

RegisterPerson

- Action : `datatransferterminal:RegisterPerson`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

GetPerson

- Action : `datatransferterminal:GetPerson`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

  Action dépendante : `datatransferterminal:GetTransferTeam`

  Ressource dépendante : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

DeregisterPerson

- Action : `datatransferterminal:DeregisterPerson`

Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

Action dépendante : `datatransferterminal:GetTransferTeam`

Ressource dépendante : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

ListPersons

- Action : `datatransferterminal:ListPersons`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

CreateReservation

- Action : `datatransferterminal:CreateReservation`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

  Action dépendante : `datatransferterminal:GetTransferTeam`

  Ressource dépendante : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

  Action dépendante : `datatransferterminal:GetPerson`

  Ressource dépendante : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

  Action dépendante : `datatransferterminal:GetFacility`

  Ressource dépendante : `arn:aws::$[replaceable]` Partition `:datatransferterminal:::facility/$[replaceable]` FacilityId ````

GetReservation

- Action : `datatransferterminal:GetReservation`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId `/reservation/$[replaceable]` ReservationId ````

  Action dépendante : `datatransferterminal:GetTransferTeam`

  Ressource dépendante : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

UpdateReservation

- Action : `datatransferterminal:UpdateReservation`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId `/reservation/$[replaceable]` ReservationId ````

  Action dépendante : `datatransferterminal:GetTransferTeam`

  Ressource dépendante : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

  Action dépendante : `datatransferterminal:GetPerson`

  Ressource dépendante : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

DeleteReservation

- Action : `datatransferterminal:DeleteReservation`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId `/person/$[replaceable]` PersonId ````

  Action dépendante : `datatransferterminal:GetTransferTeam`

Ressource dépendante : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

ListReservations

- Action : `datatransferterminal:ListReservations`

  Ressource : `:$[replaceable]` Compte de `:datatransferterminal:$[replaceable]` région de `arn:aws::$[replaceable]` partition `:transfer-team/$[replaceable]` TransferTeamId ````

ListFacilities

- Action : `datatransferterminal:ListFacilities`

  Ressource : None

GetFacility

- Action : `datatransferterminal:GetFacility`

  Ressource : `arn:aws::$[replaceable]` Partition `:datatransferterminal:::facility/$[replaceable]` FacilityId ````

GetFacilityAvailability

- Action : `datatransferterminal:GetFacilityAvailability`

  Ressource : `arn:aws::$[replaceable]` Partition `:datatransferterminal:::facility/$[replaceable]` FacilityId `/availability`

  Action dépendante : `datatransferterminal:GetFacility`

  Ressource dépendante : `arn:aws::$[replaceable]` Partition `:datatransferterminal:::facility/$[replaceable]` FacilityId `/availability`

Validation de conformité pour AWS Terminal de transfert de données

Pour savoir si un AWS service entre dans le champ d'application de programmes de conformité spécifiques, consultez les AWS services dans Étendue par programme de conformité et choisissez

le programme de conformité qui vous intéresse. Pour obtenir des informations générales, consultez Programmes de conformitéAWS.

Vous pouvez télécharger des rapports d'audit tiers à l'aide d' AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact.

Lorsque vous utilisez AWS des services, votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous les AWS services ne sont pas éligibles à la loi HIPAA.
- AWS Ressources relatives à la conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- https://d1-awsstatic-com-whitepapers-compliance-AWS- Customer-Compliance-Guides-pdf [Guides de conformité destinés aux AWS clients] — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation AWS des services et présentent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du AWS guide du développeur de configuration : le service AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub — Ce AWS service fournit une vue complète de l'état de votre sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos AWS ressources et vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Ce AWS service détecte les menaces potentielles qui pèsent sur vos AWS comptes, vos charges de travail, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte ou malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager : ce AWS service vous aide à auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS Terminal de transfert de données

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

AWS Le terminal de transfert de données est disponible partout dans le monde. Vous pouvez vous connecter à n'importe quelle AWS région accessible depuis Internet.

Enregistrement et surveillance dans le terminal de transfert de données

AWS Le terminal de transfert de données est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans le terminal de transfert de données. CloudTrail capture tous les appels d'API pour le terminal de transfert de données sous forme d'événements. Les appels capturés incluent des appels provenant de la console du terminal de transfert de données et des appels de code vers les opérations de l'API du terminal de transfert de données. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour le terminal de transfert de données. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite au terminal de transfert de données, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur le terminal de transfert de données dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans le terminal de transfert de données, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris les événements relatifs à Data Transfer Terminal, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions du terminal de transfert de données sont enregistrées CloudTrail et documentées dans la section Références de l'API du terminal de transfert de données : actions et ressources de ce guide.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification root ou AWS celles de l'utilisateur Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Comprendre les entrées du fichier journal du terminal de transfert de données

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Sécurité de l'infrastructure dans AWS Terminal de transfert de données

En tant que service géré, AWS Data Transfer Terminal est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc {https---d0-awsstatic-com-whitepapers-security-AWS-Security-Whitepaper-pdf} [Amazon Web Services : présentation des processus de sécurité].

Vous utilisez des appels d'API AWS publiés pour accéder au terminal de transfert de données via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous vous recommandons le certificat TLS 1.2 ou une version ultérieure. Les clients doivent également prendre en charge les suites de chiffrement à parfaite confidentialité (PFS) telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser le AWS Security Token Service (AWS STS) pour générer des informations de sécurité temporaires afin de signer les demandes.

Historique du document pour le guide de l'utilisateur du terminal de transfert de données

Le tableau suivant décrit l'historique des documents de ce guide.

Modification	Description	Date
Mettre à jour la disposition	Mises à jour de la mise en page du document et modifications mineures du verbiage et du contenu.	1er janvier 2025
Publication initiale	Date de lancement de la documentation d'origine.	1er décembre 2024

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.