aws

Guide de l’utilisateur

AWS Elemental MediaConnect

AWS Elemental MediaConnect: Guide de l’utilisateur

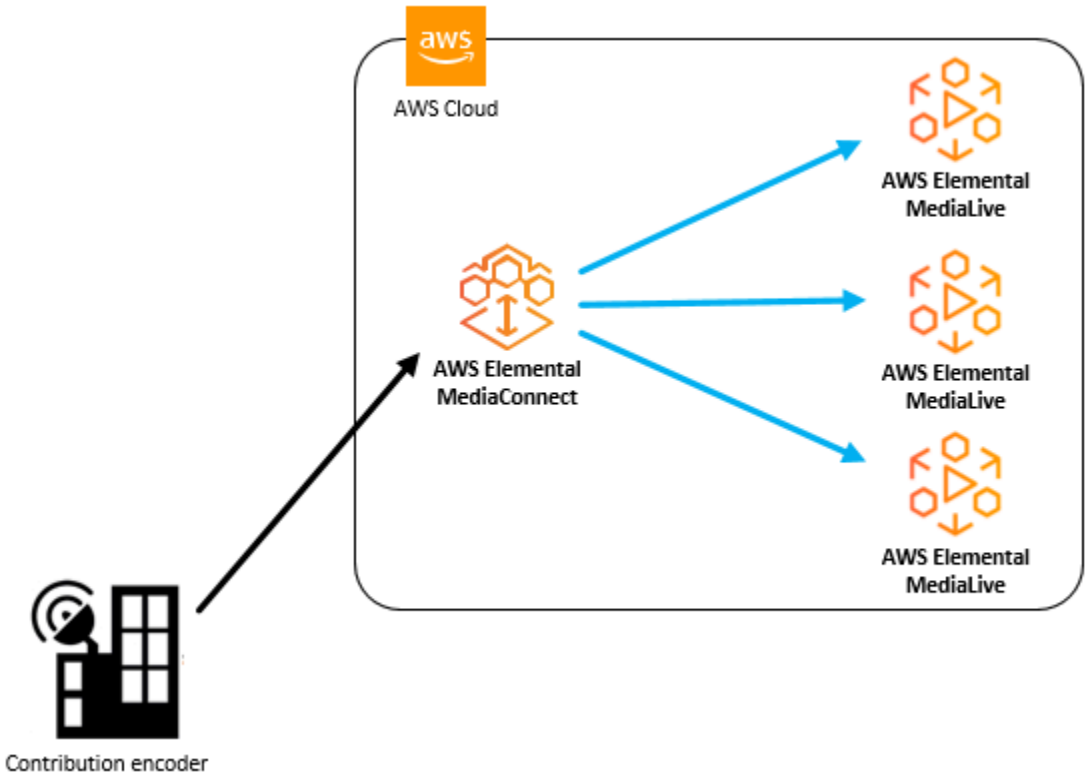
Table of Contents

Qu'est-ce qu'AWS Elemental ? MediaConnect

AWS Elemental MediaConnect est un service qui permet aux diffuseurs et aux autres fournisseurs de vidéos premium d'ingérer de manière fiable des vidéos en direct dans le AWS cloud et de les distribuer vers de multiples destinations à l'intérieur ou à l'extérieur du cloud. AWS MediaConnect fournit la fiabilité, la sécurité et la visibilité auxquelles vous êtes habitué avec les méthodes de distribution existantes, associées à la flexibilité et à la rentabilité qu'offre la transmission par Internet.

Pour l'ingestion, vous envoyez du contenu à AWS MediaConnect Elemental à partir d'un encodeur de contribution sur site, qui code votre vidéo dans un seul fichier mezzanine de haute qualité pour la contribution dans le cloud. Une fois que la vidéo est dans le AWS cloud, MediaConnect elle est envoyée vers les sorties que vous spécifiez, telles qu'un encodeur cloud, un autre MediaConnect flux ou une destination sur site.

L'illustration suivante montre le flux de travail de base selon lequel AWS Elemental MediaConnect ingère des vidéos en direct dans le cloud et les distribue en toute sécurité vers plusieurs destinations.



Dans AWS Elemental MediaConnect, vous créez un flux pour établir un transport entre une source et une ou plusieurs sorties. Vous pouvez également partager du contenu avec d'autres AWS comptes

en créant des droits. Cela permet au compte destinataire de créer un flux en utilisant votre contenu comme source.

Avec AWS Elemental MediaConnect, vous pouvez effectuer les opérations suivantes :

- Ingérez des vidéos en direct dans le AWS cloud.
- Diffusez des vidéos en direct vers plusieurs destinations à l'intérieur ou à l'extérieur du AWS Cloud.
- Abonnez-vous à un flux vidéo en direct fourni par un autre AWS compte. (Cela nécessite l'autorisation de l'auteur du contenu par le biais d'un droit.)
- Envoyez du contenu d'une AWS région à une autre.

Rubriques

MediaConnect concepts et terminologie

ARN

Un nom de ressource Amazon, qui est un identifiant unique pour toute AWS ressource.

Zone de disponibilité

Emplacement spécifique où les ressources de AWS cloud computing sont hébergées. Les zones de disponibilité d'une AWS région sont connectées les unes aux autres avec une faible latence, un débit élevé et un réseau hautement redondant. De plus, ils sont physiquement séparés et isolés les uns des autres. Vous pouvez choisir de créer des MediaConnect flux dans différentes zones de disponibilité à des fins de redondance.

Région AWS

Zone géographique dans laquelle se trouvent une ou plusieurs zones de disponibilité. Chaque AWS région est indépendante des autres régions. Vous pouvez créer des MediaConnect flux

dans différentes régions pour distribuer du contenu à des destinataires situés dans différentes régions du monde. Pour plus d'informations sur AWS les régions et leurs zones de disponibilité, consultez l'infrastructure mondiale AWS.

Flux CDI

Un MediaConnect flux qui transporte du contenu de haute qualité légèrement compressé à l'aide du format JPEG XS. Le contenu est démultiplexé en flux multimédia distincts pour les données audio, vidéo ou auxiliaires. Chaque flux CDI peut utiliser plusieurs flux multimédia pour la source et plusieurs flux multimédias pour chaque sortie. MediaConnect utilise la technologie réseau AWS Cloud Digital Interface (AWS CDI) pour ingérer du contenu conforme à la norme de transport SMPTE 2110, partie 22.

Encodeur de contribution

Encodeur qui reçoit un flux vidéo en direct et code le flux en un seul flux mezzanine de haute qualité pour le transport ou le traitement ultérieur en un flux à débit adaptatif (ABR).

Distribution

Résultat de la création de résultats pointant vers MediaConnect des flux dans d'autres AWS régions, dans le but de diffuser du contenu dans différentes zones géographiques.

Droits

Autorisation accordée pour autoriser un AWS compte à accéder au contenu d'un MediaConnect flux spécifique. L'auteur du contenu accorde un droit à un AWS compte spécifique (l'abonné). Une fois qu'un droit est accordé, l'abonné peut créer un flux en utilisant le flux de l'expéditeur comme source. Vous ne pouvez octroyer des droits qu'aux flux de transport.

Flux

Connexion entre une ou plusieurs sources vidéo et une ou plusieurs sorties. Pour chaque flux, vous spécifiez le protocole de transport à utiliser, les informations de chiffrement et les détails relatifs à la source. MediaConnect renvoie un point de terminaison d'ingestion où vous pouvez envoyer votre vidéo en direct sous forme de flux unicast unique. Le service réplica et distribue la vidéo vers chaque sortie que vous spécifiez, quelle soit à l'intérieur ou à l'extérieur du Cloud AWS. Il existe deux types de flux : le flux de transport et le JPEG XS.

Flux multimédia

Piste ou flux multimédia unique contenant des données vidéo, audio ou auxiliaires. Après avoir ajouté un flux multimédia à un flux, vous pouvez l'associer aux sources et aux sorties de ce flux, à

condition qu'elles utilisent le protocole CDI ou le protocole ST 2110 JPEG XS. Chaque source ou sortie peut consister en un ou plusieurs flux multimédia.

Ruisseau en mezzanine

Un flux vidéo légèrement compressé qui occupe moins d'espace qu'un flux non compressé en pleine résolution. La qualité d'un flux mezzanine est suffisamment élevée pour être utilisée comme source de création d'encodages finaux destinés aux appareils grand public.

Offre

Un discount MediaConnect offert en échange d'un engagement à utiliser une certaine quantité de bande passante sortante chaque mois. Lorsque vous achetez une offre, elle devient une réservation.

Compte d'initiateur

Un AWS compte qui a été utilisé pour créer un flux avec au moins un droit.

Sortie

Destination à laquelle vous souhaitez MediaConnect envoyer la vidéo ingérée. Une sortie peut avoir le même protocole ou un protocole différent de la source.

Politique

Une politique IAM, qui est utilisée pour gérer l'accès àAWS.

Protocole

Ensemble de règles utilisées pour la transmission de fichiers. MediaConnect fournit des options de protocole (telles que Zixi, RTP et RTP-FEC) qui implémentent une couche de qualité de service (QoS) afin de permettre au service de fonctionner avec des vidéos en direct de qualité mezzanine.

Récepteur

Le destinataire d'un flux provenant de MediaConnect. Un récepteur est une entité, à l'intérieur ou à l'extérieur du AWS Cloud, capable de recevoir des flux RTP ou Zixi. Il peut s'agir d'un affilié, d'un encodeur cloud ou d'un autre MediaConnect flux.

Réservation

Un engagement à utiliser une quantité spécifique de bande passante sortante chaque mois pendant une durée spécifiée. En retour, vous payez un tarif horaire réduit pour cette bande passante. Lorsque vous achetez une offre, elle devient une réservation.

Réplication

Résultat de la création d'un flux avec plusieurs sorties. La source est répliquée pour produire plusieurs sorties. La réplication est utile lorsque vous souhaitez distribuer vos flux vidéo sur plusieurs flux de travail au sein de votre propre compte ou partager votre contenu avec d'autres AWS comptes.

Ressource

Une entité avec AWS laquelle vous pouvez travailler. Chaque AWS ressource se voit attribuer un Amazon Resource Name (ARN) qui fait office d'identifiant unique. Voici MediaConnect les ressources et leurs formats ARN :

- Indemnité : `aws:mediaconnect:`*`region`*`:`*`account-id`*`:entitlement:`*`resourceID`*`:`*`resourceName`*
- Débit : `aws:mediaconnect:`*`region`*`:`*`account-id`*`:flow:`*`resourceID`*`:`*`resourceName`*
- Sortie : `aws:mediaconnect:`*`region`*`:`*`account-id`*`:output:`*`resourceID`*`:`*`resourceName`*
- Source : `aws:mediaconnect:`*`region`*`:`*`account-id`*`:source:`*`resourceID`*`:`*`resourceName`*

Partage

Autoriser un autre AWS compte à accéder au contenu de votre flux. Pour partager votre contenu, vous (l'auteur) accordez un droit à un autre AWS compte (l'abonné).

Source

Contenu vidéo externe incluant des informations de configuration (cryptage et type de source) et une adresse réseau. Chaque flux a au moins une source. Une source standard provient d'une source autre qu'un autre MediaConnect flux, tel qu'un encodeur local. Une source autorisée provient d'un MediaConnect flux appartenant à un autre AWS compte et qui a accordé un droit à votre compte.

Compte d'abonné

Un AWS compte qui a obtenu l'accès au contenu d'un MediaConnect flux AWS Elemental appartenant à un autre AWS compte (le compte d'origine). Cette autorisation est accordée lorsque l'expéditeur définit un droit pour l'abonné. Le droit permet à l'abonné de créer un flux qui utilise le contenu de l'expéditeur comme source.

Débit du flux de transport

MediaConnect Flux qui transporte du contenu compressé. Les données audio, vidéo et auxiliaires doivent être combinées, ou multiplexées, en un seul flux. La qualité est suffisamment élevée pour être utilisée comme source pour créer des encodages finaux destinés aux appareils grand public. Vous pouvez ajouter des sorties pour indiquer où vous souhaitez que le contenu soit envoyé et comment vous souhaitez qu'il soit transporté. Vous pouvez également accorder des droits pour permettre à un autre AWS compte d'accéder au contenu.

Interface VPC

Connexion entre un flux et un cloud privé virtuel (VPC) créée à l'aide du service Amazon Virtual Private Cloud (Amazon VPC).

Établissement d'une liste blanche

Autoriser un bloc d'adresses IP de routage interdomaine sans classe (CIDR) à servir de source à votre flux. MediaConnect

Services connexes

- AWS CloudTrailest un service qui vous permet de surveiller les appels passés à l' CloudTrail API de votre compte, y compris les appels passés par la console de AWS gestion et d'autres services. AWS CLI Pour plus d'informations, consultez le AWS CloudTrailGuide de l'utilisateur .
- Amazon CloudWatch est un service de surveillance des ressources du AWS cloud et des applications que vous utilisezAWS. Utilisez CloudWatch les événements pour suivre les modifications de l'état des flux dans AWS Elemental MediaConnect. Pour plus d'informations, consultez la CloudWatch documentation Amazon.
- AWS Identity and Access Management (IAM) est un service Web qui vous permet de contrôler l'accès aux ressources AWS de vos utilisateurs. Utilisez IAM pour contrôler les personnes autorisées à utiliser vos ressources AWS (authentification) et les ressources que les utilisateurs peuvent utiliser et de quelle manière (autorisation). Pour plus d'informations, veuillez consulter Configuration.
- AWS Elemental MediaLiveest un service vidéo qui permet de créer facilement et de manière fiable des sorties en direct à des fins de diffusion et de diffusion en continu. Pour plus d'informations, consultez le AWS Elemental MediaLiveGuide de l'utilisateur .

Accès MediaConnect

Vous pouvez accéder à AWS Elemental MediaConnect en utilisant l'une des méthodes suivantes :

- AWSConsole de gestion : les procédures décrites dans ce guide expliquent comment utiliser la console AWS de gestion pour effectuer des tâches pour MediaConnect. Pour y accéder à MediaConnect l'aide de la console :

  ```
  https://<region>.console.aws.amazon.com/mediaconnect/home
  ```

- AWS Command Line Interface— Pour plus d'informations, consultez le guide de AWS Command Line Interface l'utilisateur. Pour accéder à l' MediaConnect aide du point de terminaison de la CLI :

  ```
  aws mediaconnect
  ```

- MediaConnect API AWS Elemental — Pour plus d'informations sur les actions d'API et sur la manière de faire des demandes d'API, consultez la référence des AWS Elemental MediaConnectAPI. Pour accéder à l' MediaConnect aide du point de terminaison de l'API REST :

  ```
  https://mediaconnect.<region>.amazonaws.com
  ```

- AWSSDK — Si vous utilisez un langage de programmation qui AWS fournit un SDK pour, vous pouvez utiliser un SDK pour accéder à AWS Elemental. MediaConnect Les kits SDK simplifient l'authentification, s'intègrent facilement à votre environnement de développement et permettent d'accéder facilement aux commandes MediaConnect . Pour plus d'informations, veuillez consulter Outils pour Amazon Web Services.
- AWSOutils pour Windows PowerShell — Pour plus d'informations, consultez le guide de AWS Tools for Windows PowerShell l'utilisateur.

Tarification pour MediaConnect

Comme avec les autres produits AWS, il n'y a aucun contrat ni engagement minimum pour utiliser MediaConnect.

Pour les flux de transport, des frais horaires vous sont facturés lorsque le flux est en cours d'exécution, et des frais par Go pour les sorties diffusées sur Internet. Des frais par Go vous sont également facturés pour les données d'entrée ou de sortie dans la même région. En général, des débits plus élevés entraînent des frais plus élevés par heure.

Pour les flux CDI, des frais horaires vous sont facturés lorsque le flux est en cours d'exécution, et des frais horaires pour chaque sortie livrée vers n'importe quelle destination. Les débits courants et les débits par sortie varient en fonction de la taille de la vidéo. Les sorties SD sont moins chères que les sorties HD, qui sont moins chères que les sorties UHD.

Pour plus d'informations sur les deux types de flux, consultez AWS Elemental MediaConnect Pricing.

Régions et points de terminaison pour MediaConnect

Pour réduire la latence des données dans vos applications, AWS Elemental MediaConnect propose un point de terminaison régional pour effectuer vos demandes :

```
https://mediaconnect.<region>.amazonaws.com
```

Pour consulter la liste complète des AWS régions disponibles, consultez la section MediaConnect Points de terminaison et quotas AWS Elemental dans le AWS manuel de référence général. MediaConnect

Cas d'utilisation d'AWS Elemental MediaConnect

Cette section fournit des cas d'utilisation métier simplifiés pour vous aider à comprendre les différentes manières d'implémenter AWS Elemental MediaConnect pour diffuser du contenu AWS dans le cloud et au-delà. Les cas d'utilisation présentés dans cette section sont décrits en termes généraux, sans les mécanismes d'utilisation de l' MediaConnect API pour obtenir les résultats souhaités.

Votre MediaConnect implémentation dépend de votre cas d'utilisation :

- À des fins de contribution, MediaConnect utilisez-le pour ingérer le contenu d'un encodeur sur site dans le Cloud. AWS Selon le type de contenu que vous ingérez, vous pouvez créer un flux de transport ou un flux CDI.
- Pour la distribution, utilisez MediaConnect pour diffuser du contenu dans différentes zones géographiques.
- Pour les droits, utilisez-le MediaConnect pour partager votre contenu avec d'autres AWS comptes.
- Pour la réplication et la surveillance, utilisez-le MediaConnect pour distribuer la vidéo vers plusieurs destinations et permettre la surveillance de plusieurs signaux vidéo en temps réel.

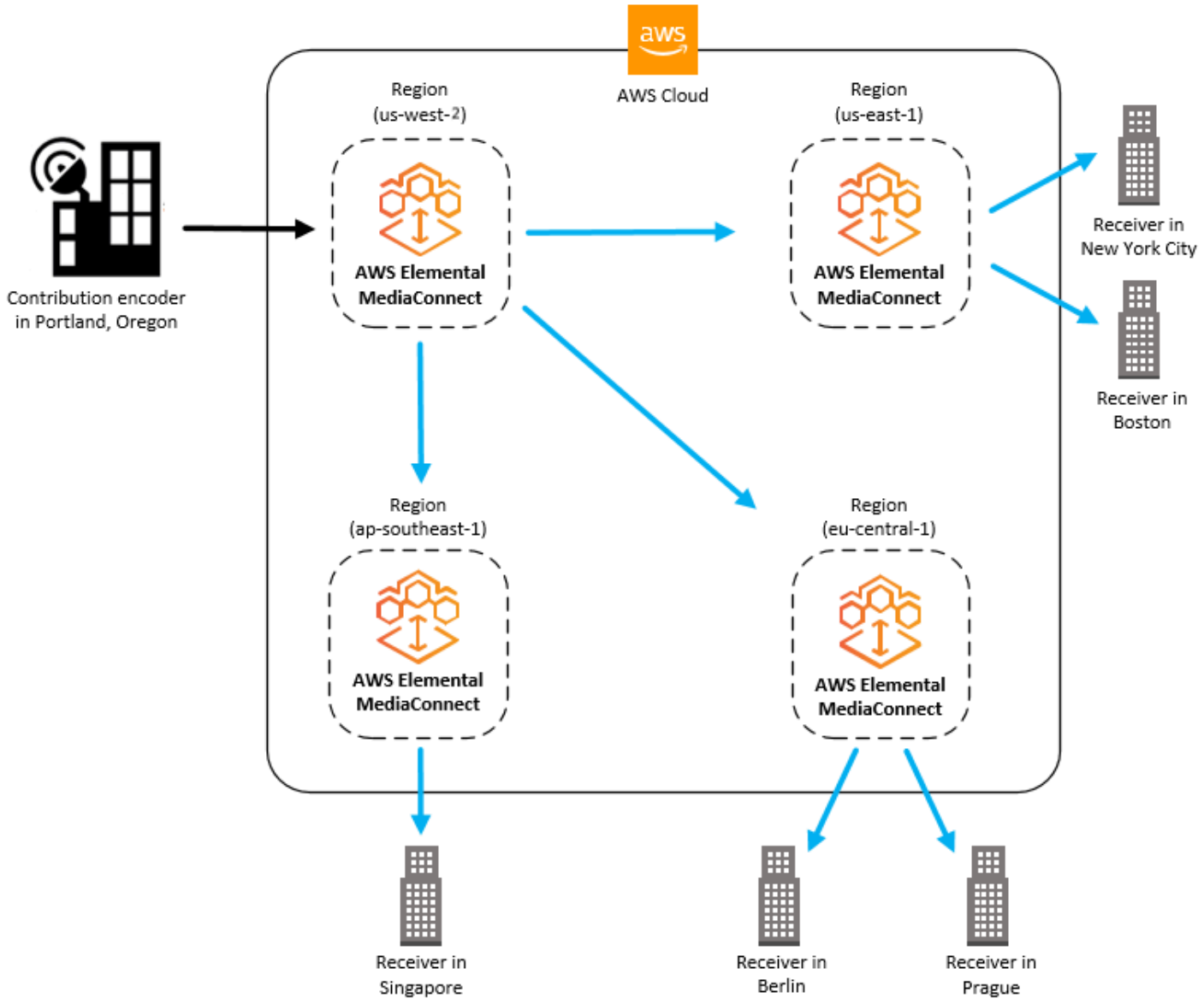
Rubriques

Cas d'utilisation : distribution

Vous pouvez utiliser AWS Elemental MediaConnect pour distribuer votre contenu dans différentes zones géographiques. Supposons, par exemple, que votre encodeur de contribution local soit situé à Portland, dans l'Oregon, et que vos destinataires soient situés dans le monde entier. (Un récepteur est une entité qui recevra du contenu de votre flux. Il peut s'agir d'un encodeur dans le cloud, d'un encodeur sur site chez votre destinataire ou d'un autre MediaConnect flux.) Vous configurez votre MediaConnect flux initial dans la région us-west-1, qui est la AWS région physique la plus proche

de votre encodeur. Une fois que votre contenu est dans le AWS cloud, vous l'envoyez à d'autres MediaConnect flux situés dans des régions plus proches de vos destinataires.

L'illustration suivante montre un encodeur de contribution sur site situé à Portland, dans l'Oregon, qui télécharge du contenu MediaConnect dans le cloud. AWS Le flux possède trois sorties qui envoient du contenu à d'autres flux dans différentes AWS régions. Ces flux secondaires sont plus proches des récepteurs, situés dans différentes villes du monde.

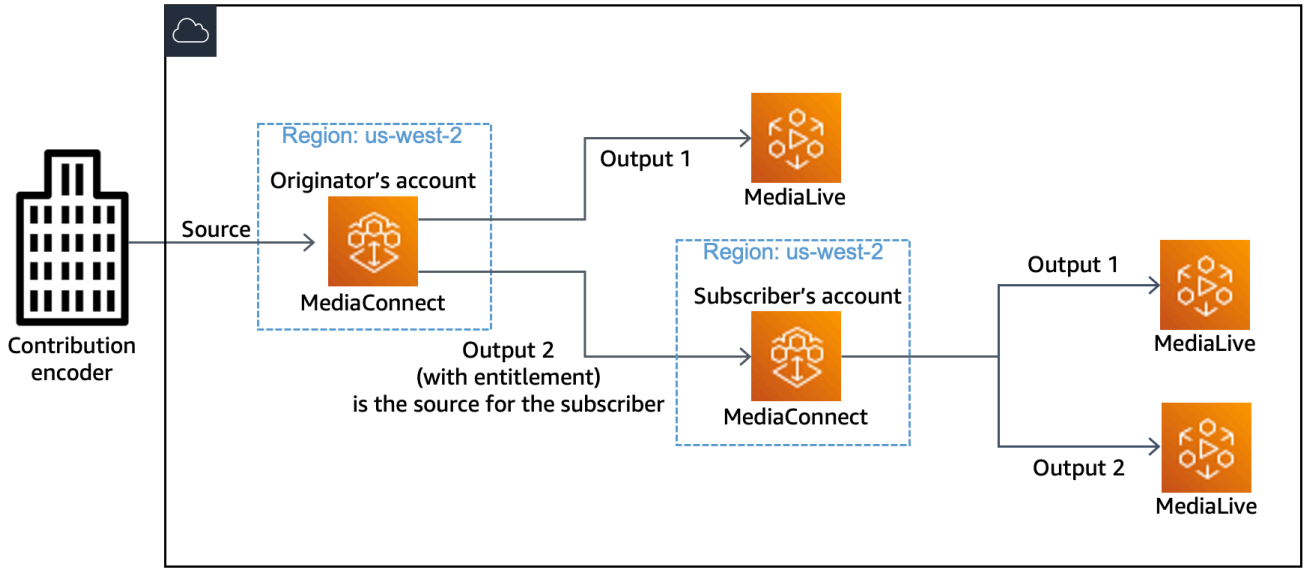


Cas d'utilisation : droits

Les droits permettent à un titulaire de AWS compte de partager le contenu d'un flux de transport avec d'autres titulaires de AWS compte. Par exemple, une entreprise sportive souhaite partager un flux (jeu de baseball) avec une chaîne de télévision locale. Un diffuseur sportif (l'émetteur) crée un droit sur le flux Baseball-Game pour permettre l'accès à la chaîne de télévision locale (l'abonné). La chaîne de télévision locale crée un flux AWS Elemental en utilisant une sortie du MediaConnect flux Baseball-Game comme source.

L'abonné doit configurer son flux MediaConnect dans la même région que le flux d'origine.

L'illustration suivante montre comment partager du contenu dans un flux de transport avec un autre AWS abonné. La sortie du flux de l'expéditeur peut être utilisée comme source du flux de l'abonné.

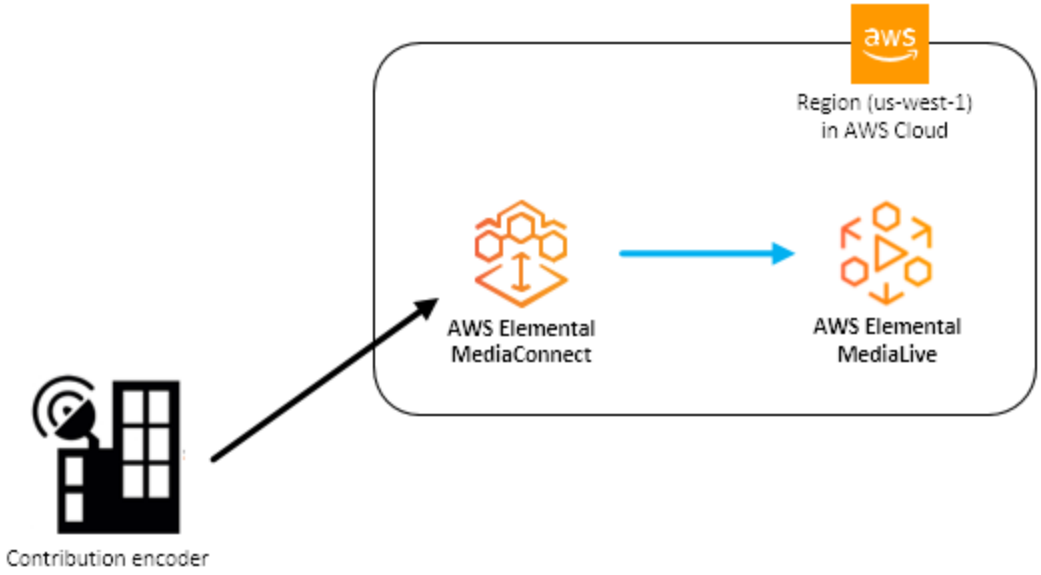


Cas d'utilisation : contribution aux flux de transport

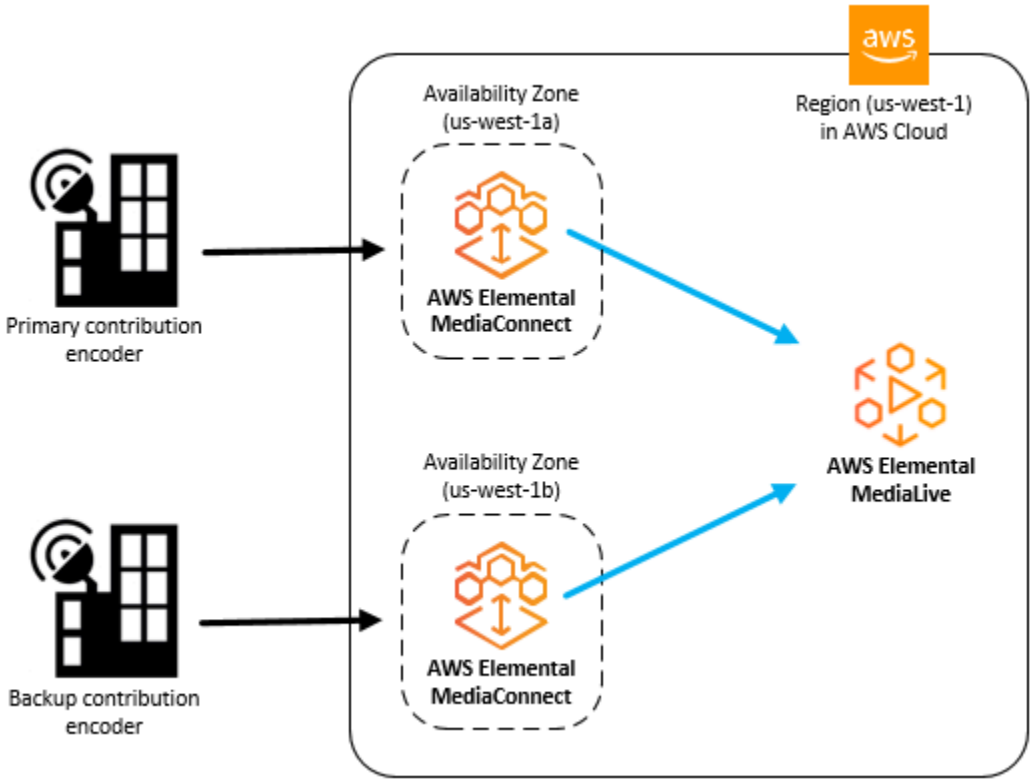
Vous pouvez utiliser AWS Elemental MediaConnect pour intégrer votre contenu depuis un encodeur de contribution sur site dans le cloud. AWS La source de votre MediaConnect flux provient de votre encodeur de contribution sur site, et la sortie pointe vers votre encodeur dans le cloud, par exemple. AWS Elemental MediaLive Si votre contenu source n'est pas compressé, vous pouvez utiliser un flux de travail CDI.

Pour la redondance, vous pouvez configurer votre flux de manière à ce qu'il comporte deux sorties pointant vers votre encodeur cloud. Une autre configuration de redondance inclut deux encodeurs de contribution locaux (un principal et un de sauvegarde) qui envoient chacun du contenu à un flux différent. MediaConnect La sortie de chaque flux pointe ensuite vers le même encodeur cloud.

L'illustration suivante montre un encodeur de contribution sur site qui télécharge du contenu MediaConnect dans le cloud. AWS La sortie du flux pointe vers un MediaLive canal.



L'illustration suivante montre deux encodeurs de contribution sur site, l'un principal et l'autre de sauvegarde, qui téléchargent le même contenu MediaConnect dans le AWS cloud. Il existe deux flux, chacun avec une sortie. Les deux sorties pointent vers un seul MediaLive canal.



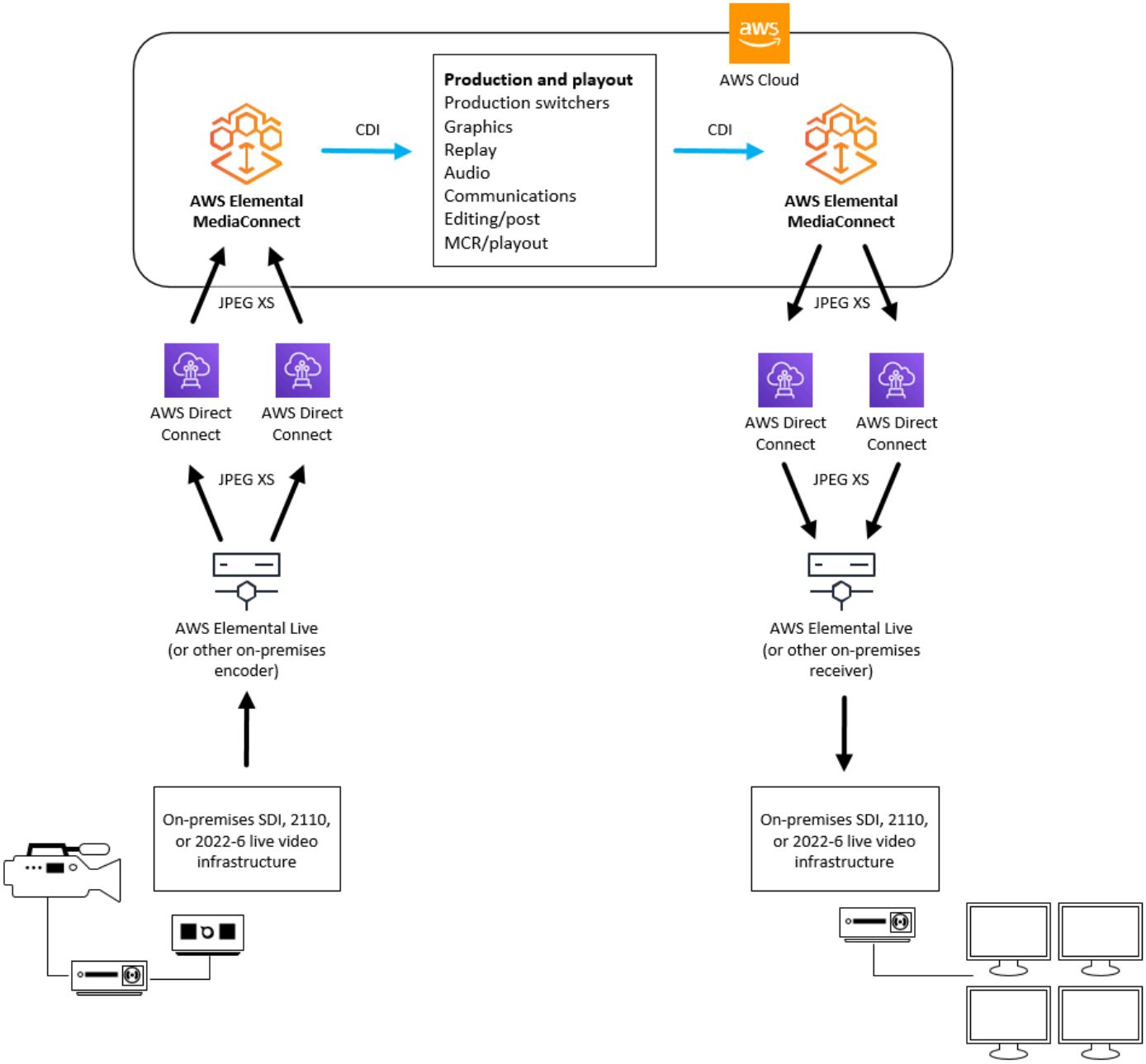
Cas d'utilisation : contribution aux flux CDI

Avec AWS Elemental MediaConnect and AWS Direct Connect, vous pouvez relier votre réseau vidéo en direct sur site (SDI, ¶ 6 ou 2110) à votre réseau vidéo en direct (CDI) VPC. MediaConnectutilise le codec JPEG XS pour réduire considérablement la bande passante de votre AWS Direct Connect réseau. MediaConnect prend en charge la norme SMPTE 2110 (parties 22, 30 et 40) pour le transfert vidéo, audio et de métadonnées. MediaConnect convertit le contenu en flux CDI prêts à être utilisés par d'autres services dans le cloud, tels que AWS Elemental MediaLive. Lorsque le contenu VPC de votre cloud est prêt à être redistribué sur les réseaux locaux, vous pouvez l'utiliser MediaConnect pour reconvertir les flux CDI selon la norme SMPTE 2110 (parties 22, 30 et 40) pour le transport.

À des fins de redondance, lorsque vous transportez du contenu entre votre configuration sur site et le AWS cloud, configurez deux connexions. AWS Direct Connect Assurez-vous de configurer l' AWS Elemental Live appliance avec des paramètres correspondant aux MediaConnect flux. Pour plus d'informations sur la configuration de l'appliance, consultez la section Entrées et sorties SMPTE 2110 dans le guide de l'AWS Elemental Live utilisateur.

> **Note**
>
> Les sorties CDI ne prenant pas en charge les transferts entre zones de disponibilité, utilisez les sorties ST 2110 JPEG XS si vous souhaitez envoyer du contenu vers une autre zone de disponibilité.

L'illustration suivante montre un flux de travail qui crée un pont entre votre infrastructure vidéo en direct sur site et le AWS cloud.



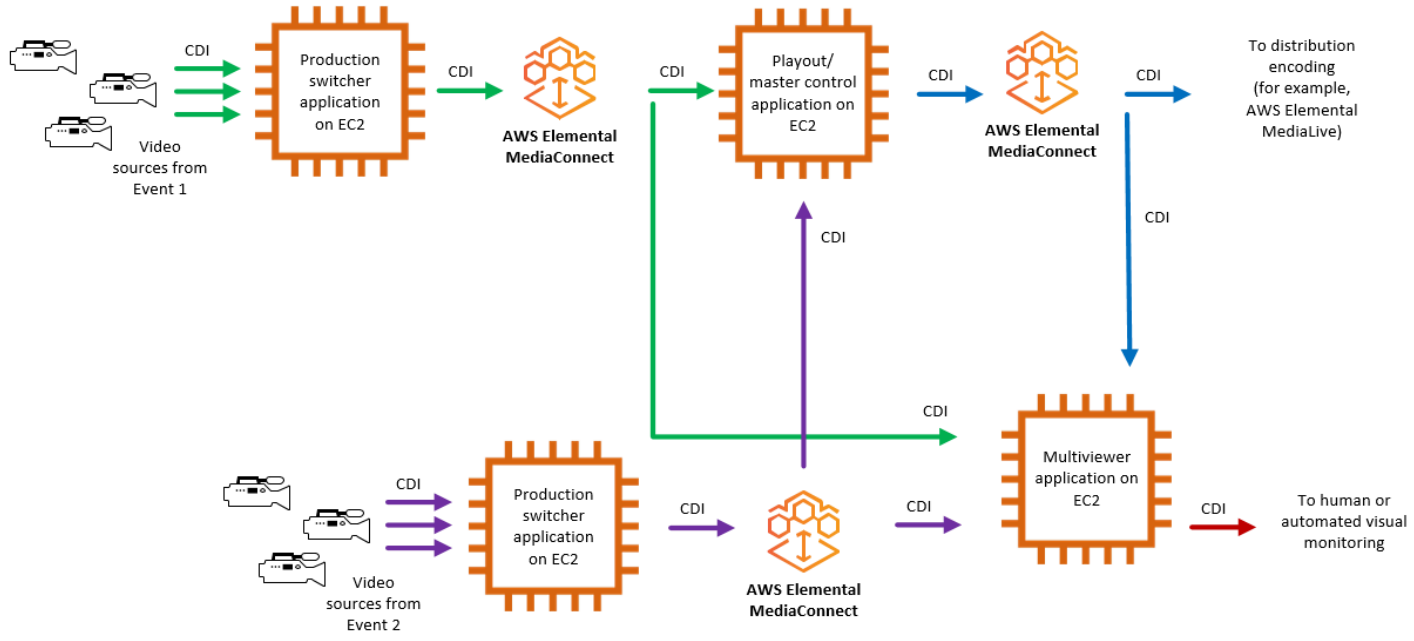
Cas d'utilisation : réplication et surveillance des flux CDI

Vous pouvez utiliser AWS Elemental MediaConnect pour répliquer et distribuer des vidéos vers plusieurs destinations et surveiller les multiples signaux vidéo en temps réel.

Par exemple, vous pouvez alterner entre plusieurs événements en direct qui se déroulent sur différents sites pour créer une diffusion en sortie unique. À l'aide d'un flux de travail MediaConnect CDI, vous pouvez prendre les sorties de plusieurs commutateurs de production et les envoyer à

un commutateur de commande principal et à une application multiviewer. Vous pouvez utiliser un autre flux CDI pour envoyer la sortie finale à l'encodeur de distribution (par exemple, AWS Elemental MediaLive), ainsi qu'à l'application multiviewer. L'équipe de production reçoit la sortie du multiviewer, ce qui lui permet de surveiller les multiples signaux vidéo en temps réel.

L'illustration suivante montre comment utiliser les flux de travail MediaConnect CDI pour répliquer et distribuer des vidéos vers plusieurs destinations. Vous pouvez créer une sortie unique à partir de contenu vidéo provenant de plusieurs événements, et également envoyer la sortie de plusieurs signaux pour une surveillance en temps réel.



Configuration d'AWS Elemental MediaConnect

Avant de commencer à utiliser AWS Elemental MediaConnect, vous devez vous inscrire AWS (si vous n'avez pas encore de AWS compte) et créer des utilisateurs et des rôles IAM pour autoriser l'accès à. MediaConnect Cela inclut la création d'un rôle IAM pour vous-même. Si vous souhaitez utiliser le chiffrement pour protéger votre contenu, vous devez également y stocker vos clés de chiffrement AWS Secrets Manager, puis MediaConnect autoriser leur obtention à partir de votre compte Secrets Manager.

Cette section vous guide à travers les étapes requises pour configurer les utilisateurs et les rôles afin d'accéder à AWS Elemental MediaConnect. Pour obtenir des informations générales et supplémentaires sur la gestion des identités et des accès pour MediaConnect, voirthe section called "Gestion des identités et des accès".

Rubriques

Inscrivez-vous pour AWS

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

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

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

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des

ressources de ce compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, consultez la section Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Création de rôles non administrateurs

Les utilisateurs du groupe Administrateurs d'un compte ont accès à tous les AWS services et ressources de ce compte. L'octroi d'un accès direct à toutes les AWS ressources va à l'encontre de la meilleure pratique qui consiste à appliquer les autorisations les moins privilégiées à un utilisateur. Cette section décrit comment créer des rôles avec des autorisations limitées à AWS Elemental MediaConnect. Cette section décrit également comment vos utilisateurs peuvent assumer ce rôle pour octroyer des informations d'identification sécurisées et temporaires.

Rubriques

Étape 1 : créer une politique pour les non-administrateurs

Créez deux politiques pour AWS Elemental MediaConnect : l'une pour fournir un accès en lecture/écriture et l'autre pour fournir un accès en lecture seule. Exécutez ces étapes une seule fois pour chaque stratégie. Vous associerez ultérieurement ces politiques aux rôles. Ces rôles peuvent ensuite être temporairement assumés par les utilisateurs pour accorder l'accès à MediaConnect.

Pour créer des stratégies

1. Utilisez votre identifiant de AWS compte ou votre alias de compte, ainsi que les informations d'identification de votre utilisateur administrateur, pour vous connecter à la console IAM.
2. Dans le volet de navigation de la console, choisissez Stratégies.
3. Sur la page Politiques, créez une politique nommée `MediaConnectAllAccess` qui autorise toutes les actions sur toutes les ressources d'AWS Elemental MediaConnect :

   a. Choisissez Créer une politique.

   b. Choisissez l'onglet JSON et collez la stratégie suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mediaconnect:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:DescribeAvailabilityZones"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
         {
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
```

```
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
           "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
                }
            }
        }
    ]
}
```

Cette politique autorise toutes les actions sur toutes les ressources d'AWS Elemental MediaConnect.

c. Choisissez Suivant : Balises.

d. Choisissez Suivant : Vérification.

e. Sur la page Réviser et créer, dans le champ Nom de la politique**`MediaConnectAllAccess`**, entrez puis choisissez Créer une politique.

4. Sur la page Politiques, créez une politique en lecture seule nommée d'après AWS `MediaConnectReadOnlyAccess` Elemental : MediaConnect

a. Choisissez Créer une politique.

b. Choisissez l'onglet JSON et collez la stratégie suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mediaconnect:List*",
                "mediaconnect:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "ec2:DescribeAvailabilityZones"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
         {
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
           "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
                }
            }
        }
    ]
} .
```

c. Choisissez Suivant : Balises.

d. Choisissez Suivant : Vérification.

e. Sur la page Réviser et créer, dans le champ Nom de la politique**`MediaConnectReadOnlyAccess`**, entrez puis choisissez Créer une politique.

Étape 2 : créer des rôles non administrateurs

Vous pouvez créer un rôle pour chaque politique et les utilisateurs peuvent assumer ce rôle, plutôt que d'associer des politiques individuelles à chaque utilisateur. À l'aide de la procédure suivante, créez deux rôles : un pour la MediaConnectAllAccessstratégie et un pour la MediaConnectReadOnlyAccessstratégie.

Pour créer des rôles

1. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles).
2. Sur la page Rôles, créez un rôle d'administrateur à l'aide de la `MediaConnectAllAccess` politique suivante :

   a. Sélectionnez Créer un rôle.

   b. Dans la section Sélectionner une entité de confiance, sélectionnez un AWS compte.

   c. Dans la section Un AWS compte, sélectionnez le compte auprès duquel les utilisateurs joueront ce rôle.

      i. Si un tiers doit accéder à ce rôle, il est recommandé de sélectionner Exiger un identifiant externe. Pour plus d'informations sur les identifiants externes, consultez : Utilisation d'un identifiant externe pour l'accès de tiers dans le guide de l'utilisateur IAM.

      ii. Il est recommandé d'exiger l'authentification multifactorielle (MFA). Vous pouvez cocher la case à côté de Exiger le MFA. Pour plus d'informations sur l'authentification multifactorielle, consultez : Authentification multifactorielle (MFA) dans le guide de l'utilisateur IAM.

   d. Choisissez Next pour accéder à la section Ajouter des autorisations.

   e. Dans la section Politique d'autorisations, choisissez la MediaConnectAllAccesspolitique que vous avez créée dans la procédure de l'étape 3a : Créer une politique.

   f. Vérifiez que les bonnes politiques sont ajoutées à ce groupe, puis choisissez Next.

   g. Dans la section Nom, révision et création, nommez le rôle`MediaConnectAdmins`. (Facultatif) Ajoutez une description du rôle. Sélectionnez Créer le rôle.

3. Sur la page Rôles, créez un rôle d'administrateur à l'aide de la `MediaConnectReadOnlyAccess` politique suivante :

   a. Sélectionnez Créer un rôle.

   b. Dans la section Sélectionner une entité de confiance, sélectionnez un AWS compte.

   c. Dans la section Un AWS compte, sélectionnez le compte auprès duquel les utilisateurs joueront ce rôle.

      i. Si un tiers doit accéder à ce rôle, il est recommandé de sélectionner Exiger un identifiant externe. Pour plus d'informations sur les identifiants externes, consultez : Utilisation d'un identifiant externe pour l'accès de tiers dans le guide de l'utilisateur IAM.

ii. Il est recommandé d'exiger l'authentification multifactorielle (MFA). Vous pouvez cocher la case à côté de Exiger le MFA. Pour plus d'informations sur l'authentification multifactorielle, consultez : Authentification multifactorielle (MFA) dans le guide de l'utilisateur IAM.

d. Choisissez Next pour accéder à la section Ajouter des autorisations.

e. Dans la section Politique d'autorisations, choisissez la MediaConnectReadOnlyAccesspolitique que vous avez créée dans la procédure de l'étape 3a : Créer une politique.

f. Vérifiez que les bonnes politiques sont ajoutées à ce groupe, puis choisissez Next.

g. Dans la section Nom, révision et création, nommez le rôle`MediaConnectReaders`. (Facultatif) Ajoutez une description du rôle. Sélectionnez Créer le rôle.

Étape 3 : assumer le rôle

Après avoir créé une politique et l'avoir attachée à un rôle, vos utilisateurs devront assumer ce rôle pour bénéficier d'un accès sécurisé et temporaire MediaConnect.

Consultez les ressources suivantes pour en savoir plus sur l'octroi d'autorisations aux utilisateurs pour qu'ils assument le rôle et sur la manière dont les utilisateurs peuvent passer au rôle depuis la console ou AWS CLI.

- Accorder à un utilisateur l'autorisation de changer de rôle : https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_permissions-to-switch.html
- Changement de rôle (console) : https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html
- Changement de rôle (AWS CLI) : https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-cli.html

(Facultatif) Configurer le chiffrement

Vous pouvez protéger votre contenu d'une utilisation non autorisée grâce au chiffrement. Si votre source est chiffrée, AWS Elemental MediaConnect peut la déchiffrer. En outre, le service peut chiffrer les sorties et les droits. AWS Elemental MediaConnect propose deux options pour chiffrer le contenu : la clé statique et le protocole SPEKE (Secure Packager and Encoder Key Exchange). Les

étapes de configuration du chiffrement dépendent du type de chiffrement que vous choisissez. Pour plus d’informations, consultez les ressources suivantes :

- Configuration du chiffrement par clé statique à l'aide d'AWS Elemental MediaConnect
- Configuration du chiffrement SPEKE à l'aide d'AWS Elemental MediaConnect

(Facultatif) Installez le AWS CLI

Pour utiliser le AWS CLI avec AWS Elemental MediaConnect, installez la dernière version AWS CLI . Pour plus d'informations sur l'installation AWS CLI ou la mise à niveau vers la dernière version, consultez la section Installation du AWS Command Line Interface dans le guide de AWS Command Line Interface l'utilisateur.

Premiers pas avec AWS Elemental MediaConnect

Ce didacticiel de mise en route vous explique comment utiliser AWS Elemental MediaConnect pour créer et partager des flux. Le didacticiel est basé sur un scénario dans lequel vous souhaitez effectuer toutes les opérations suivantes :

- Accédez à une diffusion vidéo en direct d'une cérémonie de remise de prix qui se déroule à New York.
- Distribuez votre vidéo à un affilié de Boston qui ne possède pas de AWS compte et souhaite que le contenu soit envoyé vers son encodeur local.
- Partagez votre vidéo avec un affilié de Philadelphie qui souhaite utiliser son AWS compte pour diffuser la vidéo sur ses trois stations locales.

Rubriques

Prérequis

Avant de pouvoir utiliser AWS ElementalMediaConnect, vous devez disposer d'un AWS compte et des autorisations appropriées pour accéder aux MediaConnect composants, les afficher et les modifier. Suivez la procédure de la section Configuration d'AWS Elemental MediaConnect, puis revenez à ce didacticiel.

Étape 1 : accéder à AWS Elemental MediaConnect

Après avoir configuré votre AWS compte et créé des rôles IAM, vous vous connectez à la console pour AWS MediaConnect Elemental.

Pour accéder à AWS Elemental MediaConnect

- Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.

Étape 2 : créer un flux

Tout d'abord, vous créez un MediaConnect flux AWS Elemental pour ingérer votre vidéo depuis votre encodeur sur site dans le cloud. AWS Dans le cadre de ce didacticiel, nous utilisons les informations suivantes :

- Nom du flux : AwardsNycShow
- Nom de la source : AwardsNYCSource
- Protocole source : Zixi push
- Identifiant du stream Zixi : NYCFeed ZixiAwards
- Bloc d'adresses CIDR envoyant le contenu : 10.24.34.0/23
- Chiffrement de source : Aucun

Pour créer un flux

1. Sur la page Flux, choisissez Create flow.
2. Dans la section Détails, pour Nom, entrez**`AwardsNYCShow`**.
3. Pour Zone de disponibilité, choisissez N'importe laquelle.
4. Dans la section Source, pour Type de source, sélectionnez Source standard.
5. Pour Name (Nom), saisissez **`AwardsNYCSource`**.
6. Pour le protocole, choisissez Zixi push. AWS Elemental MediaConnect renseignera la valeur du port d'ingestion.
7. Pour Stream ID, entrez**`ZixiAwardsNYCFeed`**.
8. Pour Allowlist CIDR, entrez. **`10.24.34.0/23`**
9. Choisissez Create flow (Créer un flux).

Étape 3 : ajouter une sortie

Pour envoyer du contenu à votre affilié à Boston, vous devez ajouter une sortie à votre flux. Cette sortie enverra votre vidéo à l'encodeur local de votre affilié de Boston. Dans le cadre de ce didacticiel, nous utilisons les informations suivantes :

- Nom de sortie : AwardsNycOutput
- Protocole de sortie : Zixi push
- Identifiant du stream Zixi : ZixiAwardsOutput
- Adresse IP de l'encodeur local de la filiale de Boston : 198.51.100.11
- Chiffrement de sortie : Aucun

Pour ajouter une sortie

1. Sur la page Flux, sélectionnez le **`AwardsNYCShow`** flux.
2. Choisissez l'onglet Outputs.
3. Choisissez Ajouter une sortie.
4. Pour Name (Nom), saisissez **`AwardsNYCOutput`**.
5. Pour Type de sortie, sélectionnez Sortie standard.
6. Pour le protocole, choisissez Zixi push.
7. Pour Stream ID, entrez**`ZixiAwardsOutput`**.
8. Pour l'adresse IP de destination, entrez**`198.51.100.11`**.
9. Pour Port, entrez **`1024`**.
10. Choisissez Ajouter une sortie.

Étape 4 : accorder un droit

Vous devez autoriser votre affilié de Philadelphie à utiliser votre contenu comme source pour son MediaConnect flux AWS Elemental. Dans le cadre de ce didacticiel, nous utilisons les informations suivantes :

- Nom du droit : PhillyTeam
- ID de AWS compte de l'affilié de Philadelphie : 222233334444
- Chiffrement de sortie : Aucun

Pour accorder un droit

1. Choisissez l'onglet Droits.
2. Choisissez le droit à une subvention.
3. Pour Name (Nom), saisissez **`PhillyTeam`**.
4. Pour Abonné, entrez**`222233334444`**.
5. Choisissez le droit à une subvention.

Étape 5 : Partagez les informations avec vos affiliés

Maintenant que vous avez créé votre MediaConnect flux AWS Elemental avec une sortie pour votre affilié de Boston et un droit pour votre affilié de Philadelphie, vous devez communiquer les détails du flux.

Votre affilié de Boston recevra le flux sur son encodeur sur site. Les détails concernant l'endroit où envoyer votre flux vidéo ont été fournis par votre filiale de Boston, et vous n'avez pas besoin de fournir d'autres informations. Une fois que vous avez démarré votre flux, le contenu sera envoyé à l'adresse IP que vous avez spécifiée lors de la création du flux.

Votre affilié de Philadelphie doit créer son propre MediaConnect flux AWS Elemental, en utilisant votre flux comme source. Vous devez fournir les informations suivantes à votre filiale de Philadelphie :

- ARN du titre : vous pouvez trouver cette valeur dans l'onglet Entitlement de la page de détails du flux AwardsNycShow.
- Région : Il s'agit de la AWS région dans laquelle vous avez créé le flux AwardsNycShow.

Étape 6 : Nnettoyer

Pour éviter des frais inutiles, veillez à supprimer tous les flux inutiles. Vous devez arrêter le flux avant de pouvoir le supprimer.

Pour arrêter votre flux

1. Sur la page Flux, sélectionnez le **`AwardsNYCShow`** flux.

   La page de détails du flux AwardsNycShow s'affiche.

2. Choisissez Stop (Arrêter).

Pour supprimer votre flux

1. Sur la page des détails du flux AwardsNYCShow, choisissez Supprimer.

   Un message de confirmation s'affiche.
2. Choisissez Supprimer le flux.

Flux dans AWS Elemental MediaConnect

Un flux est un transport entre une source et une ou plusieurs destinations. Lorsque vous créez un flux, vous spécifiez la source, un nom et une zone de disponibilité. Après avoir créé un flux, vous pouvez ajouter des sorties pour indiquer où vous souhaitez que votre contenu soit envoyé et comment vous souhaitez qu'il soit transporté.

MediaConnect prend en charge deux types de flux :

- Les flux de transport transportent du contenu compressé qui est multiplexé (les données audio, vidéo et auxiliaires sont combinées) en un seul flux. La qualité est suffisamment élevée pour être utilisée comme source pour créer des encodages finaux destinés aux appareils grand public. Vous pouvez ajouter des sorties pour indiquer où vous souhaitez que le contenu soit envoyé et comment vous souhaitez qu'il soit transporté.

  Vous pouvez autoriser le partage du contenu avec un autre AWS compte. Un utilisateur du compte abonné peut ensuite créer un nouveau MediaConnect flux en utilisant votre flux comme source. Lorsque cela se produit, le service génère une sortie sur votre flux pour représenter le flux qui alimente le flux de l'abonné.

  Il est important de gérer le nombre de sorties et de droits sur le flux. Chaque flux de transport ne peut avoir que 50 sorties. Bien que vous puissiez accorder jusqu'à 50 droits par flux, chacun de ces droits générera une sortie. Par exemple, vous créez un flux nommé **`BasketballGame`** et vous ajoutez 40 sorties qui envoient du contenu aux encodeurs locaux. Vous accordez également 30 autorisations pour partager votre contenu avec d'autres AWS comptes. Lorsque vos abonnés créent des flux en utilisant **`BasketballGame`** comme source, le service génère de nouvelles sorties pour chacun de ces abonnés. Une fois que les 10 premiers abonnés ont créé des **`BasketballGame`** flux, votre flux atteint son nombre maximum de sorties (40 pour les sorties d'origine que vous avez créées et 10 autres que le service a créées pour les flux d'abonnement). Lorsque le 11e abonné essaie de créer un flux en utilisant **`BasketballGame`** comme source, le service renvoie une erreur.
- Les flux CDI transportent du contenu de haute qualité non compressé ou légèrement compressé vers et depuis le AWS cloud. Vous pouvez configurer un flux CDI pour utiliser le format JPEG XS pour transporter du contenu légèrement compressé. Le contenu est démultiplexé en flux multimédia distincts pour les données audio, vidéo ou auxiliaires. Chaque flux CDI peut utiliser plusieurs flux multimédia pour la source et plusieurs flux multimédias pour chaque sortie.

MediaConnect utilise la technologie réseau AWS Cloud Digital Interface (AWS CDI) pour transporter du contenu conforme à la norme de transport SMPTE 2110, partie 22.

Rubriques

Création d'un flux

Un flux est une connexion entre une ou plusieurs sources et une ou plusieurs sorties ou droits.

La méthode que vous utilisez pour créer un flux dépend du type de flux que vous souhaitez créer et du type de contenu de la source :

- Flux de flux de transport avec une source standard : utilise du contenu provenant de toute source autre qu'une source VPC ou une source autorisée.
- Flux de transport avec une source autorisée — Utilise du contenu appartenant à un autre AWS compte qui a accordé un droit à votre compte.
- Flux de flux de transport avec une source VPC : utilise du contenu compressé provenant d'un VPC que vous configurez.
- Flux CDI — Utilise du contenu non compressé provenant d'un VPC que vous configurez.

> **Note**
>
> Si vous souhaitez créer un flux de transport qui utilise des sources redondantes pour le basculement, créez le flux avec l'une des sources. Une fois le flux créé, ajoutez l'autre source. Étant donné MediaConnect que les deux sources sont traitées comme la source principale, peu importe celle que vous spécifiez lors de la création du flux pour la première

fois. Si votre flux utilise une source autorisée, vous ne pouvez pas ajouter de seconde source. Pour assurer la redondance avec les flux de travail CDI, créez deux flux distincts.

Création d'un flux de transport utilisant une source standard

Les flux de transport transportent du contenu compressé qui est mixé en un seul flux.

Un flux utilise une source standard lorsque le contenu provient d'un autre endroit qu'un VPC (source VPC) ou un autre AWS compte (source intitulée).

Important

Si la source de votre flux nécessite un chiffrement, configurez le chiffrement avant de commencer cette procédure.

Création d'un flux de transport utilisant une source standard (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez Créer un flux.
3. Dans la section Détails, pour Nom, spécifiez le nom de votre flux. Ce nom fera partie de l'ARN de ce flux.

   Note

   MediaConnect vous permet de créer plusieurs flux portant le même nom. Toutefois, nous vous encourageons à utiliser des noms de flux uniques au sein d'une AWS région pour faciliter l'organisation. Une fois que vous avez créé un flux, vous ne pouvez pas en modifier le nom.

4. Pour Zone de disponibilité, choisissez une zone de disponibilité pour votre flux. Utilisez cette option lorsque vous configurez des flux redondants. Sinon, vous pouvez laisser ce champ sous la forme Any. Si vous laissez la valeur par défaut, le service attribuera de manière aléatoire une zone de disponibilité dans la AWS région actuelle, ou si votre source provient d'un VPC, le service attribuera la zone de disponibilité du sous-réseau VPC au flux.
5. Déterminez le protocole utilisé par votre source.

> **Note**
>
> Si vous souhaitez spécifier des sources redondantes pour le basculement, créez le flux avec l'une des sources. Une fois le flux créé, mettez-le à jour pour activer le basculement sur la source et ajoutez la seconde source au flux. Étant donné MediaConnect que les deux sources sont traitées comme la source principale, peu importe celle que vous spécifiez lors de la création du flux pour la première fois.

6. Pour obtenir des instructions spécifiques en fonction de votre type de source et de votre protocole, choisissez l'un des onglets suivants :

   RIST

   1. Dans la section Source, pour Type de source, choisissez Source standard.
   2. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console.
   3. Pour Protocole, choisissez RIST.
   4. Pour le port d'ingestion, spécifiez le port sur lequel le flux écoutera le contenu entrant.

      > **Note**
      >
      > Le protocole RIST nécessite un port supplémentaire pour la correction des erreurs. Pour répondre à cette exigence, MediaConnect réserve le port égal à +1 par rapport au port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000 et 4001.

   5. Pour Allowlist CIDR, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

      > **Important**
      >
      > Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

6. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
7. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 1 et 15 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 2 000 ms.

RTP or RTP-FEC

1. Dans la section Source, pour Type de source, choisissez Source standard.
2. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
3. Pour Protocole, choisissez RTP ou RTP-FEC.
4. Pour le port d'ingestion, spécifiez le port sur lequel le flux écoutera le contenu entrant.

> **Note**
>
> Le protocole RTP-FEC nécessite deux ports supplémentaires pour la correction des erreurs. Pour répondre à cette exigence, MediaConnect réserve les ports +2 et +4 à partir du port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000, 4002 et 4004.

5. Pour Allowlist CIDR, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

> **Important**
>
> Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

6. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.

SRT listener

1. Dans la section Source, pour Type de source, choisissez Source standard.
2. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
3. Pour Protocol, choisissez SRT listener.
4. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
5. Pour le bloc d'adresse CIDR Allowlist, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

   > **Important**
   >
   > Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

6. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.
7. Pour Adresse de l'écouteur source, entrez l'adresse que MediaConnect vous utiliserez pour la connexion SRT. L'adresse peut être une adresse IP ou un nom de domaine.
8. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
9. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
10. Pour Latence minimale, spécifiez la taille minimale de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger

les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.

11. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :

    a. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.

    b. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

SRT caller

1. Dans la section Source, pour Type de source, choisissez Source standard.
2. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
3. Pour Protocol, choisissez SRT Caller.
4. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
5. Pour Adresse de l'écouteur source, entrez l'adresse que MediaConnect vous utiliserez pour la connexion SRT. L'adresse peut être une adresse IP ou un nom de domaine.

6. Pour le port de l'écouteur source, entrez le port MediaConnect qui sera utilisé pour la connexion SRT.
7. Pour Débit maximal (facultatif), spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
8. Pour Latence minimale, spécifiez la taille minimale de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

   Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.
9. Pour Stream ID (facultatif), entrez un identifiant pour le flux. Cet identifiant peut être utilisé pour communiquer des informations sur le flux.
10. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
    a. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
    b. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

Zixi push

1. Dans la section Source, pour Type de source, choisissez Source standard.

2. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
3. Pour Protocole, choisissez Zixi push.

> **Note**
>
> MediaConnect attribue le port entrant aux sources push Zixi au moment de la création. Le numéro de port 2088 sera attribué automatiquement.

4. Pour Allowlist CIDR, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

> **Important**
>
> Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

5. Pour Stream ID, spécifiez l'ID de flux défini dans le chargeur Zixi.

> **Important**
>
> Si vous laissez ce champ vide, le service utilise le nom de la source comme identifiant du flux. Comme l'ID du flux doit correspondre à la valeur définie dans le chargeur Zixi, vous devez spécifier l'ID du flux s'il n'est pas exactement le même que le nom de la source.

6. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 0 et 60 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 6 000 ms.

7. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
   a. Pour le type de déchiffrement, choisissez Clé statique.
   b. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   c. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.
   d. Pour Algorithme de déchiffrement, choisissez le type de chiffrement utilisé pour chiffrer la source.

Zixi push for AWS Elemental Link UHD device

Pour utiliser un AWS Elemental Link appareil comme source pour MediaConnect, vous devez créer un flux push Zixi en suivant la procédure suivante. Après avoir créé le flux push Zixi, vous devez configurer l' AWS Elemental Link appareil à l'aide de. MediaLive Consultez les instructions de MediaLive configuration suivantes pour terminer le processus après avoir créé le flux : Utilisation d'un appareil dans un flux dans le guide de MediaLive l'utilisateur. Assurez-vous d'avoir accès aux deux MediaConnect et MediaLive de suivre ces étapes.

1. Dans la section Source, pour Type de source, choisissez Source standard.
2. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
3. Pour Protocole, choisissez Zixi push.

> **Note**
>
> MediaConnect attribue le port entrant aux sources push Zixi au moment de la création. Le numéro de port 2088 sera attribué automatiquement.

4. Pour le bloc d'adresse CIDR Allowlist, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

> **Important**
>
> Si vous connaissez la plage d'adresses IP publiques que votre appareil Link utilise pour se connecter à Internet, entrez ce bloc CIDR. Notez qu'il ne s'agit pas de la même adresse IP de l' AWS Elemental Link appareil. Si vous ne pouvez pas obtenir ces informations, il est possible de configurer le bloc CIDR pour qu'il soit ouvert à toutes les adresses IP possibles en utilisant 0.0.0.0/0. Généralement, il n'est pas recommandé d'attribuer un bloc CIDR ouvert à l'ensemble d'Internet (0.0.0.0/0). Toutefois, si cette méthode doit être utilisée, les données transférées sont cryptées à l'aide du cryptage AES-128.

5. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 0 et 60 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 6 000 ms. La valeur de latence maximale doit correspondre à la valeur de latence configurée sur l' AWS Elemental Link appareil. Pour plus d'informations sur la configuration de la latence de l'appareil Link, voir : Configuration de l'appareil dans le guide de AWS Elemental MediaLive l'utilisateur
6. Pour le déchiffrement, choisissez Activer et procédez comme suit :
   a. Pour le type de déchiffrement, choisissez Clé statique.
   b. Pour Algorithme de déchiffrement, choisissez AES-128. AWS Elemental Link nécessite AES-128, ne sélectionnez pas un autre algorithme.
   c. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   d. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

Fujitsu-QoS

1. Dans la section Source, pour Type de source, choisissez Source standard.
2. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.

3. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
4. Pour Adresse IP de l'expéditeur, spécifiez l'adresse IP de l'expéditeur avec laquelle vous souhaitez que le flux établisse une connexion. Le flux communique avec l'adresse IP spécifiée pour établir une connexion avec l'expéditeur.
5. Pour Port de contrôle de l'expéditeur, spécifiez le port utilisé par le flux pour envoyer des demandes sortantes afin d'établir une connexion avec l'expéditeur.
6. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 300 et 2 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

7. Au bas de la page, choisissez Create flow.

> **Note**
>
> Le flux ne démarre pas automatiquement. Vous devez démarrer le flux manuellement.

8. Ajoutez des sorties pour spécifier où vous souhaitez MediaConnect envoyer le contenu, ou accordez des droits pour permettre aux utilisateurs d'autres AWS comptes de s'abonner à votre contenu.

Créez un flux de transport utilisant une source standard (AWS CLI)

1. Créez un fichier JSON contenant les détails du flux que vous souhaitez créer.

   L'exemple suivant montre la structure du contenu du fichier :

```
{
  "Name": "AwardsShow",
  "Outputs": [
    {
      "Destination": "198.51.100.5",
      "Description": "RTP output",
```

```
      "Name": "RTPOutput",
      "Protocol": "rtp",
      "Port": 5020
    }
  ],
  "Source": {
    "Name": "AwardsShowSource",
    "Protocol": "rtp-fec",
    "AllowlistCidr": "10.24.34.0/23"
  }
}
```

2. Dans le AWS CLI, utilisez la `create-flow` commande :

```
aws mediaconnect create-flow --cli-input-json file://rtp.json --profile PMprofile
```

L'exemple suivant illustre la valeur de retour :

```
{
  "Flow": {
    "EgressIp": "203.0.113.0",
    "AvailabilityZone": "us-east-1d",
    "Name": "AwardsShow",
    "Status": "STANDBY",
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow",
    "Source": {
            "SourceArn": "arn:aws:mediaconnect:us-
east-1:111122223333:source:3-4aBC56dEF78hiJ90-4de5fG6Hi78Jk:AwardsShowSource",

            "Name": "AwardsShowSource",
            "IngestPort": 5000,
            "AllowlistCidr": "10.24.34.0/23",
            "IngestIp": "198.51.100.15",
            "Transport": {
                "Protocol": "rtp-fec",
                "MaxBitrate": 80000000
            }
        },
        "Entitlements": [],
        "Outputs": [
            {
                "Port": 5020,
```

```
                "Name": "AwardsShowOutput",
                "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:AwardsShowOutput",

                "Description": "RTP-FEC Output",
                "Destination": "198.51.100.5",
                "Transport": {
                    "Protocol": "rtp",
                    "SmoothingLatency": 0
                }
            }
        ]
    }
}
```

Création d'un flux de transport utilisant une source autorisée

Les flux de transport transportent du contenu compressé qui est mixé en un seul flux. Une source autorisée est un contenu provenant d'un autre AWS compte.

Création d'un flux de transport utilisant une source autorisée (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez Créer un flux.
3. Dans la section Détails, pour Nom, spécifiez le nom de votre flux. Ce nom fera partie de l'ARN de ce flux.

   > **Note**
   >
   > MediaConnect vous permet de créer plusieurs flux portant le même nom. Toutefois, nous vous encourageons à utiliser des noms de flux uniques au sein d'une AWS région pour faciliter l'organisation. Une fois que vous avez créé un flux, vous ne pouvez pas en modifier le nom.

4. Pour Zone de disponibilité, choisissez une zone de disponibilité pour votre flux. Utilisez cette option lorsque vous configurez des flux redondants. Sinon, vous pouvez laisser ce champ sous la forme Any. Si vous laissez la valeur par défaut, le service attribuera de manière aléatoire une zone de disponibilité dans la AWS région actuelle, ou si votre source provient d'un VPC, le service attribuera la zone de disponibilité du sous-réseau VPC au flux.

> **Note**
>
> Si votre source provient de votre VPC, la zone de disponibilité de votre flux doit correspondre à celle de votre sous-réseau VPC. Nous vous recommandons de laisser la valeur Any et de laisser le service s'assurer que la zone de disponibilité est correctement définie.

5. Dans la section Source, pour Type de source, sélectionnez Source autorisée.
6. Pour l'ARN d'autorisation, choisissez l'autorisation appropriée. Cette liste inclut tous les droits qui vous ont été accordés.

> **Tip**
>
> Vous pouvez cliquer dans ce champ et commencer à saisir le nom du titre. MediaConnect filtrera la liste pour n'inclure que les droits dont le nom correspond à celui que vous avez saisi.

7. Choisissez Create flow (Créer un flux).

> **Note**
>
> Le flux ne démarre pas automatiquement. Vous devez démarrer le flux manuellement.

8. Ajoutez des sorties pour spécifier où vous souhaitez MediaConnect envoyer le contenu, ou accordez des droits pour permettre aux utilisateurs d'autres AWS comptes de s'abonner à votre contenu.

Création d'un flux de transport utilisant une source VPC

Les flux de transport transportent du contenu compressé qui est mixé en un seul flux.

Lorsque vous créez un flux qui utilise une source provenant de votre cloud privé virtuel (VPC), votre contenu ne passe pas par l'Internet public. Ceci est utile pour des raisons de sécurité et de fiabilité. Vous configurez votre VPC, puis vous créez un flux doté d'une interface avec ce VPC. Vous pouvez également créer un flux basé sur un droit accordé par un autre AWS compte pour vous permettre d'utiliser son contenu (intitulé source) ou une source standard.

Important

Avant de commencer cette procédure, assurez-vous que les étapes suivantes ont été effectuées :

- Dans Amazon VPC, configurez votre VPC et les groupes de sécurité associés. Pour plus d'informations sur les VPC, consultez le Guide de l'utilisateur Amazon VPC. Pour plus d'informations sur la configuration des groupes de sécurité pour qu'ils fonctionnent avec votre interface VPC, consultez. Considérations relatives aux groupes de sécurité
- Dans IAM, configurez-le en MediaConnect tant que service de confiance.
- Si la source de votre flux nécessite un chiffrement, configurez le chiffrement.

Création d'un flux de transport utilisant une source VPC (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez Créer un flux.
3. Dans la section Détails, pour Nom, spécifiez le nom de votre flux. Ce nom fera partie de l'ARN de ce flux.

   Note

   MediaConnect vous permet de créer plusieurs flux portant le même nom. Toutefois, nous vous encourageons à utiliser des noms de flux uniques au sein d'une AWS région pour faciliter l'organisation. Une fois que vous avez créé un flux, vous ne pouvez pas en modifier le nom.

4. Pour Zone de disponibilité, choisissez N'importe laquelle ou choisissez la zone de disponibilité dans laquelle réside votre sous-réseau VPC. Nous vous recommandons de laisser la valeur Any et de laisser le service s'assurer que la zone de disponibilité est correctement définie.
5. Dans la section Source, pour Type de source, choisissez la source VPC.
6. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console.
7. Déterminez le protocole utilisé par votre source.

> **Note**
>
> Si vous souhaitez spécifier des sources redondantes pour le basculement, créez le flux avec l'une des sources. Une fois le flux créé, mettez-le à jour pour activer le basculement sur la source et ajoutez la seconde source au flux. Étant donné MediaConnect que les deux sources sont traitées comme la source principale, peu importe celle que vous spécifiez lors de la création du flux pour la première fois.

8. Pour obtenir des instructions spécifiques en fonction de votre protocole, sélectionnez l'un des onglets suivants :

   RIST

   1. Pour Protocole, choisissez RIST.
   2. Pour le port d'ingestion, spécifiez le port sur lequel le flux écoutera le contenu entrant.

      > **Note**
      >
      > Le protocole RIST nécessite un port supplémentaire pour la correction des erreurs. Pour répondre à cette exigence, MediaConnect réserve le port égal à +1 par rapport au port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000 et 4001.

   3. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
   4. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
   5. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 1 et 15 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 2 000 ms.

RTP or RTP-FEC

1. Pour Protocole, choisissez RTP ou RTP-FEC.
2. Pour le port d'ingestion, spécifiez le port sur lequel le flux écoutera le contenu entrant.

> **Note**
>
> Le protocole RTP-FEC nécessite deux ports supplémentaires pour la correction des erreurs. Pour répondre à cette exigence, MediaConnect réserve les ports +2 et +4 à partir du port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000, 4002 et 4004.

3. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
4. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.

SRT listener

1. Dans la section Source, pour Type de source, choisissez la source VPC.
2. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
3. Pour Protocol, choisissez SRT listener.
4. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
5. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
6. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.
7. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
8. Pour Latence minimale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long

dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 2 000 ms.

Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.

9. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
   a. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   b. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

SRT caller

1. Dans la section Source, pour Type de source, choisissez la source VPC.
2. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
3. Pour Protocol, choisissez SRT Caller.
4. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
5. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.

6. Pour Port du récepteur source, entrez le port que le flux utilisera pour extraire la source.
7. Pour Débit maximal (facultatif), spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
8. Pour Latence minimale, spécifiez la taille minimale de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

   Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.
9. Pour Stream ID (facultatif), entrez un identifiant pour le flux. Cet identifiant peut être utilisé pour communiquer des informations sur le flux.
10. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
    a. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
    b. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

Zixi push

1. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
2. Pour Protocole, choisissez Zixi push.

> **Note**
>
> MediaConnect attribue le port entrant aux sources VPC push Zixi au moment de la création. Un numéro de port 2090-2099 sera attribué automatiquement.

3. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
4. Pour Stream ID, spécifiez l'ID de flux défini dans le chargeur Zixi.

> **Important**
>
> Si vous laissez ce champ vide, le service utilise le nom de la source comme identifiant du flux. Comme l'ID du flux doit correspondre à la valeur définie dans le chargeur Zixi, vous devez spécifier l'ID du flux s'il n'est pas exactement le même que le nom de la source.

5. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 0 et 60 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 6 000 ms.
6. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
   a. Pour le type de déchiffrement, choisissez Clé statique.
   b. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.

c. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

d. Pour Algorithme de déchiffrement, choisissez le type de chiffrement utilisé pour chiffrer la source.

Fujitsu-QoS

1. Pour Protocole, choisissez Fujitsu-QOS.
2. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.
3. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
4. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
5. Pour Adresse IP de l'expéditeur, spécifiez l'adresse IP de l'expéditeur avec laquelle vous souhaitez que le flux établisse une connexion. Le flux communique avec l'adresse IP spécifiée pour établir une connexion avec l'expéditeur.
6. Pour Port de contrôle de l'expéditeur, spécifiez le port utilisé par le flux pour envoyer des demandes sortantes afin d'établir une connexion avec l'expéditeur.
7. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 300 et 2 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

9. Pour chaque VPC que vous souhaitez connecter au flux, procédez comme suit :

1. Dans la section Interface VPC, choisissez Ajouter une interface VPC.
2. Dans Nom, spécifiez le nom de votre interface VPC. Le nom de l'interface VPC doit être unique dans le flux.
3. Pour l'ARN du rôle, spécifiez le nom de ressource Amazon (ARN) du rôle que vous avez créé lors de votre configuration MediaConnect en tant que service fiable.
4. Pour VPC, choisissez l'ID du VPC à utiliser.

> **Note**
>
> Si le VPC que vous souhaitez ne figure pas dans la liste, vérifiez qu'il a été configuré dans Amazon Virtual Private Cloud et que vous disposez des autorisations IAM pour le consulter.

5. Pour Sous-réseau, choisissez le sous-réseau VPC que vous MediaConnect souhaitez utiliser pour configurer votre configuration VPC. Vous devez en choisir au moins un et vous pouvez en choisir autant que vous le souhaitez.
6. Pour les groupes de sécurité, spécifiez les groupes de sécurité VPC que vous MediaConnect souhaitez utiliser pour configurer votre configuration VPC. Vous devez choisir au moins un groupe de sécurité.

10. Au bas de la page, choisissez Create flow.

> **Note**
>
> Le flux ne démarre pas automatiquement. Vous devez démarrer le flux manuellement.

11. Ajoutez des sorties pour spécifier où vous souhaitez MediaConnect envoyer le contenu, ou accordez des droits pour permettre aux utilisateurs d'autres AWS comptes de s'abonner à votre contenu.

Création d'un flux CDI

Un flux CDI transporte du contenu de haute qualité non compressé ou légèrement compressé vers et depuis le AWS cloud. Vous pouvez configurer un flux CDI pour utiliser le format JPEG XS pour transporter du contenu légèrement compressé. Le contenu est démultiplexé en flux multimédia distincts pour les données audio, vidéo ou auxiliaires. Chaque flux CDI peut utiliser plusieurs flux multimédia pour la source et plusieurs flux multimédias pour chaque sortie. MediaConnect utilise la technologie réseau AWS Cloud Digital Interface (AWS CDI) pour transporter du contenu conforme à la norme de transport SMPTE 2110, partie 22.

Les flux CDI ne prennent en charge que les sources provenant d'un cloud privé virtuel (VPC) que vous avez configuré à l'aide d'Amazon VPC. Vous configurez votre VPC, puis vous créez un flux doté d'une interface avec ce VPC.

MediaConnect ne prend pas en charge deux sources sur les flux CDI. Pour la redondance avec les sources ST 2110 JPEG XS, vous pouvez spécifier deux interfaces VPC entrantes sur un flux multimédia individuel. Pour assurer la redondance avec les sources CDI, créez un second flux.

Important

Avant de commencer cette procédure, assurez-vous que les étapes suivantes ont été effectuées :

- Passez en revue le flux de travail suggéré présenté dansContribution aux flux de CDI.
- Dans Amazon VPC, configurez votre VPC et les groupes de sécurité associés. Pour plus d'informations sur les VPC, consultez le Guide de l'utilisateur Amazon VPC. Pour plus d'informations sur la configuration des groupes de sécurité pour qu'ils fonctionnent avec votre interface VPC, consultez. Considérations relatives aux groupes de sécurité
- Dans IAM, configurez-le en MediaConnect tant que service de confiance.

Création d'un AWS CDI flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez Créer un flux.
3. Dans la section Détails, pour Nom, spécifiez le nom de votre flux. Ce nom fera partie de l'ARN de ce flux.

   Note

   MediaConnect vous permet de créer plusieurs flux portant le même nom. Toutefois, nous vous encourageons à utiliser des noms de flux uniques au sein d'une AWS région pour faciliter l'organisation. Une fois que vous avez créé un flux, vous ne pouvez pas en modifier le nom.
4. Pour Zone de disponibilité, choisissez la zone de disponibilité dans laquelle réside votre sous-réseau VPC.
5. Dans la section Source, pour Type de source, choisissez la source VPC.
6. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console.
7. Passez à la section de l'interface VPC.

8. Pour chaque VPC que vous souhaitez connecter au flux, procédez comme suit :

    1. Choisissez Ajouter une interface VPC.
    2. Dans Nom, spécifiez le nom de votre interface VPC. Le nom de l'interface VPC doit être unique dans le flux.
    3. Pour Type, choisissez le type d'adaptateur réseau que vous MediaConnect souhaitez utiliser sur cette interface. Si vous souhaitez utiliser cette interface pour une source ou une sortie CDI, vous devez choisir EFA comme type.
    4. Pour l'ARN du rôle, spécifiez le nom de ressource Amazon (ARN) du rôle que vous avez créé lors de votre configuration MediaConnect en tant que service fiable.
    5. Pour VPC, choisissez l'ID du VPC à utiliser.

        > **Note**
        >
        > Si le VPC que vous souhaitez ne figure pas dans la liste, vérifiez qu'il a été configuré dans Amazon Virtual Private Cloud et que vous disposez des autorisations IAM pour le consulter.

    6. Pour Sous-réseau, choisissez le sous-réseau VPC que vous MediaConnect souhaitez utiliser pour configurer votre configuration VPC. Vous devez en choisir au moins un et vous pouvez en choisir autant que vous le souhaitez.
    7. Pour les groupes de sécurité, spécifiez les groupes de sécurité VPC que vous MediaConnect souhaitez utiliser pour configurer votre configuration VPC. Vous devez choisir au moins un groupe de sécurité.

9. Pour chaque flux multimédia que vous souhaitez ajouter au flux, procédez comme suit :

    1. Dans la section Diffusions multimédia, choisissez Ajouter un flux multimédia.
    2. Dans le champ Nom, spécifiez un nom descriptif qui vous aidera à distinguer ce flux multimédia des autres flux.
    3. Dans Description, spécifiez une description qui vous aidera à vous souvenir de l'utilisation de ce flux multimédia.
    4. Pour Stream ID, spécifiez un identifiant unique pour le flux multimédia.

        Si la source ou l'une des sorties utilise le protocole CDI, spécifiez la valeur attendue par les systèmes de production et de diffusion.

Si la source et toutes les sorties utilisent le protocole ST 2110 JPEG XS, spécifiez une valeur unique par rapport à celle des autres flux multimédias du flux.

5. Choisissez Options avancées pour afficher les options supplémentaires en fonction de votre type de diffusion.
6. Pour obtenir des instructions spécifiques sur les options avancées en fonction de votre type de stream, choisissez l'un des onglets suivants :

   Audio

   a. Pour le type de diffusion, choisissez Audio.
   b. Pour Fréquence d'horloge multimédia, spécifiez la fréquence d'échantillonnage du flux. Cette valeur est mesurée en Hz.
   c. Dans Langue, spécifiez la langue de l'audio. Cette valeur doit être dans un format reconnu par le récepteur.
   d. Pour Ordre des canaux, spécifiez le format du canal audio.
   e. Choisissez Ajouter un flux multimédia.

   Video

   a. Pour le type de diffusion, choisissez Vidéo.

      MediaConnect Fournit une valeur par défaut représentant le paramètre recommandé pour de nombreux champs. Modifiez la valeur par défaut si nécessaire.

   b. La fréquence d'horloge multimédia est la fréquence d'échantillonnage du flux, définie sur 90 000. Cette valeur est mesurée en Hz.
   c. Pour le format vidéo, spécifiez la résolution de la vidéo.
   d. Pour Fréquence d'images exacte, spécifiez la fréquence d'images de la vidéo. Cette valeur doit être représentée en images par seconde.
   e. Pour la colorimétrie, spécifiez le format utilisé pour la représentation des couleurs dans la vidéo.
   f. Pour le mode de numérisation, spécifiez la méthode utilisée pour numériser la vidéo entrante.
      - Choisissez Entrelacer si la vidéo entrante est entrelacée (par exemple, 480i ou 1080i).
      - Choisissez Progressive si la vidéo entrante est progressive (par exemple, 720p ou 1080p).

- Choisissez une image segmentée progressive si la vidéo entrante est au format PSF (par exemple, 1080psf).

g. Pour le TCS, spécifiez le système de caractéristiques de transfert (TCS) utilisé dans la vidéo.

h. Pour Range, spécifiez la plage de codage de la vidéo.

i. Pour LE PAR, spécifiez le rapport d'accès aux pixels (PAR) de la vidéo.

j. Choisissez Ajouter un flux multimédia.

Ancillary data

a. Pour le type de flux, choisissez Données auxiliaires.

b. La fréquence d'horloge multimédia est la fréquence d'échantillonnage du flux, définie sur 90 000. Cette valeur est mesurée en Hz.

c. Choisissez Ajouter un flux multimédia.

10. Revenez à la section Sources.
11. Déterminez le protocole utilisé par votre source.
12. Pour obtenir des instructions spécifiques en fonction de votre protocole, sélectionnez l'un des onglets suivants :

CDI

1. Pour Protocole, choisissez CDI.
2. Dans Description, entrez une description qui vous rappellera ultérieurement l'origine de cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
3. Pour le port entrant, spécifiez le port sur lequel le flux écoutera le contenu entrant. Cette valeur peut être comprise entre 1024 et 65535, à l'exception de 2077 et 2088 (ces ports sont réservés à d'autres protocoles).
4. Pour l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
5. Pour chaque flux multimédia que vous souhaitez utiliser dans le cadre de la source, procédez comme suit.

a. Pour Nom du flux multimédia, choisissez le nom du flux multimédia.

b. Pour le nom du codage, acceptez la valeur par défaut.

- Pour les flux de données auxiliaires, le nom de codage est **`smpte291`**.
- Pour les flux audio, le nom de codage est **`pcm`**.

- Pour la vidéo, le nom du codage est **raw**.

ST 2110 JPEG XS

1. Pour Protocole, choisissez ST 2110 JPEG XS.
2. Dans Description, entrez une description qui vous rappellera ultérieurement l'origine de cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
3. Pour la zone tampon de synchronisation maximale, spécifiez la taille de la mémoire tampon que vous MediaConnect souhaitez utiliser pour synchroniser les données source entrantes. Cette valeur est mesurée en millisecondes (ms).
4. Pour le nom d'interface VPC 1, choisissez l'une des interfaces VPC que vous souhaitez utiliser comme source.
5. Pour le nom d'interface VPC 2, choisissez une deuxième interface VPC que vous souhaitez utiliser comme source. Il n'y a aucune priorité entre les interfaces VPC 1 et 2.
6. Pour chaque flux multimédia que vous souhaitez utiliser dans le cadre de la source, procédez comme suit.
   a. Pour Nom du flux multimédia, choisissez le nom du flux multimédia.
   b. Pour le nom du codage, acceptez la valeur par défaut.
      - Pour les flux de données auxiliaires, le nom de codage est **smpte291**.
      - Pour les flux audio, le nom de codage est **pcm**.
      - Pour la vidéo, le nom du codage est **jxsv**.
   c. Pour le port entrant, spécifiez le port sur lequel le flux écoutera le contenu entrant. Cette valeur peut être comprise entre 1024 et 65535, à l'exception de 2077 et 2088 (ces ports sont réservés à d'autres protocoles).

13. Au bas de la page, choisissez Create flow.

> **Note**
>
> Le flux ne démarre pas automatiquement. Vous devez démarrer le flux manuellement.

14. Ajoutez des sorties pour spécifier où vous MediaConnect souhaitez envoyer le contenu.

Création d'un AWS CDI flux (AWS CLI)

Pour utiliser le AWS CLI pour créer un flux, vous devez utiliser la `create-flow` commande. Pour simplifier la création du flux, nous vous suggérons d'utiliser la `create-flow` commande associée à l'`--cli-input-json`option. `--cli-input-json`Cette option vous oblige à créer un fichier JSON avec les paramètres nécessaires pour votre nouveau flux. L'étape 1 de cette procédure fournit un exemple d'une manière possible de configurer ce fichier JSON. Pour plus d'informations sur la `create-flow` commande et l'`--cli-input-json`option, voir : AWS CLI Command Reference create-flow

1. Créez un fichier JSON contenant les détails du flux que vous souhaitez créer.

   L'exemple suivant montre la structure du contenu du fichier. Cet exemple utilise une source JPEG XS pour créer une AWS CDI sortie avec les attributs suivants :

   - 2 interfaces Amazon VPC, 1 EFA (Elastic Fabric Adapter) et 1 ENA (Elastic Network Adapter)
   - 1 flux vidéo, 1 flux audio et 1 flux de données auxiliaire

```
{
    "Name": "AwardsShow",

    "MediaStreams": [
        {
            "Attributes": {
                "Fmtp": {
                    "Colorimetry": "BT709",
                    "ExactFramerate": "60000/1001",
                    "Par": "1:1",
                    "Range": "NARROW",
                    "ScanMode": "progressive",
                    "Tcs": "SDR"
                }
            },
            "ClockRate": 90000,
            "MediaStreamId": 0,
            "MediaStreamName": "video-stream",
            "MediaStreamType": "video",
            "VideoFormat": "1080p"
        },
        {
            "Attributes": {
```

```
                "Fmtp": {
                    "ChannelOrder": "SMPTE2110.(ST)"
                }
            },
            "ClockRate": 48000,
            "MediaStreamId": 1,
            "MediaStreamName": "audio-stream",
            "MediaStreamType": "audio"
        },
        {
            "ClockRate": 90000,
            "MediaStreamId": 2,
            "MediaStreamName": "anc-stream",
            "MediaStreamType": "ancillary-data"
        }
    ],

    "Outputs": [
        {
            "Name": "cdi-output",
            "Protocol": "cdi",
            "Description": "cdi-output to medialive",
            "Destination": "198.51.100.5",
            "MediaStreamOutputConfigurations": [
                {
                    "EncodingName": "raw",
                    "MediaStreamName": "video-stream"
                },
                {
                    "EncodingName": "pcm",
                    "MediaStreamName": "audio-stream"
                }
            ],
            "Port": 5000,
            "VpcInterfaceAttachment": {
                "VpcInterfaceName": "efa-name"
            }
        }
    ],

    "Source": {
        "Name": "jxs-input",
        "Protocol": "st2110-jpegxs",
        "Description": "jxs-input to cdi-output",
```

```
        "MaxSyncBuffer": 100,
        "MediaStreamSourceConfigurations": [
            {
                "EncodingName": "jxsv",
                "InputConfigurations": [
                    {
                        "InputPort": 5011,
                        "Interface": {
                            "Name": "efa-name"
                        }
                    },
                    {
                        "InputPort": 5011,
                        "Interface": {
                            "Name": "ena-name"
                        }
                    }
                ],
                "MediaStreamName": "video-stream"
            },
            {
                "EncodingName": "pcm",
                "InputConfigurations": [
                    {
                        "InputPort": 5001,
                        "Interface": {
                            "Name": "efa-name"
                        }
                    },
                    {
                        "InputPort": 5001,
                        "Interface": {
                            "Name": "ena-name"
                        }
                    }
                ],
                "MediaStreamName": "audio-stream"
            }
        ]
    },

    "VpcInterfaces": [
        {
            "Name": "efa-name",
```

```
            "NetworkInterfaceType": "efa",
            "RoleArn": "arn:aws:iam::111122223333:role/MediaConnectAccessRole",
            "SecurityGroupIds": [
                "sg-1234567890abcdef0"
            ],
            "SubnetId": "subnet-abcdef01234567890"
        },
        {
            "Name": "ena-name",
            "NetworkInterfaceType": "ena",
            "RoleArn": "arn:aws:iam::111122223333:role/MediaConnectAccessRole",
            "SecurityGroupIds": [
                "sg-1234567890abcdef0"
            ],
            "SubnetId": "subnet-abcdef01234567890"
        }
    ]
}
```

2. Dans le AWS CLI, utilisez la `create-flow` commande.

```
aws mediaconnect create-flow --cli-input-json file://filename.json --
profile YourProfile
```

L'exemple suivant illustre la valeur de retour :

```
{
    "Flow": {
        "AvailabilityZone": "us-west-2a",
        "Description": "jxs-input to cdi-output",
        "EgressIp": "203.0.113.0",
        "Entitlements": [],
        "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
DwtfUlYOUVABAQNR-c94d84ce4215:AwardsShow",
        "MediaStreams": [
            {
                "Attributes": {
                    "Fmtp": {
                        "Colorimetry": "BT709",
                        "ExactFramerate": "60000/1001",
                        "Par": "1:1",
                        "Range": "NARROW",
                        "ScanMode": "progressive",
```

```
                    "Tcs": "SDR"
                }
            },
            "ClockRate": 90000,
            "Fmt": 96,
            "MediaStreamId": 0,
            "MediaStreamName": "video-stream",
            "MediaStreamType": "video",
            "VideoFormat": "1080p"
        },
        {
            "Attributes": {
                "Fmtp": {
                    "ChannelOrder": "SMPTE2110.(ST)"
                }
            },
            "ClockRate": 48000,
            "Fmt": 97,
            "MediaStreamId": 1,
            "MediaStreamName": "audio-stream",
            "MediaStreamType": "audio"
        },
        {
            "ClockRate": 90000,
            "Fmt": 98,
            "MediaStreamId": 2,
            "MediaStreamName": "anc-stream",
            "MediaStreamType": "ancillary-data"
        }
    ],
    "Name": "AwardsShow",
    "Outputs": [
        {
            "Description": "cdi-output to medialive",
            "Destination": "198.51.100.5",
            "MediaStreamOutputConfigurations": [
                {
                    "EncodingName": "raw",
                    "MediaStreamName": "video-stream"
                },
                {
                    "EncodingName": "pcm",
                    "MediaStreamName": "audio-stream"
                }
```

```
                ],
                "Name": "cdi-output",
                "OutputArn": "arn:aws:mediaconnect:us-west-2:111122223333:output:1-
DwtfUlYOUVABAQNR-c94d84ce4215:cdi-output",
                "Port": 5000,
                "Transport": {
                    "Protocol": "cdi"
                },
                "VpcInterfaceAttachment": {
                    "VpcInterfaceName": "efa-name"
                }
            }
        ],
        "Source": {
            "Description": "jxs-input to cdi-output",
            "MediaStreamSourceConfigurations": [
                {
                    "EncodingName": "jxs-input",
                    "InputConfigurations": [
                        {
                            "InputIp": "203.0.113.1",
                            "InputPort": 5011,
                            "Interface": {
                                "Name": "efa-name"
                            }
                        },
                        {
                            "InputIp": "203.0.113.2",
                            "InputPort": 5011,
                            "Interface": {
                                "Name": "ena-name"
                            }
                        }
                    ],
                    "MediaStreamName": "video-stream"
                },
                {
                    "EncodingName": "pcm",
                    "InputConfigurations": [
                        {
                            "InputIp": "203.0.113.3",
                            "InputPort": 5001,
                            "Interface": {
                                "Name": "efa-name"
```

```
                        }
                    },
                    {
                        "InputIp": "203.0.113.4",
                        "InputPort": 5001,
                        "Interface": {
                            "Name": "ena-name"
                        }
                    }
                ],
                "MediaStreamName": "audio-stream"
            }
        ],
        "Name": "jxs-input",
        "SourceArn": "arn:aws:mediaconnect:us-west-2:111122223333:source:1-
DwtfUlYOUVABAQNR-c94d84ce4215:jxs-input",
        "Transport": {
            "MaxSyncBuffer": 100,
            "Protocol": "st2110-jpegxs"
        }
    },
    "Sources": [
        {
            "Description": "jxs-input to cdi-output",
            "MediaStreamSourceConfigurations": [
                {
                    "EncodingName": "jxsv",
                    "InputConfigurations": [
                        {
                            "InputIp": "203.0.113.173",
                            "InputPort": 5011,
                            "Interface": {
                                "Name": "efa-name"
                            }
                        },
                        {
                            "InputIp": "203.0.113.114",
                            "InputPort": 5011,
                            "Interface": {
                                "Name": "ena-name"
                            }
                        }
                    ],
                    "MediaStreamName": "video-stream"
```

```
                    },
                    {
                        "EncodingName": "pcm",
                        "InputConfigurations": [
                            {
                                "InputIp": "203.0.113.173",
                                "InputPort": 5001,
                                "Interface": {
                                    "Name": "efa-name"
                                }
                            },
                            {
                                "InputIp": "203.0.113.114",
                                "InputPort": 5001,
                                "Interface": {
                                    "Name": "ena-name"
                                }
                            }
                        ],
                        "MediaStreamName": "audio-stream"
                    }
                ],
                "Name": "jxs-input",
                "SourceArn": "arn:aws:mediaconnect:us-west-2:111122223333:source:1-
DwtfUlYOUVABAQNR-c94d84ce4215:jxs-input",
                "Transport": {
                    "MaxSyncBuffer": 100,
                    "Protocol": "st2110-jpegxs"
                }
            }
        ],
        "Status": "STANDBY",
        "VpcInterfaces": [
            {
                "Name": "efa-name",
                "NetworkInterfaceIds": [
                    "eni-0ae6ca9ea6673a2a7"
                ],
                "NetworkInterfaceType": "efa",
                "RoleArn": "arn:aws:iam::111122223333:role/MediaConnectAccessRole",
                "SecurityGroupIds": [
                    "sg-1234567890abcdef0"
                ],
                "SubnetId": "subnet-abcdef01234567890"
```

```
            },
            {
                "Name": "ena-name",
                "NetworkInterfaceIds": [
                    "eni-0cbabcf978eeb00a2"
                ],
                "NetworkInterfaceType": "ena",
                "RoleArn": "arn:aws:iam::111122223333:role/MediaConnectAccessRole",
                "SecurityGroupIds": [
                    "sg-1234567890abcdef0"
                ],
                "SubnetId": "subnet-abcdef01234567890"
            }
        ]
    }
}
```

Afficher une liste de flux

Vous pouvez consulter la liste de vos MediaConnect flux AWS Elemental dans une région spécifique AWS .

Pour afficher la liste des flux (console)

- Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.

  La page Flux apparaît, répertoriant tous les flux associés à votre compte.

Pour afficher la liste des flux (AWS CLI)

- Dans le AWS CLI, utilisez la `list-flows` commande :

  ```
  aws mediaconnect list-flows --profile PMprofile
  ```

  L'exemple suivant illustre la valeur de retour :

  ```
  {
    "Flows": [
      {
        "AvailabilityZone": "us-west-2a",
  ```

```
      "Description": "Temporary listed flow description",
      "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
      "Name": "BasketballGame",
      "SourceType": "OWNED",
      "Status": "STOPPING"
    },
    {
      "AvailabilityZone": "us-west-2d",
      "Description": "Temporary listed flow description",
      "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:2-3aBC45dEF67hiJ8k-2AbC34DE5fGa6:AwardsShow",
      "Name": "AwardsShow",
      "SourceType": "OWNED",
      "Status": "STANDBY"
    }
  ]
}
```

Afficher les détails d'un flux

Vous pouvez consulter les détails d'un flux, tels que l'ARN, la zone de disponibilité, le statut, la source, les droits et les sorties.

Pour afficher les détails d'un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux que vous souhaitez afficher.

   La page de détails de ce flux apparaît. Cette page comprend les onglets suivants :

   - L'onglet Source affiche des détails sur la source de ce flux, notamment une indication indiquant si le flux est connecté à la source.
   - L'onglet Sorties affiche les détails de chaque sortie que vous avez créée pour ce flux.
   - L'onglet Droits affiche tous les droits que vous avez accordés dans le cadre de ce flux.
   - L'onglet Interfaces VPC affiche une liste des connexions de ce flux avec les clouds privés virtuels (VPC) basés sur le service Amazon Virtual Private Cloud (Amazon VPC).

- L'onglet Flux multimédia affiche la liste des flux multimédias créés sur ce flux. Chaque flux multimédia représente un composant différent d'une vidéo, tel que la vidéo, l'audio ou les données auxiliaires.
- L'onglet Alertes affiche un journal des alertes actives sur ce flux.

Pour afficher les détails d'un flux (AWS CLI)

- Dans le AWS CLI, utilisez la `describe-flow` commande :

```
aws mediaconnect describe-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow
```

L'exemple suivant illustre la valeur de retour :

```
{
    "Flow": {
        "EgressIp": "54.201.4.39",
        "AvailabilityZone": "us-east-1b",
        "Status": "ACTIVE",
        "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow",
        "Entitlements": [
            {
                "EntitlementArn": "arn:aws:mediaconnect:us-
east-1:111122223333:entitlement:1-AaBb11CcDd22EeFf-34DE5fG12AbC:MyEntitlement",
                "Description": "Assign to this account",
                "Name": "MyEntitlement",
                "Subscribers": [
                    "444455556666"
                ]
            }
        ],
        "Description": "NYC awards show",
        "Name": "AwardsShow",
        "Outputs": [
            {
                "Port": 2355,
                "Name": "NYC",
                "Transport": {
                    "SmoothingLatency": 0,
                    "Protocol": "rtp-fec"
```

```
                },
                "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYC",
                "Destination": "192.0.2.0"
            },
            {
                "Port": 3025,
                "Name": "LA",
                "Transport": {
                    "SmoothingLatency": 0,
                    "Protocol": "rtp-fec"
                },
                "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-987655dEF67hiJ89-c34de5fG678h:LA",
                "Destination": "192.0.2.0"
            }
        ],
        "Source": {
            "IngestIp": "54.201.4.39",
            "SourceArn": "arn:aws:mediaconnect:us-
east-1:111122223333:source:3-4aBC56dEF78hiJ90-4de5fG6Hi78Jk:ShowSource",
            "Transport": {
                "MaxBitrate": 80000000,
                "Protocol": "rtp"
            },
            "IngestPort": 1069,
            "Description": "Saturday night show",
            "Name": "ShowSource",
            "WhitelistCidr": "10.24.34.0/23"
        }
    }
}
```

Démarrer un flux

Après avoir créé un flux, vous devez le démarrer. Vous pouvez également arrêter et redémarrer un flux à tout moment.

Pour démarrer un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.

2. Sur la page Flux, choisissez le nom du flux que vous souhaitez démarrer.

   La page de détails de ce flux apparaît.

3. Sélectionnez Démarrer.

Pour démarrer un flux (AWS CLI)

- Dans le AWS CLI, utilisez la `start-flow` commande :

```
aws mediaconnect start-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame --
profile PMprofile
```

L'exemple suivant illustre la valeur de retour :

```
{
  "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
  "Status": "STARTING"
}
```

Arrêter un flux

Lorsque vous arrêtez un flux actif, il devient immédiatement indisponible pour les clients qui accèdent à la sortie directement depuis votre MediaConnect flux AWS Elemental ou via un droit. Si vous souhaitez supprimer un flux actif, vous devez d'abord l'arrêter avant de pouvoir le supprimer.

Pour arrêter un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux que vous souhaitez arrêter.

   La page de détails de ce flux apparaît.

3. Choisissez Arrêter.

   L'état du flux passe à Standby. Le flux s'arrête immédiatement et n'est plus visible pour les clients qui accèdent au résultat directement depuis votre MediaConnect flux ou via un droit.

Pour arrêter un flux (AWS CLI)

- Dans le AWS CLI, utilisez la `stop-flow` commande :

```
aws mediaconnect stop-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame --
profile PMprofile
```

L'exemple suivant illustre la valeur de retour :

```
{
  "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
  "Status": "STOPPING"
}
```

Mettre à jour un flux

Vous pouvez modifier la source, les droits et les sorties d'un flux même si le flux est en cours d'exécution. Toutefois, vous ne pouvez pas modifier le nom, l'ARN ou la zone de disponibilité du flux. Pour plus d'informations, consultez les rubriques suivantes :

- Gestion des balises dans un flux
- Mettre à jour la source
- Mise à jour des sorties
- Mise à jour des flux multimédias
- Mise à jour des droits
- Ajouter une interface VPC à un flux

Gestion des balises dans un flux

Vous pouvez utiliser des balises pour suivre la facturation et l'organisation de vos MediaConnect flux, sources, sorties et droits AWS Elemental. Ce sont les mêmes étiquettes qui AWS Billing and Cost Management permettent d'organiser votre AWS facture. Pour plus d'informations sur l'utilisation des balises pour la répartition des coûts, voir Utiliser les balises de répartition des coûts pour les rapports de facturation personnalisés dans le guide de AWS Billing l'utilisateur.

Pour ajouter des balises à un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux auquel vous souhaitez ajouter des balises.

   La page de détails de ce flux apparaît.
3. Dans la section Détails, choisissez Gérer les balises.
4. Choisissez Gérer les balises, puis Ajouter une étiquette.
5. Pour chaque balise que vous souhaitez ajouter, procédez comme suit :

   a. Saisissez une clé et une valeur. Par exemple, votre clé peut être **`sports`** et votre valeur peut être**`golf`**.

   b. Choisissez Ajouter une balise.
6. Choisissez Mettre à jour.

Pour modifier les balises d'un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux contenant les balises que vous souhaitez modifier.

   La page de détails de ce flux apparaît.
3. Dans la section Détails, choisissez Gérer les balises.
4. Choisissez Gérer les balises.
5. Mettez à jour les balises, le cas échéant.
6. Choisissez Mettre à jour.

Pour supprimer des balises d'un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux auquel vous souhaitez ajouter des balises.

   La page de détails de ce flux apparaît.
3. Dans la section Détails, choisissez Gérer les balises.
4. Choisissez Gérer les balises.
5. Choisissez Supprimer le tag à côté de chaque tag que vous souhaitez supprimer.

6. Choisissez Mettre à jour.

Supprimer un flux

Lorsque vous supprimez un flux actif, il devient immédiatement indisponible pour les clients qui accèdent au résultat directement depuis votre MediaConnect flux AWS Elemental ou via un droit. Une fois que vous avez supprimé un flux, vous ne pouvez pas le récupérer.

Si le flux est actif, vous devez l'arrêter avant de pouvoir le supprimer.

Pour supprimer un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux que vous souhaitez supprimer.

   La page de détails de ce flux apparaît.
3. Vérifiez le champ État pour vérifier que le flux est en mode veille.
4. Si le statut du flux est Actif, choisissez Stop.
5. Sélectionnez Delete (Supprimer).

   Un message de confirmation s'affiche.
6. Choisissez Supprimer le flux.

   Le flux n'est plus visible pour les clients qui accèdent au résultat directement depuis votre MediaConnect flux ou via un droit. La suppression complète du flux peut prendre jusqu'à cinq minutes.

Pour supprimer un flux (AWS CLI)

- Dans le AWS CLI, utilisez la `delete-flow` commande :

```
aws mediaconnect delete-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame --
profile PMprofile
```

L'exemple suivant illustre la valeur de retour :

```
{
```

```
  "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
  "Status": "DELETING"
}
```

Sources dans AWS Elemental MediaConnect

Une source d' MediaConnect entrée peut être tout élément fournissant un flux vidéo en direct, comme ce qui suit :

- Un encodeur sur site
- Un autre flux AWS Elemental MediaConnect
- Une AWS Elemental MediaLive sortie
- Un système de diffusion (basé sur le cloud ou sur site)

Pour obtenir la liste des protocoles pris en charge que vous pouvez utiliser pour votre source, consultezProtocoles.

Depuis la MediaConnect console, vous pouvez consulter CloudWatch les métriques Amazon pour surveiller l'état de santé de la source d'un flux actif.

Rubriques

- Ajouter une source à un flux existant
- Mettre à jour la source d'un flux
- Basculement à la source
- Gestion des balises sur une source
- Supprimer une source d'un flux
- Ports source

Ajouter une source à un flux existant

Pour les flux de transport, vous pouvez ajouter une deuxième source de basculement. Les deux sources du flux doivent utiliser le même protocole. (Cependant, vous pouvez avoir une source qui utilise le RTP et l'autre qui utilise le RTP-FEC.) Pour plus d'informations sur le basculement de source, consultezBasculement à la source.

La méthode que vous utilisez pour ajouter une deuxième source à un flux dépend du type de source que vous souhaitez utiliser :

- Source standard — Utilise du contenu provenant de toute source autre qu'une source VPC ou une source autorisée.
- Source VPC — Utilise le contenu provenant d'un VPC que vous configurez.

MediaConnect ne prend pas en charge deux sources sur les flux autorisés ou sur les flux CDI. Pour la redondance avec les sources ST 2110 JPEG XS, vous pouvez spécifier deux interfaces VPC entrantes sur un flux multimédia individuel. Pour assurer la redondance avec les sources CDI, créez un second flux.

Depuis la MediaConnect console, vous pouvez consulter CloudWatch les métriques Amazon pour surveiller l'état de santé de la source d'un flux actif.

Ajouter une source standard à un flux existant

Vous pouvez ajouter une seconde source à un flux existant pour le basculement. Les deux sources du flux doivent utiliser le même protocole. (Cependant, vous pouvez avoir une source qui utilise le RTP et l'autre qui utilise le RTP-FEC.) Pour plus d'informations sur le basculement de source, consultezBasculement à la source.

Pour ajouter une source standard à un flux existant (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux que vous souhaitez mettre à jour.
3. Choisissez l'onglet Source.
4. Dans la section Configuration du basculement de la source, choisissez Modifier.
5. Dans la fenêtre Modifier la configuration du basculement de source, assurez-vous que le basculement est défini sur Active.

   > **Note**
   >
   > Si vous activez le basculement sur un flux en cours d'exécution, vous risquez de rencontrer une brève interruption de la sortie du flux.

6. Dans le menu déroulant du mode Failover, sélectionnez le mode à utiliser avec votre protocole source. Pour obtenir la liste des modes pris en charge par chaque protocole, voir Prise en charge du basculement pour les protocoles sources

7. Pour la fenêtre de restauration, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une mémoire tampon plus grande signifie un délai plus long dans la transmission du flux, mais plus de place pour la correction des erreurs. Une mémoire tampon plus petite signifie un délai plus court, mais moins de place pour la correction des erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 200 ms.
8. Choisissez Mettre à jour.
9. Dans la section Sources, choisissez Ajouter.
10. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console.
11. Pour Type de source, choisissez Source standard.
12. Déterminez le protocole utilisé par votre source.

> **Note**
>
> Toutes les sources d'un flux doivent utiliser le même protocole. Cependant, vous pouvez avoir une source qui utilise le RTP et l'autre qui utilise le RTP-FEC.

13. Pour obtenir des instructions spécifiques en fonction de votre protocole, sélectionnez l'un des onglets suivants :

    RIST

    1. Pour Protocole, choisissez RIST.
    2. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.

       > **Note**
       >
       > Le protocole RIST nécessite un port supplémentaire pour la correction des erreurs. Pour répondre à cette exigence, MediaConnect réserve le port égal à +1 par rapport au port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000 et 4001.

    3. Pour Allowlist CIDR, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

> **Important**
>
> Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

4. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
5. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 1 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

RTP or RTP-FEC

1. Pour Protocole, choisissez RTP ou RTP-FEC.
2. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.

> **Note**
>
> Le protocole RTP-FEC nécessite deux ports supplémentaires pour corriger les erreurs. Pour répondre à cette exigence, MediaConnect réserve les ports +2 et +4 à partir du port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000, 4002 et 4004.

3. Pour Allowlist CIDR, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

> **Important**
>
> Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

4. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.

SRT listener

1. Pour Protocol, choisissez SRT listener.
2. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
3. Pour le bloc CIDR Allowlist, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

> **Important**
>
> Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

4. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.
5. Pour Adresse de l'écouteur source, entrez l'adresse que MediaConnect vous utiliserez pour la connexion SRT. L'adresse peut être une adresse IP ou un nom de domaine.
6. Pour Débit maximal (facultatif), spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
7. Pour Latence minimale, spécifiez la taille minimale de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger

les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.

8. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
   a. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   b. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

SRT caller

1. Pour Protocol, choisissez SRT Caller.
2. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
3. Pour Adresse de l'écouteur source, entrez l'adresse que MediaConnect vous utiliserez pour la connexion SRT. L'adresse peut être une adresse IP ou un nom de domaine.
4. Pour le port de l'écouteur source, entrez le port MediaConnect qui sera utilisé pour la connexion SRT.
5. Pour Débit maximal (facultatif), spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.

6. Pour Latence minimale, spécifiez la taille minimale de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

   Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.
7. Pour Stream ID (facultatif), entrez un identifiant pour le flux. Cet identifiant peut être utilisé pour communiquer des informations sur le flux.
8. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
   a. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   b. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

Zixi push

1. Pour Protocole, choisissez Zixi push.

   AWS Elemental MediaConnect renseigne la valeur du port entrant.
2. Pour Allowlist CIDR, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

> **Important**
>
> Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

3. Pour Stream ID, spécifiez l'ID de flux défini dans le chargeur Zixi.

> **Important**
>
> L'ID du flux doit correspondre à la valeur définie dans le chargeur Zixi. Si vous laissez ce champ vide, MediaConnect utilise le nom de la source comme identifiant du flux. Si l'ID du flux n'est pas exactement le même que le nom de la source, vous devez le saisir manuellement.

4. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 0 et 60 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 6 000 ms.
5. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
   a. Pour le type de déchiffrement, choisissez Clé statique.
   b. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   c. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.
   d. Pour Algorithme de déchiffrement, choisissez le type de chiffrement utilisé pour chiffrer la source.

Zixi push for AWS Elemental Link UHD device

Après avoir créé la source push Zixi supplémentaire, vous devez configurer l' AWS Elemental Link appareil à l'aide de. MediaLive Consultez les instructions de MediaLive configuration suivantes pour terminer le processus une fois que vous avez créé la source : Utilisation d'un appareil dans un flux dans le guide de MediaLive l'utilisateur. Assurez-vous d'avoir accès aux deux MediaConnect et MediaLive de suivre ces étapes.

> **Note**
>
> Zixi Push pour appareils AWS Elemental Link UHD ne prend en charge que le mode failover. Le mode Fusion n'est pas pris en charge.

1. Pour Protocole, choisissez Zixi push.

   AWS Elemental MediaConnect renseigne la valeur du port entrant.

2. Pour Allowlist CIDR, spécifiez une plage d'adresses IP autorisées à contribuer au contenu de votre source. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

   > **Important**
   >
   > Si vous connaissez la plage d'adresses IP publiques que votre appareil Link utilise pour se connecter à Internet, entrez ce bloc CIDR. Notez qu'il ne s'agit pas de l'adresse IP de l'appareil AWS Elemental Link. Si vous ne pouvez pas obtenir ces informations, il est possible de configurer le bloc CIDR pour qu'il soit ouvert à toutes les adresses IP possibles en utilisant 0.0.0.0/0. Généralement, il n'est pas recommandé d'attribuer un bloc CIDR ouvert à l'ensemble d'Internet (0.0.0.0/0). Toutefois, si cette méthode doit être utilisée, les données transférées sont cryptées à l'aide du cryptage AES-128.

3. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger

les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 0 et 60 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 6 000 ms. La valeur de latence maximale doit correspondre à la valeur de latence configurée sur l' AWS Elemental Link appareil. Pour plus d'informations sur la configuration de la latence de l'appareil Link, voir : Configuration de l'appareil dans le guide de AWS Elemental MediaLive l'utilisateur

4. Pour le déchiffrement, choisissez Activer et procédez comme suit :
   a. Pour le type de déchiffrement, choisissez Clé statique.
   b. Pour Algorithme de déchiffrement, choisissez AES-128. AWS Elemental Link nécessite AES-128, ne sélectionnez pas un autre algorithme.
   c. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   d. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

14. Choisissez Enregistrer.

Ajouter une source VPC à un flux existant

Vous pouvez ajouter une seconde source à un flux de transport existant à des fins de basculement. Les deux sources du flux doivent être identiques sur le plan binaire (elles proviennent du même encodeur) et elles doivent utiliser le même protocole. (Cependant, vous pouvez avoir une source qui utilise le RTP et l'autre qui utilise le RTP-FEC.) Pour plus d'informations sur le basculement de source, consultezBasculement à la source.

Important

Avant de commencer cette procédure, assurez-vous que les étapes suivantes ont été effectuées :

- Dans Amazon VPC, configurez votre VPC et les groupes de sécurité associés. Pour plus d'informations sur les VPC, consultez le Guide de l'utilisateur Amazon VPC. Pour plus d'informations sur la configuration des groupes de sécurité pour qu'ils fonctionnent avec votre interface VPC, consultez. Considérations relatives aux groupes de sécurité
- Dans IAM, configurez-le en MediaConnect tant que service de confiance.

- Si la source de votre flux nécessite un chiffrement, configurez le chiffrement.

MediaConnect ne prend pas en charge deux sources sur les flux CDI. Pour la redondance avec les sources ST 2110 JPEG XS, vous pouvez spécifier deux interfaces VPC entrantes sur un flux multimédia individuel. Pour assurer la redondance avec les sources CDI, créez un second flux.

Pour ajouter une source VPC à un flux existant (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux que vous souhaitez mettre à jour.
3. Choisissez l'onglet Source.
4. Dans la section Configuration du basculement de la source, choisissez Modifier.
5. Dans la fenêtre Modifier la configuration du basculement de source, assurez-vous que le basculement est défini sur Activé.

   > **Note**
   >
   > Si vous activez le basculement sur un flux en cours d'exécution, vous risquez de rencontrer une brève interruption de la sortie du flux.

6. Pour la fenêtre de restauration, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une mémoire tampon plus grande signifie un délai plus long dans la transmission du flux, mais plus de place pour la correction des erreurs. Une mémoire tampon plus petite signifie un délai plus court, mais moins de place pour la correction des erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 200 ms.
7. Choisissez Mettre à jour.
8. Dans la section Sources, choisissez Ajouter une source.
9. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console.
10. Pour Type de source, choisissez la source VPC.
11. Déterminez le protocole utilisé par votre source.

> **Note**
>
> Toutes les sources d'un flux doivent utiliser le même protocole. Cependant, vous pouvez avoir une source qui utilise le RTP et l'autre qui utilise le RTP-FEC.

12. Pour obtenir des instructions spécifiques en fonction de votre protocole, sélectionnez l'un des onglets suivants :

    RIST

    1. Pour le protocole, RIST sera automatiquement sélectionné.
    2. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.

       > **Note**
       >
       > Le protocole RIST nécessite un port supplémentaire pour la correction des erreurs. Pour répondre à cette exigence, MediaConnect réserve le port égal à +1 par rapport au port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000 et 4001.

    3. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
    4. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
    5. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 1 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

    RTP or RTP-FEC

    1. Pour Protocole, choisissez RTP ou RTP-FEC.
    2. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.

> **Note**
>
> Le protocole RTP-FEC nécessite deux ports supplémentaires pour corriger les erreurs. Pour répondre à cette exigence, MediaConnect réserve les ports +2 et +4 à partir du port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000, 4002 et 4004.

3. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
4. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.

SRT listener

1. Pour le protocole, l'écouteur SRT sera automatiquement sélectionné.
2. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
3. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
4. Pour le port entrant, spécifiez le port sur lequel le flux écoute le contenu entrant.
5. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
6. Pour Latence minimale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 2 000 ms.

   Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un.

`Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.

7. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
   a. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   b. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

SRT caller

1. Pour le protocole, l'appelant SRT sera automatiquement sélectionné.
2. Dans Description de la source, entrez une description qui vous rappellera ultérieurement d'où provient cette source. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
3. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
4. Pour le port de l'écouteur source, entrez le port MediaConnect qui sera utilisé pour la connexion SRT.
5. Pour Adresse de l'écouteur source, entrez l'adresse que MediaConnect vous utiliserez pour la connexion SRT. L'adresse peut être une adresse IP ou un nom de domaine.
6. Pour Débit maximal, spécifiez le débit maximal attendu (en bits par seconde) pour le flux. Nous vous recommandons de spécifier une valeur deux fois supérieure au débit réel.
7. Pour Latence minimale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 2 000 ms.

Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.

8. Pour Stream ID (facultatif), entrez un identifiant pour le flux. Cet identifiant peut être utilisé pour communiquer des informations sur le flux.
9. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
   a. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   b. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.

Zixi push

1. Pour le protocole, Zixi push sera automatiquement sélectionné.

   AWS Elemental MediaConnect renseigne la valeur du port entrant.
2. Pour le nom de l'interface VPC, choisissez le nom de l'interface VPC que vous souhaitez utiliser comme source.
3. Pour Stream ID, spécifiez l'ID de flux défini dans le chargeur Zixi.

> **Important**
>
> L'ID du flux doit correspondre à la valeur définie dans le chargeur Zixi. Si vous laissez ce champ vide, MediaConnect utilise le nom de la source comme identifiant du flux. Si l'ID du flux n'est pas exactement le même que le nom de la source, vous devez le saisir manuellement.

4. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 0 et 60 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 6 000 ms.
5. Si la source est chiffrée, choisissez Activer dans la section Déchiffrement et procédez comme suit :
   a. Pour le type de déchiffrement, choisissez Clé statique.
   b. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   c. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.
   d. Pour Algorithme de déchiffrement, choisissez le type de chiffrement utilisé pour chiffrer la source.

13. Choisissez Enregistrer.

Mettre à jour la source d'un flux

Vous pouvez mettre à jour la source d'un flux existant, même si le flux est en cours d'exécution.

Pour mettre à jour la source d'un flux existant (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux que vous souhaitez mettre à jour.
3. Choisissez l'onglet Source.
4. Choisissez la source que vous souhaitez mettre à jour.
5. Choisissez Mettre à jour.
6. Apportez les modifications appropriées, puis choisissez la source de mise à jour.

Pour mettre à jour la source d'un flux existant (AWS CLI)

- Dans le AWS CLI, utilisez la update-flow-source commande :

```
aws mediaconnect update-flow-source --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow --source-
arn arn:aws:mediaconnect:us-east-1:111122223333:source:2-3aBC45dEF67hiJ89-
c34de5fG678h:AwardsShowSource --allowlist-cidr 10.24.34.0/24 --profile PMprofile
```

L'exemple suivant illustre la valeur de retour :

Basculement à la source

Le basculement de source est une configuration qui implique deux sources redondantes pour un flux de transport. Cette redondance permet de minimiser les perturbations de votre flux vidéo. Pour utiliser le basculement de source, vous spécifiez deux sources pour le flux, puis vous choisissez l'une des deux options pour le mode de basculement : Merge ou Failover.

- Le mode Fusion combine les sources en un seul flux, ce qui permet une restauration progressive après toute perte d'une source unique. Si vous définissez le mode de basculement sur Merge, vous pouvez définir la fenêtre de restauration, qui correspond à la taille de la mémoire tampon (délai) que vous MediaConnect souhaitez conserver. Une fenêtre de restauration plus longue signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une fenêtre de restauration plus courte signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Les sources utilisées de cette manière doivent être identiques sur le plan binaire, ce qui signifie qu'elles doivent provenir du même encodeur. MediaConnect doit également recevoir du contenu provenant des deux sources en même temps. De plus, si les sources utilisent le protocole RTP, elles doivent avoir des en-têtes RTP avec des numéros de séquence alignés et elles doivent également être conformes à la norme SMPTE ST

  > **Note**
  >
  > La norme SMPTE ST ÷ 7 est une norme développée par le groupe Society of Motion Picture and Television Engineers (SMPTE). La norme ST 4—7 définit une méthode qui remplace les paquets manquants par des paquets dans un flux identique et redondant. Ce type de basculement nécessite un petit tampon de latence dans votre flux de travail afin de laisser le temps de MediaConnect récupérer les paquets des deux flux.

- Le mode failover permet de basculer entre un flux principal et un flux de secours. Cette commutation facilite la transition vers un flux plus fiable. Si vous définissez le mode de

basculement sur Failover, vous pouvez spécifier une source comme source principale. La deuxième source sert de sauvegarde. Si vous ne spécifiez pas de source principale, MediaConnect traitez les deux sources avec la même priorité et basculez vers la source disponible selon les besoins.

MediaConnect utilise les deux modes de basculement de la manière suivante :

- En mode Fusion, MediaConnect utilise le contenu des deux sources. Le flux sélectionne de manière aléatoire l'une des sources pour commencer. S'il manque un paquet à cette source, le flux extrait le paquet manquant de l'autre source. Par exemple, si le flux utilise la source A et que le paquet 123 est absent, il MediaConnect extrait le paquet 123 de la source B et continue à utiliser la source A. Dans ce mode, les deux sources sont identiques sur le plan binaire/conformes à ST et 7.
- En mode Failover, si vous ne spécifiez pas de source principale, utilise MediaConnect aléatoirement l'une des sources pour fournir le contenu du flux. S'il MediaConnect ne reçoit pas de données de la source pendant 500 millisecondes, le flux passe à l'autre source et peut continuer à passer d'une source à l'autre selon les besoins. Si vous spécifiez une source principale, MediaConnect utilisez cette source pour fournir le contenu du flux. Le flux passe à l'autre source si la source principale n'envoie pas de données pendant 500 millisecondes, et revient à la source principale dès que les données sont renvoyées.

> **Note**
>
> MediaConnect ne prend pas en charge le basculement de source sur les flux CDI ou sur les flux d'autorisations. Pour plus d'informations sur la création de redondance avec les flux CDI, rendez-vous sur :. Création d'un flux CDI De plus, vous ne pouvez pas ajouter une seconde source à un flux existant pour le basculement si vous utilisez les protocoles Zixi Pull ou Fujitsu-QOS.

Prise en charge du basculement pour les protocoles sources

Le tableau suivant décrit les protocoles source qui prennent en charge le basculement.

Protocole	Ce protocole prend-il en charge le basculement de source ?	Combien de sources peut-on ajouter ?	Modes de basculement pris en charge
POIGNET	Oui	2	Fusion ou basculement
RTP	Oui	2	Fusion ou basculement
RTP-FEC	Oui	2	Fusion ou basculement
écouteur SRT	Oui	2	Failover uniquement
appelant SRT	Oui	2	Failover uniquement
Pull Zixi	Non	Aucune - Le Zixi Pull ne peut pas être utilisé comme source.	Le basculement de source n'est pas pris en charge
Zixi Push	Oui	2	Fusion ou basculement
Zixi Push pour l'UHD AWS Elemental Link	Oui	2	Failover uniquement
Fujitsu QoS	Non	1	Le basculement de source n'est pas pris en charge
CDI	Non	1	Le basculement de source n'est pas pris en charge
ST 2110 JPEG XS	Non	1	Le basculement de source n'est pas pris en charge

Protocole	Ce protocole prend-il en charge le basculement de source ?	Combien de sources peut-on ajouter ?	Modes de basculement pris en charge
Flux de droits	Non	1	Le basculement de source n'est pas pris en charge

Gestion des balises sur une source

Vous pouvez utiliser des balises pour suivre la facturation et l'organisation de vos MediaConnect flux, sources, sorties et droits AWS Elemental. Ce sont les mêmes étiquettes qui AWS Billing and Cost Management permettent d'organiser votre AWS facture. Pour plus d'informations sur l'utilisation des balises pour la répartition des coûts, voir Utiliser les balises de répartition des coûts pour les rapports de facturation personnalisés dans le guide de AWS Billing l'utilisateur.

Pour ajouter des balises à une source (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé à la source à laquelle vous souhaitez ajouter des balises.
3. Choisissez l'onglet Sources.

   La liste des sources de ce flux s'affiche.
4. Choisissez la source à laquelle vous souhaitez ajouter des balises.
5. Choisissez Gérer les balises.
6. Choisissez à nouveau Gérer les balises, puis choisissez Ajouter une étiquette.
7. Pour chaque balise que vous souhaitez ajouter, procédez comme suit :

   a. Saisissez une clé et une valeur. Par exemple, votre clé peut être **`sports`** et votre valeur peut être**`golf`**.

   b. Choisissez Ajouter une balise.
8. Choisissez Mettre à jour.

Pour modifier les balises d'une source (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé à la source pour laquelle vous souhaitez modifier les balises.
3. Choisissez l'onglet Sources.

   La liste des sources de ce flux s'affiche.
4. Choisissez la source pour laquelle vous souhaitez modifier les balises.
5. Choisissez Gérer les balises.
6. Choisissez à nouveau Gérer les tags.
7. Mettez à jour les balises, le cas échéant.
8. Choisissez Mettre à jour.

Pour supprimer des balises d'une source (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé à la source dont vous souhaitez supprimer les balises.
3. Choisissez l'onglet Sources.

   La liste des sources de ce flux s'affiche.
4. Choisissez la source dont vous souhaitez supprimer les balises.
5. Choisissez Gérer les balises.
6. Choisissez à nouveau Gérer les tags.
7. Choisissez Supprimer le tag à côté de chaque tag que vous souhaitez supprimer.
8. Choisissez Mettre à jour.

Supprimer une source d'un flux

Si un flux possède plusieurs sources, vous pouvez supprimer l'une des sources même si le flux est en cours d'exécution.

Pour supprimer une source d'un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux.
3. Choisissez l'onglet Source.
4. Choisissez la source que vous souhaitez supprimer.
5. Sélectionnez Remove (Supprimer).

Ports source

Chaque source d'un flux doit utiliser un port différent (pour les exceptions, voir la note). Certains protocoles nécessitent des ports supplémentaires pour corriger les erreurs. Pour les sources qui utilisent ces protocoles, AWS Elemental réserve MediaConnect automatiquement les ports supplémentaires nécessaires. Tous les MediaConnect protocoles utilisent des ports UDP. Le tableau suivant répertorie les ports supplémentaires, le cas échéant, réservés par le service.

> **Important**
>
> Il existe une exception aux exigences de port pour les sources qui utilisent le protocole Zixi. Pour les sources Zixi standard, toutes les sources utilisent le port 2088. Pour les sources Zixi VPC, les sources utiliseront une plage de ports entrants comprise entre 2090 et 2099. La plage de ports 2090-2099 est réservée exclusivement aux sources Zixi VPC et ne peut pas être utilisée par un autre protocole source. Le port source du VPC Zixi est attribué MediaConnect lors de la création de la source.

Protocole	Ports nécessaires	Ports requis
CDI	Port	Port que vous spécifiez. Il s'agit du seul port nécessaire pour la source.
POIGNET	Port et port+1	Le port que vous spécifiez , plus un port supplémen taire. MediaConnectréserve automatiquement un port égal

Protocole	Ports nécessaires	Ports requis
		à +1 par rapport au port que vous avez spécifié. Par exemple, si vous spécifiez le port 3000 pour cette sortie, le service réserve également le port 3001.
RTP	Port	Port que vous spécifiez. Il s'agit du seul port nécessaire pour la sortie.
RTP-FEC	Port, port+2 et port+4	Le port que vous spécifiez, plus deux ports supplémen taires. MediaConnectréserve automatiquement les ports +2 et +4 à partir du port que vous avez spécifié. Par exemple, si vous spécifiez le port 2000 pour cette sortie, le service réserve également les ports 2002 et 2004 pour la correction des erreurs.
écouteur SRT	Port	Port que vous spécifiez. Il s'agit du seul port nécessaire pour la source.
appelant SRT	Port	Port que vous spécifiez. Il s'agit du seul port nécessaire pour la source.

Protocole	Ports nécessaires	Ports requis
Fujitsu QoS	Port et port+1	Le port que vous spécifiez , plus un port supplémen taire. MediaConnectréserve automatiquement un port égal à +1 par rapport au port que vous avez spécifié.
ST 2110 JPEG XS	Port	Port que vous spécifiez. Il s'agit du seul port nécessaire pour la source.
Zixi Push	Port	Pour les sources standard : utilise MediaConnect automatiquement le port 2088. Pour les sources VPC : attribue MediaConnect automatiquement un port compris entre 2090 et 2099 lors de la création de la source. La plage de ports 2090-2099 est réservée exclusivement aux sources Zixi VPC et ne peut pas être utilisée par un autre protocole source.

Sorties en MediaConnect

Les sorties sont les différentes destinations vers lesquelles vous MediaConnect souhaitez envoyer le contenu de votre flux. Vous pouvez ajouter et supprimer des sorties à tout moment, même lorsque le flux est actif. Ces sorties sont envoyées à l'adresse IP que vous spécifiez. Cette option est utile si vous avez l'intention d'envoyer votre contenu vers un encodeur local.

Pour les flux de transport, vous pouvez autoriser le partage de votre contenu avec un autre AWS compte (compte abonné). Lorsque l'abonné crée un flux en utilisant votre contenu comme source, AWS Elemental MediaConnect génère une sortie sur votre flux.

> **Note**
>
> Si vous désactivez un droit après que l'abonné a créé un flux basé sur ce droit, la sortie associée reste dans votre flux. Cette sortie continue à être prise en compte dans votre nombre maximum de sorties. Pour supprimer une sortie associée à un droit, révoquez le droit.

Rubriques

Ajouter des sorties à un flux

Pour les flux de transport, vous pouvez ajouter jusqu'à 50 sorties. Toutefois, pour des performances optimales, suivez les instructions fournies dansBonnes pratiques. Chaque sortie doit avoir un nom, un protocole, une adresse IP et un port.

> **Note**
>
> Si vous avez l'intention de définir un droit pour une sortie, ne créez pas la sortie. Accordez plutôt un droit. Lorsque l'abonné crée un flux en utilisant votre contenu comme source, le service crée une sortie sur votre flux.

La méthode que vous utilisez pour ajouter une sortie à un flux dépend du type de sortie que vous souhaitez ajouter :

- Sortie standard (flux de transport) : envoie du contenu compressé vers toute destination autre qu'un cloud privé virtuel (VPC) que vous avez configuré à l'aide d'Amazon Virtual Private Cloud.
- Sortie VPC (flux de transport) : envoie du contenu compressé à un VPC que vous avez configuré à l'aide d'Amazon Virtual Private Cloud.
- Sortie VPC (flux CDI) : envoie du contenu non compressé à un VPC que vous avez configuré à l'aide d'Amazon Virtual Private Cloud.

Ajouter des sorties standard à un flux

Pour les flux de transport, vous pouvez ajouter jusqu'à 50 sorties. Toutefois, pour des performances optimales, suivez les instructions fournies dansBonnes pratiques. Une sortie standard est envoyée à toute destination ne faisant pas partie d'un cloud privé virtuel (VPC) que vous avez créé à l'aide d'Amazon Virtual Private Cloud.

> **Note**
>
> Les flux CDI ne prennent pas en charge les sorties standard.

Pour ajouter une sortie standard à un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux auquel vous souhaitez ajouter une sortie.

   La page de détails de ce flux apparaît.
3. Choisissez l'onglet Outputs.
4. Choisissez Ajouter une sortie.

5. Dans Nom, spécifiez le nom de votre sortie. Cette valeur est un identifiant qui n'est visible que sur la MediaConnect console AWS Elemental et qui n'est pas visible pour l'utilisateur final.
6. Pour Type de sortie, choisissez Sortie standard.
7. Dans Description, entrez une description qui vous rappellera ultérieurement où va cette sortie. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
8. Déterminez le protocole que vous souhaitez utiliser pour la sortie.
9. Pour obtenir des instructions spécifiques en fonction du protocole que vous souhaitez utiliser, sélectionnez l'un des onglets suivants :

   RIST

   1. Pour Protocole, choisissez RIST.
   2. Pour l'adresse IP, choisissez l'adresse IP à laquelle vous souhaitez envoyer la sortie.
   3. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.

      > **Note**
      >
      > Le protocole RIST nécessite un port supplémentaire pour la correction des erreurs. Pour répondre à cette exigence, AWS Elemental MediaConnect réserve le port +1 à partir du port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000 et 4001.

   4. Pour lisser la latence, spécifiez le délai supplémentaire que vous souhaitez utiliser pour le lissage de sortie. Nous vous recommandons de spécifier une valeur de 0 ms pour désactiver le lissage. Toutefois, si le récepteur ne parvient pas à traiter le flux correctement, spécifiez une valeur comprise entre 100 et 1 000 ms. AWS Elemental MediaConnect tente ainsi de corriger l'instabilité provenant de la source du flux. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 0 ms.

   RTP or RTP-FEC

   1. Pour Protocole, choisissez RTP ou RTP-FEC.
   2. Pour l'adresse IP, choisissez l'adresse IP à laquelle vous souhaitez envoyer la sortie.
   3. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.

> **Note**
>
> Le protocole RTP-FEC nécessite deux ports supplémentaires pour corriger les erreurs. Pour répondre à cette exigence, AWS Elemental MediaConnect réserve les ports +2 et +4 à partir du port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000, 4002 et 4004.

4. Pour lisser la latence, spécifiez le délai supplémentaire que vous souhaitez utiliser pour le lissage de sortie. Nous vous recommandons de spécifier une valeur de 0 ms pour désactiver le lissage. Toutefois, si le récepteur ne parvient pas à traiter le flux correctement, spécifiez une valeur comprise entre 100 et 1 000 ms. AWS Elemental MediaConnect tente ainsi de corriger l'instabilité provenant de la source du flux. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 0 ms.

SRT listener

1. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
2. Pour Protocol, choisissez SRT listener.
3. Pour Latence minimale, spécifiez la taille minimale de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

   Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le

MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.

4. Pour la liste d'autorisation CIDR, spécifiez une plage d'adresses IP autorisées à afficher le contenu de votre sortie. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

   > **Important**
   >
   > Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

5. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.
6. Si vous souhaitez chiffrer la vidéo lorsqu'elle est envoyée vers cette sortie, procédez comme suit :
   a. Dans la section Chiffrement, choisissez Activer.
   b. Le type de chiffrement ne sera pas sélectionnable. srt-password est le seul cryptage disponible pour ce protocole.
   c. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   d. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker le mot de passe SRT.

SRT caller

1. Pour Protocole, choisissez SRT-Caller.
2. Pour Latence minimale, spécifiez la taille minimale de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise

entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.

3. Pour Adresse IP de destination, entrez l'adresse IP ou le domaine de destination de la sortie.
4. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.
5. Si vous souhaitez chiffrer la vidéo lorsqu'elle est envoyée vers cette sortie, procédez comme suit :
   a. Dans la section Chiffrement, choisissez Activer.
   b. Le type de chiffrement ne sera pas sélectionnable. SRT-Password est le seul cryptage disponible pour ce protocole.
   c. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   d. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker le mot de passe SRT.

Fujitsu-QoS

1. Pour Protocole, choisissez Fujitsu-QOS.
2. Pour Port, choisissez le port sur lequel vous souhaitez échanger des paquets de contrôle avec le récepteur. Pour plus d'informations sur les ports, consultezDestinations de sortie.
3. Pour la liste d'autorisation CIDR, spécifiez une plage d'adresses IP autorisées à afficher le contenu de votre sortie. Formatez les adresses IP sous la forme d'un bloc CIDR (Classless

Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

> **Important**
>
> Spécifiez un bloc CIDR aussi précis que possible. N'incluez que les adresses IP auxquelles vous souhaitez ajouter du contenu à votre flux. Si vous spécifiez un bloc CIDR trop large, il est possible que des tiers envoient du contenu à votre flux.

Zixi pull

1. Pour Protocol, choisissez Zixi pull.
2. Pour Stream ID, entrez la valeur Stream configurée lorsque vous avez ajouté l'entrée sur le récepteur Zixi. Dans le récepteur Zixi, cette valeur se trouve dans la section Paramètres du flux.

   > **Important**
   >
   > Si vous laissez ce champ vide, le service utilise le nom de sortie comme identifiant du flux. Comme l'ID de flux doit correspondre à la valeur définie dans le récepteur Zixi, vous devez spécifier l'ID de flux s'il n'est pas exactement le même que le nom de sortie.

3. Pour Remote ID, entrez la valeur d'ID attribuée au récepteur Zixi. Dans le récepteur Zixi, cette valeur se trouve dans le menu des paramètres généraux et est étiquetée ID. La valeur de l'ID se trouve également sur la page d'état du récepteur Zixi.
4. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 0 et 60 000 ms. Si vous laissez ce champ vide, le service utilise la latence définie dans le récepteur.
5. Pour la liste d'autorisations CIDR, spécifiez une plage d'adresses IP autorisées à récupérer le contenu de votre source. Formatez les adresses IP sous la forme d'un

bloc CIDR (Classless Inter-Domain Routing), par exemple 10.24.34.0/23. Pour plus d'informations sur la notation de bloc d'adresse CIDR, consultez RFC 4632.

> **Tip**
>
> Pour spécifier un bloc CIDR supplémentaire, choisissez Ajouter. Vous pouvez spécifier jusqu'à trois blocs CIDR.

6. Si vous souhaitez chiffrer la vidéo lorsqu'elle est envoyée vers cette sortie, procédez comme suit :
   a. Dans la section Chiffrement, choisissez Activer.
   b. Pour Type de chiffrement, choisissez Clé statique.
   c. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   d. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.
   e. Pour Algorithme de chiffrement, choisissez le type de chiffrement que vous souhaitez utiliser pour chiffrer la source.

Zixi push

1. Pour Protocole, choisissez Zixi push.
2. Pour l'adresse IP, choisissez l'adresse IP à laquelle vous souhaitez envoyer la sortie.
3. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.
4. Pour Stream ID, entrez l'ID de flux défini dans le récepteur Zixi.

> **Important**
>
> Si vous laissez ce champ vide, le service utilise le nom de sortie comme identifiant du flux. Comme l'ID de flux doit correspondre à la valeur définie dans le récepteur Zixi, vous devez spécifier l'ID de flux s'il n'est pas exactement le même que le nom de sortie.

5. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus

long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 0 et 60 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 6 000 ms.

6. Si vous souhaitez chiffrer la vidéo lorsqu'elle est envoyée vers cette sortie, procédez comme suit :
   a. Dans la section Chiffrement, choisissez Activer.
   b. Pour Type de chiffrement, choisissez Clé statique.
   c. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   d. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.
   e. Pour Algorithme de chiffrement, choisissez le type de chiffrement que vous souhaitez utiliser pour chiffrer la source.

10. Choisissez Ajouter une sortie.

Pour ajouter une sortie à un flux (AWS CLI)

1. Créez un fichier JSON contenant les détails de la sortie que vous souhaitez ajouter au flux.

   L'exemple suivant montre la structure du contenu du fichier :

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
    "Outputs": [
        {
            "Description": "RTP-FEC Output",
            "Destination": "192.0.2.12",
            "Name": "RTPOutput",
            "Port": 5020,
            "Protocol": "rtp-fec",
            "SmoothingLatency": 100
        }
    ]
}
```

2. Dans le AWS CLI, utilisez la `add-flow-output` commande :

```
aws mediaconnect add-flow-outputs --flow-arn "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame" --cli-
input-json file://addFlowOutput.txt --region us-west-2
```

L'exemple suivant illustre la valeur de retour :

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
    "Outputs": [
        {
            "Name": "RTPOutput",
            "Port": 5020,
            "Transport": {
                "SmoothingLatency": 100,
                "Protocol": "rtp-fec"
            },
            "Destination": "192.0.2.12",
            "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:RTPOutput",
            "Description": "RTP-FEC Output"
        }
    ]
}
```

Ajouter des sorties VPC à un flux

Une sortie VPC est envoyée vers un cloud privé virtuel (VPC) que vous avez créé à l'aide d'Amazon Virtual Private Cloud.

Pour les flux de transport, vous pouvez ajouter des sorties (jusqu'à 50) même si le flux est actif. Pour les flux CDI, vous pouvez ajouter des sorties (jusqu'à 10) uniquement si le flux est en mode veille. Pour des performances optimales, suivez les instructions fournies dansBonnes pratiques.

Pour ajouter une sortie VPC à un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux auquel vous souhaitez ajouter une sortie.

La page de détails de ce flux apparaît.

3. Choisissez l'onglet Outputs.
4. Choisissez Ajouter une sortie.
5. Dans Nom, spécifiez le nom de votre sortie. Cette valeur est un identifiant qui n'est visible que sur la MediaConnect console AWS Elemental et qui n'est pas visible pour l'utilisateur final.
6. Pour Type de sortie, choisissez sortie VPC.
7. Pour Protocole, choisissez le protocole approprié.
8. Dans Description, entrez une description qui vous rappellera ultérieurement où va cette sortie. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
9. Déterminez le protocole que vous souhaitez utiliser pour la sortie. Les options du protocole dépendent du type de flux.

   - Pour les flux de transport, les options de protocole sont les suivantes : RTP, RTP-FEC, RIST, SRT et Zixi.
   - Pour les flux CDI, les options de protocole sont les suivantes : CDI et ST 2110 JPEG XS.
10. Pour obtenir des instructions spécifiques en fonction du protocole que vous souhaitez utiliser, sélectionnez l'un des onglets suivants :

    RIST

    1. Pour Protocole, choisissez RIST.
    2. Pour l'adresse IP, choisissez l'adresse IP à laquelle vous souhaitez envoyer la sortie.
    3. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.

       > **Note**
       >
       > Le protocole RIST nécessite un port supplémentaire pour la correction des erreurs. Pour répondre à cette exigence, AWS Elemental MediaConnect réserve le port +1 à partir du port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000 et 4001.

    4. Pour lisser la latence, spécifiez le délai supplémentaire que vous souhaitez utiliser pour le lissage de sortie. Nous vous recommandons de spécifier une valeur de 0 ms pour désactiver le lissage. Toutefois, si le récepteur ne parvient pas à traiter le flux

correctement, spécifiez une valeur comprise entre 100 et 1 000 ms. AWS Elemental MediaConnect tente ainsi de corriger l'instabilité provenant de la source du flux. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 0 ms.

5. Pour Sortie vers VPC, choisissez le nom de l'interface VPC à laquelle vous souhaitez envoyer votre sortie.

RTP or RTP-FEC

1. Pour Protocole, choisissez RTP ou RTP-FEC.

> **Note**
>
> Les sorties RTP et RTP-FEC sont conformes à la norme SMPTE ÷ 7. Si votre récepteur en aval prend en charge la fusion de sources en 7, les sorties RTP et RTP-FEC seront compatibles.

2. Pour l'adresse IP, choisissez l'adresse IP à laquelle vous souhaitez envoyer la sortie.
3. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.

> **Note**
>
> Le protocole RTP-FEC nécessite deux ports supplémentaires pour corriger les erreurs. Pour répondre à cette exigence, AWS Elemental MediaConnect réserve les ports +2 et +4 à partir du port que vous spécifiez. Par exemple, si vous spécifiez le port 4000 pour la sortie, le service attribue les ports 4000, 4002 et 4004.

4. Pour lisser la latence, spécifiez le délai supplémentaire que vous souhaitez utiliser pour le lissage de sortie. Nous vous recommandons de spécifier une valeur de 0 ms pour désactiver le lissage. Toutefois, si le récepteur ne parvient pas à traiter le flux correctement, spécifiez une valeur comprise entre 100 et 1 000 ms. AWS Elemental MediaConnect tente ainsi de corriger l'instabilité provenant de la source du flux. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 0 ms.
5. Pour Sortie vers VPC, choisissez le nom de l'interface VPC à laquelle vous souhaitez envoyer votre sortie.

SRT listener

1. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
2. Pour Type de sortie, sélectionnez Sortie VPC.
3. Pour Protocol, choisissez SRT listener.
4. Dans Description, entrez une description qui peut vous aider à distinguer une sortie d'une autre. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
5. Pour Latence minimale, spécifiez la taille minimale de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

   Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.
6. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.
7. Pour Sortie vers VPC, choisissez le nom de l'interface VPC à laquelle vous souhaitez envoyer votre sortie.
8. Si vous souhaitez chiffrer la vidéo lorsqu'elle est envoyée vers cette sortie, procédez comme suit :

   a. Dans la section Chiffrement, choisissez Activer.

b. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.

c. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker le mot de passe SRT.

SRT caller

1. Dans Nom, spécifiez le nom de votre source. Cette valeur est un identifiant visible uniquement sur la MediaConnect console. Il n'est visible par personne en dehors du AWS compte courant.
2. Pour Type de sortie, sélectionnez Sortie VPC.
3. Pour Protocol, choisissez SRT Caller.
4. Dans Description, entrez une description qui peut vous aider à distinguer une sortie d'une autre. Il peut s'agir du nom de l'entreprise ou de notes concernant la configuration.
5. Pour Latence minimale, spécifiez la taille minimale de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise entre 100 et 15 000 ms. Si vous laissez ce champ vide, MediaConnect utilise la valeur par défaut de 2 000 ms.

   Le protocole SRT utilise une configuration de latence minimale de chaque côté de la connexion. La plus grande de ces deux valeurs est utilisée comme latence de restauration. Si le débit transmis, multiplié par la latence de récupération, est supérieur à la mémoire tampon du récepteur, la mémoire tampon débordera et le flux peut échouer avec un. `Buffer Overflow Error` Du côté du récepteur SRT, la mémoire tampon du récepteur est configurée par la valeur SRTO_RCVBUF. La taille de la mémoire tampon du récepteur est limitée par la valeur de la taille de la fenêtre de contrôle de flux (SRTO_FC). Sur le MediaConnect côté, la mémoire tampon du récepteur est calculée comme la valeur de débit maximale multipliée par la valeur de latence minimale. Pour plus d'informations sur le tampon SRT, consultez les directives de configuration SRT.
6. Pour Adresse IP de destination, entrez l'adresse IP ou le domaine de destination de la sortie.

7. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.
8. Pour Sortie vers VPC, choisissez le nom de l'interface VPC à laquelle vous souhaitez envoyer votre sortie.
9. Si vous souhaitez chiffrer la vidéo lorsqu'elle est envoyée vers cette sortie, procédez comme suit :
   a. Dans la section Chiffrement, choisissez Activer.
   b. Le type de chiffrement ne sera pas sélectionnable. SRT-Password est le seul cryptage disponible pour ce protocole.
   c. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   d. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker le mot de passe SRT.

Zixi push

1. Pour Protocole, choisissez Zixi push.
2. Pour l'adresse IP, choisissez l'adresse IP à laquelle vous souhaitez envoyer la sortie.
3. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.
4. Pour Stream ID, entrez l'ID de flux défini dans le récepteur Zixi.

> **Important**
>
> Si vous laissez ce champ vide, le service utilise le nom de sortie comme identifiant du flux. Comme l'ID de flux doit correspondre à la valeur définie dans le récepteur Zixi, vous devez spécifier l'ID de flux s'il n'est pas exactement le même que le nom de sortie.

5. Pour Latence maximale, spécifiez la taille de la mémoire tampon (délai) que vous souhaitez que le service conserve. Une valeur de latence plus élevée signifie un délai plus long dans la transmission du flux, mais une plus grande marge de manœuvre pour corriger les erreurs. Une valeur de latence plus faible signifie un délai plus court, mais moins de marge de manœuvre pour corriger les erreurs. Vous pouvez choisir une valeur comprise

entre 0 et 60 000 ms. Si vous laissez ce champ vide, le service utilise la valeur par défaut de 6 000 ms.

6. Pour Sortie vers VPC, choisissez le nom de l'interface VPC à laquelle vous souhaitez envoyer votre sortie.
7. Si vous souhaitez chiffrer la vidéo lorsqu'elle est envoyée vers cette sortie, procédez comme suit :
   a. Dans la section Chiffrement, choisissez Activer.
   b. Pour Type de chiffrement, choisissez Clé statique.
   c. Pour l'ARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsque vous avez configuré le chiffrement.
   d. Pour l'ARN secret, spécifiez l'ARN AWS Secrets Manager attribué lors de la création du secret pour stocker la clé de chiffrement.
   e. Pour Algorithme de chiffrement, choisissez le type de chiffrement que vous souhaitez utiliser pour chiffrer la source.

Fujitsu-QoS

1. Pour Protocole, choisissez Fujitsu-QOS.
2. Pour Port, choisissez le port sur lequel vous souhaitez échanger des paquets de contrôle avec le récepteur. Pour plus d'informations sur les ports, consultezDestinations de sortie.
3. Pour Sortie vers VPC, choisissez le nom de l'interface VPC à laquelle vous souhaitez envoyer votre sortie.

CDI

1. Pour Protocole, choisissez CDI.
2. Pour l'adresse IP, choisissez l'adresse IP à laquelle vous souhaitez envoyer la sortie.
3. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.
4. Pour l'interface VPC, choisissez le nom de l'interface VPC à laquelle vous souhaitez envoyer votre sortie.
5. Pour chaque flux multimédia que vous souhaitez envoyer dans le cadre de la sortie, procédez comme suit :

a. Pour Nom du flux multimédia, choisissez le nom du flux multimédia. Vous ne pouvez ajouter que les flux multimédias utilisés par la source de votre flux.

b. Pour le nom du codage, confirmez la valeur par défaut, qui est présélectionnée en fonction du type de flux multimédia.

c. Pour FMT, spécifiez le numéro du type de format (parfois appelé type de charge utile RTP) du flux multimédia. Cette valeur doit être dans un format reconnu par le récepteur.

ST 2110 JPEG XS

1. Pour Protocole, choisissez ST 2110 JPEG XS.
2. Pour l'interface VPC 1, choisissez l'une des interfaces VPC auxquelles vous souhaitez envoyer du contenu, puis choisissez l'adresse IP spécifique à laquelle vous souhaitez envoyer la sortie.
3. Pour l'interface VPC 2, choisissez une deuxième interface VPC à laquelle vous souhaitez envoyer du contenu, puis choisissez l'adresse IP spécifique à laquelle vous souhaitez envoyer la sortie. Il n'y a aucune priorité entre les interfaces VPC 1 et 2.
4. Pour chaque flux multimédia que vous souhaitez envoyer dans le cadre de la sortie, procédez comme suit :

   a. Pour Nom du flux multimédia, choisissez le nom du flux multimédia. Vous ne pouvez ajouter que les flux multimédias utilisés par la source de votre flux.

   b. Dans Nom du codage, choisissez le format utilisé pour coder les données.

      - Pour les flux de données auxiliaires, définissez le nom de codage sur**`smpte291`**.
      - Pour les flux audio, définissez le nom de codage sur**`pcm`**.
      - Pour la vidéo, définissez le nom de codage sur**`jxsv`**.

   c. Pour Port, choisissez le port que vous souhaitez utiliser lorsque le contenu est distribué sur cette sortie. Pour plus d'informations sur les ports, consultezDestinations de sortie.

   d. Pour le profil de l'encodeur, choisissez un paramètre pour la compression. Cette propriété ne s'applique que si la source utilise le protocole CDI.

   e. Pour Facteur de compression, spécifiez la valeur que vous souhaitez que le service utilise lors du calcul de la compression de la sortie. Les valeurs valides sont des nombres à virgule flottante compris entre 3,0 et 10,0 inclus. Le débit de la sortie est calculé comme suit :

      Débit de sortie = (1/CompressionFactor) * (débit source)

Cette propriété ne s'applique que si la source utilise le protocole CDI.

5. Choisissez Ajouter une sortie.

Afficher la liste des sorties d'un flux

Vous pouvez consulter la liste des sorties d'un flux, ainsi que la configuration associée à chaque sortie. Cette liste inclut les sorties que vous avez ajoutées, ainsi que les sorties qu'AWS Elemental a MediaConnect ajoutées lorsque les abonnés créent des flux en fonction des droits que vous avez accordés.

Pour afficher la liste des sorties d'un flux existant (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux que vous souhaitez afficher.

   La page de détails de ce flux apparaît.
3. Choisissez l'onglet Outputs.

   La liste des sorties pour ce flux s'affiche.

Pour afficher la liste des sorties d'un flux existant (AWS CLI)

- Dans le AWS CLI, utilisez la `describe-flow` commande :

```
aws mediaconnect describe-flow --flow-arn "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame" --
region us-east-1 --profile PMprofile
```

  La valeur renvoyée indique les détails de l'ensemble du flux, y compris toutes les sorties. L'exemple suivant illustre la valeur de retour :

```
{
  "Flow": {
    "AvailabilityZone": "us-east-1d",
    "Entitlements": [],
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
    "Name": "BasketballGame",
```

```
    "Outputs": [
      {
        "Address": "192.0.2.12",
        "Description": "RTP-FEC Output",
        "Name": "NYCOutput",
        "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYCOutput",
        "Port": 5020,
        "Protocol": "rtp-fec"
      },
      {
        "Address": "198.51.100.8",
        "Description": "RTP Output",
        "Name": "DCOutput",
        "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-987655dEF67hiJ89-c34de5fG678h:DCOutput",
        "Port": 5110,
        "Protocol": "rtp"
      }
    ],
    "Source": {
      "IngestIp": "195.51.100.21",
      "IngestPort": 5010,
      "Name": "BasketballGameSource",
      "Protocol": "rtp-fec",
      "SourceArn": "arn:aws:mediaconnect:us-
east-1:111122223333:source:3-4aBC56dEF78hiJ90-4de5fG6Hi78Jk:BasketballGameSource",
      "AllowlistCidr": "10.24.34.0/23"
    },
    "Status": "STANDBY"
  }
}
```


Mettre à jour les sorties d'un flux

Vous pouvez mettre à jour les sorties d'un flux, même lorsque le flux est actif.

Pour mettre à jour une sortie sur un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé à la sortie que vous souhaitez mettre à jour.

3. Choisissez l'onglet Outputs.

   La liste des sorties pour ce flux s'affiche.

4. Choisissez la sortie que vous souhaitez mettre à jour.

5. Choisissez Mettre à jour.

6. Effectuez les modifications appropriées, puis choisissez Save (Enregistrer).

Pour mettre à jour une sortie de flux (AWS CLI)

- Dans le AWS CLI, utilisez la `update-flow-output` commande :

```
aws mediaconnect update-flow-output --flow-arn "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame" --
output-arn "arn:aws:mediaconnect:us-east-1:111122223333:output:2-3aBC45dEF67hiJ89-
c34de5fG678h:NYCfeed" --port 5040 --region us-east-1 --profile PMprofile
```

L'exemple suivant illustre la valeur de retour :

```
{
  "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
  "Output": {
    "Address": "192.0.2.12",
    "Encryption": {
      "Algorithm": "aes256",
      "KeyType": "static-key",
      "RoleArn": "arn:aws:iam::111122223333:role/AllowMediaConnect",
      "SecretArn": "arn:aws:secretsmanager:us-west-2:111122223333:secret:SECRETID"
    },
    "Name": "Output1",
    "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:Output1",
    "Port": 5040,
    "Protocol": "rtp-fec"
  }
}
```

Gestion des balises sur une sortie

Vous pouvez utiliser des balises pour suivre la facturation et l'organisation de vos MediaConnect flux, sources, sorties et droits AWS Elemental. Ce sont les mêmes étiquettes qui AWS Billing and Cost Management permettent d'organiser votre AWS facture. Pour plus d'informations sur l'utilisation des balises pour la répartition des coûts, voir Utiliser les balises de répartition des coûts pour les rapports de facturation personnalisés dans le guide de AWS Billing l'utilisateur.

Pour ajouter des balises à une sortie (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé à la sortie à laquelle vous souhaitez ajouter des balises.
3. Choisissez l'onglet Outputs.

   La liste des sorties pour ce flux s'affiche.
4. Choisissez la sortie à laquelle vous souhaitez ajouter des balises.
5. Choisissez Gérer les balises.
6. Choisissez à nouveau Gérer les balises, puis choisissez Ajouter une étiquette.
7. Pour chaque balise que vous souhaitez ajouter, procédez comme suit :

   a. Saisissez une clé et une valeur. Par exemple, votre clé peut être **`sports`** et votre valeur peut être**`golf`**.

   b. Choisissez Ajouter une balise.
8. Choisissez Mettre à jour.

Pour modifier les balises d'une sortie (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé à la sortie pour laquelle vous souhaitez modifier les balises.
3. Choisissez l'onglet Outputs.

   La liste des sorties pour ce flux s'affiche.
4. Choisissez la sortie pour laquelle vous souhaitez modifier les balises.
5. Dans la section Détails, choisissez Gérer les balises.

6. Choisissez à nouveau Gérer les tags.
7. Mettez à jour les balises, le cas échéant.
8. Choisissez Mettre à jour.

Pour supprimer des balises d'une sortie (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé à la sortie dont vous souhaitez supprimer les balises.
3. Choisissez l'onglet Outputs.

   La liste des sorties pour ce flux s'affiche.
4. Choisissez la sortie dont vous souhaitez supprimer les balises.
5. Dans la section Détails, choisissez Gérer les balises.
6. Choisissez à nouveau Gérer les tags.
7. Choisissez Supprimer le tag à côté de chaque tag que vous souhaitez supprimer.
8. Choisissez Mettre à jour.

Supprimer les sorties d'un flux

Vous pouvez supprimer les sorties que vous avez ajoutées au flux. Si AWS Elemental a MediaConnect généré la sortie à la suite d'un droit, vous devez révoquer ce droit.

Pour supprimer une sortie d'un flux (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé à la sortie que vous souhaitez supprimer.

   La page de détails de ce flux apparaît.
3. Choisissez l'onglet Outputs.
4. Choisissez la sortie, puis choisissez Supprimer.

Pour supprimer une sortie d'un flux (AWS CLI)

- Dans le AWS CLI, utilisez la `remove-flow-output` commande :

```
aws mediaconnect remove-flow-output --flow-arn "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame" --
output-arn "arn:aws:mediaconnect:us-east-1:111122223333:output:2-3aBC45dEF67hiJ89-
c34de5fG678h:Output1" --region us-west-2
```

L'exemple suivant illustre la valeur de retour :

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
    "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:Output1"
}
```

Destinations de sortie

Chaque sortie d'un flux doit être envoyée vers une destination différente. Les paramètres qui définissent la destination dépendent du protocole, mais chaque protocole utilise un identifiant composé pour la destination. Par exemple, plusieurs sorties peuvent pointer vers la même adresse IP de destination, à condition qu'aucun de leurs ports ne se chevauche. De même, plusieurs sorties peuvent pointer vers le même identifiant de flux tant que leurs identifiants distants sont différents. Le tableau suivant indique comment chaque protocole définit la destination.

> **Note**
>
> Certains protocoles nécessitent des ports supplémentaires pour corriger les erreurs. Pour les sorties utilisant ces protocoles, AWS Elemental réserve MediaConnect automatiquement les ports supplémentaires. Le protocole définit spécifiquement les ports qui doivent être réservés. Par exemple, certains protocoles nécessitent le port+2 et le port+4 pour corriger les erreurs. Si vous spécifiez le port 5000 pour la sortie, le service attribue les ports 5000, 5002 et 5004.

Protocole	Définition de la destination	Ports requis
CDI	Ports pour chaque flux multimédia	Les ports que vous spécifiez pour chaque flux multimédi

Protocole	Définition de la destination	Ports requis
		a. Ce sont les seuls ports nécessaires pour la sortie.
POIGNET	Adresse IP, port et port+1	Le port que vous spécifiez, plus un port supplémentaire. Le service réserve automatiquement un port égal à +1 par rapport au port que vous avez spécifié. Par exemple, si vous spécifiez le port 3000 pour cette sortie, le service réserve également le port 3001.
RTP	Adresse IP et port	Le port que vous spécifiez. Il s'agit du seul port nécessaire pour la sortie.
RTP-FEC	Adresse IP, port, port+2 et port +4	Le port que vous spécifiez, plus deux ports supplémentaires. Le service réserve automatiquement les ports +2 et +4 à partir du port que vous avez spécifié. Par exemple, si vous spécifiez le port 2000 pour cette sortie, le service réserve également les ports 2002 et 2004 pour la correction des erreurs.
écouteur SRT	Liste d'autorisations CIDR et port	Le port que vous spécifiez. Il s'agit du seul port nécessaire pour la sortie.

Protocole	Définition de la destination	Ports requis
appelant SRT	Adresse IP et port	Le port que vous spécifiez. Il s'agit du seul port nécessaire pour la sortie.
Fujistu-QoS	Liste d'autorisations CIDR et port	Le port que vous spécifiez. Il s'agit du seul port nécessaire pour la sortie.
ST 2110 JPEG XS	Ports pour chaque flux multimédia	Les ports que vous spécifiez pour chaque flux multimédia. Ce sont les seuls ports nécessaires pour la sortie.
Pull Zixi	ID de flux, ID distant et liste d'autorisations CIDR	Le service utilise automatiquement le port 2077 pour ces sorties.
Zixi Push	Adresse IP, ID de flux et port	Le port que vous spécifiez est le seul port nécessaire pour la sortie.

Déterminer l'adresse IP d'une sortie

Pour les flux qui utilisent des protocoles d'écoute (tels que Zixi Pull ou SRT Listener), le récepteur a besoin de l'adresse IP de la sortie pour établir une connexion avec le flux.

Pour déterminer l'adresse IP d'une sortie

1. Sur la page Flux, choisissez le nom du flux que vous souhaitez afficher.
2. Pour obtenir des instructions spécifiques en fonction de la manière dont le contenu est envoyé à votre sortie, choisissez l'un des onglets suivants :

   Public internet

   1. Dans la section Détails, notez l'adresse IP sortante publique. Il s'agit de l'adresse IP dont le récepteur a besoin.

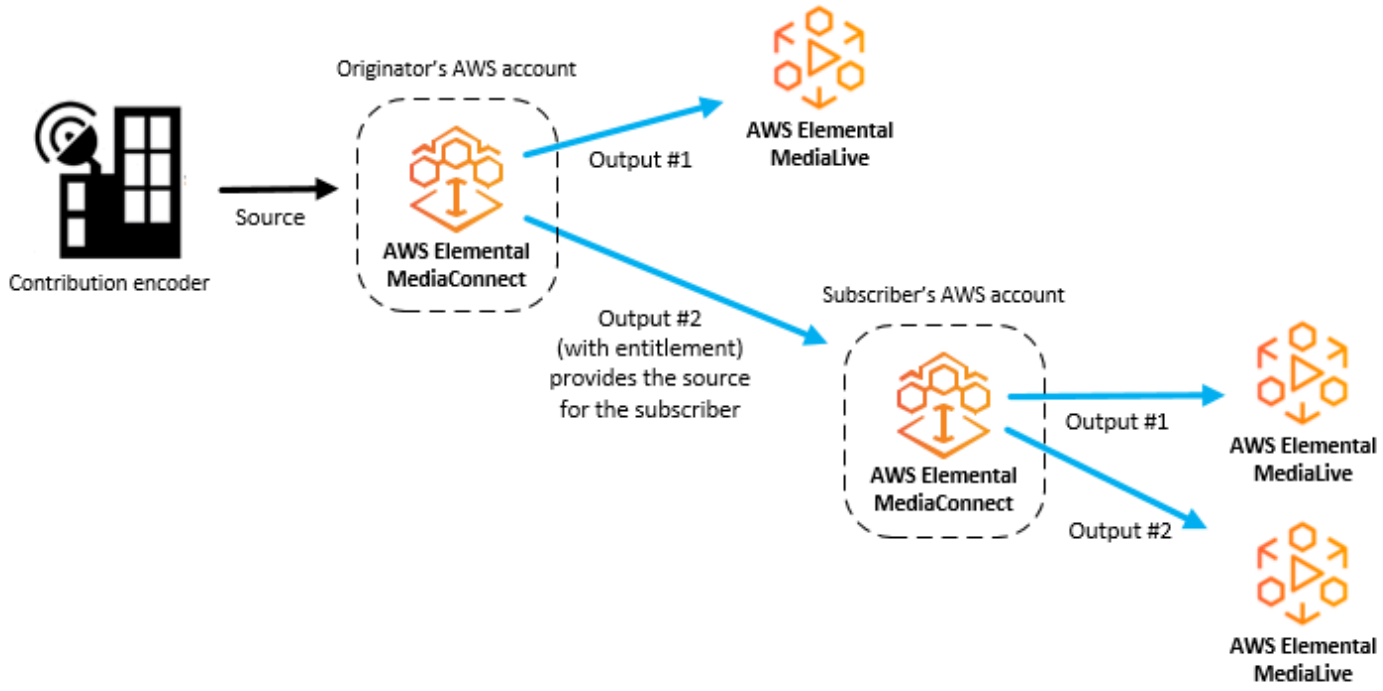
Private internet

1. Choisissez l'onglet Sorties, puis localisez la sortie que vous souhaitez afficher.
2. Sous Adresse du récepteur pour cette sortie, notez l'adresse IP. Il s'agit de l'adresse IP dont le récepteur a besoin.

Droits dans AWS Elemental MediaConnect

Les créateurs de contenu peuvent accorder le droit de partager leur contenu avec d'autresAWScomptes (comptes d'abonnés). Les abonnés peuvent ensuite configurer leur propre AWS Elemental MediaConnectflux utilisant le flux de l'expéditeur comme source. L'illustration suivante montre ce processus.

> **Note**
>
> Vous ne pouvez octroyer des droits que sur les flux de transport. MediaConnect ne prend pas en charge les droits sur les flux CDI.



Rubriques

- Partage de contenu avec d'autresAWScomptes
- Abonnement à du contenu fourni par un autreAWScompte

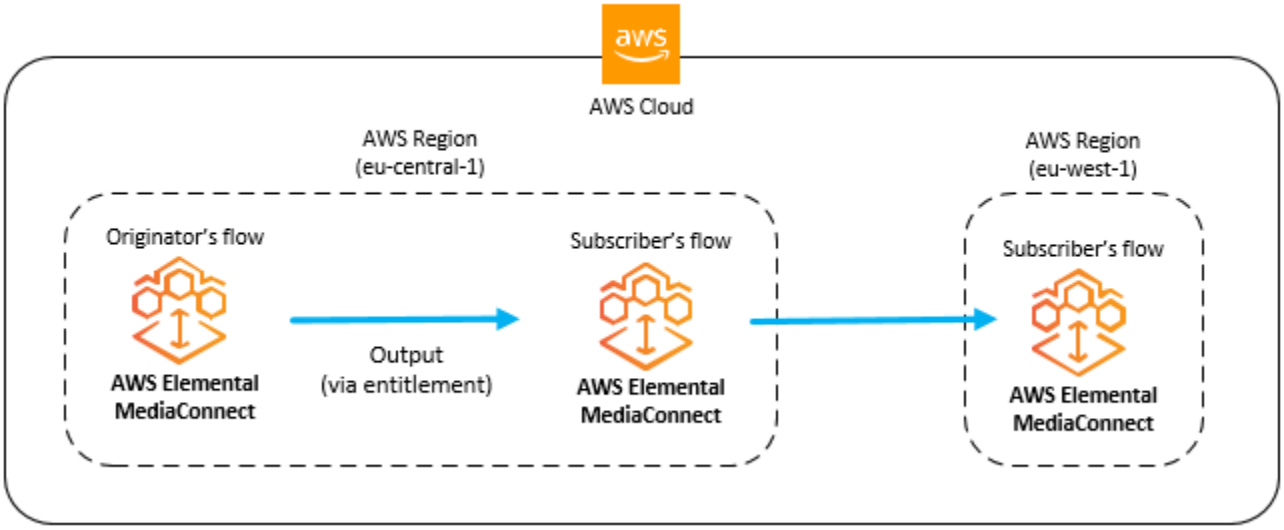
Partage de contenu avec d'autresAWScomptes

Vous pouvez accorder le droit de partager le contenu de votre AWS Elemental MediaConnect circuler avec un autreAWScompte (compte d'abonné). Lorsque l'abonné configure un flux basé sur les droits, le service génère une sortie sur votre flux pour représenter le flux entre votre flux et le flux de l'abonné. Cette sortie est comptée parmi les 50 sorties maximales que vous pouvez avoir sur votre flux.

Vous pouvez accorder, mettre à jour et révoquer des droits à tout moment, même sur un flux actif. Si vous souhaitez arrêter temporairement de diffuser du contenu vers le flux d'abonnés, vous pouvez désactiver ce droit. Plus tard, vous pourrez activer ce droit lorsque vous serez prêt à autoriser à nouveau le contenu à être diffusé sur le flux de l'abonné. Vous pouvez également spécifier le pourcentage des frais de transfert des données d'accès que vous souhaitez que l'abonné soit responsable.

> **Note**
>
> Si vous accordez un droit et plus tarddésactiverSi (pour arrêter temporairement la diffusion de contenu vers le flux d'abonnés), le droit reste associé à votre flux et est pris en compte dans votre nombre maximum de droits. Toutefois, si vousrévoquerle droit (pour arrêter définitivement de diffuser du contenu sur le flux de l'abonné), le droit est supprimé de votre flux et ne compte plus dans le nombre maximum de droits.

Après avoir accordé un droit, vous fournissez des informations sur le droit (nom,AWSRégion et détails de chiffrement) à l'abonné. L'abonné utilise ces informations pour créer un MediaConnect flux qui utilise votre flux comme source. Le flux de l'abonné doit être identiqueAWSLa région est votre flux. Si l'abonné souhaite un flux dans une autre région, il doit créer un deuxième flux dans la nouvelle région. L'illustration suivante montre ce processus.



> **Note**
>
> Vous ne pouvez octroyer des droits que sur les flux de transport. MediaConnect ne prend pas en charge les droits sur les flux CDI.

Rubriques

Octroi d'un droit sur un flux

Vous pouvez autoriser un flux existant à partager votre contenu avec un autreAWScompte (le compte d'abonné). L'abonné crée un AWS Elemental MediaConnect flux dans le mêmeAWSRégion, en utilisant votre flux comme source. Dans ce cas, le service génère une sortie sur votre flux pour représenter le flux vidéo de votre flux vers le flux de l'abonné.

L'abonné ne peut utiliser un droit qu'une seule fois.

Prérequis

Avant de pouvoir octroyer un droit, vous devez effectuer les opérations suivantes :

- Obtenez les informations de l'abonnéAWSnuméro de compte.
- Si vous souhaitez chiffrer la vidéo lorsqu'elle est envoyée de votre flux au flux de l'abonné, configurez le chiffrement à l'aide dechiffrement par clé statiqueouÉchange sécurisé de clés d'encapsulage et d'encodeur (SPEKE).

Pour accorder un droit sur un flux (console)

1. Ouvrez le MediaConnect console àhttps://console.aws.amazon.com/mediaconnect/.
2. Sur leFluxpage, choisissez le nom du flux auquel vous souhaitez accorder un droit.

   La page de détails de ce flux apparaît.
3. Choisissez leDroitsonglet.
4. ChoisissezDroit à la subvention.

   LeDroit à la subventionla page apparaît.
5. PourNom, attribuez un nom à l'autorisation qui vous aidera, ainsi qu'à l'abonné, à différencier ce flux des autres flux. Le nom fait également partie de l'ARN d'autorisation, qui est visible par l'abonné.
6. PourID du compte d'abonné, spécifiez les 12 chiffres de l'abonnéAWSidentifiant de compte. N'insérez pas de tirets dans l'identifiant.
7. PourDescriptif, spécifiez une description qui vous aidera à identifier ce droit ultérieurement. La description n'est visible que sur l'AWS Elemental MediaConnect console pour votre compte.
8. PourPourcentage des frais d'abonnement au transfert de données, spécifiez le pourcentage des frais de transfert des données d'accès que vous souhaitez que l'abonné soit responsable.AWSfacture le reste à votre compte. Par exemple, si vous spécifiez15,AWSfacture au compte de l'abonné 15 % des frais de transfert des données d'admissibilité et à votre compte les 85 % restants.

> **Note**
>
> Même si vous spécifiez que l'abonné est responsable d'une partie ou de la totalité des frais de transfert des données d'admissibilité, l'abonné n'aura pas à payer de frais tant qu'il n'aura pas créé et démarré un flux basé sur ce droit.

9. PourÉtat d'admissibilité, indiquez si vous souhaitez que le droit soit activé ou désactivé. Si le droit est activé, l'abonné peut créer un flux basé sur ce droit et commencer à diffuser du contenu immédiatement. Si le droit est désactivé, l'abonné doit attendre que vous l'activiez pour que le contenu puisse être diffusé de votre flux vers son flux.
10. Si vous souhaitez chiffrer la vidéo lorsqu'elle est envoyée de votre flux vers le flux de l'abonné, choisissez l'un des onglets suivants :

    Static key encryption

    1. Dans leChiffrementsection, choisissezActiver.
    2. PourType de chiffrement, choisissezClé statique.
    3. PourARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsqueconfigurer le chiffrement.
    4. PourARN secret, spécifiez l'ARN quiAWS Secrets Managerattribué lorsque vousa créé le secret pour stocker la clé de chiffrement.
    5. PourAlgorithme de chiffrement, choisissez le type de chiffrement que vous souhaitez utiliser pour chiffrer la source.

    SPEKE encryption

    1. Dans leChiffrementsection, choisissezActiver.
    2. PourType de chiffrement, choisissezPOINTE.
    3. PourAlgorithme de chiffrement, choisissez le type de chiffrement que vous souhaitez utiliser pour chiffrer la source.
    4. PourARN du rôle, entrez le nom de ressource Amazon (ARN) du rôle IAM qui vous permet d'envoyer vos demandes via API Gateway. Vous avez créé ce rôle lorsque vousconfigurer le chiffrement.

       L'exemple suivant montre un ARN de rôle :

```
arn:aws:iam::111122223333:role/SpekeAccess
```

5. PourID de ressource, entrez un identifiant pour le contenu. Le service l'envoie au serveur de clés pour identifier le point de terminaison actuel. Le degré d'originalité de ce système dépend de la précision avec laquelle vous souhaitez que les contrôles d'accès soient précis. L'ID de ressource est également appelé ID de contenu.

   L'exemple suivant montre un ID de ressource :

   ```
   MovieNight20171126093045
   ```

6. PourID de l'appareil, entrez la valeur de l'un des appareils que vous avez configurés avec votre fournisseur de clés de plateforme d'accès conditionnel (CA).
7. PourURL, entrez l'URL du proxy API Gateway que vous avez configuré pour communiquer avec votre serveur de clés. Le proxy API Gateway doit résider dans le mêmeRégion AWScomme MediaConnect.

   L'exemple suivant montre une URL.

   ```
   https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/
   copyProtection
   ```

8. (Facultatif) PourVecteur d'initialisation constantentrez une valeur hexadécimale de 128 bits et 16 octets représentée par une chaîne de 32 caractères, à utiliser avec la clé pour chiffrer le contenu.

11. Au bas de la page, choisissezDroit à la subvention.
12. Sur leDroitsonglet, recherchez le nouveau droit dans la liste.
13. Notez l'ARN de l'autorisation.
14. Fournissez les informations suivantes à l'abonné :

    - L'ARN d'éligibilité
    - LeAWSRégion dans laquelle vous avez créé le flux
    - La clé de chiffrement et l'algorithme si vous configurez le chiffrement sur le titre
    - Le pourcentage des frais de transfert des données d'accès à la charge de l'abonné

> **Note**
>
> MediaConnect supprime les paquets nuls afin d'optimiser la connexion de données entre le flux de l'auteur du contenu et le flux de l'abonné. Cela peut entraîner une fluctuation du débit du flux de l'abonné ou une différence entre le débit du flux de l'auteur du contenu et le flux de l'abonné. Nous vous recommandons de surveiller l'état de santé de la source en combinant les éléments suivants :`SourceBitRate`et d'autres indicateurs tels que`SourceContinuityCounter`et`SourceNotRecoveredPackets`.

Pour accorder un droit à un flux (AWS CLI)

1. Créez un fichier JSON contenant les détails des droits que vous souhaitez octroyer.

   L'exemple suivant montre la structure du contenu du fichier :

```
[
  {
    "Description": "For AnyCompany",
    "Encryption": [
      {
        "Algorithm": "aes128",
        "KeyType": "static-key",
        "RoleArn": "arn:aws:iam::111122223333:role/MediaConnect-ASM",
        "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:mySecret1"
      }
    ],
    "Name": "AnyCompany_Entitlement",
    "Subscribers": [
      "444455556666",
      "123456789012"
    ]
  },
  {
    "Description": "For Example Corp",
    "Name": "ExampleCorp",
    "Subscribers": [
      "777788889999"
    ]
```

```
  }
]
```

2. Dans l'AWS CLI, utilisez la commande `grant-flow-entitlements` :

```
aws mediaconnect grant-flow-entitlements --entitlements --flow-
arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame  --cli-input-
json file://entitlements.json
```

L'exemple suivant illustre la valeur de retour :

```
{
    "Entitlements": [
        {
            "Name": "AnyCompany_Entitlement",
            "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement",
            "Subscribers": [
                "444455556666", "123456789012"
            ],
            "Description": "For AnyCompany",
            "Encryption": {
                "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:mySecret1",
                "Algorithm": "aes128",
                "RoleArn": "arn:aws:iam::111122223333:role/MediaConnect-ASM",
                "KeyType": "static-key"
            }
        },
        {
            "Name": "ExampleCorp",
            "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-3333cccc4444dddd-1111aaaa2222:ExampleCorp",
            "Subscribers": [
                "777788889999"
            ],
            "Description": "For Example Corp"
        }
    ],
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame"
```

```
}
```

Mettre à jour un droit

Une fois qu'un droit a été créé, vous pouvez toujours mettre à jour la description, le statut et les abonnés. Si vous modifiez l'identifiant du compte d'abonné, le contenu devient indisponible pour le compte d'abonné d'origine. Si l'abonné d'origine a déjà créé un flux utilisant l'autorisation comme source, la sortie associée est supprimée de votre flux.

Pour mettre à jour un droit (console)

1. Ouvrez le MediaConnect console àhttps://console.aws.amazon.com/mediaconnect/.
2. Sur leFluxpage, choisissez le nom du flux associé au droit que vous souhaitez mettre à jour.

   La page de détails de ce flux apparaît.
3. Choisissez leDroitsonglet.
4. Choisissez le droit que vous souhaitez mettre à jour.
5. Choisissez Mettre à jour.
6. Effectuez les modifications appropriées, puis choisissez Save (Enregistrer).

Pour mettre à jour un droit sur un flux (AWS CLI)

- Dans l'AWS CLI, utilisez la commande `update-flow-entitlement` :

```
aws mediaconnect update-flow-entitlement --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame --
entitlement-arn arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement
 --description 'For AnyCompany Affiliate' --subscribers 444455556666",
 "123456789012
```

L'exemple suivant illustre la valeur de retour :

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame",
    "Entitlement": {
        "Name": "AnyCompany_Entitlement",
```

```
        "Description": "For AnyCompany Affiliate",
        "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement",
        "Encryption": {
            "KeyType": "static-key",
            "Algorithm": "aes128",
            "RoleArn": "arn:aws:iam::111122223333:role/MediaConnect-ASM",
            "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:mySecret1"
        },
        "Subscribers": [
            "444455556666", "123456789012"
        ]
    }
}
```

Gestion des balises associées à un droit

Vous pouvez utiliser des balises pour vous aider à suivre la facturation et l'organisation de votre AWS Elemental MediaConnect les flux, les sources, les sorties et les droits. Ce sont les mêmes balises que celles fournies par AWS Billing and Cost Management pour organiser votre facture AWS. Pour plus d'informations sur l'utilisation des balises pour la répartition des coûts, voirUtiliser les balises de répartition des coûts pour les rapports de facturation personnalisésdans leAWS BillingGuide de l'utilisateur.

Pour ajouter des balises à un droit (console)

1. Ouvrez le MediaConnect console àhttps://console.aws.amazon.com/mediaconnect/.
2. Sur leFluxpage, choisissez le nom du flux associé au droit auquel vous souhaitez ajouter des balises.
3. Choisissez leDroitsonglet.

   La liste des droits pour ce flux s'affiche.
4. Choisissez le droit auquel vous souhaitez ajouter des balises.
5. Choisissez Manage tags (Gérer les balises).
6. ChoisissezGérer les tags, puis choisissezAjouter un tag.
7. Pour chaque balise que vous souhaitez ajouter, procédez comme suit :

a. Entrez une clé et une valeur. Par exemple, votre clé peut être**`sports`**et votre valeur peut être**`golf`**.

b. Choisissez Ajouter une balise.

8. Choisissez Mettre à jour.

Pour modifier les balises d'un droit (console)

1. Ouvrez le MediaConnect console àhttps://console.aws.amazon.com/mediaconnect/.
2. Sur leFluxpage, choisissez le nom du flux associé au droit pour lequel vous souhaitez modifier les balises.
3. Choisissez leDroitsonglet.

   La liste des droits pour ce flux s'affiche.
4. Choisissez le droit pour lequel vous souhaitez modifier les balises.
5. Dans leDétailssection, choisissezGérer les tags.
6. Choisissez Manage tags (Gérer les balises).
7. Mettez à jour les balises, le cas échéant.
8. Choisissez Mettre à jour.

Pour supprimer des balises d'un droit (console)

1. Ouvrez le MediaConnect console àhttps://console.aws.amazon.com/mediaconnect/.
2. Sur leFluxpage, choisissez le nom du flux associé au droit dont vous souhaitez supprimer les balises.
3. Choisissez leDroitsonglet.

   La liste des droits pour ce flux s'affiche.
4. Choisissez le droit dont vous souhaitez supprimer les tags.
5. Dans leDétailssection, choisissezGérer les tags.
6. Choisissez Manage tags (Gérer les balises).
7. ChoisissezSupprimer le tagà côté de chaque balise que vous souhaitez supprimer.
8. Choisissez Mettre à jour.

Révocation d'un droit

Une fois que vous avez révoqué un droit, le contenu devient définitivement indisponible sur le compte de l'abonné. L'autorisation et la sortie associée sont supprimées de votre flux. Si vous révoquez un droit et décidez par la suite que vous devez le réaccorder, le flux de l'abonné doit être redémarré manuellement. Le flux de l'abonné ne démarrera pas automatiquement une fois le droit accordé.

Si vous souhaitez arrêter temporairement de diffuser du contenu vers le flux des abonnés,désactiverle droit à la place.

Pour révoquer un droit (console)

1. Ouvrez le MediaConnect console àhttps://console.aws.amazon.com/mediaconnect/.
2. Sur leFluxpage, choisissez le nom du flux associé au droit que vous souhaitez révoquer.

   La page de détails de ce flux apparaît.
3. Choisissez leDroitsonglet.
4. Choisissez le droit que vous souhaitez révoquer.
5. ChoisissezRévoquer.

Pour révoquer un droit sur un flux (AWS CLI)

- Dans l'AWS CLI, utilisez la commande `revoke-flow-entitlement` :

```
aws mediaconnect revoke-flow-entitlement --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame --
entitlement-arn arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement
```

  L'exemple suivant illustre la valeur de retour :

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame",
    "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement"
}
```

Désactivation temporaire d'un droit

Lorsque vous désactivez un droit, le contenu devient immédiatement indisponible pour le compte de l'abonné. Cependant, le droit et la sortie associée restent dans votre flux. Ces ressources continuent d'être prises en compte dans votre quota de résultats et de droits. Plus tard, vous pourrezactiver le droitpour rétablir l'accès.

Si vous souhaitez arrêter définitivement la diffusion de contenu vers le flux d'abonnés,révoquerle droit à la place. Cette action supprime le droit et la sortie associée de votre flux.

Pour désactiver un droit (console)

1. Ouvrez le MediaConnect console àhttps://console.aws.amazon.com/mediaconnect/.
2. Sur leFluxpage, choisissez le nom du flux associé au droit que vous souhaitez désactiver.

   La page de détails de ce flux apparaît.
3. Choisissez leDroitsonglet.
4. Choisissez le droit que vous souhaitez désactiver.
5. Choisissez Désactiver.

Activation d'un droit qui a été temporairement désactivé

Si un droit a éténandicapé, vous pouvez l'activer pour recommencer à diffuser du contenu vers le flux de l'abonné.

> **Note**
>
> Si le droit étaitrévoqué, vous ne pouvez pas l'activer. Vous devezsubventionun nouveau droit.

Pour activer un droit (console)

1. Ouvrez le MediaConnect console àhttps://console.aws.amazon.com/mediaconnect/.
2. Sur leFluxpage, choisissez le nom du flux associé au droit que vous souhaitez activer.

   La page de détails de ce flux apparaît.
3. Choisissez leDroitsonglet.
4. Choisissez le droit que vous souhaitez activer.

5. Sélectionnez Enable (Activer).

Abonnement à du contenu fourni par un autreAWScompte

Quand un autreAWSle compte (compte émetteur) donne droit à votreAWScompte (compte abonné), vous pouvez créer un flux qui utilise le contenu de l'auteur comme source. Pour vous abonner à du contenu fourni par un autreAWScompte, vous créez un flux en fonction du droit qui vous est accordé. Vous devez configurer votre flux de la même manièreAWSRégion en tant que flux d'origine.

Vous ne pouvez utiliser un droit qu'une seule fois.

> **Note**
>
> MediaConnect supprime les paquets nuls afin d'optimiser la connexion de données entre le flux de l'auteur du contenu et le flux de l'abonné. Cela peut entraîner une fluctuation du débit du flux de l'abonné ou une différence entre le débit du flux de l'auteur du contenu et le flux de l'abonné. Nous vous recommandons de surveiller l'état de santé de la source en combinant les éléments suivants :`SourceBitRate`et d'autres indicateurs tels que`SourceContinuityCounter`et`SourceNotRecoveredPackets`.

Prérequis

Avant de créer votre flux, vous devez effectuer les opérations suivantes :

- Obtenez les informations suivantes auprès de l'auteur du contenu :
  - L'ARN d'éligibilité
  - LeAWSRégion dans laquelle l'expéditeur a créé le flux
  - La clé de chiffrement et l'algorithme si l'expéditeur a configuré le chiffrement sur le titre
- Si le droit est crypté à l'aide dechiffrement par clé statique,stocker la clé de chiffrementdansAWS Secrets Manageravant de commencer cette procédure. (Si le contenu est chiffré à l'aide de SPEKE, vous n'avez rien à faire pour configurer le chiffrement.)

Pour créer un flux basé sur un droit (console)

1. Ouvrez le MediaConnect console àhttps://console.aws.amazon.com/mediaconnect/.

2. Vérifiez que vous êtes connecté au mêmeAWSRégion dans laquelle se trouve le flux de l'expéditeur.
3. Sur leFluxpage, choisissezCréer un flux.
4. Dans leDétailssection, pourNom, donnez un nom à votre flux.
5. PourZone de disponibilité, choisissez une zone de disponibilité pour votre flux. Il n'est pas nécessaire que cela corresponde à la zone de disponibilité du flux d'origine.
6. Dans leLa sourcesection, pourType de source, choisissezSource intitulée.
7. PourARN d'éligibilité, choisissez le droit approprié. Cette liste inclut tous les droits qui vous ont été accordés.

> **Tip**
>
> Vous pouvez cliquer dans ce champ et commencer à saisir le nom du titre. AWS Elemental MediaConnect filtrera la liste pour n'inclure que les droits dont le nom correspond à celui que vous avez saisi.

> **Note**
>
> Le pourcentage des frais de transfert des données d'admissibilité dont vous êtes responsable est indiqué à côté de chaque droit. Cette valeur est définie par l'auteur du contenu.

8. Si l'expéditeur a configuré le chiffrement de l'autorisation, choisissezActiverdans leDéchiffrementsection et procédez comme suit :
   a. PourType de déchiffrement, choisissezClé statique.
   b. PourARN du rôle, spécifiez l'ARN du rôle que vous avez créé lorsqueconfigurer le chiffrement.
   c. PourARN secret, spécifiez l'ARN quiAWS Secrets Managerattribué lorsque vousa créé le secret pour stocker la clé de chiffrement.
   d. PourAlgorithme de déchiffrement, choisissez le type de cryptage fourni par l'expéditeur.
9. Au bas de la page, choisissezCréer un flux.

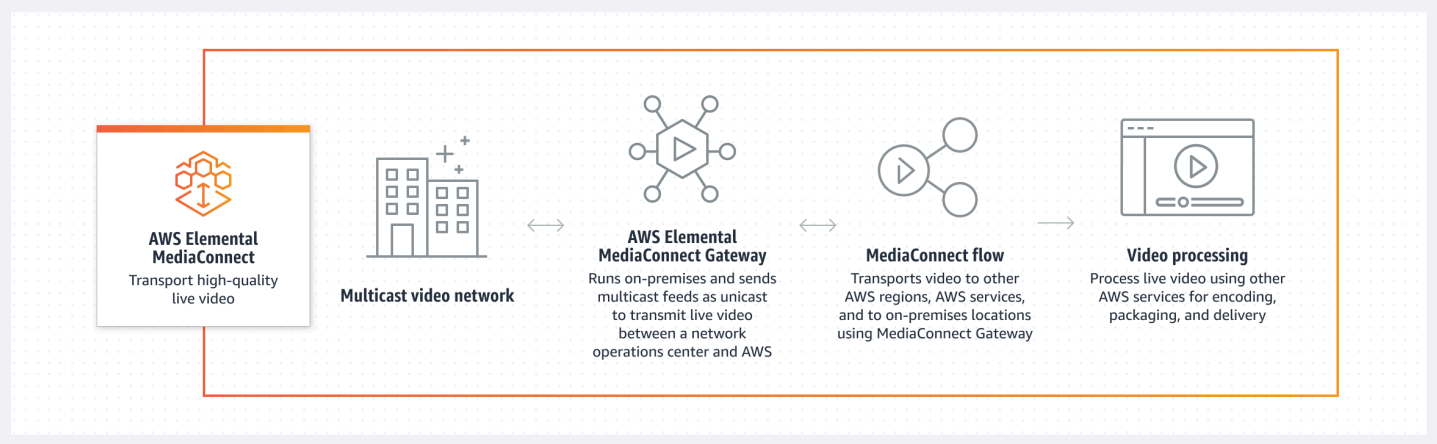
> **Note**
>
> Le flux ne démarre pas automatiquement. Vous devezdémarrer le fluxmanuellement.

10. Ajouter des sortiespour spécifier où vous souhaitez utiliser AWS Elemental MediaConnect pour envoyer le contenu, oudroits à des subventionspour autoriser les utilisateurs d'autresAWScomptes pour s'abonner à votre contenu.

Passerelle AWS Elemental MediaConnect

AWS Elemental MediaConnect Gateway est une fonctionnalité MediaConnect qui déploie des ressources sur site pour le transport de vidéos en direct vers et depuis le. AWS Cloud MediaConnect Gateway vous permet de diffuser des vidéos en direct AWS Cloud depuis le matériel sur site, ainsi que de distribuer des vidéos en direct depuis votre centre AWS Cloud de données local.

Le graphique suivant décrit un flux de travail dans lequel AWS Elemental MediaConnect Gateway s'exécute sur site et envoie des flux de multidiffusion en monodiffusion. Ce processus transmet une vidéo en direct entre le centre des opérations sur site et le AWS Cloud. À partir de là, AWS Elemental MediaConnect Gateway distribue le même contenu vers un autre emplacement sur site.



Cette section abordera les sujets suivants :

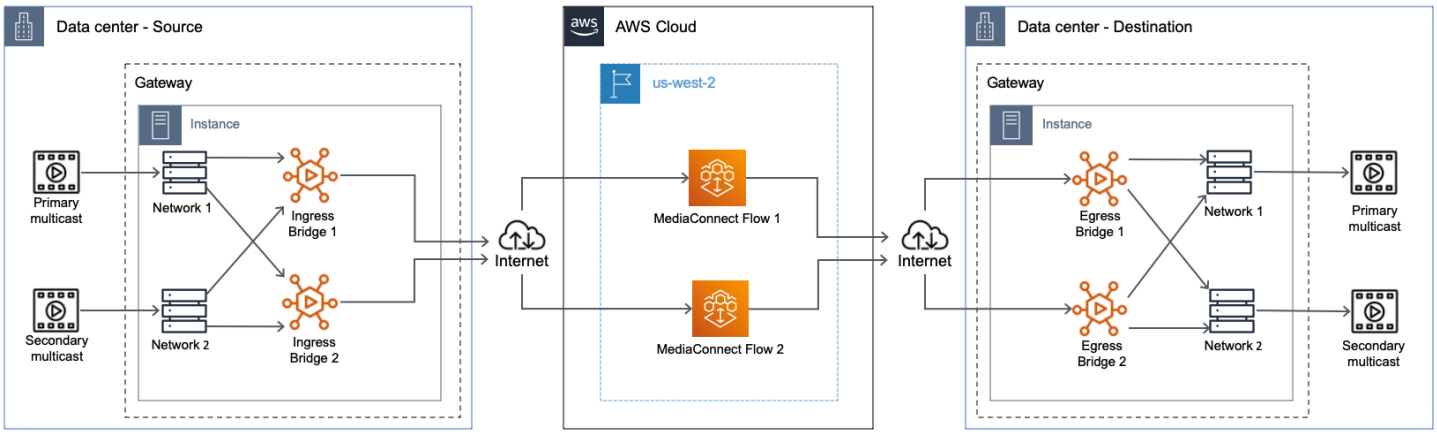
- Conditions préalables : informations sur le système local et autres considérations relatives à l'utilisation MediaConnect de Gateway.
- Composants de MediaConnect Gateway : explication de MediaConnect Gateway et de ses composants.
- Création d'une passerelle : step-by-step instructions pour créer votre passerelle et ses composants.

Composants de MediaConnect Gateway

AWS Elemental MediaConnect Gateway est composé de quatre composants principaux : les passerelles, les réseaux, les instances et les ponts. Chacun de ces composants est expliqué plus en détail dans les sections suivantes de ce guide. Ce qui suit décrit la relation de base entre ces composants :

- Passerelles : regroupement logique d'instances et de ponts. Chaque passerelle utilise des informations IP définies par l'utilisateur pour la communication entre les centres de données et le. AWS Cloud
- Réseaux : un réseau de MediaConnect passerelle est un ensemble d'informations IP que les instances et les ponts utilisent pour communiquer sur le réseau local de votre centre de données. Les informations réseau doivent correspondre au réseau local du centre de données que vous utilisez pour communiquer avec la passerelle. Chaque MediaConnect passerelle peut contenir au maximum deux réseaux. Toutes les passerelles doivent contenir au moins un réseau.
- Instances : instance de calcul exécutée sur l'équipement de votre centre de données et gérée par MediaConnect. Cette instance est une implémentation locale du MediaConnect service et est contenue dans une passerelle. Les instances utilisent des ponts pour communiquer entre votre centre de données et le AWS Cloud. Vous créez des instances en installant le logiciel sur un serveur local.
- Ponts : connexion entre les instances de votre centre de données et le AWS Cloud. Un pont peut être utilisé pour envoyer des vidéos depuis votre centre AWS Cloud de données ou depuis votre centre de données vers le AWS Cloud.

Le graphique suivant décrit les interactions de chaque composant dans un scénario de flux de travail courant. Dans ce flux de travail, la multidiffusion depuis le centre de données est ingérée dans une instance de passerelle et transmise via un pont vers MediaConnect le. AWS CloudÀ partir de AWS Cloud, la multidiffusion est distribuée vers l'instance de passerelle d'un autre centre de données.



MediaConnect Terminologie du portail

La section suivante fournit des détails sur les concepts et la terminologie de MediaConnect Gateway.

- Entrée : dans MediaConnect Gateway, l'entrée fait référence au contenu qui y est contribué AWS Cloud depuis un emplacement sur site. Si le contenu quitte votre position via un pont d'entrée, cela signifie que sa destination est AWS.
- Sortie : dans MediaConnect Gateway, la sortie fait référence au contenu distribué sur votre site à partir du. AWS Cloud Si le contenu entre dans votre position par un pont de sortie, cela signifie que sa source est AWS.
- Flux cloud : MediaConnect flux existant dans le AWS Cloud. Il s'agit généralement d'un MediaConnect flux existant que vous utilisez peut-être déjà et que vous souhaitez distribuer sur une passerelle locale.
- Source de flux : une source qui provient du AWS Cloud. Un pont de sortie utilise ce type de source.
- Source réseau : source qui provient de votre site sur site. Un pont d'entrée utilise ce type de source.
- Sortie de flux : sortie délivrée au AWS Cloud. Un pont d'entrée utilise ce type de sortie.
- Sortie réseau : sortie qui est délivrée à votre site sur site. Un pont de sortie utilise ce type de sortie.

Prérequis

Avant de pouvoir utiliser AWS Elemental MediaConnect Gateway, vous devez disposer des autorisations appropriées pour accéder aux composants, les visualiser et les modifier MediaConnect . Compte AWS En outre, vous aurez besoin d'un matériel physique conforme aux exigences de la MediaConnect passerelle répertoriées dans les sections suivantes.

Systèmes d'exploitation et architectures système pris en charge

Informations générales

AWS Elemental MediaConnect Gateway repose sur le service Amazon Elastic Container Service Anywhere (ECS Anywhere). Amazon ECS Anywhere fournit une assistance pour l'enregistrement d'une instance externe, telle qu'un serveur sur site, dans votre AWS infrastructure. En raison de cette architecture, les instances externes utilisant MediaConnect Gateway doivent être conformes aux exigences d'Amazon ECS Anywhere et aux exigences supplémentaires spécifiques à MediaConnect Gateway. Les sections suivantes répertorient les exigences en matière de matériel et de système d'exploitation (OS), en plus des exigences MediaConnect spécifiques à Gateway.

Le tableau suivant contient les quotas par défaut pour chaque composant de la MediaConnect passerelle.

Composant	Quota par défaut	Ce quota peut-il être augmenté ?
Nombre maximum de passerelles pour chaque Région AWS	3	Oui
Nombre maximal d'instances pour chaque passerelle	20	Non
Nombre maximum de ponts pour chaque passerelle	40	Non
Débit maximal pour chaque pont	100 Mbits/s	Non

Architectures système prises en charge

Le tableau suivant contient les architectures système recommandées pour vos instances de passerelle individuelles. Le système déterminera le nombre maximum de ponts pouvant être exécutés sur l'instance. Seules les architectures de processeur x86_64 sont prises en charge. MediaConnect Gateway ne prend pas en charge les processeurs basés sur ARM :

Nombre de ponts	Noyaux de vCPU (2,6 GHz)	Noyaux de vCPU (3,0 GHz)	Mémoire vive minimale (Go)	Espace disque minimal (Go)
10	2	2	4	25
25	6	4	8	25
40	10	8	16	25

Références du processeur

Les architectures des processeurs sont comparées à l'aide des processeurs suivants :

- 2,6 GHz - Intel E5-2660 v3

- 3,0 GHz - AMD 7302

Systèmes d'exploitation pris en charge

La liste suivante contient les systèmes d'exploitation (SE) et les configurations logicielles pris en charge pour vos instances MediaConnect Gateway.

Système d'exploitation recommandé

- Ubuntu 20.04

Systèmes d'exploitation pris en charge

Vous pouvez enregistrer des instances MediaConnect Gateway sur d'autres distributions Linux prises en charge par Amazon ECS Anywhere. Les systèmes d'exploitation Windows ne sont pas pris en charge par MediaConnect Gateway. Consultez le guide de l'utilisateur d'Amazon ECS pour obtenir la liste complète des distributions Linux prises en charge : Systèmes d'exploitation pris en charge

Logiciel requis

- Docker - MediaConnect Gateway nécessite que vous installiez la dernière version de Docker. Si vous utilisez une distribution Linux autre que RHEL, le script d'enregistrement d'instance fourni par MediaConnect installera Docker pour vous. Ni Docker ni les référentiels de packages ouverts de RHEL ne prennent en charge l'installation native de Docker sur RHEL. Lorsque vous utilisez RHEL, vous devez vous assurer que Docker est installé avant d'exécuter le script d'enregistrement d'instance décrit dans ce document.

Réseaux

Un réseau de passerelle est un ensemble d'informations IP qui seront utilisées par les instances et les ponts pour communiquer sur le réseau de votre centre de données local. Les informations du réseau de passerelle doivent correspondre au réseau local du centre de données que vous utilisez pour communiquer avec la passerelle. Chaque passerelle peut contenir au maximum deux réseaux. Toutes les passerelles doivent contenir au moins un réseau.

Création ou suppression d'un réseau de passerelle

Vous devez créer les réseaux lors de la création initiale d'une nouvelle passerelle. Vous ne pouvez pas ajouter ou modifier un réseau après la création initiale de la passerelle. Pour plus d'informations sur la création initiale d'une passerelle et de ses réseaux, consultezCréation d'une passerelle (console).

Pour supprimer un réseau, vous devez supprimer la passerelle qui lui est associée. Pour plus d'informations sur la suppression d'une passerelle et de ses réseaux, consultezSuppression d'une passerelle et de ses composants (console).

instances

Une instance est une instance de calcul exécutée sur l'équipement de votre centre de données et gérée par MediaConnect Gateway. Cette instance est une implémentation locale du MediaConnect service et est contenue dans une passerelle. Les instances utilisent des ponts pour communiquer entre votre centre de données et le AWS Cloud. Les instances sont créées en installant le logiciel sur un serveur local.

Enregistrement d'une instance de MediaConnect Gateway

Vous pouvez enregistrer une instance en exécutant une commande Linux personnalisée sur l'appareil qui hébergera l'instance. Vous générez la commande en suivant le processus d'enregistrement de l'instance dans le AWS Management Console.

Pour enregistrer une instance de MediaConnect Gateway

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, sélectionnez la passerelle sur laquelle vous souhaitez enregistrer l'instance.
3. Sur la page Détails de la passerelle, sélectionnez l'onglet Instances. Sélectionnez Enregistrer une instance.
4. Sur la page Register les instances de Gateway, effectuez les étapes suivantes :

    1. Pour la durée de validité de la clé d'activation, entrez le nombre de jours pendant lesquels la clé d'activation restera active. Après ce nombre de jours, la clé ne fonctionnera plus lors de l'enregistrement d'une instance de passerelle.

2. Dans le champ Nombre d'instances, entrez le nombre d'instances que vous souhaitez enregistrer sur votre passerelle avec cette clé d'activation.
3. Pour Instance role (Rôle d'instance), choisissez le rôle IAM à associer à vos instances externes.
4. Sélectionnez Générer une commande d'enregistrement.

5. Une commande Linux sera affichée. Copiez la commande. Vous devez exécuter cette commande sur chaque instance que vous souhaitez enregistrer auprès de cette passerelle.

> **Important**
>
> La partie bash du script doit être exécutée en tant que root. Si la commande n'est pas exécutée en tant que racine, une erreur est renvoyée.

6. Après quelques minutes, l'instance s'enregistrera auprès de la passerelle. Toutes les instances enregistrées sur cette passerelle apparaîtront dans l'onglet Instances.

Annulation de l'enregistrement d'une instance de passerelle

Vous pouvez annuler l'enregistrement d'une instance que vous ne souhaitez plus utiliser dans MediaConnect Gateway. En désenregistrant l'instance, elle ne prendra plus en charge les ponts et ne fera plus partie de votre passerelle. Si vous souhaitez réutiliser l'instance pour Amazon ECS Anywhere ou en tant qu'autre instance de passerelle, vous devez suivre les étapes supplémentaires de l'étape 6 pour préparer l'instance désenregistrée en vue de sa réutilisation.

Pour désenregistrer une instance de passerelle

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, sélectionnez la passerelle qui contient l'instance que vous souhaitez désenregistrer.
3. Sur la page Détails de la passerelle, sélectionnez l'onglet Instances. Sélectionnez l'ID d'instance de l'instance que vous souhaitez désenregistrer.
4. Sélectionnez Désenregistrer.
5. Confirmez le désenregistrement de l'instance en sélectionnant Désenregistrer l'instance.
6. Répétez les étapes précédentes pour toutes les instances supplémentaires dont vous avez besoin pour annuler l'enregistrement.

Pour réutiliser une instance de passerelle (facultatif)

Si vous souhaitez réutiliser l'instance pour Amazon ECS Anywhere ou en tant qu'autre instance de passerelle, vous devez suivre les étapes suivantes.

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, sélectionnez la passerelle qui contient l'instance que vous souhaitez réutiliser.
3. Sur la page Détails de la passerelle, sélectionnez l'onglet Instances. Localisez l'ID d'instance de l'instance que vous souhaitez réutiliser.
4. Assurez-vous que l'état de l'instance est Désenregistré pour l'instance que vous souhaitez réutiliser.
5. À partir d'un ordinateur disposant de cet accès, connectez-vous à l'instance via SSH.
6. Exécutez les commandes suivantes, dans l'ordre.

```
sudo docker stop $(docker ps -f "name=MediaConnectGatewayAgent" -q); \
sudo docker stop ecs-agent; \
sudo systemctl stop ecs amazon-ssm-agent; \
sudo yum remove -y amazon-ecs-init amazon-ssm-agent;  `# or apt or snap as needed`
 \
sudo rm /var/lib/ecs /etc/ecs /var/lib/amazon/ssm /var/log/ecs /var/log/amazon/ssm
 -rf; \
sudo docker rm -f ecs-agent ssm-agent; \
sudo docker container rm -f $(docker ps -a -f "name=MediaConnectGatewayAgent" -q);
 \
sudo docker volume rm -f ecsdata docker run; \
sudo pkill -f -KILL network_bootstra[p]; \
sudo pkill -KILL mcproxy;
```

Pour plus d'informations sur la suppression d'une MediaConnect passerelle et de ses réseaux, voir : Suppression d'une passerelle et de ses composants (console)

Ponts

Un pont est une connexion entre les instances de votre centre de données et le AWS Cloud. Selon le type de pont sélectionné, un pont peut être utilisé pour envoyer du contenu depuis votre centre AWS Cloud de données ou depuis votre centre de données vers le AWS Cloud.

Types de ponts

AWS Elemental MediaConnect Gateway prend en charge deux types de ponts. Chaque type de pont a un objectif différent et détermine si vous allez contribuer au contenu du site AWS Cloud ou le distribuer à un emplacement physique. Voici les deux types de ponts et leurs différentes fonctions :

Pont d'entrée : ground-to-cloud pont. Sur un pont d'entrée, le contenu provient de vos locaux et est livré au. AWS Cloud

Pont de sortie : cloud-to-ground pont. Sur un pont de sortie, le contenu provient d'un MediaConnect flux existant et est livré dans vos locaux.

Sources du pont

Pour chaque pont, vous devez créer au moins une source. La source est le contenu qui sera ingéré par la MediaConnect passerelle. L'origine du contenu source sera différente selon le type de pont sélectionné. Si vous créez plusieurs sources de pont, vous pouvez améliorer la résilience de votre

pont en activant le basculement pendant le processus de création. Les deux types de sources sont les suivants :

- Source du pont d'entrée : dans le cas d'un pont d'entrée, le contenu provient de vos locaux et est diffusé dans le cloud. Lorsque vous créez une source de pont d'entrée, vous devez sélectionner le protocole (RTP, RTP-FEC ou UDP) et saisir l'adresse IP de multidiffusion et le port du contenu provenant de vos locaux.
- Source du pont de sortie : pour un pont de sortie, le contenu provient d'un MediaConnect flux existant et est livré dans vos locaux. Lorsque vous créez une source de pont de sortie, vous devez sélectionner le MediaConnect flux que vous souhaitez envoyer dans vos locaux. Il n'est pas nécessaire de sélectionner le protocole. La source utilisera le même protocole que le flux existant.

Basculement à la source du pont

Si vous créez plusieurs sources de pont, vous pouvez améliorer la résilience de votre pont en activant le basculement pendant le processus de création. La configuration de basculement détermine le comportement d'AWS MediaConnect Elemental Gateway en cas de perte d'entrée source. Le type de pont déterminera lequel des deux modes de basculement est disponible. Les deux modes de basculement sont les suivants :

- Failover : ce mode permet de basculer entre une source principale et une source de sauvegarde. Vous pouvez spécifier une source comme source principale. La deuxième source sert de sauvegarde. Le service bascule vers la source de sauvegarde en cas de défaillance de la source principale et revient à la source principale dès qu'elle est fiable.
- Fusion : ce mode combine les sources en un seul flux, ce qui permet une restauration progressive après toute perte d'une source unique. En mode fusion, s'il manque un paquet à une source, le service extrait le paquet manquant de l'autre source.

Sorties du pont

Pour chaque pont, vous devez créer au moins une sortie. Les deux types de sorties sont les suivants :

- Sortie du pont d'entrée : dans le cas d'un pont d'entrée, le contenu provient de vos locaux et est diffusé dans le cloud. Il n'est pas nécessaire de configurer les sorties pour les types de ponts d'entrée. Lorsque vous créez un MediaConnect flux en utilisant le pont d'entrée comme source, la sortie est automatiquement créée au démarrage du flux.

- Sortie du pont de sortie : pour un pont de sortie, le contenu provient d'un MediaConnect flux existant et est livré dans vos locaux. Lorsque vous créez une sortie de pont de sortie, vous devez configurer l'adresse IP et les informations de protocole qui seront transmises à vos locaux. Les sorties du pont de sortie prennent en charge les protocoles RTP, RTP-FEC et UDP.

Création d'un pont MediaConnect Gateway

Après avoir enregistré au moins une instance sur votre passerelle, vous pouvez créer un pont. Le processus de création d'un pont varie en fonction du type de pont sélectionné à l'étape 4.

Pour créer un pont d'entrée

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, sélectionnez la passerelle sur laquelle vous souhaitez créer le pont.
3. Sur la page Détails de la passerelle, sélectionnez l'onglet Ponts. Sélectionnez Créer un pont.
4. Sur la page Créer un pont, effectuez les étapes suivantes dans la section Détails :
    1. Entrez un nom pour le pont.
    2. Pour Type de pont, sélectionnez Pont d'entrée.
    3. Entrez le débit maximal pour le contenu que vous transporterez sur le pont.
    4. Entrez le nombre maximal de sorties pour le pont.
5. Procédez ensuite aux étapes suivantes dans la section Sources. La source d'un pont d'entrée est le contenu de multidiffusion qui provient de vos locaux. Pour créer une source :
    1. Entrez un nom pour la source du pont.
    2. Sélectionnez un réseau. Il s'agit d'un réseau que vous avez créé lors du processus de configuration de la passerelle.
    3. Sélectionnez le protocole du contenu source.
    4. Entrez l'adresse IP de multidiffusion et le port de la source.
6. Si vous ajoutez plusieurs sources, vous pouvez configurer le basculement dans la section Configuration du basculement.
    a. Sélectionnez le mode Failover : Failover ou Merge
    b. Si vous sélectionnez Failover comme mode, sélectionnez l'une des sources que vous avez configurées à l'étape 5 comme source principale.

7. Sélectionnez Créer un pont.
8. Une fois le pont créé, vous pouvez le démarrer en sélectionnant Démarrer sur la page Détails du pont.

Pour créer un pont de sortie

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, sélectionnez la passerelle sur laquelle vous souhaitez créer le pont.
3. Sur la page Détails de la passerelle, sélectionnez l'onglet Ponts. Sélectionnez Créer un pont.
4. Sur la page Créer un pont, effectuez les étapes suivantes dans la section Détails :
    1. Entrez un nom pour le pont.
    2. Pour Type de pont, sélectionnez Pont de sortie.
    3. Entrez le débit maximal pour le contenu que vous transporterez sur le pont.
5. Procédez ensuite comme suit dans la section Sources :
    1. Entrez un nom pour la source du pont. Pour un pont de sortie, la source est le contenu provenant d'un MediaConnect flux et livré dans vos locaux.
    2. Sélectionnez un réseau. Il s'agit d'un réseau que vous avez créé lors du processus de configuration de la passerelle.
    3. Sélectionnez le Flow ARN. Il s'agit de l'ARN du MediaConnect flux que vous utiliserez comme source.
    4. Si ce flux utilise une interface VPC, sélectionnez-la.
6. Si vous ajoutez plusieurs sources, vous pouvez configurer le basculement dans la section Configuration du basculement.
    a. Lorsque vous sélectionnez un pont de sortie, le seul mode Failover disponible est Failover. Impossible de sélectionner la fusion.
    b. Sélectionnez l'une des sources que vous avez configurées à l'étape 5 comme source principale.
7. La dernière section de la création d'un pont de sortie est consacrée aux sorties. Procédez comme suit.
    1. Entrez un nom pour la sortie du pont.

2. Sélectionnez un réseau. Il s'agit d'un réseau que vous avez créé lors du processus de configuration de la passerelle.
3. Sélectionnez le protocole de transport que vous souhaitez utiliser pour la sortie.
4. Entrez une adresse IP pour la sortie. Il doit s'agir d'une adresse IP compatible avec votre réseau local.
5. Entrez le port de sortie. Il doit s'agir d'un port compatible avec votre réseau local.
6. Entrez un TTL (time-to-live) pour la sortie.

8. Sélectionnez Créer un pont.
9. Une fois le pont créé, vous pouvez le démarrer en sélectionnant Démarrer sur la page Détails du pont.

Création d'une passerelle (console)

L'installation commence par la création de la passerelle. Cela peut être fait dans la MediaConnect console, par programmation à l'aide de l' MediaConnect API ou en utilisant. AWS CloudFormation Après la création d'une MediaConnect passerelle et de ses réseaux, vous pouvez commencer à enregistrer des instances auprès de cette MediaConnect passerelle et à créer des ponts sur ces instances.

Rubriques

Création d'une passerelle (console)

La première étape consiste à créer la passerelle et un réseau. La passerelle est un regroupement logique d'instances et de ponts. Chaque passerelle utilise des informations IP définies par l'utilisateur pour la communication entre les centres de données et le. AWS Cloud

Pour créer une passerelle

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.

2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, choisissez Create gateway.
3. Sur la page Créer une passerelle, entrez le nom de votre passerelle. Ce nom ne pourra pas être modifié ultérieurement.
4. Pour les blocs CIDR de sortie : entrez un bloc CIDR pour la sortie de votre passerelle. Ces adresses IP doivent prendre la forme d'un bloc de routage interdomaine sans classe (CIDR) ; par exemple, 10.0.0.0/16. Ce bloc CIDR représente une plage d'adresses IP autorisées à contribuer au contenu ou à lancer des demandes de sortie pour les flux communiquant avec cette passerelle.

   > **Important**
   >
   > N'utilisez pas 0.0.0.0/0 pour les blocs CIDR de sortie. Cela ouvrira la porte d'entrée au public.

5. Dans la section Réseaux, saisissez le nom de votre premier réseau. Une passerelle peut contenir au maximum deux réseaux. Chaque nom de réseau doit être unique pour cette passerelle.
6. Entrez un bloc CIDR pour ce réseau. Pour terminer la création de la passerelle, cliquez sur le bouton Créer une passerelle.

Enregistrer une instance (console)

Après avoir créé une passerelle, vous pouvez enregistrer des instances auprès de cette passerelle. Une instance est une ressource informatique exécutée sur l'équipement de votre centre de données et gérée par MediaConnect. Cette instance est une implémentation locale du MediaConnect service et est contenue dans une passerelle. Les instances utilisent des ponts pour communiquer entre votre centre de données et le AWS cloud. Les instances sont créées en installant le logiciel sur un serveur local.

Pour enregistrer une instance

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, sélectionnez la passerelle sur laquelle vous souhaitez enregistrer l'instance.
3. Sur la page Détails de la passerelle, sélectionnez l'onglet Instances.

4. Dans l'onglet Instances, choisissez Enregistrer une instance.
5. Sur la page Register les instances de Gateway, effectuez les étapes suivantes :
    1. Pour la durée de validité de la clé d'activation, entrez le nombre de jours pendant lesquels la clé d'activation restera active. Après ce nombre de jours, la clé ne fonctionnera plus lors de l'enregistrement d'une instance de passerelle.
    2. Dans le champ Nombre d'instances, entrez le nombre d'instances que vous souhaitez enregistrer sur votre passerelle à l'aide de la clé d'activation.
    3. Pour Rôle d'instance, choisissez le rôle AWS Identity and Access Management (IAM) à associer à vos instances externes.
    4. Choisissez Générer une commande d'enregistrement.
6. Une commande Linux sera affichée. Copiez la commande. Vous devez exécuter cette commande sur chaque instance que vous souhaitez enregistrer auprès de cette passerelle.

    > **Important**
    >
    > La partie bash du script doit être exécutée en tant que root. Si la commande n'est pas exécutée en tant que racine, une erreur est renvoyée.

7. Après quelques minutes, l'instance s'enregistrera auprès de la passerelle. Toutes les instances enregistrées sur cette passerelle apparaîtront dans l'onglet Instances.

Création d'un pont (console)

Après avoir enregistré au moins une instance sur votre passerelle, vous pouvez créer un pont. Le processus de création d'un pont varie en fonction du type de pont sélectionné.

Pour créer un pont d'entrée

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, sélectionnez la passerelle sur laquelle vous souhaitez créer le pont.
3. Sur la page Détails de la passerelle, sélectionnez l'onglet Ponts.
4. Dans l'onglet Ponts, sélectionnez Créer un pont.
5. Sur la page Créer un pont, effectuez les étapes suivantes dans la section Détails :

1. Entrez un nom pour le pont.
2. Sélectionnez un type de pont d'entrée.
3. Entrez le débit maximal pour le contenu que vous transporterez sur le pont.
4. Entrez le nombre maximal de sorties pour le pont.

6. Procédez ensuite aux étapes suivantes dans la section Sources. La source d'un pont d'entrée est le contenu de multidiffusion qui provient de vos locaux :

   1. Entrez un nom pour la source du pont.
   2. Sélectionnez un réseau. Il s'agit d'un réseau que vous avez créé lors du processus de configuration de la passerelle.
   3. Sélectionnez le protocole pour cette source.
   4. Entrez l'adresse IP de multidiffusion et le port de la source.

7. Si vous ajoutez plusieurs sources, vous pouvez configurer le basculement à l'aide de la section Configuration du basculement.

   a. Sélectionnez le mode Failover : Failover ou Merge
   b. Facultatif - Si vous sélectionnez Failover comme mode, vous pouvez sélectionner l'une des sources que vous avez précédemment configurées comme source principale. Si vous ne sélectionnez pas de source principale, vous en MediaConnect sélectionnerez une au hasard.

8. Pour terminer la création du pont, choisissez Create bridge.
9. Une fois le pont créé, vous pouvez le démarrer en sélectionnant Démarrer sur la page Détails du pont.

Pour créer un pont de sortie

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, sélectionnez la passerelle sur laquelle vous souhaitez créer le pont.
3. Sur la page Détails de la passerelle, sélectionnez l'onglet Ponts. Sélectionnez Créer un pont.
4. Sur la page Créer un pont, effectuez les étapes suivantes dans la section Détails :

   1. Entrez un nom pour le pont.
   2. Sélectionnez un type de pont de sortie.

3. Entrez le débit maximal pour le contenu que vous transporterez sur le pont.

5. Procédez ensuite comme suit dans la section Sources :

   1. Entrez un nom pour la source du pont. Pour un pont de sortie, la source est le contenu provenant d'un MediaConnect flux et livré dans vos locaux.
   2. Sélectionnez un réseau. Il s'agit d'un réseau que vous avez créé lors du processus de configuration de la passerelle.
   3. Sélectionnez le Flow ARN. Il s'agit de l'ARN du MediaConnect flux que vous allez utiliser comme source.
   4. Si ce flux utilise une interface VPC, sélectionnez-la.

6. Si vous ajoutez plusieurs sources, vous pouvez configurer le basculement à l'aide de la section Configuration du basculement.

   a. Lorsque vous sélectionnez un pont de sortie, le seul mode Failover disponible est Failover. Impossible de sélectionner la fusion.

   b. Facultatif : sélectionnez l'une des sources que vous avez créées précédemment comme source principale. Si vous ne sélectionnez pas de source principale, vous en MediaConnect sélectionnerez une au hasard.

7. La dernière section de la création d'un pont de sortie est consacrée aux sorties. Procédez comme suit.

   1. Entrez un nom pour la sortie du pont.
   2. Sélectionnez un réseau. Il s'agit d'un réseau que vous avez créé lors du processus de configuration de la MediaConnect passerelle.
   3. Sélectionnez un protocole de transport pour la sortie.
   4. Entrez une adresse IP pour la sortie. Il doit s'agir d'une adresse IP compatible avec votre réseau local.
   5. Entrez le port de sortie. Il doit s'agir d'un port compatible avec votre réseau local.
   6. Entrez un TTL (time-to-live) pour la sortie.

8. Sélectionnez Créer un pont.

9. Une fois le pont créé, vous pouvez le démarrer en sélectionnant Démarrer sur la page de détails du pont.

Suppression d'une passerelle et de ses composants (console)

Pour supprimer une passerelle, vous devez d'abord supprimer tous ses composants, tels que ses réseaux, ses instances et ses ponts. Le processus de suppression d'une passerelle et de ses composants est le suivant.

Pour supprimer une passerelle

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Gateways. Dans la section Passerelles, sélectionnez la passerelle que vous souhaitez supprimer.
3. Sur la page de détails de la MediaConnect passerelle, sélectionnez l'onglet Ponts. Procédez comme suit pour supprimer les ponts :
    1. Sélectionnez le pont que vous souhaitez supprimer.
    2. Si le pont a été démarré, sélectionnez Arrêter.
    3. Lorsque le pont est arrêté, sélectionnez Supprimer.
    4. Confirmez la suppression du pont en sélectionnant Supprimer le pont.
    5. Répétez ces étapes pour tous les ponts supplémentaires que vous devez supprimer.
4. Retournez à la page Détails de la passerelle, sélectionnez l'onglet Instances. Procédez comme suit pour supprimer les instances :
    1. Sélectionnez l'instance que vous souhaitez supprimer.
    2. Sélectionnez Désenregistrer.
    3. Confirmez le désenregistrement de l'instance en sélectionnant Désenregistrer l'instance.
    4. Répétez ces étapes pour toutes les instances supplémentaires dont vous avez besoin pour annuler l'enregistrement.

    > **Note**
    >
    > FACULTATIF : Si vous souhaitez réutiliser l'instance pour Amazon ECS Anywhere ou en tant qu'autre instance de passerelle, vous devez suivre les étapes suivantes. Si ce n'est pas le cas, passez à l'étape 5.

a. Assurez-vous que l'état de l'instance est Désenregistré pour l'instance que vous souhaitez réutiliser.

b. À partir d'un ordinateur disposant de cet accès, connectez-vous à l'instance via SSH.

c. Exécutez les commandes suivantes, dans l'ordre :

```
sudo docker stop $(sudo docker ps -f "name=MediaConnectGatewayAgent" -q); \
sudo docker stop ecs-agent; \
sudo systemctl stop ecs amazon-ssm-agent; \
sudo yum remove -y amazon-ecs-init amazon-ssm-agent;  `# or apt or snap as
 needed` \
sudo rm /var/lib/ecs /etc/ecs /var/lib/amazon/ssm /var/log/ecs /var/log/amazon/
ssm -rf; \
sudo docker rm -f ecs-agent ssm-agent; \
sudo docker container rm -f $(sudo docker ps -a -f
 "name=MediaConnectGatewayAgent" -q); \
sudo docker volume rm -f ecsdata docker run; \
sudo pkill -f -KILL network_bootstra[p]; \
sudo pkill -KILL mcproxy;
```

5. Après avoir correctement supprimé tous les ponts et désenregistré toutes les instances associées à la passerelle, vous pouvez supprimer la passerelle. La suppression de la passerelle supprimera tous les réseaux créés sous cette passerelle.

   1. Dans le volet de navigation, sélectionnez Gateways.
   2. Dans la section Passerelles, sélectionnez la passerelle que vous souhaitez supprimer pour afficher la page de détails de cette passerelle.
   3. Choisissez le bouton Supprimer.
   4. Confirmez la suppression de la passerelle en choisissant Supprimer la passerelle.

Création d'une passerelle (AWS CLI)

Pour créer la passerelle à l'aide du AWS CLI, consultez les instructions suivantes.

Rubriques

Création d'une passerelle (AWS CLI)

La passerelle est un regroupement logique d'instances et de ponts. Chaque passerelle utilise des informations IP définies par l'utilisateur pour la communication entre les centres de données et le. AWS Cloud

Avant de créer une passerelle à l'aide du AWS CLI, vous aurez besoin du nom, des informations IP CIDR de sortie et des informations réseau de la passerelle que vous souhaitez créer. Stockez ces informations dans un fichier JSON sur l'ordinateur qui exécute le AWS CLI. Le fichier JSON doit être nommé`gateway.json`. L'exemple suivant montre les sections et le formatage corrects pour le fichier JSON.

```
{
    "Name": "gateway",
    "EgressCidrBlocks": [
        "10.20.30.0/24"
    ],
    "Networks": [
        {
            "Name": "blue",
            "CidrBlock": "172.31.48.0/20",
        }
    ]
}
```

Pour créer une passerelle à l'aide du AWS CLI

1. Entrez la commande suivante dans l' AWS CLI interface. Remplacez les `<region>` valeurs `<yourprofile>` et par le profil souhaité et Région AWS.

   ```
   aws --profile <yourprofile> --region <region> mediaconnect create-gateway
         --cli-input-json file://gateway.json
   ```

2. Le AWS CLI renverra une réponse comme dans l'exemple suivant.

   ```
       "Gateway": {
           "EgressCidrBlocks": [
               "10.20.30.0/24"
           ],
           "GatewayArn": "arn:aws:mediaconnect:us-
   west-2:111122223333:gateway:1-23aBC45dEF67hiJ8-12AbC34DE5fG:gateway",
   ```

```
        "GatewayState": "CREATING",
        "Name": "gateway",
        "Networks": [
            {
                "CidrBlock": "172.31.48.0/20",
                "Name": "blue"
            }
        ]
    }
}
```

3. La MediaConnect passerelle a été créée.

Enregistrer une instance (AWS CLI)

Une fois que vous avez créé une passerelle, vous pouvez enregistrer des instances auprès de cette passerelle. Une instance est une ressource informatique exécutée sur l'équipement de votre centre de données et gérée par MediaConnect. Cette instance est une implémentation locale du MediaConnect service et est contenue dans une passerelle. Les instances utilisent des ponts pour communiquer entre votre centre de données et le AWS Cloud. Les instances sont créées en installant le logiciel sur un serveur local.

L'enregistrement d'une instance à l'aide du n' AWS CLI est actuellement pas pris en charge. Suivez les instructions de la console Enregistrer une instance (console) pour enregistrer l'instance à l'aide de la AWS console.

Création d'un pont (AWS CLI)

Après avoir enregistré au moins une instance dans votre composant de passerelle, vous pouvez créer un pont. Le pont est la connexion entre les instances et le AWS Cloud.

Avant de créer un pont à l'aide du AWS CLI, vous devez recueillir les détails du pont que vous souhaitez créer. Ces informations seront stockées dans un fichier JSON sur l'ordinateur exécutant le AWS CLI. Le fichier JSON doit être nommé`bridge.json`. L'exemple suivant montre les sections et le formatage corrects pour le fichier JSON.

```
{
    "Name": "bridge",
    "PlacementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:gateway:1-23aBC45dEF67hiJ8-12AbC34DE5fG:gateway",
    "EgressGatewayBridge": {
        "MaxBitrate": 100000000
    },
    "SourceFailoverConfig": {
        "FailoverMode": "FAILOVER",
        "State": "ACTIVE"
    },
    "Sources": [
        {
            "FlowSource": {
                "Name": "Source0",
                "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
UAECXlABCQJeVwMB-95ec11ac6059:gatewayFlow",
                "NetworkName": "blue"
            }
        },
        {
            "FlowSource": {
                "Name": "Source1",
                "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
ECRZVGADYMGtPGTM-c1iPQ5FNL7Qn:gatewayFlow",
                "NetworkName": "blue",
                "FlowVpcInterfaceAttachment": {
                    "VpcInterfaceName": "VPCIF"
                }
            }
        }
    ],
    "Outputs": [
        {
            "NetworkOutput": {
                "Name": "Output0",
                "NetworkName": "blue",
                "IpAddress": "225.1.2.3",
                "Port": 5010,
                "Protocol": "rtp-fec",
                "Ttl": 8
            }
        },
```

```
        {
            "NetworkOutput": {
                "Name": "Output1",
                "NetworkName": "blue",
                "IpAddress": "225.1.2.4",
                "Port": 6010,
                "Protocol": "rtp",
                "Ttl": 250
            }
        }
    ]
}
```

Pour créer un pont à l'aide du AWS CLI

1. Entrez la commande suivante dans l' AWS CLI interface. Remplacez les `<region>` valeurs `<yourprofile>` et par le profil souhaité et Région AWS.

   ```
   aws --profile <yourprofile> --region <region> mediaconnect create-bridge
         --cli-input-json file://bridge.json
   ```

2. Le AWS CLI renverra une réponse comme dans l'exemple suivant.

```
{
    "Bridge": {
        "BridgeArn": "arn:aws:mediaconnect:us-west-2:111122223333:bridge:1-
GLxlBRLrHzzvpwyb-1dd820
66b207:bridge",
        "BridgeMessages": [],
        "BridgeState": "STANDBY",
        "EgressGatewayBridge": {
            "MaxBitrate": 100000000
        },
        "Name": "bridge",
        "Outputs": [
            {
                "NetworkOutput": {
                    "IpAddress": "225.1.2.3",
                    "Name": "Output0",
                    "NetworkName": "blue",
                    "Port": 5010,
                    "Protocol": "rtp-fec",
                    "Ttl": 8
                }
            },
            {
                "NetworkOutput": {
                    "IpAddress": "225.1.2.4",
                    "Name": "Output1",
                    "NetworkName": "blue",
                    "Port": 6010,
                    "Protocol": "rtp",
                    "Ttl": 250
                }
            }
        ],
        "PlacementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:gateway:1-23aBC45dEF67hiJ8-12AbC34DE5fG:gateway",
        "SourceFailoverConfig": {
            "FailoverMode": "FAILOVER",
            "State": "ENABLED"
        },
        "Sources": [
            {
                "FlowSource": {
                    "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
UAECXlABCQJeVwMB-95ec11ac6059:gatewayFlow",
```

```
                    "Name": "Source0",
                    "NetworkName": "blue"
                }
            },
            {
                "FlowSource": {
                    "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
ECRZVGADYMGtPGTM-c1iPQ5FNL7Qn:gatewayFlow",
                    "Name": "Source1",
                    "NetworkName": "blue",
                    "FlowVpcInterfaceAttachment": {
                        "VpcInterfaceName": "VPCIF"
                    }
                }
            }
        ]
    }
}
```

3. Le pont a été créé.

Supprimer une passerelle et ses composants (AWS CLI)

Pour supprimer une passerelle, vous devez d'abord supprimer tous ses composants, tels que ses réseaux, ses instances et ses ponts. Voici le processus de suppression d'une passerelle et de ses composants à l'aide de AWS Command Line Interface (AWS CLI).

Pour supprimer une passerelle à l'aide du AWS CLI

1. Supprimez les ponts en exécutant la commande suivante.

```
aws --profile <Profile> --region <Region> mediaconnect delete-bridge --bridge-
arn <BridgeArn>
```

2. Désenregistrez les instances en exécutant la commande suivante.

```
aws --profile <Profile> --region <Region> mediaconnect deregister-gateway-instance
 --gateway-instance-arn <GatewayArn>
```

> **Note**
>
> FACULTATIF : Si vous souhaitez réutiliser l'instance pour Amazon ECS Anywhere ou en tant qu'autre instance AWS Elemental MediaConnect Gateway, vous devez suivre les étapes suivantes. Si ce n'est pas le cas, passez à l'étape 3.

a. Assurez-vous qu'il s'`InstanceState`agit `DEREGISTERED` de l'instance que vous souhaitez réutiliser. Vous pouvez vérifier à l'aide de la `describe-gateway-instance` commande illustrée dans l'exemple suivant.

```
aws --profile <Profile> --region <Region> mediaconnect describe-gateway-
instance
      --gateway-instance-arn <GatewayInstanceArn>
```

b. À partir d'un ordinateur disposant de cet accès, connectez-vous à l'instance via SSH.

c. Exécutez les commandes suivantes, dans l'ordre.

```
sudo docker stop $(sudo docker ps -f "name=MediaConnectGatewayAgent" -q); \
sudo docker stop ecs-agent; \
sudo systemctl stop ecs amazon-ssm-agent; \
sudo yum remove -y amazon-ecs-init amazon-ssm-agent;  `# or apt or snap as
 needed` \
sudo rm /var/lib/ecs /etc/ecs /var/lib/amazon/ssm /var/log/ecs /var/log/amazon/
ssm -rf; \
sudo docker rm -f ecs-agent ssm-agent; \
sudo docker container rm -f $(sudo docker ps -a -f
 "name=MediaConnectGatewayAgent" -q); \
sudo docker volume rm -f ecsdata docker run; \
sudo pkill -f -KILL network_bootstra[p]; \
sudo pkill -KILL mcproxy;
```

3. Supprimez la passerelle. Cela supprimera tous les réseaux associés à la passerelle.

```
aws --profile <Profile> --region <Region> mediaconnect delete-gateway --gateway-
arn <GatewayArn>
```

Interfaces VPC

Un cloud privé virtuel (VPC) basé sur le service Amazon Virtual Private Cloud est votre réseau privé isolé de manière logique dans le cloud. AWS Vous pouvez configurer une interface VPC pour établir une connexion entre votre flux AWS MediaConnect Elemental et votre VPC.

Pour plus d'informations, consultez les sections suivantes.

- Création d'un flux de transport utilisant une source VPC
- Ajouter une interface VPC à un flux
- Supprimer une interface VPC d'un flux
- Ajouter une source VPC à un flux existant
- Ajouter des sorties VPC à un flux
- Considérations relatives aux groupes de sécurité pour les interfaces VPC

Ajouter une interface VPC à un flux

Pour éviter de diffuser votre contenu sur l'Internet public, vous pouvez ajouter une interface VPC à votre MediaConnect flux. Vous pouvez ajouter jusqu'à deux interfaces VPC à chaque flux.

Important

Avant de commencer cette procédure, assurez-vous que les étapes suivantes ont été effectuées :

- Dans Amazon VPC, configurez votre VPC et les groupes de sécurité associés. Pour plus d'informations sur les VPC, consultez le Guide de l'utilisateur Amazon VPC. Pour plus d'informations sur la configuration des groupes de sécurité pour qu'ils fonctionnent avec votre interface VPC, consultez. Considérations relatives aux groupes de sécurité
- Dans IAM, configurez-le en MediaConnect tant que service de confiance.

Les journaux de flux VPC peuvent être utilisés pour capturer des informations sur le trafic IP à destination et en provenance des interfaces réseau de votre VPC. Les données du journal de flux peuvent être publiées sur CloudWatch Logs, Amazon S3 ou Data Firehose. Pour plus

d'informations sur les journaux de flux VPC, consultez la section Journalisation du trafic IP à l'aide des journaux de flux VPC dans le guide de l'utilisateur Amazon VPC.

Pour ajouter une interface VPC à un flux (console)

1. Sur la page Flux, choisissez le nom du flux que vous souhaitez mettre à jour.
2. Choisissez l'onglet Interfaces VPC.
3. Choisissez Ajouter une interface VPC.
4. Dans Nom, spécifiez le nom de votre interface VPC. Le nom de l'interface VPC doit être unique dans le flux.
5. Pour le type d'interface réseau, spécifiez le type d'adaptateur réseau que vous MediaConnect souhaitez utiliser sur cette interface. Si vous ne définissez pas cette valeur, la valeur par défaut est ENA.

   > **Note**
   >
   > Vous ne pouvez ajouter qu'une seule interface VPC EFA et jusqu'à deux interfaces VPC ENA à un flux.

6. Pour l'ARN du rôle, spécifiez le nom de ressource Amazon (ARN) du rôle que vous avez créé lors de votre configuration MediaConnect en tant que service fiable.
7. Pour VPC, choisissez l'ID du VPC à utiliser.
8. Pour Sous-réseau, choisissez le sous-réseau VPC que vous MediaConnect souhaitez utiliser pour configurer votre configuration VPC. Le sous-réseau doit résider dans la même zone de disponibilité que le flux.
9. Pour les groupes de sécurité, spécifiez les groupes de sécurité VPC que vous MediaConnect souhaitez utiliser pour configurer votre configuration VPC. Vous devez choisir au moins un groupe de sécurité.

Supprimer une interface VPC d'un flux

Vous pouvez supprimer une interface VPC de votre flux si elle n'est pas utilisée comme source pour le flux. Le flux doit également être en mode veille.

> **Note**
>
> Si le flux comporte une erreur, vous devez résoudre l'erreur avant de terminer cette procédure.

Pour supprimer une interface VPC d'un flux (console)

1. Sur la page Flux, choisissez le nom du flux associé à l'interface VPC que vous souhaitez supprimer.
2. Choisissez Arrêter.

   L'état du flux passe à Standby. Le flux s'arrête immédiatement et n'est plus visible pour les clients qui accèdent au résultat directement depuis votre flux ou via un droit.
3. Choisissez l'onglet Interfaces VPC.
4. Choisissez l'interface VPC que vous souhaitez supprimer, puis choisissez Supprimer.

Considérations relatives aux groupes de sécurité pour les interfaces VPC

Lorsque vous configurez un cloud privé virtuel (VPC) dans Amazon Virtual Private Cloud, vous créez des groupes de sécurité qui contrôlent le trafic entrant et sortant. Ensuite, lorsque vous créez une interface VPC dans AWS MediaConnect Elemental, vous spécifiez les groupes de sécurité que vous MediaConnect souhaitez utiliser lorsqu'elle envoie et reçoit du contenu depuis votre VPC.

Pour garantir que le contenu peut circuler entre votre VPC et votre VPC MediaConnect, respectez les consignes suivantes :

Assurez-vous que l'interface VPC possède un groupe de sécurité avec...	Informations supplémentaires
Règle entrante qui autorise l'adresse IP privée de la ressource au sein du VPC qui envoie du contenu.	Sources Zixi : Lorsque vous créez une source VPC à l'aide du protocole Zixi, le port entrant est automatiquement attribué par. MediaConnect Le port attribué sera compris entre 2090 et 2099

Assurez-vous que l'interface VPC possède un groupe de sécurité avec...	Informations supplémentaires
	et sera attribué au moment de la création de la source. Vous devez d'abord créer la source Zixi VPC et noter le port attribué. Une fois que vous avez obtenu les informations de port attribuées, vous pouvez configurer vos groupes de sécurité.
Règle sortante qui autorise tout le trafic sortant. Par défaut, tous les groupes de sécurité incluent cette règle. Tant que vous n'avez pas supprimé cette règle du groupe de sécurité, il n'est pas nécessaire d'en créer une nouvelle.	Sur la ressource qui reçoit le trafic de votre flux, vous devez également configurer un groupe de sécurité avec une règle entrante qui autorise l'adresse IP privée de l'ID d'interface réseau associé à l'interface VPC. (Dans MediaConnect, vous pouvez consulter les détails du flux pour trouver l'ID de l'interface réseau. Ensuite, dans EC2, vous pouvez consulter les détails de l'interface réseau pour obtenir l'adresse IP.)
Une règle entrante et une règle sortante qui répondent aux exigences répertoriées ci-dessus.	Vous pouvez utiliser un groupe de sécurité comportant les deux règles ou deux groupes de sécurité (un pour chaque règle). Pour les flux CDI, le groupe de sécurité spécifié pour les interfaces VPC doit être autoréférentiel. Vérifiez que le groupe de sécurité utilisé possède le même ID de groupe de sécurité ajouté aux règles entrantes et sortantes.

Pour plus d'informations sur les groupes de sécurité, consultez le guide de l'utilisateur Amazon VPC.

Streams multimédias dans AWS Elemental MediaConnect

Un flux multimédia est un composant essentiel d'un flux CDI, que vous pouvez utiliser pour ingérer du contenu et le transporter dans le AWS Cloud via la norme de transport SMPTE 2110, partie 22. Chaque flux multimédia représente une piste ou un flux multimédia unique contenant des données vidéo, audio ou auxiliaires.

Vous définissez un flux multimédia dans le cadre du flux. Vous pouvez ensuite l'associer à une source et à plusieurs sorties sur ce flux. La source et les sorties doivent utiliser le protocole CDI ou le protocole ST 2110 JPEG XS, et peuvent consister en un ou plusieurs flux multimédia.

Le type de flux multimédia que vous créez dépend de la sortie que vous recevez ou envoyez à un appareil local, tel queAWS Elemental Live.

> **Note**
>
> Vous n'utilisez les flux multimédia que pour les flux CDI dont le protocole d'entrée et de sortie est ST 2110 avec JPEG XS. Si vous avez configuré vos flux pour utiliser le CDI comme protocole d'entrée et de sortie, vous n'avez pas besoin de flux multimédia.

Sortie AWS Elemental Live	MediaConnect type de flux multimédia
SMPTE 2110-20 : vidéo non compressée	(Non pris en charge)
SMPTE 2110-22 : vidéo compressée avec JPEG XS	Vidéo
SMPTE 2110-30 : audio PCM	Audio
SMPTE 2110-31 : audio Dolby (AC3, EAC3)	(Non pris en charge)
SMPTE 2110-40 : Données auxiliaires	Données connexes

Pour des illustrations des flux de travail CDI, voir Contribution aux flux de CDI etRéplication et surveillance CDI.

Rubriques

Ajouter un flux multimédia à un flux

Avant de pouvoir associer un flux multimédia à une source ou à une sortie, vous devez l'ajouter au flux. Après avoir ajouté un flux multimédia à un flux, vous pouvez l'associer à une source, puis à des sorties.

> **Note**
>
> Vous ne pouvez associer un flux multimédia à une sortie que s'il a déjà été associé à une source du flux.

Pour ajouter un flux multimédia à un flux

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux auquel vous souhaitez ajouter le flux multimédia.
3. Choisissez l'onglet Diffusions multimédias.
4. Choisissez Ajouter un flux multimédia.
5. Dans le champ Nom, spécifiez un nom descriptif qui vous aidera à distinguer ce flux multimédia des autres flux.
6. Dans Description, spécifiez une description qui vous aidera à vous souvenir de l'utilisation de ce flux multimédia.
7. Pour Stream ID, spécifiez un identifiant unique pour le flux multimédia.

   Si la source ou l'une des sorties utilise le protocole CDI, spécifiez la valeur attendue par les systèmes de production et de diffusion.

   Si la source et toutes les sorties utilisent le protocole ST 2110 JPEG XS, spécifiez une valeur unique par rapport à celle des autres flux multimédias du flux.
8. Choisissez Options avancées pour afficher les options supplémentaires en fonction de votre type de diffusion.

9. Pour obtenir des instructions spécifiques sur les options avancées en fonction de votre type de stream, choisissez l'un des onglets suivants :

   Audio

   1. Pour le type de diffusion, choisissez Audio.
   2. Pour Fréquence d'horloge multimédia, spécifiez la fréquence d'échantillonnage du flux. Cette valeur est mesurée en Hz.
   3. Dans Langue, spécifiez la langue de l'audio. Cette valeur doit être dans un format reconnu par le récepteur.
   4. Pour Ordre des canaux, spécifiez le format du canal audio.
   5. Choisissez Ajouter un flux multimédia.

   Video

   1. Pour le type de diffusion, choisissez Vidéo.

      MediaConnect Fournit une valeur par défaut représentant le paramètre recommandé pour de nombreux champs. Modifiez la valeur par défaut si nécessaire.
   2. La fréquence d'horloge multimédia est la fréquence d'échantillonnage du flux, définie sur 90 000. Cette valeur est mesurée en Hz.
   3. Pour le format vidéo, spécifiez la résolution de la vidéo.
   4. Pour Fréquence d'images exacte, spécifiez la fréquence d'images de la vidéo. Cette valeur doit être représentée en images par seconde.
   5. Pour la colorimétrie, spécifiez le format utilisé pour la représentation des couleurs dans la vidéo.
   6. Pour le mode de numérisation, spécifiez la méthode utilisée pour numériser la vidéo entrante.
      - Choisissez Entrelacer si la vidéo entrante est entrelacée (par exemple, 480i ou 1080i).
      - Choisissez Progressive si la vidéo entrante est progressive (par exemple, 720p ou 1080p).
      - Choisissez une image segmentée progressive si la vidéo entrante est au format PSF (par exemple, 1080psf).
   7. Pour le TCS, spécifiez le système de caractéristiques de transfert (TCS) utilisé dans la vidéo.

8. Pour Range, spécifiez la plage de codage de la vidéo.
9. Pour LE PAR, spécifiez le rapport d'accès aux pixels (PAR) de la vidéo.
10. Choisissez Ajouter un flux multimédia.

Ancillary data

1. Pour le type de flux, choisissez Données auxiliaires.
2. La fréquence d'horloge multimédia est la fréquence d'échantillonnage du flux, définie sur 90 000. Cette valeur est mesurée en Hz.
3. Choisissez Ajouter un flux multimédia.

Mettre à jour un flux multimédia

Vous pouvez mettre à jour les flux multimédia même si le flux est en cours d'exécution. Toutefois, si le flux multimédia est associé à une source ou à une sortie, vous ne pouvez pas mettre à jour son type.

Pour mettre à jour un flux multimédia sur un flux

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé au flux multimédia que vous souhaitez mettre à jour.
3. Choisissez l'onglet Diffusions multimédias.

   La liste des flux multimédias correspondant à ce flux s'affiche.
4. Choisissez le flux multimédia que vous souhaitez mettre à jour.
5. Choisissez Mettre à jour.
6. Effectuez les modifications appropriées, puis choisissez Save (Enregistrer).

Supprimer un flux multimédia

Vous pouvez supprimer un flux multimédia d'un flux si celui-ci n'est pas actif et si le flux multimédia n'est associé à aucune source ni à aucune sortie.

Pour supprimer un flux multimédia d'un flux

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux associé au flux multimédia que vous souhaitez supprimer.

   La page de détails de ce flux apparaît.
3. Choisissez l'onglet Diffusions multimédias.
4. Choisissez le flux multimédia, puis sélectionnez Supprimer.

Réservations pour AWS Elemental MediaConnect

Les réservations vous permettent de réaliser d'importantes économies sur vos MediaConnect coûts AWS Elemental en comparaison de la tarification à la demande.

Une réservation est un engagement à utiliser une quantité spécifique de bande passante sortante chaque mois pendant une durée spécifiée. En retour, vous payez un tarif horaire réduit pour cette bande passante. La réservation est attribuée et facturée sur une base mensuelle pendant toute la durée de la réservation.

Le tarif réduit s'applique à la bande passante sortante provenant de tous les MediaConnect flux de votre compte jusqu'à la quantité de bande passante spécifiée dans la réservation.

La bande passante sortante fait référence aux données transférées d'un MediaConnect flux vers un emplacement ou un point de terminaison en dehors du AWS Cloud. Cela n'inclut pas les données transférées dans votre MediaConnect flux, ni les données transférées d'un MediaConnect flux vers n'importe quel emplacement du AWS Cloud.

Pour plus d'informations sur les frais de réservation, consultez la liste des MediaConnect prix.

Fonctionnement de la facturation

La bande passante sortante réservée est facturée toutes les heures. Pour chaque cycle de facturation, AWS facture votre compte pour la bande passante sortante au tarif réduit, tel que spécifié dans votre réservation. Si votre compte utilise une bande passante sortante supérieure à celle couverte par la réservation, l'excédent est facturé aux tarifs à la demande. Si votre compte utilise moins de bande passante, vous AWS facture la quantité de bande passante sortante spécifiée dans la réservation. La bande passante non utilisée n'est pas reportée au mois suivant.

Affichage de réservations d'.

Sur la console, vous pouvez consulter les réservations que vous avez achetées.

Pour consulter la liste des réservations (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le panneau de navigation, choisissez Reservations (Réservations).

La liste de toutes les réservations que vous avez effectuées s'affiche.

Offrandes

Les offres sont des MediaConnect remises accordées en échange d'un engagement à utiliser une certaine quantité de bande passante sortante chaque mois. Les composants d'une MediaConnect offre sont les suivants :

- Durée
- Bande passante sortante
- Prix (facturé à l'heure)

Lorsque vous achetez une offre, vous spécifiez la date et l'heure de début. La ressource qui en résulte est appelée réservation car vous « réservez » une certaine quantité de bande passante sortante pendant un certain temps.

La bande passante sortante fait référence aux données transférées d'un MediaConnect flux vers un emplacement ou un point de terminaison en dehors du AWS Cloud. Cela n'inclut pas les données transférées dans votre MediaConnect flux, ni les données transférées d'un MediaConnect flux vers n'importe quel emplacement du AWS Cloud.

Affichage des offres

Sur la console, vous pouvez consulter les offres disponibles dans la AWS région actuelle.

Pour afficher la liste des offres (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, choisissez Offres.

   Une liste s'affiche, répertoriant toutes les offres disponibles dans la région actuelle.

Acheter une offre

Si aucune réservation n'est déjà active sur votre compte, vous pouvez acheter une offre pour créer une nouvelle réservation.

Pour acheter une offre (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, choisissez Offres.

   Une liste s'affiche, répertoriant toutes les offres disponibles dans la région actuelle.

   > **Note**
   >
   > Si vous avez une réservation en cours, vous ne pouvez pas acheter une autre offre.

3. Choisissez la réservation que vous souhaitez acheter, puis choisissez Acheter.

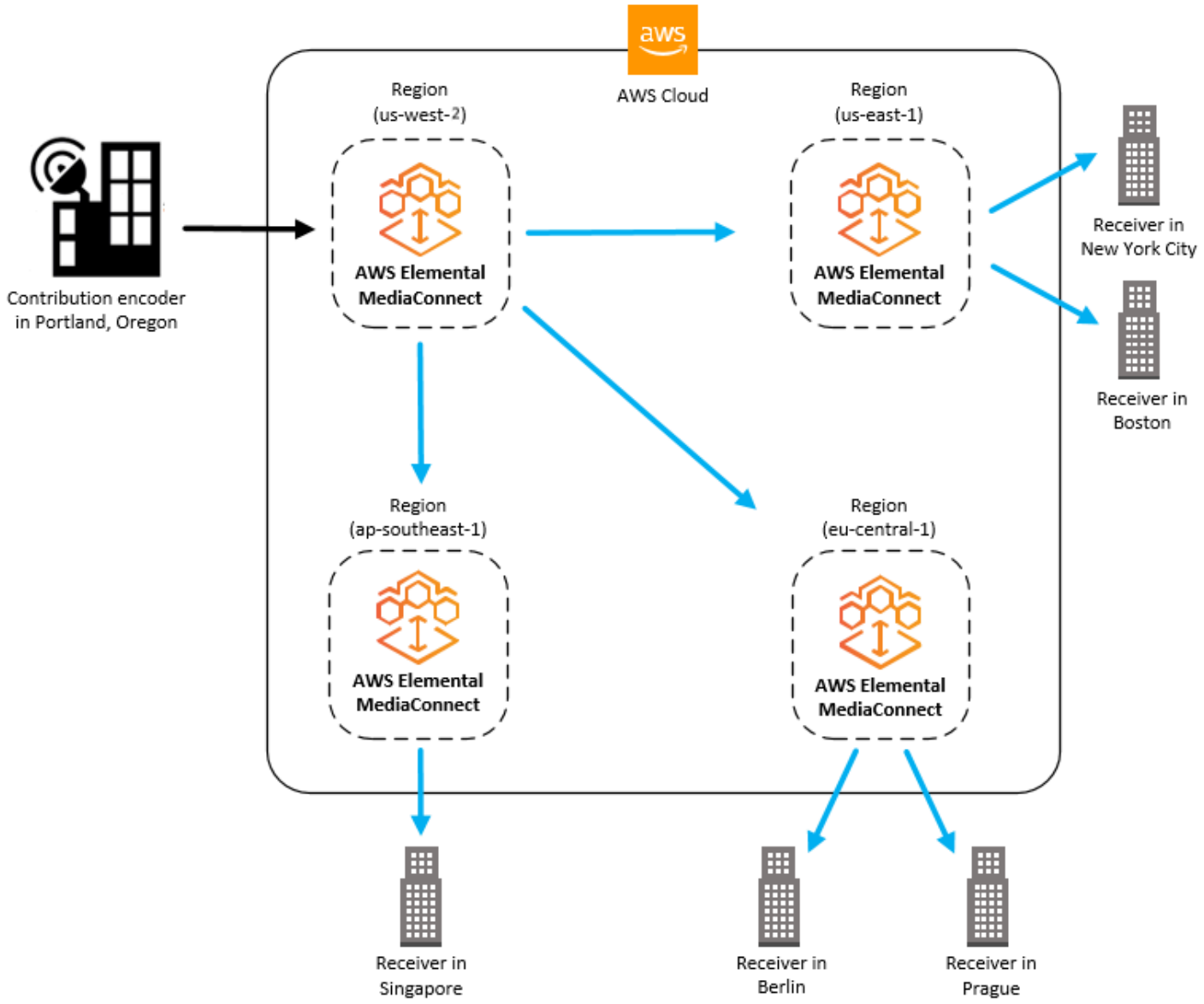
   La page Entrer les détails de la réservation s'affiche.
4. Dans le champ Name (Nom), entrez le nom de la réservation. Le nom de la réservation doit être unique dans votre compte, y compris les réservations en cours d'expiration.
5. Pour Date de début, cliquez sur l'icône du calendrier et choisissez la date à laquelle vous souhaitez que la réservation commence. Vous pouvez choisir une date dès le premier jour du mois en cours et aussi récemment qu'aujourd'hui.
6. Dans le champ Heure de début, entrez l'heure à laquelle vous souhaitez que la réservation commence. Si votre date de début se situe dans le passé, vous pouvez choisir n'importe quel moment de la journée. Si votre date de début tombe aujourd'hui, vous pouvez choisir n'importe quelle heure jusqu'à l'heure actuelle incluse.
7. Choisissez Suivant.

   La page Révision et achat s'affiche.
8. Vérifiez les détails de la réservation. Si vous avez besoin de modifier le nom de la réservation ou de commencer, choisissez Précédent et apportez les modifications. Si vous devez choisir une autre offre, choisissez Annuler et recommencez.
9. Choisissez Purchase (Acheter).

Diffusion de contenu à l'aide d'AWS Elemental MediaConnect

Vous pouvez utiliser AWS Elemental MediaConnect pour distribuer du contenu dans différentes zones géographiques. Supposons, par exemple, que votre source soit un encodeur de contribution local situé à Portland, dans l'Oregon, et que vous souhaitiez distribuer votre contenu dans le monde entier. Vous configurez votre MediaConnect flux AWS Elemental initial dans la `us-west-2` région, qui est la AWS région physique la plus proche de votre encodeur. Une fois que votre contenu est dans le AWS cloud, vous l'envoyez à d'autres MediaConnect flux situés dans des régions plus proches de vos destinataires.

L'illustration suivante montre un encodeur de contribution sur site situé à Portland, dans l'Oregon, qui télécharge du contenu vers AWS MediaConnect Elemental in the Cloud. AWS Le flux possède trois sorties qui envoient du contenu à d'autres flux dans différentes AWS régions. Ces flux secondaires sont plus proches des récepteurs, situés dans différentes villes du monde.



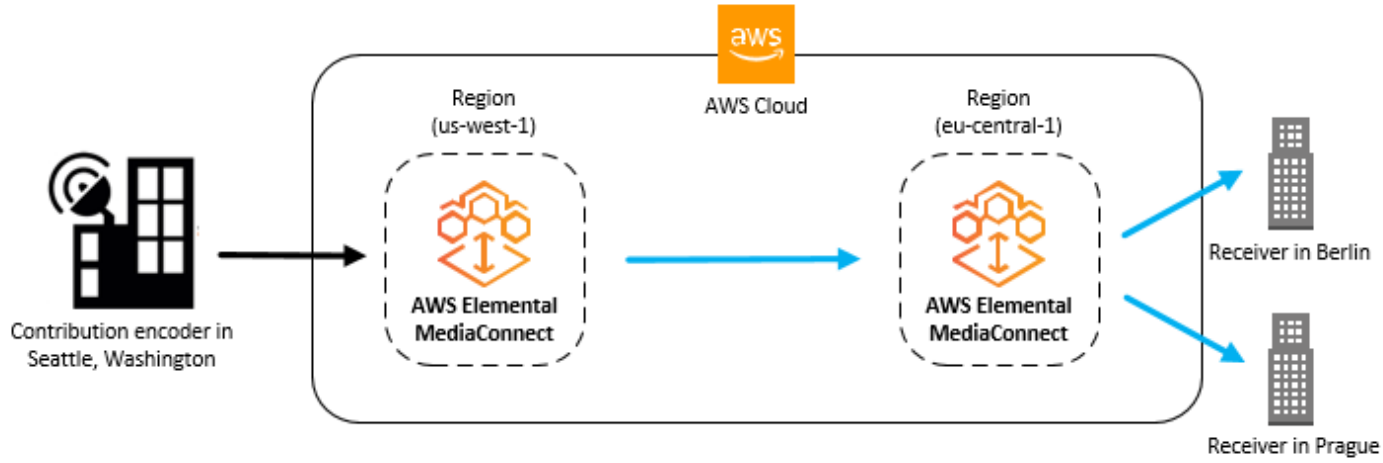
Rubriques

- Diffusion de contenu entre les régions
- Diffusion de contenu à AWS Elemental MediaLive
- Diffusion de contenu à partir d'un AWS Elemental MediaLive multiplex

Diffusion de contenu entre les régions

Vous pouvez configurer deux MediaConnect flux AWS Elemental pour distribuer du contenu d'une AWS région à l'autre. Dans ce scénario, vous créez un flux dans la région la plus proche de

votre encodeur de contribution et un second flux dans la région la plus proche de votre récepteur. L'illustration suivante montre ce processus.



Cette rubrique part du principe que vous savez déjà comment créer un flux et ajouter des sorties à un flux.

Pour distribuer du contenu entre les régions (console)

1. Dans la AWS région la plus proche de votre source, créez un flux. (Nous appellerons cela le flux A.)
2. Consultez la page de détails du flux A pour déterminer son adresse IP de sortie.
3. Dans la AWS région la plus proche de votre destination, créez un deuxième flux (flux B) avec les détails suivants :
   - Type de source : Choisissez Source standard.
   - Protocole : Choisissez Zixi Push.
   - Port entrant : si vous sélectionnez Zixi push comme protocole, ce port sera automatiquement défini sur. **2088**
   - Bloc CIDR Allowlist : entrez une valeur CIDR qui inclut l'adresse IP de sortie du flux A.
4. Consultez la page Détails, onglet Source du flux B pour déterminer son adresse IP d'ingestion.
5. Dans le flux A, créez une sortie avec les détails suivants :
   - Protocole : Choisissez Zixi Push.
   - Adresse IP : entrez l'adresse IP d'ingestion du flux B.
   - Port : Entrez**2088**.

Diffusion de contenu à AWS Elemental MediaLive

Si vous prévoyez de distribuer le contenu de votre MediaConnect flux AWS Elemental à AWS Elemental MediaLive, n'oubliez pas ce qui suit :

- Pour chaque flux vidéo, créez deux flux dans la même AWS région et dans les mêmes zones de disponibilité (par exemple`us-east-1a`). Par exemple, si vous créez deux MediaLive entrées à l'aide de MediaConnect flux, le premier flux de l'entrée 1 doit se trouver dans la même zone de disponibilité que le premier flux de l'entrée 2. Ces flux redondants serviront d'entrées principales et de secours pour le MediaLive canal.
- Créez le MediaLive canal dans la même AWS région que les flux AWS Elemental MediaConnect.
- Configurez des autorisations permettant MediaLive de communiquer avec AWS Elemental MediaConnect. Ce processus comprend les procédures suivantes :
  1. Créez une politique qui permet MediaLive de soumettre une demande à AWS Elemental MediaConnect (voir Création d'une MediaLive politique).
  2. Attribuez cette politique à un rôle pour MediaLive (voir Créer un rôle pour MediaLive). Vous aurez besoin de l'Amazon Resource Name (ARN) pour ce rôle lorsque vous spécifiez des MediaConnect flux AWS Elemental en tant qu'entrées d'un MediaLive canal.
- Créez votre AWS Elemental MediaConnect et vos MediaLive ressources dans cet ordre :
  1. Configurez des autorisations.
  2. Créez les flux AWS Elemental MediaConnect .
  3. Notez les ARN du flux.
  4. Créez les entrées sur le MediaLive canal. (Vous pouvez créer la MediaLive chaîne quand vous le souhaitez. Assurez-vous simplement de créer les entrées pour ce canal après avoir créé les flux.)

Diffusion de contenu à partir d'un AWS Elemental MediaLive multiplex

Un AWS Elemental MediaLive multiplex crée un flux de transport UDP (TS) qui transporte plusieurs programmes, également appelé flux de transport multiprogramme (MPTS). Lorsque vous créez un multiplex, vous accordez MediaLive automatiquement un droit MediaConnect à votre compte. Créez un flux basé sur ce droit et distribuez le contenu de ce flux.

Pour distribuer du contenu depuis un MediaLive multiplex (console)

1. Dans MediaLive, créez un multiplex.

   MediaLive crée un MediaConnect droit qui utilise le multiplex comme source. Le nom du droit inclut `multiplex` le nom que vous avez choisi pour le multiplex.
2. Dans MediaConnect, créez un flux basé sur le nouveau droit.
3. Ajoutez des sorties pour distribuer le contenu.

Protocoles dans AWS Elemental MediaConnect

AWS Elemental MediaConnect prend en charge différents protocoles pour les flux vidéo en direct entrants (source) et sortants (sortie) en fonction du type de flux que vous utilisez.

Pour les flux de transport, qui transportent du contenu compressé mixé (les données audio, vidéo et auxiliaires sont combinées) en un seul flux, vous utilisez les protocoles suivants :

- Le Reliable Internet Stream Transport (RIST) (profil simple uniquement) est un protocole à haute disponibilité et à faible latence qui convient aux applications longue distance. MediaConnect ne prend pas en charge le chiffrement pour les sources ou les sorties utilisant le protocole RIST.
- Le protocole de transport en temps réel (RTP) a une large applicabilité et utilise moins de bande passante que le RTP-FEC. MediaConnect ne prend pas en charge le chiffrement pour les sources ou les sorties qui utilisent le protocole RTP.
- Le protocole de transport en temps réel avec correction d'erreur directe (RTP-FEC) est largement applicable et la correction d'erreur directe (FEC) permet de réparer automatiquement toute corruption ou perte de paquets. L'utilisation de ce protocole prend plus de bande passante que le RTP sans FEC. AWS Elemental MediaConnect ne prend pas en charge le chiffrement des sources ou des sorties qui utilisent le protocole RTP-FEC.
- Le protocole SRT (Secure Reliable Transport) est un protocole à haute disponibilité et à faible latence adapté aux applications longue distance.
  - L'écouteur SRT est une implémentation du protocole SRT basée sur le pull. L'écouteur SRT peut être utilisé comme source ou sortie. L'écouteur SRT doit communiquer avec un appelant SRT.
  - L'appelant SRT est une implémentation du protocole SRT basée sur le push. L'appelant SRT peut être utilisé comme source ou sortie. L'appelant SRT doit communiquer avec un écouteur SRT.
- Zixi est un protocole hautement disponible adapté à la plupart des applications, en particulier aux cas d'utilisation impliquant de longues distances. Si votre encodeur n'est pas capable d'utiliser Zixi, vous pouvez utiliser le logiciel d'alimentation/récepteur Zixi spécialement créé pour être utilisé avec. MediaConnect Vous pouvez accéder à ce logiciel sur le site Web de Zixi, où il vous sera demandé de fournir vos informations avant de pouvoir télécharger le logiciel. Si vous configurez plusieurs flux pour la distribution, nous vous recommandons d'utiliser Zixi comme protocole pour envoyer du contenu entre les flux. MediaConnect prend en charge deux options du protocole Zixi :
  - Zixi pull utilise le protocole Zixi pour envoyer du contenu à un récepteur ou à un décodeur récepteur intégré (IRD) situé derrière un pare-feu. En outre, vous pouvez utiliser cette option

lorsque vous avez besoin d'une traduction d'adresses réseau (NAT) pour acheminer le trafic depuis MediaConnect le récepteur.

- Zixi Push utilise le protocole Zixi pour envoyer du contenu à un récepteur doté d'une adresse IP statique adressable publiquement. Utilisez cette option lorsque le récepteur ne se trouve pas derrière un pare-feu ou un routeur NAT.
- Zixi Push for AWS Elemental Link utilise le protocole Zixi Push pour connecter un appareil AWS Elemental Link UHD à un flux. MediaConnect

- Fujitsu-QOS est un protocole propriétaire à faible latence et haut débit de Fujitsu qui permet le transport depuis et vers des appareils Fujitsu depuis et vers des appareils Fujitsu. MediaConnect MediaConnect MediaConnect ne prend pas en charge le basculement de source si vous utilisez le protocole Fujitsu.

Pour les flux CDI, qui transportent du contenu de haute qualité légèrement compressé à l'aide du format JPEG XS, vous utilisez les protocoles suivants :

- L'interface numérique du cloud (AWSCDI) AWS est une technologie qui vous permet de transporter des vidéos non compressées de haute qualité dans le AWS cloud, avec une fiabilité élevée et une latence réseau de 8 millisecondes seulement.
- Le ST 2110 JPEG XS est un protocole à faible latence qui peut être utilisé sur des flux avec une compression minimale.

Support de protocole pour les sources et les sorties

Le tableau suivant décrit les protocoles qui peuvent être utilisés pour les sources, les sorties ou les deux.

Protocoles de flux de transport

Protocole	Cela peut-il être utilisé comme source ?	Cela peut-il être utilisé comme sortie ?
POIGNET	Oui	Oui
RTP	Oui	Oui
RTP-FEC	Oui	Oui

Protocole	Cela peut-il être utilisé comme source ?	Cela peut-il être utilisé comme sortie ?
écouteur SRT	Oui	Oui
appelant SRT	Oui	Oui
Pull Zixi	Non	Oui
Zixi Push	Oui	Oui
Fujitsu QoS	Oui	Oui

Protocoles CDI

Protocole	Cela peut-il être utilisé comme source ?	Cela peut-il être utilisé comme sortie ?
CDI	Oui	Oui
ST 2110 JPEG XS	Oui	Oui

Support des couleurs pour les protocoles CDI

MediaConnect Les flux CDI prennent en charge plusieurs configurations d'espace colorimétrique, de profondeur de bits et d'échantillonnage chromatique pour chaque protocole. Le tableau suivant décrit les configurations prises en charge par chaque protocole CDI.

> **Note**
>
> MediaLive ne prend actuellement pas en charge l'espace colorimétrique RGB pour les entrées CDI. Si vous souhaitez générer un flux CDI de MediaConnect à MediaLive, assurez-vous d'utiliser l'espace CbCr colorimétrique Y.

Support couleur CDI

Protocole	Configurations couleur prises en charge
CDI	• Y CbCr 10 bits 4:2:2 • RGB 10 bits 4:4:4 • RGB 12 bits 4:4:4
ST 2110 JPEG XS	• Y CbCr 10 bits 4:2:2 • RGB 10 bits 4:4:4 • RGB 12 bits 4:4:4

Sécurité dans AWS Elemental MediaConnect

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture 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. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Elemental MediaConnect, veuillez consulter AWS Services in Scope by Compliance Program (français non garanti).
- 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 son utilisation AWS Elemental MediaConnect. Les rubriques suivantes expliquent comment procéder à la configuration AWS Elemental MediaConnect pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS Elemental MediaConnect ressources.

Rubriques

Protection des données pour AWS Elemental MediaConnect

Vous pouvez protéger vos données à l'aide des outils fournis par AWS. AWS Elemental MediaConnect peut déchiffrer votre vidéo entrante (source) et chiffrer votre vidéo sortante (sorties et droits).

Trois options s'offrent à vous pour chiffrer le contenu en transit :

- Chiffrement par clé statique : vous pouvez utiliser cette option pour chiffrer les sources, les sorties et les droits. Vous stockez votre clé de chiffrement dans AWS Secrets Manager, puis vous MediaConnect autorisez l'obtention de la clé de chiffrement auprès de Secrets Manager.

  Avantages : Vous avez un contrôle total sur le stockage de la clé de chiffrement de votre compte. La clé est stockée dans AWS Secrets Manager un endroit où vous pouvez y accéder à tout moment.

  Difficultés : Toutes les parties (propriétaires de la source, du flux, des sorties et des droits) ont besoin de la clé de chiffrement. Si le contenu est partagé à l'aide d'un droit, l'auteur et l'abonné doivent enregistrer la clé de chiffrement. AWS Secrets Manager Si la clé de chiffrement change, vous devez informer toutes les parties de la nouvelle clé.
- Secure Packager and Encoder Key Exchange (SPEKE) : vous pouvez utiliser cette option pour chiffrer le contenu envoyé via un droit. Vous vous associez à un fournisseur de clés de plateforme d'accès conditionnel (CA) qui gère et fournit les clés de chiffrement. Vous autorisez ensuite Amazon API Gateway à agir en tant que proxy entre le fournisseur de clés de la plateforme CA et votre AWS compte.

  Avantages : L'auteur du contenu contrôle totalement l'accès à la clé de chiffrement. En tant que créateur de contenu, vous travaillez en partenariat avec votre fournisseur de clés de plate-forme CA qui gère la clé de chiffrement, mais vous ne gérez pas la clé elle-même et vous ne la partagez pas avec d'autres parties. Selon les capacités de votre fournisseur de clés, cette option vous permet d'attribuer des limites de temps à une clé de chiffrement ou de révoquer complètement la clé. L'abonné n'a pas besoin de configurer le chiffrement. Ces informations sont automatiquement fournies par le biais de l'autorisation.

  Défis : Vous devez travailler avec un tiers (le principal fournisseur).
- Chiffrement du mot de passe SRT (Secure Reliable Transport) : vous pouvez utiliser cette option pour chiffrer les sources et les sorties lorsque vous utilisez les protocoles SRT. Les protocoles SRT sont des protocoles à haute disponibilité et à faible latence adaptés aux applications longue

distance. Vous stockez votre mot de passe de chiffrement dans AWS Secrets Manager, puis vous MediaConnect autorisez l'obtention du mot de passe de cryptage auprès de Secrets Manager.

Avantages : Utilise l'AES 128/256 bits pour le chiffrement et le déchiffrement. Les protocoles SRT utilisent la correction d'erreurs pour minimiser les pertes de paquets. Vous avez un contrôle total sur le stockage du mot de passe de chiffrement. Le mot de passe est enregistré dans AWS Secrets Manager un endroit où vous pouvez y accéder à tout moment.

Défis : Utilisable uniquement avec les protocoles SRT. MediaConnect ne prend pas en charge le basculement de source si vous utilisez un protocole SRT.

> **Note**
>
> Le chiffrement n'est pris en charge que pour les droits, pour les sources utilisant les protocoles Zixi ou SRT et pour les sorties utilisant les protocoles Zixi ou SRT.

Rubriques

Chiffrement par clé statique dans AWS Elemental MediaConnect

Vous pouvez utiliser le chiffrement par clé statique pour protéger vos sources, vos sorties et vos droits. Vous stockez votre clé de chiffrement dans AWS Secrets Manager, puis vous MediaConnect autorisez l'obtention de la clé de chiffrement auprès de Secrets Manager.

Rubriques

Gestion des clés pour le chiffrement par clé statique

Dans AWS Elemental MediaConnect, vous pouvez utiliser le chiffrement par clé statique pour sécuriser le contenu des sources, des sorties et des droits. Pour utiliser cette méthode, vous stockez une clé de chiffrement sous forme de secret dans AWS Secrets Manager lequel vous MediaConnect autorisez AWS Elemental à accéder à ce secret. Secrets Manager protège votre clé de chiffrement, en permettant uniquement aux entités que vous spécifiez dans une politique AWS Identity and Access Management (IAM) d'y accéder.

Avec le chiffrement par clé statique, tous les participants (le propriétaire de la source, du flux et les sorties ou droits éventuels) ont besoin de la clé de chiffrement. Si le contenu est partagé à l'aide d'un droit, les deux propriétaires du AWS compte doivent y stocker la clé de chiffrement. AWS Secrets Manager

Pour plus d'informations, consultez Configuration du chiffrement par clé statique.

Configuration du chiffrement par clé statique à l'aide d'AWS Elemental MediaConnect

Avant de créer un flux avec une source chiffrée, une sortie ou un droit utilisant le chiffrement par clé statique, vous devez effectuer les étapes suivantes :

Étape 1 — Stockez votre clé de chiffrement en tant que secret dans AWS Secrets Manager.

Étape 2 — Créez une politique IAM qui permet à AWS MediaConnect Elemental de lire le secret dans lequel vous l'avez stocké. AWS Secrets Manager

Étape 3 — Créez un rôle IAM et associez la politique que vous avez créée à l'étape 2. Configurez ensuite AWS Elemental MediaConnect en tant qu'entité de confiance autorisée à assumer ce rôle et à effectuer des demandes au nom de votre compte.

> **Note**
>
> MediaConnect prend en charge le chiffrement uniquement pour les droits, ainsi que pour les sources et les sorties utilisant les protocoles Zixi et SRT. Votre clé enregistrée dans Secrets Manager pour le protocole Zixi est une clé statique au format hexadécimal. SRT utilise une clé d'accès pour le chiffrement.

Étape 1 : Stockez votre clé de chiffrement dans AWS Secrets Manager

Pour utiliser le chiffrement par clé statique afin de chiffrer votre contenu AWS MediaConnect Elemental, vous devez AWS Secrets Manager créer un secret qui stocke la clé de chiffrement. Vous devez créer le secret et la ressource (source, sortie ou autorisation) qui utilise le secret dans le même AWS compte. Vous ne pouvez pas partager des secrets entre comptes.

> **Note**
>
> Si vous utilisez deux flux pour distribuer des vidéos d'une AWS région à l'autre, vous devez créer deux secrets (un secret dans chaque région).

Pour stocker une clé de chiffrement dans Secrets Manager

1. Obtenez la clé de chiffrement auprès de l'entité qui gère la source.
2. Connectez-vous à la AWS Secrets Manager console à l'adresse https://console.aws.amazon.com/secretsmanager/.
3. Dans la page Stocker un nouveau secret, pour Sélectionner un type de secret, choisissez Autre type de secrets.
4. Pour les paires clé/valeur, choisissez Plaintext.
5. Effacez le texte de la zone et remplacez-le uniquement par la valeur de la clé de chiffrement. Pour les clés hexadécimales, vérifiez la longueur de la clé pour vous assurer qu'elle correspond à la longueur spécifiée pour le type de chiffrement. Par exemple, une clé de chiffrement AES-256 doit comporter 64 chiffres, car chaque chiffre a une taille de 4 bits.
6. Pour Sélectionner la clé de chiffrement, conservez le paramètre par défaut défini sur DefaultEncryptionClé.
7. Choisissez Suivant.
8. Pour Nom du secret, spécifiez un nom pour votre secret qui vous aidera à l'identifier ultérieurement. Par exemple, **`2018-12-01_baseball-game-source`**.
9. Choisissez Suivant.
10. Dans la section Configurer la rotation automatique, choisissez Désactiver la rotation automatique.
11. Choisissez Suivant, puis Stocker.

La page de détails de votre nouveau secret apparaît et affiche des informations telles que le nom ARN du secret.

12. Notez l'ARN secret fourni par Secrets Manager. Vous aurez besoin de cette information dans la procédure suivante.

Étape 2 : créer une politique IAM pour permettre à AWS MediaConnect Elemental d'accéder à votre secret

À l'étape 1, vous avez créé un secret et l'avez enregistré dans AWS Secrets Manager. Au cours de cette étape, vous créez une politique IAM qui permet à AWS MediaConnect Elemental de lire le secret que vous avez stocké.

Pour créer une politique IAM permettant d'accéder MediaConnect à votre secret

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, choisissez Stratégies.
3. Choisissez Create policy, puis sélectionnez l'onglet JSON.
4. Entrez une politique qui utilise le format suivant :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-west-2:111122223333:secret:aes256-7g8H9i"
      ]
    }
  ]
}
```

Dans `Resource` cette section, chaque ligne représente l'ARN d'un secret différent que vous avez créé. Pour obtenir plus d'exemples, consultez Exemples de politiques IAM pour les secrets dans AWS Secrets Manager.

5. Choisissez Examiner une politique.
6. Dans Nom, entrez un nom pour votre politique, tel que**`SecretsManagerForMediaConnect`**.
7. Choisissez Créer une politique.

Étape 3 : créer un rôle IAM avec une relation de confiance

À l'étape 2, vous avez créé une politique IAM qui autorise l'accès en lecture au secret dans AWS Secrets Manager lequel vous l'avez stocké. Au cours de cette étape, vous créez un rôle IAM et attribuez la politique à ce rôle. Vous définissez ensuite AWS Elemental MediaConnect comme une entité de confiance qui peut assumer le rôle. Cela permet d' MediaConnect avoir un accès en lecture à votre secret.

Pour créer un rôle avec une relation de confiance

1. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles).
2. Sur la page Rôle, choisissez Créer un rôle.
3. Sur la page Créer un rôle, dans Sélectionner le type d'entité approuvée, choisissez service AWS (la valeur par défaut).
4. Sous Choisir le service qui utilisera ce rôle, choisissez EC2.

   Vous choisissez EC2 car AWS MediaConnect Elemental ne figure pas actuellement dans cette liste. Le choix d'EC2 vous permet de créer un rôle. Dans une étape ultérieure, vous modifierez ce rôle pour inclure MediaConnect au lieu d'EC2.
5. Sélectionnez Next: Permissions (Étape suivante : autorisations).
6. Pour Joindre des politiques d'autorisation, entrez le nom de la politique que vous avez créée à l'étape 2, par exemple**`SecretsManagerForMediaConnect`**.
7. Pour SecretsManagerReadWrite, cochez la case, puis choisissez Suivant : Révision.
8. Pour Nom du rôle (Role name), saisissez un nom. Nous vous recommandons vivement de ne pas utiliser le nom `MediaConnectAccessRole` car il est réservé. Utilisez plutôt un nom qui inclut `MediaConnect` et décrit l'objectif de ce rôle, tel que**`MediaConnect-ASM`**.

9. Pour la description du rôle, remplacez le texte par défaut par une description qui vous aidera à vous souvenir de l'objectif de ce rôle. Par exemple, **`Allows MediaConnect to view secrets stored in AWS Secrets Manager.`**
10. Sélectionnez Créer un rôle.
11. Dans le message de confirmation qui apparaît en haut de votre page, choisissez le nom du rôle que vous venez de créer.
12. Sélectionnez l'onglet Trust relationships (Relations d'approbation), puis Edit trust policy (Modifier la relation d'approbation).
13. dans la fenêtre Modifier la politique de confiance, apportez les modifications suivantes au JSON :

    - Pour le service, remplacez `ec2.amazonaws.com` par `mediaconnect.amazonaws.com`
    - Pour plus de sécurité, définissez des conditions spécifiques pour la politique de confiance. Cela se limitera MediaConnect à l'utilisation des seules ressources de votre compte. Pour ce faire, utilisez une condition globale telle que l'ID de compte, l'ARN du flux, ou les deux. Consultez l'exemple suivant de politique de confiance conditionnelle. Pour plus d'informations sur les avantages en matière de sécurité liés à la situation mondiale, consultez la section Prévention interservices de la confusion des adjoints.

      > **Note**
      >
      > L'exemple suivant utilise à la fois les conditions d'ID de compte et d'ARN du flux. Votre politique sera différente si vous n'utilisez pas les deux conditions. Si vous ne connaissez pas l'ARN complet du flux ou si vous spécifiez plusieurs flux, utilisez la clé de condition de contexte `aws:SourceArn` global avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:mediaconnect:*:111122223333:*`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "mediaconnect.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:mediaconnect:us-
west-2:111122223333:flow:*:flow-name"
                }
            }
        }
    ]
}
```

14. Choisissez Mettre à jour la politique d'approbation.
15. Sur la page Résumé, prenez note de la valeur du champ ARN de rôle. Il se présente comme suit : `arn:aws:iam::111122223333:role/MediaConnectASM`.

Chiffrement SPEKE dans AWS Elemental MediaConnect

Vous pouvez utiliser le Secure Packager and Encoder Key Exchange (SPEKE) avec AWS Elemental MediaConnect pour chiffrer un droit. Cela vous permet, en tant qu'auteur du contenu, de contrôler totalement les autorisations associées à ce contenu. Cette utilisation est une personnalisation de l'architecture basée sur le cloud SPEKE décrite dans la documentation SPEKE.

Rubriques

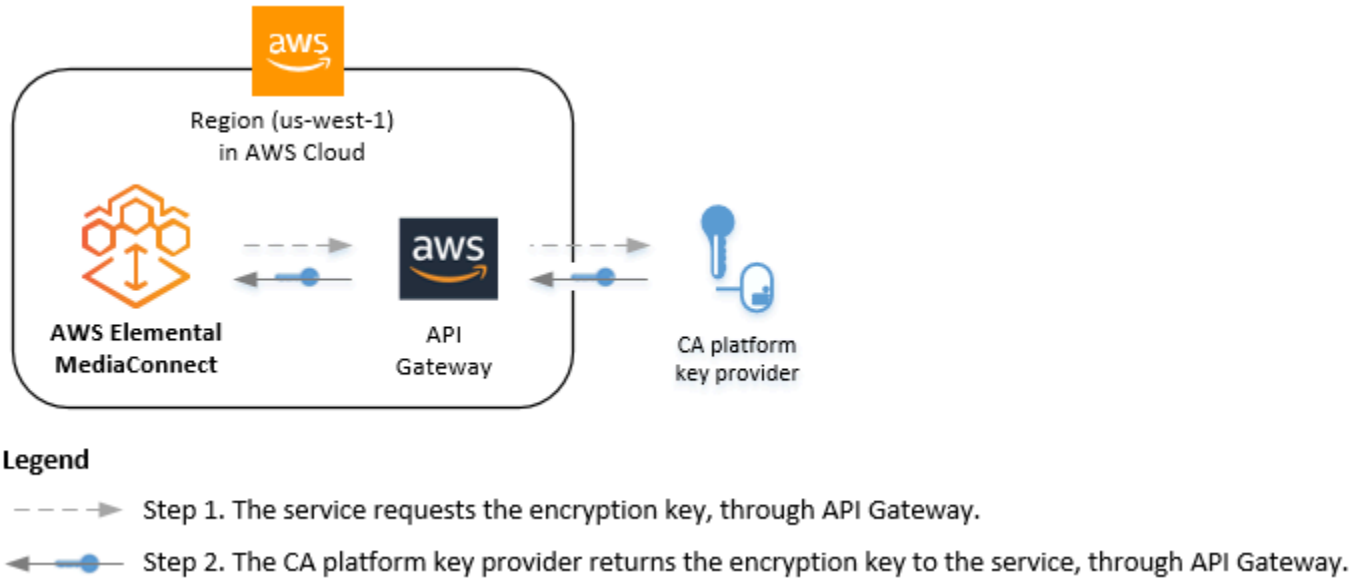
- Gestion des clés pour SPEKE
- Configuration du chiffrement SPEKE à l'aide d'AWS Elemental MediaConnect

Gestion des clés pour SPEKE

Avec une implémentation SPEKE, un système d'accès conditionnel (CA) fournit des clés à AWS MediaConnect Elemental pour le chiffrement et le déchiffrement du contenu. API Gateway agit comme un proxy pour la communication entre le service et le fournisseur de clés de la plate-forme CA. Chaque MediaConnect flux AWS Elemental doit résider dans la même AWS région que son proxy API Gateway.

L'illustration suivante montre comment AWS Elemental MediaConnect obtient la clé de chiffrement ou de déchiffrement à l'aide de SPEKE. Dans le flux de l'expéditeur, le service obtient la clé de

chiffrement et l'utilise pour chiffrer le contenu avant de l'envoyer via l'autorisation. Dans le flux d'abonnés, le service obtient la clé de déchiffrement lorsque le contenu est reçu de l'autorisation.



Voici les principaux services et composants :

- AWS Elemental MediaConnect — Fournit et contrôle la configuration du chiffrement pour le flux. AWS Elemental MediaConnect obtient les clés de chiffrement auprès du fournisseur de clés de la plateforme CA via Amazon API Gateway. À l'aide des clés de chiffrement, AWS Elemental MediaConnect chiffre le contenu (pour le flux de l'expéditeur) ou le déchiffre (pour le flux de l'abonné).
- API Gateway : gère les rôles fiables des clients et les communications par proxy entre le crypteur et le fournisseur de clés. API Gateway fournit des fonctionnalités de journalisation et permet aux clients de contrôler leurs relations avec le chiffreur et avec la plateforme CA. L'API Gateway doit résider dans la même AWS région que le crypteur.
- Fournisseur de clés de plate-forme CA : fournit des clés de chiffrement et de déchiffrement à AWS MediaConnect Elemental via une API compatible Speke.

Pour plus d'informations, consultez Configuration du chiffrement SPEKE.

Configuration du chiffrement SPEKE à l'aide d'AWS Elemental MediaConnect

Avant de pouvoir octroyer un droit utilisant le chiffrement SPEKE, vous devez effectuer les étapes suivantes :

Étape 1. — Adhérez à un fournisseur de clés de plateforme d'accès conditionnel (CA) qui gérera votre clé de chiffrement. Au cours de ce processus, vous créez une API dans Amazon API Gateway qui envoie des demandes au nom d'AWS Elemental MediaConnect au fournisseur clé.

Étape 2 — Créez une politique IAM qui permet à l'API que vous avez créée à l'étape 1 d'agir en tant que proxy pour envoyer des demandes au fournisseur de clés.

Étape 3. — Créez un rôle IAM et associez la politique que vous avez créée à l'étape 2. Configurez ensuite AWS Elemental en MediaConnect tant qu'entité de confiance autorisée à assumer ce rôle et à accéder au point de terminaison API Gateway en votre nom.

Étape 1 : Adhérez à un fournisseur CA

Pour utiliser SPEKE avec AWS MediaConnect Elemental, vous devez disposer d'un fournisseur de clés de plate-forme CA. Les AWS partenaires suivants fournissent des solutions d'accès conditionnel (CA) pour la MediaConnect personnalisation de SPEKE :

- Verimatrix

Si vous êtes à l'origine de contenu, contactez votre fournisseur de clés de plate-forme CA pour obtenir de l'aide concernant le processus d'intégration. Avec l'aide de votre fournisseur clé de plate-forme CA, vous gérez qui a accès à quel contenu.

Pendant le processus d'intégration, prenez note des points suivants :

- ARN de la demande de **POST** méthode : nom de ressource Amazon (ARN) AWS attribué à la demande que vous créez dans API Gateway.
- Vecteur d'initialisation constant (facultatif) : valeur hexadécimale de 128 bits et 16 octets représentée par une chaîne de 32 caractères, à utiliser avec la clé pour chiffrer le contenu.
- ID de l'appareil : identifiant unique pour chaque appareil que vous configurez avec le fournisseur de clés. Chaque appareil représente un destinataire différent pour votre contenu.
- ID de ressource : identifiant unique que vous créez pour chaque élément de contenu que vous configurez avec le fournisseur de clés.
- URL : URL attribuée par AWS l'API que vous créez dans Amazon API Gateway.

Vous aurez besoin de ces valeurs ultérieurement, lorsque vous configurerez le droit dans MediaConnect.

Étape 2 : créer une politique IAM pour autoriser API Gateway à agir en tant que proxy

À l'étape 1, vous avez travaillé avec un fournisseur de clés de plate-forme CA qui gère votre clé de chiffrement. Au cours de cette étape, vous créez une politique IAM qui permet à API Gateway de faire des demandes en votre nom. API Gateway agit comme un proxy pour la communication entre votre compte et le fournisseur clé.

Pour créer une politique IAM pour un proxy API Gateway

1. Dans le volet de navigation de la console IAM, choisissez Stratégies.
2. Choisissez Create policy, puis sélectionnez l'onglet JSON.
3. Entrez une politique qui utilise le format suivant :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "execute-api:Invoke"
      ],
      "Resource": [
        "arn:aws:execute-api:us-west-2:111122223333:1abcdefghi/*/POST/*"
      ]
    }
  ]
}
```

   Dans `Resource` cette section, remplacez l'exemple Amazon Resource Name (ARN) par l'ARN de la demande de `POST` méthode que vous avez créée dans API Gateway avec le fournisseur de clés de la plateforme CA.
4. Choisissez Examiner une politique.
5. Pour Name (Nom), saisissez **`APIGateway-Proxy-Access`**.
6. Sélectionnez Create policy (Créer une politique).

Étape 3 : créer un rôle IAM avec une relation de confiance

À l'étape 2, vous avez créé une politique d'accès au proxy APIGateway qui permet à API Gateway d'agir en tant que proxy et de faire des demandes en votre nom. Au cours de cette étape, vous créez un rôle IAM et associez les autorisations suivantes :

- La politique d'accès au proxy APIGateway-proxy permet à Amazon API Gateway d'agir en tant que proxy en votre nom afin de pouvoir effectuer des demandes entre votre compte et le fournisseur de clés de la plate-forme CA. Il s'agit de la politique que vous avez créée à l'étape 1.
- Une politique de relation de confiance permet à AWS Elemental MediaConnect d'assumer le rôle en votre nom. Vous allez créer cette politique dans le cadre de la procédure suivante.

Pour créer un rôle IAM avec une relation de confiance

1. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles).
2. Sur la page Rôle, choisissez Créer un rôle.
3. Sur la page Créer un rôle, dans Sélectionner le type d'entité approuvée, choisissez service AWS (la valeur par défaut).
4. Sous Choisir le service qui utilisera ce rôle, choisissez EC2.

   Vous choisissez EC2 car AWS MediaConnect Elemental ne figure pas actuellement dans cette liste. Le choix d'EC2 vous permet de créer un rôle. Dans une étape ultérieure, vous modifierez ce rôle pour inclure MediaConnect au lieu d'EC2.
5. Sélectionnez Next: Permissions (Étape suivante : autorisations).
6. Pour les politiques de filtrage, choisissez Gestion par le client.
7. Cochez la case à côté de APIGateway-Proxy-Access, puis choisissez Next : Tags.
8. Entrez les valeurs des balises (facultatif), puis choisissez Next : Review.
9. Pour Nom du rôle, entrez un nom tel que**`SpekeAccess`**.
10. Pour la description du rôle, remplacez le texte par défaut par une description qui vous aidera à vous souvenir de l'objectif de ce rôle. Par exemple, **`Allows AWS Elemental MediaConnect to talk to API Gateway on my behalf.`**
11. Sélectionnez Créer un rôle.
12. Dans le message de confirmation qui apparaît en haut de votre page, choisissez le nom du rôle que vous venez de créer.

13. Choisissez Relations de confiance, puis sélectionnez Modifier la relation de confiance.
14. Pour le document de stratégie, modifiez la politique pour qu'elle ressemble à ceci :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "mediaconnect.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

15. Choisissez Mettre à jour la politique d'approbation.
16. Sur la page Résumé, prenez note de la valeur du champ ARN de rôle. Il se présente comme suit : `arn:aws:iam::111122223333:role/SpekeAccess`.

Chiffrement des mots de passe SRT dans AWS Elemental MediaConnect

Vous pouvez utiliser l'option de chiffrement du mot de passe SRT (Secure Reliable Transport) pour chiffrer les sources et les sorties lorsque vous utilisez les protocoles SRT. Les protocoles SRT sont des protocoles à haute disponibilité et à faible latence adaptés aux applications longue distance. Vous stockez votre mot de passe de chiffrement dans AWS Secrets Manager, puis vous MediaConnect autorisez l'obtention du mot de passe de cryptage auprès de Secrets Manager.

Rubriques

- Gestion des mots de passe pour le chiffrement des mots de passe SRT
- Configuration du chiffrement des mots de passe SRT à l'aide d'AWS Elemental MediaConnect

Gestion des mots de passe pour le chiffrement des mots de passe SRT

Dans AWS Elemental MediaConnect, vous pouvez utiliser le chiffrement des mots de passe SRT pour sécuriser le contenu des sources et des sorties. Pour utiliser cette méthode, vous stockez un mot de passe SRT sous forme de secret dans AWS Secrets Manager lequel vous autorisez AWS MediaConnect Elemental à accéder à ce secret. Secrets Manager protège votre mot de passe, en

permettant uniquement aux entités que vous spécifiez dans une politique AWS Identity and Access Management (IAM) d'y accéder.

Avec le chiffrement par mot de passe SRT, tous les participants (le propriétaire de la source, du flux et des sorties éventuelles) ont besoin du mot de passe SRT.

Pour plus d'informations, consultez Configuration du chiffrement des mots de passe SRT.

Configuration du chiffrement des mots de passe SRT à l'aide d'AWS Elemental MediaConnect

Avant de créer un flux avec une source chiffrée ou une sortie utilisant le chiffrement par mot de passe SRT, vous devez effectuer les étapes suivantes :

Étape 1 — Stockez votre mot de passe SRT en tant que secret dans AWS Secrets Manager.

Étape 2 — Créez une politique IAM qui permet à AWS MediaConnect Elemental de lire le secret dans lequel vous l'avez stocké. AWS Secrets Manager

Étape 3 — Créez un rôle IAM et associez la politique que vous avez créée à l'étape 2. Configurez ensuite AWS Elemental MediaConnect en tant qu'entité de confiance autorisée à assumer ce rôle et à effectuer des demandes au nom de votre compte.

Étape 1 : Enregistrez votre mot de passe de cryptage dans AWS Secrets Manager

Pour utiliser le chiffrement de mot de passe SRT afin de chiffrer votre contenu AWS MediaConnect Elemental, vous devez AWS Secrets Manager créer un secret qui stocke le mot de passe. Vous devez créer le secret et la ressource (source ou sortie) qui utilise le secret dans le même AWS compte. Vous ne pouvez pas partager des secrets entre comptes.

> **Note**
>
> Si vous utilisez deux flux pour distribuer des vidéos d'une AWS région à l'autre, vous devez créer deux secrets (un secret dans chaque région).

Si vous créez un nouveau mot de passe SRT pour chiffrer une sortie, nous vous recommandons de suivre la politique de mot de passe suivante :

- Longueur minimale du mot de passe de 10 caractères et maximale de 80 caractères

- Au minimum trois des types de caractères suivants : majuscules, minuscules, chiffres et les symboles **! @ # $ % ^ & * ( ) _ + - = [ ] { } | '**
- Ne pas être identique au nom de votre AWS compte ou à votre adresse e-mail

Pour enregistrer un mot de passe dans Secrets Manager

1. Connectez-vous à la AWS Secrets Manager console à l'adresse https://console.aws.amazon.com/secretsmanager/.
2. Dans la page Stocker un nouveau secret, pour Sélectionner un type de secret, choisissez Autre type de secrets.
3. Pour les paires clé/valeur, choisissez Plaintext.
4. Effacez le texte de la zone et remplacez-le uniquement par la valeur du mot de passe SRT.
5. Pour la clé de chiffrement, conservez le réglage par défaut sur aws/secretsmanager.
6. Choisissez Suivant.
7. Pour Nom du secret, spécifiez un nom pour votre secret qui vous aidera à l'identifier ultérieurement. Par exemple, **`2018-12-01_baseball-game-source`**.
8. Choisissez Suivant.
9. Dans la section Configurer la rotation automatique, laissez la rotation automatique désactivée.
10. Choisissez Suivant, puis Stocker. Sur l'écran suivant, sélectionnez le nom du secret que vous avez créé.

    La page de détails de votre nouveau secret apparaît et affiche des informations telles que le nom ARN du secret.
11. Notez l'ARN secret fourni par Secrets Manager. Vous aurez besoin de cette information dans la procédure suivante.

Étape 2 : créer une politique IAM pour permettre à AWS MediaConnect Elemental d'accéder à votre secret

À l'étape 1, vous avez créé un secret et l'avez enregistré dans AWS Secrets Manager. Au cours de cette étape, vous créez une politique IAM qui permet à AWS MediaConnect Elemental de lire le secret que vous avez stocké.

Pour créer une politique IAM permettant d'accéder MediaConnect à votre secret

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, choisissez Stratégies.
3. Choisissez Create policy, puis sélectionnez l'onglet JSON.
4. Entrez une politique qui utilise le format suivant :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-west-2:111122223333:secret:aes256-7g8H9i"
      ]
    }
  ]
}
```

   Dans `Resource` cette section, chaque ligne représente l'ARN d'un secret différent que vous avez créé. Entrez l'ARN secret de la procédure précédente. Choisissez Suivant : Balises.
5. Choisissez Suivant : Vérification.
6. Dans Nom, entrez un nom pour votre politique, tel que**`SecretsManagerForMediaConnect`**.
7. Choisissez Créer une politique.

Étape 3 : créer un rôle IAM avec une relation de confiance

À l'étape 2, vous avez créé une politique IAM qui autorise l'accès en lecture au secret dans AWS Secrets Manager lequel vous l'avez stocké. Au cours de cette étape, vous créez un rôle IAM et attribuez la politique à ce rôle. Vous définissez ensuite AWS Elemental MediaConnect comme une entité de confiance qui peut assumer le rôle. Cela permet d' MediaConnect avoir un accès en lecture à votre secret.

Pour créer un rôle avec une relation de confiance

1. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles).
2. Sur la page Rôle, choisissez Créer un rôle.
3. Sur la page Créer un rôle, dans Sélectionner le type d'entité approuvée, choisissez service AWS (la valeur par défaut).
4. Sous Choisir le service qui utilisera ce rôle, choisissez EC2.

   Vous choisissez EC2 car AWS MediaConnect Elemental ne figure pas actuellement dans cette liste. Le choix d'EC2 vous permet de créer un rôle. Dans une étape ultérieure, vous modifierez ce rôle pour inclure MediaConnect au lieu d'EC2.
5. Sélectionnez Next: Permissions (Étape suivante : autorisations).
6. Pour Joindre des politiques d'autorisation, entrez le nom de la politique que vous avez créée à l'étape 2, par exemple**`SecretsManagerForMediaConnect`**.
7. Pour SecretsManagerForMediaConnect, cochez la case, puis choisissez Next.
8. Pour Nom du rôle (Role name), saisissez un nom. Nous vous recommandons vivement de ne pas utiliser le nom `MediaConnectAccessRole` car il est réservé. Utilisez plutôt un nom qui inclut `MediaConnect` et décrit l'objectif de ce rôle, tel que**`MediaConnect-ASM`**.
9. Pour la description du rôle, remplacez le texte par défaut par une description qui vous aidera à vous souvenir de l'objectif de ce rôle. Par exemple, **`Allows MediaConnect to view secrets stored in AWS Secrets Manager.`**
10. Sélectionnez Créer un rôle.
11. Dans le message de confirmation qui apparaît en haut de votre page, choisissez le nom du rôle que vous venez de créer.
12. Sélectionnez l'onglet Trust relationships (Relations d'approbation), puis Edit trust policy (Modifier la relation d'approbation).
13. Pour Modifier la politique de confiance, passez `ec2.amazonaws.com` à`mediaconnect.amazonaws.com`.

    Le document de stratégie doit maintenant ressembler à l'exemple suivant :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "mediaconnect.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

14. Choisissez Mettre à jour une politique.
15. Sur la page Résumé, prenez note de la valeur du champ ARN de rôle. Il se présente comme suit : `arn:aws:iam::111122223333:role/MediaConnectASM`.

Confidentialité du trafic inter-réseau

Pour acheminer le trafic directement entre MediaConnect et votre réseau d'entreprise via un cloud privé virtuel (VPC)

1. Configurez une connexion privée entre votre Amazon VPC et votre réseau d'entreprise. Configurez une connexion VPN IPSec sur Internet ou une connexion physique privée à l'aide d'une AWS Direct Connect connexion. AWS Direct Connect vous permet d'établir une interface virtuelle privée depuis votre réseau local directement vers votre Amazon VPC, vous fournissant ainsi une connexion réseau privée à haut débit entre votre réseau et votre VPC. Avec plusieurs interfaces virtuelles, vous pouvez établir une connectivité privée avec plusieurs VPC tout en préservant l'isolation du réseau. Pour plus d'informations, consultez Qu'est-ce que le Site-to-Site VPN AWS ? et Qu'est-ce que AWS Direct Connect ?
2. Créez un flux qui utilise une source VPC. Au cours de ce processus, vous ajoutez une interface VPC à votre flux pour établir la connexion initiale entre votre VPC et votre flux. Vous spécifiez également cette même interface VPC comme source pour le nouveau flux.

> **Note**
>
> Si votre flux existe déjà, vous pouvez le mettre à jour pour ajouter une interface VPC, puis ajouter une autre source utilisant cette interface VPC.

Gestion des identités et des accès pour AWS Elemental MediaConnect

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

Public ciblé

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

Utilisateur du service : si vous utilisez le MediaConnect service 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 nouvelles MediaConnect fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans MediaConnect, consultez Résolution des problèmes liés AWS à l' MediaConnectidentité et à l'accès Elemental.

Administrateur du service — Si vous êtes responsable des MediaConnect ressources de votre entreprise, vous avez probablement un accès complet à MediaConnect. C'est à vous de déterminer les MediaConnect fonctionnalités et les ressources auxquelles les utilisateurs de votre service 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 manière dont votre entreprise peut utiliser IAM avec MediaConnect, voirComment AWS Elemental MediaConnect fonctionne avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à MediaConnect. Pour consulter des exemples de politiques MediaConnect basées sur l'identité que vous pouvez utiliser dans IAM, consultez. AWS Exemples de politiques élémentaires basées sur MediaConnect l'identité

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 IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

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 IAM Identity Center Les utilisateurs (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 au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS 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 vous-même les demandes, consultez la section Signature des demandes AWS 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, veuillez consulter Multi-factor authentication (Authentification multifactorielle) dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root 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 root, consultez Tâches nécessitant les informations d'identification de l'utilisateur root dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule 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 tels que les 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 de faire pivoter les 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 en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS 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. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM 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 jeux d'autorisations, veuillez consulter la rubrique Jeux d'autorisations dans le Guide de l'utilisateur 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.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, 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 Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. 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 de 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, l'action que vous effectuez est susceptible de lancer une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, 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 personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Fonction du 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 une fonction du service

à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire 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. 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.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des 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 Présentation 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 le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un Groupes d'utilisateurs IAM ou un rôle IAM. 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 Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des 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 au sein de votre Compte AWS. 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, veuillez consulter Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

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 des 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 IAM ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations qui en résultent représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace 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 Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle de service (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la séance obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations, consultez Politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues 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.

En savoir plus

Pour plus d'informations sur la gestion des identités et des accès pour MediaConnect, consultez les pages suivantes :

- Comment MediaConnect fonctionne avec IAM
- Exemples de politiques basées sur l'identité
- Exemples de stratégies basées sur les ressources
- Exemples de politiques relatives aux secrets dans AWS Secrets Manager
- Résolution des problèmes

Comment AWS Elemental MediaConnect fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à MediaConnect, vous devez comprendre quelles fonctionnalités IAM sont disponibles. MediaConnect Pour obtenir une vue d'ensemble de la façon dont MediaConnect les autres AWS services fonctionnent avec IAM, consultez la section AWS Services qui fonctionnent avec IAM dans le Guide de l'utilisateur d'IAM.

Rubriques

MediaConnectPolitiques basées sur l'identité

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. MediaConnect prend en charge des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, veuillez consulter Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Actions

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 quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

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

Les actions de politique en MediaConnect cours utilisent le préfixe suivant avant l'action :`mediaconnect:`. Par exemple, pour autoriser quelqu'un à consulter une liste de droits avec l'opération d' MediaConnect`ListEntitlements`API, vous devez inclure l'`mediaconnect:ListEntitlements`action dans sa politique. Les déclarations de politique doivent inclure un `NotAction` élément `Action` ou. MediaConnect définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
      "mediaconnect:action1",
      "mediaconnect:action2"
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `List`, incluez l'action suivante :

```
"Action": "mediaconnect:List*"
```

Pour consulter la liste des MediaConnect actions, consultez la section Actions définies par AWS Elemental MediaConnect dans le guide de l'utilisateur IAM.

Ressources

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 pour lesquels 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 sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

MediaConnect possède les ARN suivants :

```
arn:${Partition}:mediaconnect:${Region}:${Account}:entitlement:${resourceID}:
${resourceName}
arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${resourceID}:${resourceName}
arn:${Partition}:mediaconnect:${Region}:${Account}:output:${resourceID}:${resourceName}
arn:${Partition}:mediaconnect:${Region}:${Account}:source:${resourceID}:${resourceName}
```

Pour plus d'informations sur le format des ARN, consultez les sections Amazon Resource Names (ARN) et AWS Service Namespaces.

Par exemple, pour spécifier le `1-23aBC45dEF67hiJ8-12AbC34DE5fG` flux dans votre instruction, utilisez l'ARN suivant :

```
"Resource": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame"
```

Pour spécifier tous les flux appartenant à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:mediaconnect:us-east-1:111122223333:flow:*"
```

Certaines MediaConnect actions, telles que celles relatives à la création de ressources, ne peuvent pas être effectuées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

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

De nombreuses actions d' MediaConnect API impliquent plusieurs ressources. `RemoveFlowOutput`Supprime, par exemple, une sortie d'un flux particulier, de sorte qu'un utilisateur IAM doit disposer d'autorisations pour le flux et la sortie. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
      "resource1",
      "resource2"
```

Pour consulter la liste des types de MediaConnect ressources et de leurs ARN, consultez la section Ressources définies par AWS Elemental MediaConnect dans le guide de l'utilisateur IAM. Pour savoir

avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, voir Actions définies par AWS Elemental MediaConnect.

Clés de condition

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 `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` 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 associées à l'instruction 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.

Exemples

Pour consulter des exemples de politiques MediaConnect basées sur l'identité, consultez. AWS Exemples de politiques élémentaires basées sur MediaConnect l'identité

MediaConnect politiques basées sur les ressources

AWS Elemental MediaConnect ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les balises MediaConnect

AWS Elemental MediaConnect ne prend pas en charge le balisage des ressources ni le contrôle de l'accès en fonction des balises.

MediaConnect Rôles IAM

Un rôle IAM est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec MediaConnect

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle intercompte. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

MediaConnect prend en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

MediaConnect ne prend pas en charge les rôles liés à un service.

Rôles de service

Cette fonction permet à un service d'endosser une fonction du service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les fonctions du service s'affichent dans votre compte IAM et sont la propriété du compte. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

MediaConnect ne prend pas en charge les rôles de service.

AWS Exemples de politiques élémentaires basées sur MediaConnect l'identité

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou modifier les ressources MediaConnect . Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS

Management Console AWS CLI, ou. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Pour savoir comment créer une stratégie IAM basée sur l'identité à l'aide de ces exemples de documents de stratégie JSON, veuillez consulter Création de stratégies dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer MediaConnect des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. 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 Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder 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 de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser 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 service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer 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 de plus amples informations, consultez Validation de politique 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, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par 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 MediaConnect console

Pour accéder à la MediaConnect console AWS Elemental, vous devez disposer d'un minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les informations relatives MediaConnect aux ressources 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 et rôles IAM) tributaires de cette politique.

Pour garantir que ces entités peuvent toujours utiliser la MediaConnect console, associez également la politique AWS gérée suivante aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "mediaconnect:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
```

```
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "cloudwatch:GetMetricData"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
           "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
              }
          }
      }
  ]
}
```

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

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 l'API AWS CLI or AWS .

```
{
    "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": "*"
        }
    ]
}
```

AWS Exemples de politiques basées MediaConnect sur les ressources élémentaires

Pour accéder à la AWS Elemental MediaConnect console, vous devez disposer d'un ensemble minimal d'autorisations vous permettant de répertorier et d'afficher les détails MediaConnect des ressources de votre AWS compte. Les politiques IAM de cette section présentent des exemples de politiques qui autorisent des actions spécifiques sur les ressources dans AWS Elemental MediaConnect.

Autoriser l'accès en lecture à toutes les ressources dans AWS Elemental MediaConnect

Pour accéder à la AWS Elemental MediaConnect console, vous devez disposer d'une politique qui définit les actions que vous êtes autorisé à effectuer sur les MediaConnect ressources de votre AWS compte. La politique IAM ci-dessous fournit les autorisations suivantes :

- La section consacrée aux `mediaconnect:Describe*` actions `mediaconnect:List*` et permet d'accéder en lecture seule à toutes les ressources que vous créez dans. AWS Elemental MediaConnect
- La section consacrée à l'`ec2:DescribeAvailabilityZones`action permet au service d'obtenir des informations sur la zone de disponibilité dans laquelle se trouve le flux. Cette partie de la politique est obligatoire.
- La section consacrée à l'`cloudwatch:GetMetricData`action permet au service d'obtenir des métriques auprès d'Amazon CloudWatch. Cette partie de la politique est obligatoire.
- La section consacrée à l'`iam:PassRole`action permet à IAM de transmettre un rôle AWS Elemental MediaConnect au service afin de communiquer avec IAM afin d'assumer un rôle au nom du service. Cela autorise le service à assumer ultérieurement le rôle et à effectuer des actions en votre nom. Cette partie de la politique est obligatoire.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mediaconnect:List*",
                "mediaconnect:Describe*"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:DescribeAvailabilityZones"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
         {
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
           "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
                }
            }
        }
    ]
}
```

Autoriser toutes les actions sur toutes les AWS Elemental MediaConnect ressources

Chaque utilisateur de AWS Elemental MediaConnect doit disposer d'une politique qui définit les autorisations sur les AWS Elemental MediaConnect ressources. La politique IAM ci-dessous fournit les autorisations suivantes :

- La section consacrée à l'`mediaconnect:*`action autorise toutes les actions sur toutes les ressources que vous créez dans AWS Elemental MediaConnect.

- La section consacrée à l'`ec2:DescribeAvailabilityZones`action permet au service d'obtenir des informations sur la zone de disponibilité dans laquelle se trouve le flux. Cette partie de la politique est obligatoire.
- La section consacrée à l'`cloudwatch:GetMetricData`action permet au service d'obtenir des métriques auprès d'Amazon CloudWatch. Cette partie de la politique est obligatoire.
- La section consacrée à l'`iam:PassRole`action permet à IAM de transmettre un rôle AWS Elemental MediaConnect au service afin de communiquer avec IAM afin d'assumer un rôle au nom du service. Cela autorise le service à assumer ultérieurement le rôle et à effectuer des actions en votre nom. Cette partie de la politique est obligatoire.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mediaconnect:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:DescribeAvailabilityZones"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
         {
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
           "Resource": "*",
```

```
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS Elemental MediaConnect Permettre de créer et de gérer des interfaces réseau dans votre VPC

Cet exemple de politique IAM permet à AWS MediaConnect Elemental de créer et de gérer des interfaces réseau dans votre VPC afin que le contenu puisse circuler de votre VPC vers. MediaConnect Si vous souhaitez connecter votre VPC à votre flux, vous devez configurer cette politique.

- La section consacrée aux `ec2:` actions permet de MediaConnect créer, de lire, de mettre à jour et de supprimer des interfaces réseau dans votre VPC. Cette partie de la politique est obligatoire.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:describeNetworkInterfaces",
                "ec2:describeSecurityGroups",
                "ec2:describeSubnets",
                "ec2:createNetworkInterface",
                "ec2:createNetworkInterfacePermission",
                "ec2:deleteNetworkInterface",
                "ec2:deleteNetworkInterfacePermission"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Exemples de politiques IAM pour les secrets dans AWS Secrets Manager

Au cours de l'installation, vous créez une politique IAM à laquelle vous attribuez AWS Elemental MediaConnect. Cette politique permet MediaConnect de lire les secrets que vous y avez enregistrés AWS Secrets Manager. Les paramètres de cette stratégie sont à votre entière discrétion. La politique peut aller de la plus restrictive (autoriser l'accès à des secrets spécifiques uniquement) à la moins restrictive (autoriser l'accès à tout secret que vous créez à l'aide de ce AWS compte). Nous vous recommandons d'utiliser la stratégie la plus restrictive à titre de bonne pratique. Toutefois, les exemples figurant dans cette section vous montrent comment configurer des stratégies avec différents niveaux de restriction. Étant donné que seul un accès en lecture aux secrets est MediaConnect nécessaire, tous les exemples de cette section montrent uniquement les actions nécessaires pour lire les valeurs que vous stockez.

Rubriques

Autoriser l'accès en lecture à des secrets spécifiques dans AWS Secrets Manager

La politique IAM suivante autorise l'accès en lecture à des ressources spécifiques (secrets) que vous créez dans AWS Secrets Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-west-2:111122223333:secret:aes128-1a2b3c",
                "arn:aws:secretsmanager:us-west-2:111122223333:secret:aes192-4D5e6F",
                "arn:aws:secretsmanager:us-west-2:111122223333:secret:aes256-7g8H9i"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": "secretsmanager:ListSecrets",
            "Resource": "*"
        }
    ]
}
```

Autoriser l'accès en lecture à tous les secrets créés dans une région spécifique dans AWS Secrets Manager

La politique IAM suivante autorise l'accès en lecture à tous les secrets que vous créez dans une AWS région spécifique dans AWS Secrets Manager. Cette stratégie s'applique aux ressources que vous avez déjà créées et à toutes les ressources que vous créez à l'avenir dans la région spécifiée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:*"
        },
        {
            "Effect": "Allow",
            "Action": "secretsmanager:ListSecrets",
            "Resource": "*"
        }
    ]
}
```

Autoriser l'accès en lecture à toutes les ressources dans AWS Secrets Manager

La stratégie IAM suivante permet l'accès en lecture à toutes les ressources que vous créez dans AWS Secrets Manager. Cette stratégie s'applique aux ressources que vous avez déjà créées et à toutes les ressources que vous créerez à l'avenir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds",
                "secretsmanager:ListSecrets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWSpolitiques gérées pour AWS ElementalMediaConnect

UnAWSune politique gérée est une politique autonome créée et administrée parAWS.AWSles politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l'esprit queAWSles politiques gérées peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tousAWSclients à utiliser. Nous vous recommandons de réduire davantage les autorisations en définissantpolitiques gérées par le clientqui sont spécifiques à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les stratégies gérées par AWS. SiAWSmet à jour les autorisations définies dans unAWSpolitique gérée, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée.AWSest le

plus susceptible de mettre à jour unAWSpolitique gérée lors d'une nouvelleService AWSest lancée ou de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la rubrique Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS Politique gérée par: MediaConnectGatewayInstanceRolePolicy

Vous pouvez attacher la politique `MediaConnectGatewayInstanceRolePolicy` à vos identités IAM.

Cette politique autorise l'enregistrementMediaConnectInstances de passerelle vers unMediaConnectPasserelle. Cette politique sera associée à un rôle. L'entité assumant le rôle sera en mesure d'enregistrer des instances auprès de la passerelle.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "MediaConnectGateway",
   "Effect": "Allow",
   "Action": [
    "mediaconnect:DiscoverGatewayPollEndpoint",
    "mediaconnect:PollGateway",
    "mediaconnect:SubmitGatewayStateChange"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS Politique gérée par: AWSMediaConnectServicePolicy

Vous ne pouvez pas joindreAWSMediaConnectServicePolicyà vos entités IAM. Cette politique est attachée à un rôle lié au service qui permet à MediaConnect d'effectuer des actions en votre nom. Pour plus d'informations, visitezUtilisation de rôles liés à un service.

Cette politique est attachée au rôle lié à un service AWSServiceRoleForMediaConnect. Cette politique permet au rôle lié au service de gérer les ressources Amazon ECS en votre nom. AWS ElementalMediaConnectGateway utilise Amazon ECS comme base pour la mise en œuvre sur site d'AWS ElementalMediaConnectPasserelle etMediaConnectdoit être en mesure de créer, de mettre à jour et de supprimer des ressources Amazon ECS selon les besoins.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ecs:UpdateService",
    "ecs:DeleteService",
    "ecs:CreateService",
    "ecs:DescribeServices",
    "ecs:PutAttributes",
    "ecs:DeleteAttributes",
    "ecs:RunTask",
    "ecs:ListTasks",
    "ecs:StartTask",
    "ecs:StopTask",
    "ecs:DescribeTasks",
    "ecs:DescribeContainerInstances",
    "ecs:UpdateContainerInstancesState"
   ],
   "Resource": "*",
   "Condition": {
    "ArnLike": {
```

```
      "ecs:cluster": "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    }
   }
  },
  {
```

Mises à jour MediaConnect vers des politiques gérées par AWS

Consultez le détail des mises à jour des politiques gérées par AWS pour MediaConnect depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS duMediaConnect historique du documentpage.

Modification	Description	Date
LeMediaConnectpolitique géréeMediaConnectGatewayInstanceRolePolicya été ajouté.	Cette politique autorise l'enregistrementMediaConnectInstances de passerelle vers unMediaConnectPasserelle.	12 AVRIL 2023
LeMediaConnectpolitique géréeAWSMediaConnectServicePolicya été ajouté.	Cette politique est utilisée par un rôle de lien de service et accorde des autorisations d'accèsAWSservices et ressources utilisés parMediaConnect.	12 AVRIL 2023
MediaConnect a démarré le suivi des modifications	MediaConnect a commencé à suivre les modifications pour ses politiques gérées par AWS.	12 AVRIL 2023

Utilisation des rôles liés aux services pour MediaConnect

AWS Elemental MediaConnect utilise des rôles liés à des services AWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à MediaConnect. Les rôles liés à un service sont prédéfinis par MediaConnect et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service simplifie la configuration de MediaConnect, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. MediaConnect définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul MediaConnect peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources MediaConnect sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour MediaConnect

MediaConnectutilise le rôle lié à un service appelé appelé « Le rôle lié à un service appelé AWSServiceRoleForMediaConnect: Le rôle lié à un service appelé : Le rôle lié à un service appelé : Le rôle lié à AWS service appelé « rôle lié à un service appelé : Le rôle lié à un service MediaConnect

Le rôle lié à un service AWSServiceRoleForMediaConnect approuve les services suivants pour endosser le rôle :

- `MediaConnect`

La politique d'autorisation nommée MediaConnectServiceRolePolicy permet MediaConnect d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `ecs:CreateCluster, ecs:RegisterTaskDefinition, ecs:DescribeTaskDefinition, ecs:ListAttributes,`

`ecs:UpdateContainerInstancesState, ecs:DeregisterContainerInstance` sur la ressource `arn:aws:ecs:*:*:*`

- Action : `ecs:UpdateCluster, ecs:UpdateClusterSettings, ecs:DescribeClusters` sur la ressource `arn:aws:ecs:*:*:cluster/MediaConnect`
- Action : `ecs:CreateService, ecs:UpdateService, ecs:RunTask, ecs:StartTask, ecs:StopTask, ecs:ExecuteCommand, ecs:PutAttributes, ecs:DeleteAttributes, ecs:DescribeServices, ecs:DescribeTasks, ecs:ListTasks` sur `arn:aws:ecs:*:*:*` une ressource présentant l'état de `StringLike: {ecs:Cluster: arn:aws:ecs:*:*:cluster/MediaConnect}`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour MediaConnect

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une MediaConnect ressource associée dansAWS Management Console, ou dans l'AWS CLIAWSAPI, MediaConnect crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. De même, si vous utilisiez le MediaConnect service avant le 1er janvier 2023, quand il commençait à prendre en charge les rôles liés à un service, MediaConnect créait le AWSServiceRoleForMediaConnect rôle dans votre compte. Pour en savoir plus, consultez Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez le rôle lié à un MediaConnect service, il MediaConnect crée de nouveau le rôle lié à un service pour vous.

Vous pouvez également utiliser la console pour créer un cas d'utilisation. MediaConnect
Dans l'interface AWS CLI ou l'API AWS, créez un rôle lié à un service avec le nom de service `MediaConnect`. Pour de plus amples informations, consultez Création d'un rôle lié à un service dans

le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour MediaConnect

MediaConnect ne vous permet pas de modifier le rôle lié à un service AWSServiceRoleForMediaConnect. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour MediaConnect

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service MediaConnect utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources MediaConnect utilisées par le service AWSServiceRoleForMediaConnect

1. Supprimez tous les ponts de toutes les passerelles.
2. Désenregistrez toutes les instances sur toutes les passerelles.
3. Supprimez toutes les passerelles.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForMediaConnect. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service MediaConnect

MediaConnect prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et points de terminaison MediaConnect.

Configuration d'AWS Elemental en MediaConnect tant que service de confiance

Vous pouvez utiliser AWS Identity and Access Management (IAM) pour contrôler quelles AWS ressources sont accessibles par quels utilisateurs et applications. Cela inclut la configuration d'autorisations permettant à AWS Elemental de MediaConnect communiquer avec d'autres services au nom de votre compte. Pour configurer AWS Elemental en MediaConnect tant qu'entité de confiance, vous devez effectuer les étapes suivantes :

Étape 1. — Créez une politique IAM qui régit les actions que vous souhaitez autoriser.

Étape 2 — Créez un rôle IAM avec une relation de confiance et associez la politique que vous avez créée à l'étape précédente.

Étape 1 : créer une politique IAM pour autoriser des actions spécifiques

Au cours de cette étape, vous créez une politique IAM qui régit les actions que vous souhaitez autoriser.

Pour créer la stratégie IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Policies (Politiques).
3. Choisissez Create policy, puis sélectionnez l'onglet JSON.
4. Entrez une politique qui utilise le format JSON. Pour obtenir des exemples relatifs à , consultez les rubriques suivantes :
   - Exemple de stratégie pour la connexion à votre VPC
   - Exemples de politiques relatives aux secrets dans AWS Secrets Manager
5. Choisissez Examiner une politique.
6. Dans Nom, entrez le nom de votre politique.
7. Choisissez Créer une politique.

Étape 2 : créer un rôle IAM avec une relation de confiance

À l'étape 1, vous avez créé une politique IAM qui régit les actions que vous souhaitez autoriser. Au cours de cette étape, vous créez un rôle IAM et attribuez la politique à ce rôle. Vous définissez ensuite AWS Elemental MediaConnect comme une entité de confiance qui peut assumer le rôle.

Pour créer un rôle avec une relation de confiance

1. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles).
2. Sur la page Rôle, choisissez Créer un rôle.
3. Sur la page Créer un rôle, dans Sélectionner le type d'entité approuvée, choisissez service AWS (la valeur par défaut).
4. Sous Choisir le service qui utilisera ce rôle, choisissez EC2.

   Vous choisissez EC2 car il n' MediaConnect est pas inclus dans cette liste actuellement. Le choix d'EC2 vous permet de créer un rôle. Dans une étape ultérieure, vous modifierez ce rôle pour inclure MediaConnect au lieu d'EC2.
5. Sélectionnez Next: Permissions (Étape suivante : autorisations).
6. Pour Joindre des politiques d'autorisation, entrez le nom de la politique que vous avez créée à l'étape 1.
7. Cochez la case à côté du nom de la politique, puis choisissez Suivant : Tags.
8. (Facultatif) Ajoutez des métadonnées à l'utilisateur en associant les balises sous forme de paires clé-valeur. Pour plus d'informations sur l'utilisation des identifications dans IAM, consultez Étiquetage des entités IAM dans le Guide de l'utilisateur IAM.
9. Choisissez Next: Review (Suivant : Vérification).
10. Pour Nom du rôle (Role name), saisissez un nom. Le nom `MediaConnectAccessRole` est réservé, vous ne pouvez donc pas l'utiliser. Utilisez plutôt un nom comprenant `MediaConnect`, qui décrit l'objectif de ce rôle.
11. Pour la description du rôle, remplacez le texte par défaut par une description qui vous aidera à vous souvenir de l'objectif de ce rôle.
12. Sélectionnez Créer un rôle.
13. Dans le message de confirmation qui apparaît en haut de votre page, choisissez le nom du rôle que vous venez de créer en sélectionnant Afficher le rôle.
14. Choisissez l'onglet Relations de confiance, puis sélectionnez Modifier la politique de confiance.
15. dans la fenêtre Modifier la politique de confiance, apportez les modifications suivantes au JSON :

- Pour le service, remplacez `ec2.amazonaws.com` par `mediaconnect.amazonaws.com`
- Pour plus de sécurité, définissez des conditions spécifiques pour la politique de confiance. Cela se limitera MediaConnect à l'utilisation des seules ressources de votre compte. Pour ce faire, utilisez une condition globale telle que l'ID de compte, l'ARN du flux, ou les deux. Consultez l'exemple suivant de politique de confiance conditionnelle. Pour plus d'informations sur les avantages en matière de sécurité liés à la situation mondiale, consultez la section Prévention interservices de la confusion des adjoints.

> **Note**
>
> L'exemple suivant utilise à la fois les conditions d'ID de compte et d'ARN du flux. Votre politique sera différente si vous n'utilisez pas les deux conditions. Si vous ne connaissez pas l'ARN complet du flux ou si vous spécifiez plusieurs flux, utilisez la clé de condition de contexte `aws:SourceArn` global avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:mediaconnect:*:111122223333:*`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "mediaconnect.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:mediaconnect:us-
west-2:111122223333:flow:*:flow-name"
                }
            }
        }
    ]
```

```
}
```

16. Choisissez Mettre à jour une politique.
17. Sur la page Résumé, prenez note de la valeur du champ ARN de rôle. Il se présente comme suit : `arn:aws:iam::111122223333:role/MediaConnectASM`.

Prévention du problème de l'adjoint confus entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. Dans AWS, l'emprunt d'identité entre services peut entraîner le problème de député confus. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous vous recommandons d'utiliser les clés contextuelles `aws:SourceArn`du flux et de la condition `aws:SourceAccount`globale dans les politiques relatives aux ressources afin de limiter les autorisations qu'AWS Elemental MediaConnect accorde à un autre service sur la ressource. Utilisez les flux `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition `aws:SourceArn` globale avec l'ARN complet du flux. Si vous ne connaissez pas l'ARN complet du flux ou si vous spécifiez plusieurs flux, utilisez la clé de contexte de condition `aws:SourceArn` globale avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:mediaconnect:*:`*`111122223333`*`:*`.

L'exemple suivant montre comment utiliser les clés de contexte de condition globale `aws:SourceArn` et `aws:SourceAccount` dans MediaConnect afin d'éviter le problème de l'adjoint confus.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "mediaconnect.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:mediaconnect:us-
west-2:111122223333:flow:1-ABCDEFGHJxyzMNoP-a1234bc12345:flow-name"
                }
            }
        }
    ]
}
```

Résolution des problèmes liés AWS à l' MediaConnectidentité et à l'accès Elemental

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

Rubriques

- Je ne suis pas autorisé à effectuer une action dans MediaConnect
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes MediaConnect ressources

Je ne suis pas autorisé à effectuer une action dans MediaConnect

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit lorsque l'`mateojackson`utilisateur essaie d'utiliser la console pour afficher les détails d'un flux mais ne dispose pas des `mediaconnect:DescribeFlow` autorisations nécessaires.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 mediaconnect:DescribeFlow on resource: myExampleFlow
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource `myExampleFlow` à l'aide de l'action `mediaconnect:DescribeFlow`.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes MediaConnect ressources

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 en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises MediaConnect en charge, consultezComment AWS Elemental MediaConnect fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues 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 découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Journalisation et surveillance

Cette section fournit une présentation des options de consignation et surveillance dans AWS Elemental MediaConnect à des fins de sécurité. Pour plus d'informations sur la journalisation et la surveillance, MediaConnect voirSurveillance et balisage.

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS Elemental MediaConnect et des performances de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. AWS fournit plusieurs outils pour surveiller vos MediaConnect ressources et répondre aux incidents potentiels :

CloudWatch Alarmes Amazon

À l'aide d' CloudWatch alarmes, vous observez une seule métrique sur une période que vous spécifiez. Si la métrique dépasse un seuil donné, une notification est envoyée à une rubrique Amazon SNS ou à une politique AWS Auto Scaling. CloudWatch les alarmes n'appellent pas d'actions car elles se trouvent dans un état particulier. L'état doit avoir changé et avoir été conservé pendant un nombre de périodes spécifié. Pour plus d'informations, consultez Surveillance avec des métriques CloudWatch.

AWS CloudTrail journaux

CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Elemental MediaConnect. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite MediaConnect, 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 plus d'informations, consultez Journalisation des appels d'API avec AWS CloudTrail.

AWS Trusted Advisor

Trusted Advisor s'appuie sur les meilleures pratiques apprises en servant des centaines de milliers de AWS clients. Trusted Advisor inspecte votre AWS environnement, puis émet des recommandations lorsque des opportunités se présentent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité. Tous les AWS clients ont accès à cinq chèques Trusted Advisor. Les clients disposant d'un plan de support Business ou Enterprise peuvent consulter tous les Trusted Advisor chèques.

Pour plus d'informations, consultez AWS Trusted Advisor.

Validation de conformité pour AWS Elemental MediaConnect

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de

conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

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

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  > **Note**
  >
  > Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans plusieurs 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 guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes 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 — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et 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— Cela vous Service AWS permet d'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 Elemental MediaConnect

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 de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives 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.

Sécurité de l'infrastructure dans AWS Elemental MediaConnect

En tant que service géré, AWS Elemental MediaConnect est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder MediaConnect via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.

- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral 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 AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

MediaConnectpoints de terminaison VPC d'interface () AWS PrivateLink

Vous pouvez utiliser un point de terminaison d'un VPC d'interface pour conserver tout le trafic de demandes d'MediaConnectAPI entre votre VPC et MediaConnect le réseau Amazon, améliorant ainsi la sécurité de votre VPC. Les points de terminaison d'un VPC ni d'interface n'ont pas besoin d'une passerelle Internet ni d'un périphérique d'un périphérique NAT ni d'une passerelle d'un périphérique NAT ni d'une passerelle d'interface. Les points de terminaison d'un VPC reposent surAWS PrivateLink, une technologie que vous pouvez utiliser pour accéder de façon privée à MediaConnect des API avec des adresses IP.

Pour en savoir plus sur AWS PrivateLink et les points de terminaison d'un VPC, veuillez consulter la rubrique Points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de terminaison de VPC MediaConnect

Avant de configurer un point de terminaison d'interface pourMediaConnect, consulter Propriétés et limites des points de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

- Les points de terminaison d'un VPC ne prennent pas en charge les demandes inter-régions pour le moment. Veillez à créer votre point de terminaison dans la même région que celle avec laquelle vous souhaitez interagirMediaConnect.
- Les points de terminaison d'un VPC prennent uniquement en charge le DNS fourni par Amazon via Amazon Route 53. Si vous souhaitez utiliser votre propre DNS, vous pouvez utiliser le transfert DNS conditionnel. Pour en savoir plus, consultez Jeux d'options DHCP dans le Guide de l'utilisateur Amazon VPC.
- Le groupe de sécurité attaché au point de terminaison d'un VPC doit autoriser les connexions entrantes sur le port 443 à partir du sous-réseau privé du VPC.

Création de points de terminaison d'un VPC pour MediaConnect

Vous pouvez créer un point de terminaison d'interface pour MediaConnect utiliser la console Amazon VPC ou d'AWS Command Line Interface(AWS CLI). Suivez la procédure décrite dans la section Création d'un point de terminaison d'interface du Guide de l'utilisateur Amazon VPC.

Contrôle de l'accès aux points de terminaison VPC pour MediaConnect

Vous pouvez contrôler l'accès à MediaConnect en attachant une stratégie de point de terminaison à votre point de terminaison de votre VPC. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : stratégie de point de terminaison d'un VPC pour les actions

Voici un exemple de stratégie de point de terminaison pour MediaConnect. Lorsqu'elle est attachée à un point de terminaison, cette politique accorde l'accès aux actions MediaConnect répertoriées pour tous les principaux sur toutes les ressources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "mediaconnect:action-1",
            "mediaconnect:action-2",
            "mediaconnect:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Surveillance et balisage dans AWS Elemental MediaConnect

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'AWS Elemental MediaConnect et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller MediaConnect, signaler tout problème et prendre des mesures automatiques le cas échéant :

- MediaConnect la surveillance des sources de flux affiche des informations détaillées sur un flux source et son support de programme. Vous pouvez consulter les messages d'état relatifs au flux ainsi que les détails relatifs au programme (vidéo, audio et autres données). Pour de plus amples informations, veuillez consulter la section Surveillance des flux sources de ce guide.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.
- Amazon CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux AWS ressources. CloudWatch Les événements permettent une informatique automatisée axée sur les événements, car vous pouvez rédiger des règles qui surveillent certains événements et déclenchent des actions automatisées dans d'autres AWS services lorsque ces événements se produisent. Pour plus d'informations, consultez le guide de l'utilisateur Amazon CloudWatch Events.
- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre le nombre de paquets abandonnés et non récupérés sur vos flux AWS MediaConnect Elemental et vous avertir automatiquement lorsque ces valeurs dépassent un certain nombre. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Surveillance des métadonnées des sources AWS Elemental MediaConnect

MediaConnect la surveillance des métadonnées de la source affiche des informations sur le flux de transport et son support de programme. Vous pouvez consulter les messages d'état relatifs à la

source du flux ainsi que les détails relatifs aux données vidéo, audio et autres du programme. La surveillance des métadonnées source peut être utilisée avec la MediaConnect console AWS CLI, l'API ou le SDK. Pour plus d'informations sur l'API, voir : `DescribeFlowSourceMetadata`dans le Guide de référence de l'MediaConnect API.

> **Note**
>
> Si vous utilisez plusieurs sources pour votre flux, les métadonnées de la source ne sont affichées que pour la source actuellement utilisée par le flux.

Détails des métadonnées de la source

Les sections suivantes fournissent des détails sur le type d'informations affichées par la surveillance des métadonnées source.

Alertes et messages

La section des alertes actives de l'onglet Console des métadonnées source et la section des messages de la réponse `DescribeFlowSourceMetadata` API/CLI peuvent contenir des messages d'état contenant plus d'informations sur le flux de transport. En cas MediaConnect de détection d'un problème ou d'impossibilité de récupérer les métadonnées du flux source, un message d'état associé sera affiché.

Programmes

La section des programmes contient des informations sur les programmes individuels contenus dans le flux de transport. Cette section contient les champs suivants :

Champ	Détails
Numéro du programme	Numéro de programme de ce programme.
Programme PID	Le programme Packet Identifier (PID).
PCR PID	Le PID de référence d'horloge du programme (PCR) de ce programme.
Nom du programme	Le nom de ce programme.

Champ	Détails
Streams	Les sections imbriquées contiennent des informations sur les types de flux vidéo, audio et de données.

Streams

La section des flux est imbriquée dans chaque programme de flux de transport individuel. Cette section contient les champs suivants :

Champ	Détails
Type de flux	Type de contenu contenu dans ce flux. Cette valeur peut être vidéo, audio, de données ou inconnue.
Codec	Le codec du flux. Cette valeur varie en fonction du type de flux. Par exemple, un type de flux vidéo peut afficher une valeur H264 tandis qu'un type de flux audio affiche une valeur AAC.
PID	L'identifiant de paquet (PID) du flux.

Exemple de réponse API/CLI aux métadonnées de la source

Voici un exemple de réponse de l'`DescribeFlowSourceMetadata`API/CLI. Dans cet exemple, il existe deux programmes. Chaque programme comporte un flux vidéo et deux flux audio. Le premier programme possède un flux de données SCTE-35. Le deuxième programme possède un type de flux non valide sur le PID 139. Le type de flux non valide est indiqué par le code d'état dans la section des messages et le type de `Unknown` flux dans la section du programme.

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
    "TransportMediaInfo": {
```

```
        "Messages": [
            {
                "StatusCode": "InvalidType",
                "Message": "We could not determine the type of pid 139 on program 2"
            }
        ],
        "Programs": [
          {
                "ProgramNumber": 1,
                "ProgramPid": 16,
                "PcrPid": 56,
                "ProgramName": "Basketball HD",
                "Streams": [
                    {
                        "StreamType": "Video",
                        "Codec": "H264",
                        "Pid": 126
                    },
                    {
                        "StreamType": "Audio",
                        "Codec": "AAC",
                        "Pid": 127
                    },
                    {
                        "StreamType": "Audio",
                        "Codec": "AAC",
                        "Pid": 128
                    },
                    {
                        "StreamType": "Data",
                        "Codec": "SCTE35",
                        "Pid": 129
                    }
                ]
          },
          {
                "ProgramNumber": 2,
                "ProgramPid": 26,
                "PcrPid": 66,
                "ProgramName": "Basketball SD",
                "Streams": [
                    {
                        "StreamType": "Video",
                        "Codec": "H264",
```

```
                        "Pid": 136
                    },
                    {
                        "StreamType": "Audio",
                        "Codec": "AAC",
                        "Pid": 137

                    },
                    {
                        "StreamType": "Audio",
                        "Codec": "AAC",
                        "Pid": 138

                    },
                    {
                        "StreamType": "Unknown",
                        "Codec": "Unknown",
                        "Pid": 139
                    }
                ]
            }
        ]
    },
}
```

Utilisation de la surveillance des métadonnées source (console)

Vous pouvez récupérer les dernières métadonnées de la source à MediaConnect l'aide de la console.

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans l'écran Flux, sélectionnez le flux que vous souhaitez inspecter.
3. Sélectionnez l'onglet Métadonnées de la source.
4. L'onglet des métadonnées de la source contient une liste extensible de chaque alerte, programme et flux actifs pour la source du flux sélectionné.

Utilisation de la surveillance des métadonnées source (AWS CLI)

Vous pouvez récupérer les dernières métadonnées de la source à MediaConnect l'aide du AWS CLI. L'exemple suivant montre la AWS CLI commande et la valeur de retour pour un scénario typique.

1. Dans le AWS CLI, utilisez la `describe-flow-source-metadata` commande avec l'`--flow-arn`option du flux que vous souhaitez inspecter.

```
aws mediaconnect describe-flow-source-metadata --flow-arn arn:aws:mediaconnect:us-east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow
```

2. La valeur renvoyée contiendra les informations multimédia relatives à la source du flux sélectionné. Voici un exemple générique du format de la valeur de retour. Dans cet exemple, il n'y a aucun message à afficher.

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow",
    "Messages": [],
    "Timestamp": "2023-12-06T19:57:54Z",
    "TransportMediaInfo": {
        "Programs": [
            {
                "PcrPid": 1000,
                "ProgramNumber": 1,
                "ProgramPid": 2000,
                "ProgramName": "AwardsShow HD",
                "Streams": [
                    {
                        "StreamType": "Video",
                        "Codec": "H264",
                        "Pid": 256
                    },
                    {
                        "StreamType": "Audio",
                        "Codec": "AAC",
                        "Pid": 257
                    },
                    {
                        "StreamType": "Data",
                        "Codec": "SCTE35",
                        "Pid": 258
                    }
                ]
            }
        ]
    }
```

```
}
```

Surveillance d'AWS Elemental à l'aide des métriques MediaConnect Amazon CloudWatch

Vous pouvez surveiller AWS Elemental à MediaConnect l'aide d'AWS Elemental CloudWatch, qui collecte les données brutes et les traite en métriques lisibles en temps quasi réel. Ces statistiques sont conservées pendant 15 mois, afin que vous puissiez accéder aux informations historiques et avoir une meilleure idée des performances de votre application ou service Web. La plupart MediaConnect des indicateurs sont accessibles sur des périodes aussi courtes qu'une seconde. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Vous pouvez consulter CloudWatch les métriques de vos flux directement sur la MediaConnect console. Sur la console, vous pouvez consulter ces statistiques sur des périodes aussi courtes qu'une seconde ou 30 minutes.

> **Note**
>
> MediaConnect Les métriques de passerelle ne sont pas disponibles pendant les périodes de haute résolution (une seconde). Vous devez sélectionner une période d'au moins une minute.

Définition d'une métrique

AWS Elemental MediaConnect collecte des données qui constituent la base des métriques. Il collecte ces points de données chaque seconde et les envoie immédiatement à Amazon. CloudWatch Vous pouvez l'utiliser CloudWatch pour générer des métriques pour ces points de données.

Une métrique est un ensemble de points de données auquel une agrégation (une statistique) a été appliquée et qui comporte une période et une plage de temps. Par exemple, vous pouvez demander la métrique des paquets abandonnés sous forme de moyenne (la statistique) pour une période d'une minute sur 10 minutes (la plage de temps). Le résultat de cette demande est de 10 mesures (car la plage divisée par la période est de 10).

Période

La plupart MediaConnect des métriques ont une période de haute résolution, ce qui signifie que la période minimale est d'une seconde. MediaConnect Les métriques de passerelle sont les seules métriques non disponibles pendant une période de haute résolution.

Plage horaire

Chaque période a une plage de temps maximale. Par exemple, si vous spécifiez 1 jour comme plage de temps, vous ne pourrez pas récupérer les métriques avec une période de 10 secondes.

Période	Plage de temps maximale
1 seconde	Les 3 dernières heures
5 secondes	
10 secondes	
30 secondes	
60 secondes	Les 360 dernières heures (15 jours)
300 secondes (5 minutes)	Les 1512 dernières heures (63 jours)
900 secondes (15 minutes)	
3 600 secondes (1 heure) ou plus	Les 455 derniers jours (15 mois)

Les périodes n'ont pas de plage de temps minimale. Mais il arrive un moment où les statistiques que vous appliquez n'ont aucun sens si votre période est courte. Supposons, par exemple, que vous définissiez la période à une seconde. Cela signifie que cela CloudWatch récupère un point de données. Vous ne pouvez pas obtenir de moyenne, de minimum ou de maximum pour un point de données. Cependant, cela ne signifie pas que la métrique n'a aucun sens. La métrique concerne plutôt le point de données brut, sans aucune statistique.

Durée de stockage maximale

Les statistiques sont disponibles pour les 15 derniers mois. Assurez-vous de spécifier une période qui autorise la plage de temps que vous souhaitez.

Affichage des métriques

Vous pouvez consulter certaines statistiques dans la MediaConnect console. Vous pouvez consulter tous les indicateurs dans la CloudWatch console. Vous pouvez également récupérer des métriques à l'aide de la CLI, de l'API REST ou de n'importe quel AWS SDK.

Sur la CloudWatch console, le taux de rafraîchissement minimal des métriques est de 30 secondes.

Pour afficher les métriques sur la MediaConnect console

Vous pouvez consulter certaines statistiques dans la MediaConnect console. Vous pouvez consulter les statistiques actuelles, allant d'une heure à une semaine. (Pour consulter d'autres mesures ou pour consulter l'historique des mesures, vous devez utiliser la CloudWatch console.)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Flux. Sur la page Flux, choisissez le flux souhaité. La page Détails s'affiche.
3. Choisissez l'onglet Health. Les métriques prises en MediaConnect charge dans cet onglet apparaissent.
4. Choisissez la période et la plage horaire. Par exemple, 1 jour passé (période de 5 minutes).

Pour afficher les métriques à l'aide de la CloudWatch console

Sur la CloudWatch console, vous pouvez consulter tous les MediaConnect indicateurs pour n'importe quel intervalle de temps, qu'il s'agisse des indicateurs actuels ou des indicateurs historiques. L'affichage des métriques sur la CloudWatch console est payant.

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, choisissez Metrics, puis All metrics. Dans la moitié inférieure de la page, l'onglet Parcourir affiche des cartes avec des noms.

   Aucune carte n'apparaît si vous êtes complètement nouveau dans le AWS domaine et si vous n'avez effectué aucune action qui crée des statistiques dans un service.
3. Sélectionnez la carte nommée AWS/MediaConnect.

   Cette carte apparaît uniquement si vous avez lancé au moins un flux au cours des 15 derniers mois dans la AWS région actuellement sélectionnée CloudWatch. Cette carte n'apparaîtra pas si

vous n'avez jamais lancé de MediaConnect flux. Dans ce cas, revenez à cette procédure après avoir créé et démarré un flux.

(Une carte nommée MediaConnectpeut apparaître dans la section espace de noms personnalisé de la page. Cette carte est destinée à l'ancien espace de noms pour les MediaConnect métriques. Les deux espaces de noms sont devenus des doublons l'un de l'autre en septembre 2022, il n'y a donc aucun avantage à choisir cette carte. Choisissez toujours AWS/MediaConnect.)

4. L'onglet Parcourir dans la moitié inférieure de la page affiche désormais les dimensions. Choisissez la dimension de métrique. Par exemple, choisissez Flow ARN.

   L'onglet Parcourir affiche désormais un tableau avec une colonne indiquant la dimension choisie (par exemple, Flow ARN) et une colonne répertoriant toutes les métriques. Vous pouvez trier le tableau.

5. Sélectionnez une ou plusieurs lignes. Dès que vous sélectionnez une ligne, elle apparaît dans le graphique dans la moitié supérieure de la page.
6. Dans la moitié inférieure de la page, choisissez l'onglet Statistiques graphiques.
7. Dans les choix situés à droite de l'onglet, spécifiez la statistique et la période.

   Lorsque vous choisissez la période, le graphique est actualisé pour afficher la plage de temps maximale pour cette période. Si le graphique est désormais vide sur la gauche, vous pouvez ajuster la chronologie dans les choix en haut à droite du graphique. Choisissez un chiffre inférieur pour que tout l'espace soit rempli. Par exemple, remplacez 1w par 1d.

Pour consulter les statistiques à l'aide du AWS CLI

- À partir d'une invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/MediaConnect"
```

MediaConnectMesures AWS Elemental pour surveiller l'état des flux

AWS Elemental MediaConnect envoie des métriques à. CloudWatch Vous pouvez consulter des indicateurs spécifiques pour évaluer l'état de votre flux. Si le flux ne fonctionne pas correctement, ces mesures peuvent vous aider à déterminer l'origine du problème. Pour plus de détails sur chaque métrique, consultez les tableaux de cette section.

Pour plus d'informations sur les métriques de source, consultezMesures permettant de surveiller l'état de santé de la source.

> **Note**
>
> Les métriques suivies par MediaConnect adhèrent à la norme telle que définie par la spécification TR 101 290.

Rubriques

Métriques de débit

Le tableau suivant répertorie les métriques réseau auxquelles AWS Elemental MediaConnect envoie des données. CloudWatch

Métrique	Description
`ARQRecovered`	Nombre de paquets abandonnés qui ont été récupérés par une demande de répétition automatique (ARQ). Cette métrique ne s'applique pas aux flux qui reçoivent du contenu provenant d'une autorisation ou aux flux qui ont plusieurs sources. Pour les flux qui ont plusieurs sources, utilisez la métrique SourceArq Recovered pour afficher les données de chaque source. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
ARQRequests	Le nombre de paquets retransmis qui ont été demandés par le biais d'une demande de répétition automatique (ARQ) et reçus. Cette métrique ne s'applique pas aux flux qui reçoivent du contenu provenant d'une autorisation ou aux flux qui ont plusieurs sources. Pour les flux qui ont plusieurs sources, utilisez la métrique SourceArqRequests pour afficher les données de chaque source. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
BitRate	Débit de la vidéo entrante (source). Unités : bits par seconde (b/s) Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`Connected`	État de la source. Une valeur de 1 indique que la source est connectée et une valeur de 0 (zéro) indique que la source est déconnectée. Cette métrique s'applique uniquement aux sources qui utilisent les protocoles Zixi, SRT, Fujitsu ou RIST. Unités : aucune Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
`Disconnections`	Le nombre de fois où l'état de la source est passé de connecté à déconnecté. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
`DroppedPackets`	Le nombre de paquets perdus pendant le transport. Cette valeur est mesurée avant toute correction d'erreur. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
FECPackets	Nombre de paquets transmis à l'aide de la correction d'erreur directe (FEC) et reçus. Cette métrique s'applique uniquement aux flux dont une source utilise les protocoles RTP-FEC, Zixi ou Fujitsu. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'une autorisation ou aux flux qui ont plusieurs sources. Pour les flux qui ont plusieurs sources, utilisez la métrique SourceFec Packets pour afficher les données de chaque source. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
FECRecovered	Nombre de paquets transmis à l'aide de la correction d'erreur directe (FEC), perdus pendant le transit et récupérés. Cette métrique s'applique uniquement aux flux dont une source utilise les protocoles RTP-FEC, Zixi ou Fujitsu. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'une autorisation ou aux flux qui ont plusieurs sources. Pour les flux qui ont plusieurs sources, utilisez la métrique SourceFecRecovered pour afficher les données de chaque source. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
MergeActive	État de fusion de toutes les sources du flux. La valeur 1 indique que toutes les sources sont fusionnées. Une valeur de 0 (zéro) indique qu'au moins une source n'est pas fusionnée activement avec le code 7. Unités : aucune Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
MergeLatency	La valeur maximale pour SourceMergeLatency. Unités : millisecondes Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
NotRecoveredPackets	Nombre de paquets perdus pendant le transit et qui n'ont pas été récupérés par correction d'erreur. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`OverflowPackets`	Nombre de paquets perdus en transit parce que la vidéo nécessitait plus de mémoire tampon que ce qui était disponible. Cette métrique ne s'applique pas aux flux qui reçoivent du contenu provenant d'une autorisation ou aux flux qui ont plusieurs sources. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
`PacketLossPercent`	Pourcentage de paquets perdus pendant le transit, même s'ils ont été récupérés. Unités : pourcentage Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
`RecoveredPackets`	Nombre de paquets perdus pendant le transit, mais récupérés. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`RoundTripTime`	Le temps nécessaire à la source pour envoyer un signal et recevoir un accusé de réception d'AWS Elemental. MediaConnect Cette métrique ne s'applique pas aux flux qui reçoivent du contenu provenant d'une autorisation ou aux flux qui ont plusieurs sources. Pour les flux qui ont plusieurs sources, utilisez la SourceRoundTripTime métrique pour afficher les données de chaque source. Unités : millisecondes Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
`TotalPackets`	Nombre total de paquets reçus. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
`FailoverSwitches`	Nombre total de fois que le flux passe d'une source à l'autre lors de l'utilisation du mode Failover pour le basculement de source.

TR 101 290 Métriques de priorité 1

Le tableau suivant répertorie les métriques TR 101 290 Priority 1 auxquelles AWS Elemental MediaConnect envoie. CloudWatch

Métrique	Description
`ContinuityCounter`	Le nombre de fois qu'une erreur de continuité s'est produite. Cette erreur indique un ordre de paquets incorrect ou des paquets perdus.

Métrique	Description
	Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
PATError	Nombre de fois qu'une erreur de table d'association de programmes (PAT) s'est produite. Cette erreur indique que le PAT est manquant. Le PAT répertori e les programmes disponibles dans un flux de transport (TS) et pointe vers les tables de mappage des programmes (PMT). Le décodeur a besoin du PAT pour faire son travail. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
PIDError	Nombre de fois qu'une erreur d'identifiant de paquet (PID) s'est produite. Cette erreur indique qu'il manque le flux de données associé à un PID. Les PID sont des identifiants qui indiquent l'emplacement des flux vidéo, audio et de données. Cette erreur peut se produire une fois que le flux de transport a été multiplexé puis remultiplexé. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
PMTError	Nombre de fois qu'une erreur de table de mappage des programmes (PMT) s'est produite. Cette erreur se produit lorsque le PMT n'est pas reçu au moins toutes les 500 millisecondes (ms). Chaque PMT contient une liste de PID, qui aident les décodeurs à réassembler les données. Le décodeur a besoin des PMT pour faire son travail. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
TSByteError	Nombre de fois qu'une erreur d'octet dans le flux de transport s'est produite. Cette erreur indique que l'octet de synchronisation n'est pas apparu après le nombre d'octets prescrit. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
TSSyncLoss	Nombre de fois qu'une erreur de perte de synchronisation TS s'est produite. Cette erreur se produit après au moins deux erreurs d'octets TS consécutives. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

TR 101 290 Métriques de priorité 2

Le tableau suivant répertorie les métriques TR 101 290 Priority 2 auxquelles AWS Elemental MediaConnect envoie. CloudWatch

Métrique	Description
`CATError`	Nombre de fois qu'une erreur de table d'accès conditionnel (CAT) s'est produite. Cette erreur indique que le CAT n'est pas présent. Le CAT indique au décodeur récepteur intégré (IRD) où trouver les messages de gestion pour les systèmes d'accès conditionnel (CA) utilisés. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
`CRCError`	Nombre de fois qu'une erreur de contrôle de redondance cyclique (CRC) s'est produite. Cette erreur se produit lorsqu'un CRC détermine que les données sont corrompues. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
`PCRAccuracyError`	Nombre de fois qu'une erreur de précision du registre d'horloge du programme (PCR) s'est produite. Cette erreur se produit lorsque la valeur de la PCR transmise diffère de plus de 500 nanosecondes (ns) de ce qui est attendu. Lorsqu'un flux est codé, le codeur attribue des valeurs PCR périodiques à l'horloge du programme de l'encodeur. Le décodeur s'appuie sur ces valeurs pour garantir la synchronisation du flux.

Métrique	Description
	Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
PCRError	Le nombre de fois qu'une erreur PCR s'est produite. Cette erreur se produit lorsque les valeurs PCR ne sont pas envoyées assez fréquemment. Le service s'appuie sur des PCR réguliers et fréquents pour réinitialiser l'horloge du système local à 27 MHz. Bien que l'erreur se produise lorsque l'intervalle dépasse 100 millisecondes (ms), les meilleures pratiques stipulent que les PCR doivent être reçues au moins toutes les 40 ms. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
PTSError	Nombre de fois qu'une erreur d'horodatage de présentation (PTS) s'est produite. Cette erreur se produit lorsqu'un horodatage de présentation (PTS) n'est pas reçu au moins toutes les 700 ms. Cela peut se produire si le PTS est envoyé moins fréquemment ou pas du tout. La cause la plus courante de cette erreur est le brouillage du flux de transport (TS). Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`TransportError`	Nombre de fois qu'une erreur de transport principale s'est produite. Cette erreur indique que le paquet TS est inutilisable. Lorsque cette erreur se produit, ignorez toutes les autres erreurs TR 101 290 pour ce paquet. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux

Métriques de maintenance

Le tableau suivant répertorie les métriques de maintenance des flux auxquelles AWS Elemental MediaConnect envoie. CloudWatch

Métrique	Description
`MaintenanceScheduled`	La maintenance est planifiée pour le flux. Unités : nombre Dimensions valides : • Flux (ARN) • Tous les flux
`MaintenanceRescheduled`	MediaConnect n'est pas en mesure d'effectuer la maintenance à la date et à l'heure prévues précédemment. Une nouvelle date et heure ont été automatiquement attribuées par MediaConnect pour la maintenance de ce flux. Unités : nombre Dimensions valides : • Flux (ARN)

Métrique	Description
	• Tous les flux
MaintenanceCanceled	La maintenance de ce flux est annulée par MediaConnect. Unités : nombre Dimensions valides : • Flux (ARN) • Tous les flux
MaintenanceStarted	La maintenance de ce flux a débuté et est actuellement en cours. Unités : nombre Dimensions valides : • Flux (ARN) • Tous les flux
MaintenanceSucceeded	La maintenance s'est terminée avec succès pour ce flux. Unités : nombre Dimensions valides : • Flux (ARN) • Tous les flux
MaintenanceFailed	La maintenance ne s'est pas terminée correctement pour ce flux. Unités : nombre Dimensions valides : • Flux (ARN) • Tous les flux

MediaConnectMesures AWS Elemental pour surveiller l'état de santé de la source

AWS Elemental MediaConnect envoie des métriques à. CloudWatch Vous pouvez consulter des indicateurs spécifiques pour évaluer l'état de santé de la source de votre flux. Si le flux ne fonctionne pas correctement, ces mesures peuvent vous aider à déterminer si le problème provient de la source. Pour plus de détails sur chaque métrique, consultez les tableaux de cette section.

Pour plus d'informations sur les métriques de flux, consultezDes métriques pour surveiller l'état du flux.

> **Note**
>
> Les métriques suivies par MediaConnect adhèrent à la norme telle que définie par la spécification TR 101 290.

Rubriques

- Métriques de la source
- TR 101 290 Métriques de priorité 1
- TR 101 290 Métriques de priorité 2

Métriques de la source

Le tableau suivant répertorie les métriques de source auxquelles AWS Elemental MediaConnect envoie des messages. CloudWatch

Métrique	Description
`SourceARQ Recovered`	Nombre de paquets abandonnés qui ont été récupérés par une demande de répétition automatique (ARQ). Cette métrique s'applique aux sources qui utilisent le protocole RIST, Zixi, SRT ou Fujitsu-QOS. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : nombre Dimensions valides :

Métrique	Description
	• ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceARQ Requests`	Le nombre de paquets retransmis qui ont été demandés par le biais d'une demande de répétition automatique (ARQ) et reçus. Cette métrique s'applique aux sources qui utilisent le protocole RIST, Zixi, SRT ou Fujitsu-QOS. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`SourceBitRate`	Débit de la vidéo entrante (source). Unités : bits par seconde (b/s) Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux **Note** MediaConnect supprime les paquets nuls afin d'optimiser la connexion de données entre le flux de l'auteur du contenu et le flux de l'abonné. Cela peut entraîner une fluctuation du débit du flux de l'abonné ou une différence entre le débit du flux de l'auteur du contenu et le flux de l'abonné. Nous vous recommandons de surveiller l'état de santé de la source en combinant d'`SourceBitRate` autres indicateurs tels que `SourceContinuityCounter` et`SourceNotRecovered Packets` .

Métrique	Description
SourceConnected	État de la source. Une valeur de 1 indique que la source est connectée et une valeur de 0 (zéro) indique que la source est déconnectée. Cette métrique s'applique uniquement aux sources qui utilisent le protocole Zixi, SRT ou Fujitsu-QOS. Unités : aucune Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
SourceDisconnections	Le nombre de fois où l'état de la source est passé de connecté à déconnecté. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
SourceDroppedPackets	Le nombre de paquets perdus pendant le transport. Cette valeur est mesurée avant toute correction d'erreur. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`SourceFEC Packets`	Nombre de paquets transmis à l'aide de la correction d'erreur directe (FEC) et reçus. Cette métrique s'applique uniquement aux sources qui utilisent les protocoles RTP-FEC, Zixi ou Fujitsu. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceFEC Recovered`	Nombre de paquets transmis à l'aide de la correction d'erreur directe (FEC), perdus pendant le transit et récupérés. Cette métrique s'applique uniquemen t aux sources qui utilisent les protocoles RTP-FEC, Zixi ou Fujitsu. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`SourceMergeActive`	Une indication du statut de la source par rapport aux autres sources. Cette métrique est utile lorsque le flux possède plusieurs sources de basculement et que vous utilisez le mode de basculement Merge. Une valeur de 1 indique que le flux possède plusieurs sources et que cette source est activement utilisée, avec une fusion à 7. La valeur 0 (zéro) indique que le flux n'utilise pas la source pour former le flux. Unités : aucune Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceSelected`	Une indication si une source est utilisée comme entrée pour l'ingestion de flux. Cette métrique s'applique si votre flux utilise le basculement à la source et si le mode de basculement est défini sur Failover. Une valeur de 1 indique que la source est utilisée comme entrée. La valeur 0 (zéro) indique que le flux est utilisé comme flux de sauvegarde. Unités : aucune Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
SourceMergeLatency	Durée pendant laquelle cette source suit la source principale. Si cette source est la source principale, la valeur est 0 (zéro). Unités : millisecondes Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
SourceMergeStatusWarnMismatch	Une métrique d'état avertissant que le flux reçoit des sources incompatibles. Cela signifie que les paquets abandonnés ne seront pas récupérés, ce qui nuira à la fiabilité du réseau. Cette métrique s'applique uniquement aux sources utilisant le basculement en mode fusion. Le basculement en mode fusion nécessite que les deux sources soient binaires identiques. Pour être identiques sur le plan binaire, les sources doivent provenir du même encodeur. Cela permettra aux sources de partager les paquets manquants, car les paquets sont identiques. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`SourceMergeStatusWarnSolo`	Une métrique d'état avertissant que le flux ne reçoit qu'une seule source. Cela signifie que les paquets abandonnés ne seront pas récupérés, ce qui nuira à la fiabilité du réseau. Cette métrique s'applique uniquement aux sources utilisant le basculement en mode fusion. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceNotRecoveredPackets`	Nombre de paquets perdus pendant le transit et qui n'ont pas été récupérés par correction d'erreur. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`SourceMissingPackets`	Un paquet était absent des deux flux sources, ce qui signifie que le paquet n'a pas pu être récupéré. Cette métrique s'applique uniquement aux sources utilisant le basculement en mode fusion. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceOverflowPackets`	Nombre de paquets perdus en transit parce que la vidéo nécessitait plus de mémoire tampon que ce qui était disponible. Cette métrique ne s'applique pas aux flux qui reçoivent du contenu provenant d'une autorisation ou aux flux qui ont plusieurs sources. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`SourcePacketLossPercent`	Pourcentage de paquets perdus pendant le transit, même s'ils ont été récupérés. Unités : pourcentage Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceRecoveredPackets`	Nombre de paquets perdus pendant le transit, mais récupérés. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceRoundTripTime`	Le temps nécessaire à la source pour envoyer un signal et recevoir un accusé de réception d'AWS Elemental. MediaConnect Cette métrique s'applique aux sources qui utilisent le protocole RIST, Zixi, SRT ou Fujitsu-QOS. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : millisecondes Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`SourceTotalPackets`	Nombre total de paquets reçus. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceTotalBytes`	Quantité totale d'octets transférés MediaConnect depuis la source. Unités : octets Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceDroppedPayloads`	Charges utiles perdues pendant le transport MediaConnect vers la source. Une charge utile est une image vidéo ou un échantillon audio. Les charges utiles peuvent être constituées de plusieurs paquets. Les métriques de charge utile ne sont applicables que lors de l'utilisation du CDI. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
SourceLatePayloads	Paquets d'une charge utile qui arrivent en dehors de la période de tampon de synchronisation maximale configurée. Une charge utile est une image vidéo ou un échantillon audio. Les charges utiles peuvent être constituées de plusieurs paquets. Les métriques de charge utile ne sont applicables que lors de l'utilisation du CDI. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
SourceTotalPayloads	Quantité totale de charges utiles livrées MediaConnect depuis la source. Une charge utile est une image vidéo ou un échantillon audio. Les charges utiles peuvent être constituées de plusieurs paquets. Les métriques de charge utile ne sont applicables que lors de l'utilisation du CDI. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

TR 101 290 Métriques de priorité 1

Le tableau suivant répertorie les métriques TR 101 290 Priority 1 auxquelles AWS Elemental MediaConnect envoie. CloudWatch

Métrique	Description
SourceContinuityCounter	Le nombre de fois qu'une erreur de continuité s'est produite. Cette erreur indique un ordre de paquets incorrect ou des paquets perdus. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
SourcePATError	Nombre de fois qu'une erreur de table d'association de programmes (PAT) s'est produite. Cette erreur indique que le PAT est manquant. Le PAT répertorie les programmes disponibles dans un flux de transport (TS) et pointe vers les tables de mappage des programmes (PMT). Le décodeur a besoin du PAT pour faire son travail. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
SourcePIDError	Nombre de fois qu'une erreur d'identifiant de paquet (PID) s'est produite. Cette erreur indique qu'il manque le flux de données associé à un PID. Les PID sont des identifiants qui indiquent l'emplacement des flux vidéo, audio et de données. Cette erreur peut se produire une fois que le TS a été multiplexé puis remultiplexé. Unités : nombre Dimensions valides :

Métrique	Description
	• ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourcePMTError`	Nombre de fois qu'une erreur de table de mappage des programmes (PMT) s'est produite. Cette erreur se produit lorsque le PMT n'est pas reçu au moins toutes les 500 millisecondes (ms). Chaque PMT contient une liste de PID, qui aident les décodeurs à réassembler les données. Le décodeur a besoin des PMT pour faire son travail. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
`SourceTSByteError`	Nombre de fois qu'une erreur d'octet TS s'est produite. Cette erreur indique que l'octet de synchronisation n'est pas apparu après le nombre d'octets prescrit. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
SourceTSSyncLoss	Nombre de fois qu'une erreur de perte de synchronisation TS s'est produite. Cette erreur se produit après au moins deux erreurs d'octets TS consécutives. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

TR 101 290 Métriques de priorité 2

Le tableau suivant répertorie les métriques TR 101 290 Priority 2 auxquelles AWS Elemental MediaConnect envoie. CloudWatch

Métrique	Description
SourceCATError	Nombre de fois qu'une erreur de table d'accès conditionnel (CAT) s'est produite. Cette erreur indique que le CAT n'est pas présent. Le CAT indique au décodeur récepteur intégré (IRD) où trouver les messages de gestion pour les systèmes d'accès conditionnel (CA) utilisés. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
SourceCRCError	Nombre de fois qu'une erreur de contrôle de redondance cyclique (CRC) s'est produite. Cette erreur se produit lorsqu'un CRC détermine que les données sont corrompues. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
SourcePCRAccuracyError	Nombre de fois qu'une erreur de précision du registre d'horloge du programme (PCR) s'est produite. Cette erreur se produit lorsque la valeur de la PCR transmise diffère de plus de 500 nanosecondes (ns) de ce qui est attendu. Lorsqu'un flux est codé, le codeur attribue des valeurs PCR périodiques à partir de l'horloge du programme de l'encodeur. Le décodeur s'appuie sur ces valeurs pour garantir la synchronisation du flux. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
SourcePCR Error	Le nombre de fois qu'une erreur PCR s'est produite. Cette erreur se produit lorsque les valeurs PCR ne sont pas envoyées assez fréquemment. Le service s'appuie sur des PCR réguliers et fréquents pour réinitialiser l'horloge du système local à 27 MHz. Bien que l'erreur se produise lorsque l'intervalle dépasse 100 millisecondes (ms), les meilleures pratiques stipulent que les PCR doivent être reçues au moins toutes les 40 ms. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux
SourcePTS Error	Nombre de fois qu'une erreur d'horodatage de présentation (PTS) s'est produite. Cette erreur se produit lorsqu'un horodatage de présentation (PTS) n'est pas reçu au moins toutes les 700 ms. Cela peut se produire si le PTS est envoyé moins fréquemment ou pas du tout. La cause la plus courante de cette erreur est le brouillage du TS. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
SourceTransportError	Nombre de fois qu'une erreur de transport principale s'est produite. Cette erreur indique que le paquet TS est inutilisable. Lorsque cette erreur se produit, ignorez toutes les autres erreurs TR 101 290 pour ce paquet. Unités : nombre Dimensions valides : • ARN source • Flux (ARN) • Zone de disponibilité • Tous les flux

Des MediaConnect métriques AWS Elemental pour surveiller l'état de santé des sorties

AWS Elemental MediaConnect envoie des métriques à. CloudWatch Vous pouvez consulter des métriques spécifiques pour évaluer l'état de la sortie de votre flux.

> **Note**
>
> Les métriques suivies par MediaConnect adhèrent à la norme telle que définie par la spécification TR 101 290.

Rubriques

- Métriques de sortie pour les protocoles de flux de transport
- Métriques de sortie pour les protocoles CDI

Métriques de sortie pour les protocoles de flux de transport

Métrique	Description
`ConnectedOutputs`	Le nombre de sorties actuellement connectées. Cette métrique s'applique aux sorties utilisant le protocole Zixi, Fujitsu ou SRT. Unités : nombre Dimensions valides : • Flux (ARN) • Zone de disponibilité • Tous les flux
`OutputConnected`	État de la sortie. Une valeur de 1 indique que la sortie est connectée, et une valeur de 0 (zéro) indique que la sortie est déconnectée. Cette métrique s'applique aux sorties qui utilisent le protocole Zixi ou SRT. Unités : aucune Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux
`OutputDisconnections`	Le nombre de fois où l'état de sortie est passé de connecté à déconnecté. Cette métrique s'applique aux sorties qui utilisent le protocole Zixi ou SRT. Unités : nombre Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité

Métrique	Description
	• Tous les flux
`OutputBitrate`	Débit de la vidéo sortante (sortie). Cette métrique s'applique aux sorties qui utilisent les protocoles SRT ou Fujitsu-QOS ou qui produisent des sorties vers. MediaLive Unités : bits par seconde (b/s) Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux **Note** La `OutputBitrate` valeur peut varier en fonction du protocole sélectionné en raison des paquets autres que des charges utiles, des paquets retransmis, des en-têtes de paquets et d'autres paquets spécifiques au protocole. En raison de ces facteurs, la valeur du débit indiquée par cette métrique peut varier entre les sorties.
`OutputTotalPackets`	Nombre total de paquets envoyés à la sortie. Cette métrique s'applique aux sorties qui utilisent les protocoles SRT ou Fujitsu-QOS ou qui produisent des sorties vers. MediaLive Unités : nombre Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`OutputFEC Packets`	Nombre de paquets transmis à l'aide de la correction d'erreur directe (FEC) et reçus. Cette métrique s'applique aux sorties utilisant le protocole Fujitsu. Unités : nombre Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux
`OutputARQ Requests`	Le nombre de paquets retransmis qui ont été demandés par le biais d'une demande de répétition automatique (ARQ) et reçus. Cette métrique s'applique aux sorties qui utilisent le protocole SRT ou à la sortie vers MediaLive. Unités : nombre Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`OutputRes entPackets`	Le nombre de paquets qui ont été retransmis vers la destination de sortie. Cette métrique s'applique aux sorties qui utilisent le protocole SRT ou à la sortie vers MediaLive. Unités : nombre Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux
`OutputRou ndTripTime`	Le temps nécessaire à la sortie pour envoyer un signal et recevoir un accusé de réception de la destination de sortie. Cette métrique s'applique aux sorties qui utilisent le protocole SRT ou à la sortie vers MediaLive. Unités : millisecondes Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux

Métrique	Description
`OutputNotRecoveredPackets`	Nombre de paquets perdus pendant le transit et qui n'ont pas été récupérés par correction d'erreur. Cette métrique s'applique aux sorties vers MediaLive. Unités : nombre Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux

Métriques de sortie pour les protocoles CDI

Métrique	Description
`OutputTotalBytes`	Quantité totale d'octets MediaConnect transférés depuis la sortie. Cette métrique n'est applicable que lors de l'utilisation du CDI. Unités : octets Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux
`OutputDroppedPayloads`	Charges utiles perdues pendant le transport entre la sortie MediaConnect et la sortie. Une charge utile est une image vidéo ou un échantillon audio. Les charges utiles peuvent être constituées de plusieurs paquets. Les métriques de charge utile ne sont applicables que lors de l'utilisation du CDI. Unités : nombre Dimensions valides :

Métrique	Description
	• ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux
`OutputLatePayloads`	Paquets d'une charge utile qui arrivent en sortie en dehors MediaConnect de la mémoire tampon interne. Une charge utile est une image vidéo ou un échantillon audio. Les charges utiles peuvent être constituées de plusieurs paquets. Les métriques de charge utile ne sont applicables que lors de l'utilisation du CDI. Unités : nombre Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux
`OutputTotalPayloads`	Quantité totale de charges utiles livrées depuis MediaConnect la sortie. Une charge utile est une image vidéo ou un échantillon audio. Les charges utiles peuvent être constituées de plusieurs paquets. Les métriques de charge utile ne sont applicables que lors de l'utilisation du CDI. Unités : nombre Dimensions valides : • ARN de sortie • Flux (ARN) • Zone de disponibilité • Tous les flux

Des MediaConnect métriques AWS Elemental pour surveiller la santé des médias

AWS Elemental MediaConnect envoie des métriques à. CloudWatch Vous pouvez consulter des indicateurs spécifiques pour évaluer l'état des médias transmis par MediaConnect. Les indicateurs de santé des médias répertoriés ci-dessous ne s'appliquent qu'aux flux Transport Stream (TS). Pour plus de détails sur chaque métrique, consultez le tableau de cette section.

Métriques relatives aux médias

Le tableau suivant répertorie les métriques multimédias auxquelles AWS Elemental MediaConnect envoie des messages. CloudWatch

Métrique	Description
`ConsecutiveDrops`	Nombre de paquets de données déposés d'affilée lors de la transmission de données vers ou depuis MediaConnect. Unités : nombre Protocoles pris en charge : • Zixi Statistiques prises en charge : • Maximum • Minimum • Moyenne Ensembles de dimensions valides : • Flux (ARN) • ARN source • Zone de disponibilité • Tous les flux

Métrique	Description
`ConsecutiveNotRecovered`	Nombre de paquets de données qui n'ont pas été restaurés d'affilée. Après la suppression d'un paquet de données, la correction d'erreur tente de le récupérer. Cette métrique permet d'identifier les périodes prolongées de paquets de données qui ont été abandonnés et non restaurés. Unités : nombre Protocoles pris en charge : • Zixi Statistiques prises en charge : • Maximum • Minimum • Moyenne Ensembles de dimensions valides : • Flux (ARN) • ARN source • Zone de disponibilité • Tous les flux

Métrique	Description
`Jitter`	La gigue actuelle du réseau, mesurée en millisecondes. L'instabilité du réseau est une mesure de l'évolution de la latence. Une augmentation de l'instabilité du réseau indique une incohérence de la latence et peut avoir un impact négatif sur la qualité. Unités : millisecondes (ms) Protocoles pris en charge : • Tous les protocoles Transport Stream (TS) Statistiques prises en charge : • Maximum • Minimum • Moyenne Ensembles de dimensions valides : • Flux (ARN) • ARN source • Zone de disponibilité • Tous les flux

Métrique	Description
`Latency`	La latence du flux ou de la source. La latence est le temps nécessaire pour que les paquets de données voyagent de votre source à MediaConnect. Unités : millisecondes (ms) Protocoles pris en charge : • Tous les protocoles Transport Stream (TS) Statistiques prises en charge : • Maximum • Minimum • Moyenne Ensembles de dimensions valides : • Flux (ARN) • ARN source • Zone de disponibilité • Tous les flux

Métrique	Description
`ConnectionAttempts`	Le nombre de tentatives de reconnexion. Si le MediaConnect flux ou la source perd sa connexion, il tentera de se reconnecter automatiquement. Unités : nombre Protocoles pris en charge : • Zixi • écouteur SRT • appelant SRT Statistiques prises en charge : • Somme Ensembles de dimensions valides : • Flux (ARN) • ARN source • Zone de disponibilité • Tous les flux

Métrique	Description
`SourceUptime`	Le nombre de secondes pendant lesquelles la source est active. Si la source est déconnectée ou si le délai de connexion est expiré, cette métrique est remise à zéro. Unités : nombre Protocoles pris en charge : • Tous les protocoles Transport Stream (TS) Statistiques prises en charge : • Maximum • Minimum • Moyenne Ensembles de dimensions valides : • Flux (ARN) • ARN source • Zone de disponibilité • Tous les flux

Des MediaConnect métriques AWS Elemental pour surveiller l'état de la passerelle

AWS Elemental MediaConnect envoie des métriques à. CloudWatch Vous pouvez consulter des indicateurs spécifiques pour évaluer l'état de santé de vos passerelles. Si le flux entrant ou sortant de la passerelle est défectueux, ces mesures peuvent vous aider à déterminer l'origine du problème. Pour plus de détails sur chaque métrique, consultez les tableaux de cette section.

> **Note**
>
> MediaConnect Les métriques de passerelle ne sont pas disponibles pendant les périodes de haute résolution (une seconde). Vous devez sélectionner une période d'au moins une minute.

Rubriques

Métriques d'entrée de la passerelle

Le tableau suivant répertorie les métriques d'entrée de passerelle auxquelles AWS MediaConnect Elemental envoie des données. CloudWatch

Métrique	Description
`IngressBridgeBitRate`	Débit de la source du pont d'entrée, après la fusion en cas de basculement. Cette source provient de votre centre de données local. Unités : bits par seconde (bps) Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgeCATError`	Nombre de fois qu'une erreur de table d'accès conditionnel (CAT) s'est produite. Cette erreur indique que le CAT n'est pas présent. Le CAT indique au décodeur récepteur intégré (IRD) où trouver les messages de gestion pour les systèmes d'accès conditionnel (CA) utilisés. Unités : nombre Ensembles de dimensions valides :

Métrique	Description
	• Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgeCRCError`	Nombre de fois qu'une erreur de contrôle de redondance cyclique (CRC) s'est produite. Cette erreur se produit lorsqu'un CRC détermine que les données sont corrompues. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgeContinuityCounter`	Le nombre de fois qu'une erreur de continuité s'est produite. Cette erreur indique un ordre de paquets incorrect ou des paquets perdus. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgeDroppedPackets`	Le nombre de paquets perdus pendant le transport. Cette valeur est mesurée avant toute correction d'erreur. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`IngressBridgeFailoverSwitches`	Nombre total de fois que le pont bascule entre les sources lors de l'utilisation du mode Failover pour le basculement de source. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgeMergeActive`	État de fusion de toutes les sources du pont. La valeur 1 indique que toutes les sources sont fusionnées. Une valeur de 0 (zéro) indique qu'au moins une source n'est pas fusionnée activement avec le code 7. Unités : aucune Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgeNotRecoveredPackets`	Nombre de paquets perdus pendant le transit et qui n'ont pas été récupérés par correction d'erreur. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`IngressBridgePATError`	Nombre de fois qu'une erreur de table d'association de programmes (PAT) s'est produite. Cette erreur indique que le PAT est manquant. Le PAT répertorie les programmes disponibles dans un flux de transport (TS) et pointe vers les tables de mappage des programmes (PMT). Le décodeur a besoin du PAT pour faire son travail. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgePCRAccuracyError`	Nombre de fois qu'une erreur de précision du registre d'horloge du programme (PCR) s'est produite. Cette erreur se produit lorsque la valeur de la PCR transmise diffère de plus de 500 nanosecondes (ns) de ce qui est attendu. Lorsqu'un flux est codé, le codeur attribue des valeurs PCR périodiques à l'horloge du programme de l'encodeur. Le décodeur s'appuie sur ces valeurs pour garantir la synchronisation du flux. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`IngressBridgePCRError`	Le nombre de fois qu'une erreur PCR s'est produite. Cette erreur se produit lorsque les valeurs PCR ne sont pas envoyées assez fréquemment. Le service s'appuie sur des PCR réguliers et fréquents pour réinitialiser l'horloge du système local à 27 MHz. Bien que l'erreur se produise lorsque l'intervalle dépasse 100 millisecondes (ms), les meilleures pratiques stipulent que les PCR doivent être reçues au moins toutes les 40 ms. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgePIDError`	Nombre de fois qu'une erreur d'identifiant de paquet (PID) s'est produite. Cette erreur indique qu'il manque le flux de données associé à un PID. Les PID sont des identifiants qui indiquent l'emplacement des flux vidéo, audio et de données. Cette erreur peut se produire une fois que le flux de transport a été multiplexé puis remultiplexé. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`IngressBridgePMTError`	Nombre de fois qu'une erreur de table de mappage des programmes (PMT) s'est produite. Cette erreur se produit lorsque le PMT n'est pas reçu au moins toutes les 500 millisecondes (ms). Chaque PMT contient une liste de PID, qui aident les décodeurs à réassembler les données. Le décodeur a besoin des PMT pour faire son travail. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgePTSError`	Nombre de fois qu'une erreur d'horodatage de présentation (PTS) s'est produite. Cette erreur se produit lorsqu'un horodatage de présentation (PTS) n'est pas reçu au moins toutes les 700 ms. Cela peut se produire si le PTS est envoyé moins fréquemment ou pas du tout. La cause la plus courante de cette erreur est le brouillage du flux de transport (TS). Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgePacketLossPercent`	Pourcentage de paquets perdus pendant le transit, même s'ils ont été récupérés. Unités : pourcentage Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`IngressBridgeRecoveredPackets`	Nombre de paquets perdus pendant le transit, mais récupérés. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgeTSByteError`	Nombre de fois qu'une erreur d'octet dans le flux de transport s'est produite. Cette erreur indique que l'octet de synchronisation n'est pas apparu après le nombre d'octets prescrit. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgeTSSyncLoss`	Nombre de fois qu'une erreur de perte de synchronisation du flux de transport s'est produite. Cette erreur se produit après au moins deux erreurs d'octets consécutives dans le flux de transport. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`IngressBridgeTotalPackets`	Nombre total de paquets reçus. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`IngressBridgeTransportError`	Nombre de fois qu'une erreur de transport principale s'est produite. Cette erreur indique que le paquet du flux de transport est inutilisable. Lorsque cette erreur se produit, ignorez toutes les autres erreurs TR 101 290 pour ce paquet. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Mesures relatives à la source d'entrée de la passerelle

Le tableau suivant répertorie les métriques des sources d'entrée de la passerelle auxquelles AWS MediaConnect Elemental envoie des données. CloudWatch

Métrique	Description
`IngressBridgeSourceARQRecovered`	Nombre de paquets abandonnés qui ont été récupérés par une demande de répétition automatique (ARQ). Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont

Métrique	Description
	• ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceARQRequests`	Le nombre de paquets retransmis qui ont été demandés par le biais d'une demande de répétition automatique (ARQ) et reçus. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceBitRate`	Débit de la source du pont d'entrée, avant toute fusion par basculement. Cette source provient de votre centre de données local. Unités : bits par seconde (bps) Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceCATError`	Nombre de fois qu'une erreur de table d'accès conditionnel (CAT) s'est produite. Cette erreur indique que le CAT n'est pas présent. Le CAT indique au décodeur récepteur intégré (IRD) où trouver les messages de gestion pour les systèmes d'accès conditionnel (CA) utilisés. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau

Métrique	Description
`IngressBridgeSourceCRCError`	Nombre de fois qu'une erreur de contrôle de redondance cyclique (CRC) s'est produite. Cette erreur se produit lorsqu'un CRC détermine que les données sont corrompues. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceContinuityCounter`	Le nombre de fois qu'une erreur de continuité s'est produite. Cette erreur indique un ordre de paquets incorrect ou des paquets perdus. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceDroppedPackets`	Le nombre de paquets perdus pendant le transport. Cette valeur est mesurée avant toute correction d'erreur. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau

Métrique	Description
`IngressBridgeSourceFECPackets`	Nombre de paquets transmis à l'aide de la correction d'erreur directe (FEC) et reçus. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceFECRecovered`	Nombre de paquets transmis à l'aide de la correction d'erreur directe (FEC), perdus pendant le transit et récupérés. Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceMergeActive`	Une indication du statut de la source par rapport aux autres sources. Cette métrique est utile lorsque le pont possède plusieurs sources de basculement et que vous utilisez le mode de basculement Merge. Une valeur de 1 indique que le pont possède plusieurs sources et que cette source est activement utilisée, avec une fusion à 7. La valeur 0 (zéro) indique que le pont n'utilise pas la source pour former le flux. Unités : aucune Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau

Métrique	Description
`IngressBridgeSourceMergeLatency`	Durée pendant laquelle cette source suit la source principale. Si cette source est la source principale, la valeur est 0 (zéro). Unités : millisecondes Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceNotRecoveredPackets`	Nombre de paquets perdus pendant le transit et qui n'ont pas été récupérés par correction d'erreur. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceOverflowPackets`	Nombre de paquets perdus en transit parce que la vidéo nécessitait plus de mémoire tampon que ce qui était disponible. Cette métrique ne s'applique pas aux flux qui reçoivent du contenu provenant d'une autorisation ou aux flux qui ont plusieurs sources. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau

Métrique	Description
IngressBridgeSourcePATError	Nombre de fois qu'une erreur de table d'association de programmes (PAT) s'est produite. Cette erreur indique que le PAT est manquant. Le PAT répertorie les programmes disponibles dans un flux de transport (TS) et pointe vers les tables de mappage des programmes (PMT). Le décodeur a besoin du PAT pour faire son travail. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
IngressBridgeSourcePCRAccuracyError	Nombre de fois qu'une erreur de précision du registre d'horloge du programme (PCR) s'est produite. Cette erreur se produit lorsque la valeur de la PCR transmise diffère de plus de 500 nanosecondes (ns) de ce qui est attendu. Lorsqu'un flux est codé, le codeur attribue des valeurs PCR périodiques à partir de l'horloge du programme de l'encodeur. Le décodeur s'appuie sur ces valeurs pour garantir la synchronisation du flux. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau

Métrique	Description
`IngressBridgeSourcePCRError`	Le nombre de fois qu'une erreur PCR s'est produite. Cette erreur se produit lorsque les valeurs PCR ne sont pas envoyées assez fréquemment. Le service s'appuie sur des PCR réguliers et fréquents pour réinitialiser l'horloge du système local à 27 MHz. Bien que l'erreur se produise lorsque l'intervalle dépasse 100 millisecondes (ms), les meilleures pratiques stipulent que les PCR doivent être reçues au moins toutes les 40 ms. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourcePIDError`	Nombre de fois qu'une erreur d'identifiant de paquet (PID) s'est produite. Cette erreur indique qu'il manque le flux de données associé à un PID. Les PID sont des identifiants qui indiquent l'emplacement des flux vidéo, audio et de données. Cette erreur peut se produire une fois que le flux de transport a été multiplexé puis remultiplexé. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau

Métrique	Description
`IngressBridgeSourcePMTError`	Nombre de fois qu'une erreur de table de mappage des programmes (PMT) s'est produite. Cette erreur se produit lorsque le PMT n'est pas reçu au moins toutes les 500 millisecondes (ms). Chaque PMT contient une liste de PID, qui aident les décodeurs à réassembler les données. Le décodeur a besoin des PMT pour faire son travail. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourcePTSError`	Nombre de fois qu'une erreur d'horodatage de présentation (PTS) s'est produite. Cette erreur se produit lorsqu'un horodatage de présentation (PTS) n'est pas reçu au moins toutes les 700 ms. Cela peut se produire si le PTS est envoyé moins fréquemment ou pas du tout. La cause la plus courante de cette erreur est le brouillage du TS. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourcePacketLossPercent`	Pourcentage de paquets perdus pendant le transit, même s'ils ont été récupérés. Unités : pourcentage Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau

Métrique	Description
`IngressBridgeSourceRecoveredPackets`	Nombre de paquets perdus pendant le transit, mais récupérés. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceRoundTripTime`	Le temps nécessaire à la source pour envoyer un signal et recevoir un accusé de réception d'AWS Elemental. MediaConnect Cela ne s'applique pas aux flux qui reçoivent du contenu provenant d'un droit. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceTSByteError`	Nombre de fois qu'une erreur d'octet dans le flux de transport s'est produite. Cette erreur indique que l'octet de synchronisation n'est pas apparu après le nombre d'octets prescrit. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau

Métrique	Description
`IngressBridgeSourceTSSyncLoss`	Nombre de fois qu'une erreur de perte de synchronisation du flux de transport s'est produite. Cette erreur se produit après au moins deux erreurs d'octets consécutives dans le flux de transport. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceTotalPackets`	Nombre total de paquets reçus. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau
`IngressBridgeSourceTransportError`	Nombre de fois qu'une erreur de transport principale s'est produite. Cette erreur indique que le paquet du flux de transport est inutilisable. Lorsque cette erreur se produit, ignorez toutes les autres erreurs TR 101 290 pour ce paquet. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont • ARN de passerelle, ID d'instance, nom du réseau

Métriques de sortie de la passerelle

Le tableau suivant répertorie les métriques de sortie de passerelle auxquelles AWS MediaConnect Elemental envoie des données. CloudWatch

Métrique	Description
`EgressBridgeBitRate`	Le débit de la source du pont de sortie, après la fusion en cas de basculement. Cette source provient d'un MediaConnect flux. Unités : bits par seconde (bps) Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgeCATError`	Nombre de fois qu'une erreur de table d'accès conditionnel (CAT) s'est produite. Cette erreur indique que le CAT n'est pas présent. Le CAT indique au décodeur récepteur intégré (IRD) où trouver les messages de gestion pour les systèmes d'accès conditionnel (CA) utilisés. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgeCRCError`	Nombre de fois qu'une erreur de contrôle de redondance cyclique (CRC) s'est produite. Cette erreur se produit lorsqu'un CRC détermine que les données sont corrompues. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgeContinuityCounter`	Le nombre de fois qu'une erreur de continuité s'est produite. Cette erreur indique un ordre de paquets incorrect ou des paquets perdus. Unités : nombre

Métrique	Description
	Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
EgressBridgeDroppedPackets	Le nombre de paquets perdus pendant le transport. Cette valeur est mesurée avant toute correction d'erreur. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
EgressBridgeFailoverSwitches	Nombre total de fois que le pont bascule entre les sources lors de l'utilisation du mode Failover pour le basculement de source. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
EgressBridgeMergeActive	État de fusion de toutes les sources du pont. La valeur 1 indique que toutes les sources sont fusionnées. Une valeur de 0 (zéro) indique qu'au moins une source n'est pas fusionnée activement avec le code 7. Unités : aucune Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`EgressBridgeNotRecoveredPackets`	Nombre de paquets perdus pendant le transit et qui n'ont pas été récupérés par correction d'erreur. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgePATError`	Nombre de fois qu'une erreur de table d'association de programmes (PAT) s'est produite. Cette erreur indique que le PAT est manquant. Le PAT répertorie les programmes disponibles dans un flux de transport (TS) et pointe vers les tables de mappage des programmes (PMT). Le décodeur a besoin du PAT pour faire son travail. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgePCRAccuracyError`	Nombre de fois qu'une erreur de précision du registre d'horloge du programme (PCR) s'est produite. Cette erreur se produit lorsque la valeur de la PCR transmise diffère de plus de 500 nanosecondes (ns) de ce qui est attendu. Lorsqu'un flux est codé, le codeur attribue des valeurs PCR périodiques à l'horloge du programme de l'encodeur. Le décodeur s'appuie sur ces valeurs pour garantir la synchronisation du flux. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`EgressBridgePCRError`	Le nombre de fois qu'une erreur PCR s'est produite. Cette erreur se produit lorsque les valeurs PCR ne sont pas envoyées assez fréquemment. Le service s'appuie sur des PCR réguliers et fréquents pour réinitialiser l'horloge du système local à 27 MHz. Bien que l'erreur se produise lorsque l'intervalle dépasse 100 millisecondes (ms), les meilleures pratiques stipulent que les PCR doivent être reçues au moins toutes les 40 ms. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgePIDError`	Nombre de fois qu'une erreur d'identifiant de paquet (PID) s'est produite. Cette erreur indique qu'il manque le flux de données associé à un PID. Les PID sont des identifiants qui indiquent l'emplacement des flux vidéo, audio et de données. Cette erreur peut se produire une fois que le flux de transport a été multiplexé puis remultiplexé. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`EgressBridgePMTError`	Nombre de fois qu'une erreur de table de mappage des programmes (PMT) s'est produite. Cette erreur se produit lorsque le PMT n'est pas reçu au moins toutes les 500 millisecondes (ms). Chaque PMT contient une liste de PID, qui aident les décodeurs à réassembler les données. Le décodeur a besoin des PMT pour faire son travail. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgePTSError`	Nombre de fois qu'une erreur d'horodatage de présentation (PTS) s'est produite. Cette erreur se produit lorsqu'un horodatage de présentation (PTS) n'est pas reçu au moins toutes les 700 ms. Cela peut se produire si le PTS est envoyé moins fréquemment ou pas du tout. La cause la plus courante de cette erreur est le brouillage du flux de transport (TS). Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgePacketLossPercent`	Pourcentage de paquets perdus pendant le transit, même s'ils ont été récupérés. Unités : pourcentage Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`EgressBridgeRecoveredPackets`	Nombre de paquets perdus pendant le transit, mais récupérés. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgeTSByteError`	Nombre de fois qu'une erreur d'octet dans le flux de transport s'est produite. Cette erreur indique que l'octet de synchronisation n'est pas apparu après le nombre d'octets prescrit. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgeTSSyncLoss`	Nombre de fois qu'une erreur de perte de synchronisation du flux de transport s'est produite. Cette erreur se produit après au moins deux erreurs d'octets consécutives dans le flux de transport. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Métrique	Description
`EgressBridgeTotalPackets`	Nombre total de paquets reçus. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance
`EgressBridgeTransportError`	Nombre de fois qu'une erreur de transport principale s'est produite. Cette erreur indique que le paquet du flux de transport est inutilisable. Lorsque cette erreur se produit, ignorez toutes les autres erreurs TR 101 290 pour ce paquet. Unités : nombre Ensembles de dimensions valides : • Pont ARN • ARN de passerelle, ID d'instance

Mesures relatives à la source de sortie de la passerelle

Le tableau suivant répertorie les métriques de source de sortie de passerelle auxquelles AWS MediaConnect Elemental envoie des données. CloudWatch

Métrique	Description
`EgressBridgeSourceBitRate`	Débit de la source du pont de sortie, avant toute fusion par basculement. Cette source provient d'un MediaConnect flux. Unités : bits par seconde (bps) Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité

Métrique	Description
`EgressBridgeSourceCATError`	Nombre de fois qu'une erreur de table d'accès conditionnel (CAT) s'est produite. Cette erreur indique que le CAT n'est pas présent. Le CAT indique au décodeur récepteur intégré (IRD) où trouver les messages de gestion pour les systèmes d'accès conditionnel (CA) utilisés. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourceCRCError`	Nombre de fois qu'une erreur de contrôle de redondance cyclique (CRC) s'est produite. Cette erreur se produit lorsqu'un CRC détermine que les données sont corrompues. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourceContinuityCounter`	Le nombre de fois qu'une erreur de continuité s'est produite. Cette erreur indique un ordre de paquets incorrect ou des paquets perdus. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité

Métrique	Description
`EgressBridgeSourceDroppedPackets`	Le nombre de paquets perdus pendant le transport. Cette valeur est mesurée avant toute correction d'erreur. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourceMergeActive`	Une indication du statut de la source par rapport aux autres sources. Cette métrique est utile lorsque le pont possède plusieurs sources de basculement et que vous utilisez le mode de basculement Merge. Une valeur de 1 indique que le pont possède plusieurs sources et que cette source est activement utilisée, avec une fusion à 7. La valeur 0 (zéro) indique que le pont n'utilise pas la source pour former le flux. Unités : aucune Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourceMergeLatency`	Durée pendant laquelle cette source suit la source principale. Si cette source est la source principale, la valeur est 0 (zéro). Unités : millisecondes Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité

Métrique	Description
`EgressBridgeSourceNotRecoveredPackets`	Nombre de paquets perdus pendant le transit et qui n'ont pas été récupérés par correction d'erreur. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourcePATError`	Nombre de fois qu'une erreur de table d'association de programmes (PAT) s'est produite. Cette erreur indique que le PAT est manquant. Le PAT répertorie les programmes disponibles dans un flux de transport (TS) et pointe vers les tables de mappage des programmes (PMT). Le décodeur a besoin du PAT pour faire son travail. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourcePCRAccuracyError`	Nombre de fois qu'une erreur de précision du registre d'horloge du programme (PCR) s'est produite. Cette erreur se produit lorsque la valeur de la PCR transmise diffère de plus de 500 nanosecondes (ns) de ce qui est attendu. Lorsqu'un flux est codé, le codeur attribue des valeurs PCR périodiques à partir de l'horloge du programme de l'encodeur. Le décodeur s'appuie sur ces valeurs pour garantir la synchronisation du flux. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité

Métrique	Description
`EgressBridgeSourcePCRError`	Le nombre de fois qu'une erreur PCR s'est produite. Cette erreur se produit lorsque les valeurs PCR ne sont pas envoyées assez fréquemment. Le service s'appuie sur des PCR réguliers et fréquents pour réinitialiser l'horloge du système local à 27 MHz. Bien que l'erreur se produise lorsque l'intervalle dépasse 100 millisecondes (ms), les meilleures pratiques stipulent que les PCR doivent être reçues au moins toutes les 40 ms. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourcePIDError`	Nombre de fois qu'une erreur d'identifiant de paquet (PID) s'est produite. Cette erreur indique qu'il manque le flux de données associé à un PID. Les PID sont des identifiants qui indiquent l'emplacement des flux vidéo, audio et de données. Cette erreur peut se produire une fois que le flux de transport a été multiplexé puis remultiplexé. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité

Métrique	Description
`EgressBridgeSourcePMTError`	Nombre de fois qu'une erreur de table de mappage des programmes (PMT) s'est produite. Cette erreur se produit lorsque le PMT n'est pas reçu au moins toutes les 500 millisecondes (ms). Chaque PMT contient une liste de PID, qui aident les décodeurs à réassembler les données. Le décodeur a besoin des PMT pour faire son travail. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourcePTSError`	Nombre de fois qu'une erreur d'horodatage de présentation (PTS) s'est produite. Cette erreur se produit lorsqu'un horodatage de présentation (PTS) n'est pas reçu au moins toutes les 700 ms. Cela peut se produire si le PTS est envoyé moins fréquemment ou pas du tout. La cause la plus courante de cette erreur est le brouillage du TS. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourcePacketLossPercent`	Pourcentage de paquets perdus pendant le transit, même s'ils ont été récupérés. Unités : pourcentage Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité

Métrique	Description
`EgressBridgeSourceRecoveredPackets`	Nombre de paquets perdus pendant le transit, mais récupérés. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourceTSByteError`	Nombre de fois qu'une erreur d'octet dans le flux de transport s'est produite. Cette erreur indique que l'octet de synchronisation n'est pas apparu après le nombre d'octets prescrit. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourceTSSyncLoss`	Nombre de fois qu'une erreur de perte de synchronisation du flux de transport s'est produite. Cette erreur se produit après au moins deux erreurs d'octets consécutives dans le flux de transport. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité

Métrique	Description
`EgressBridgeSourceTotalPackets`	Nombre total de paquets reçus. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité
`EgressBridgeSourceTransportError`	Nombre de fois qu'une erreur de transport principale s'est produite. Cette erreur indique que le paquet du flux de transport est inutilisable. Lorsque cette erreur se produit, ignorez toutes les autres erreurs TR 101 290 pour ce paquet. Unités : nombre Ensembles de dimensions valides : • ARN du pont, nom de la source du pont, ARN du flux • ARN de passerelle, ID d'instance, zone de disponibilité

Utilisation de métriques pour résoudre les problèmes

Vous pouvez surveiller l'état de votre flux en consultant les métriques MediaConnect envoyées par AWS Elemental. CloudWatch En particulier, si vous rencontrez un problème sur votre MediaConnect flux, ces mesures peuvent vous aider à isoler le problème. Les indicateurs spécifiques à surveiller dépendent du protocole utilisé par votre source. Consultez les listes ci-dessous, qui sont triées par protocole source.

Rubriques

- Des indicateurs pour vérifier si votre source provient d'un droit
- Indicateurs à surveiller si vous utilisez des passerelles

Indicateurs pour vérifier si votre source utilise le protocole RIST

Si le protocole de votre source est RIST, observez les indicateurs ci-dessous pour évaluer l'état de santé de votre source.

- `ARQRecovered`
- `ARQRequests`
- `DroppedPackets`
- `NotRecoveredPackets`
- `OverflowPackets`
- `PacketLossPercent`
- `RecoveredPackets`
- `RoundTripTime`
- `TotalPackets`

Des métriques pour vérifier si votre source utilise le protocole RTP

Si le protocole de votre source est le RTP, observez les indicateurs ci-dessous pour évaluer l'état de santé de votre source.

- `DroppedPackets`
- `OverflowPackets`
- `RoundTripTime`
- `TotalPackets`

Des métriques pour vérifier si votre source utilise le protocole RTP-FEC

Si le protocole de votre source est RTP-FEC, observez les métriques ci-dessous pour évaluer l'état de votre source.

- `DroppedPackets`
- `FECPackets`

- FECRecovered
- NotRecoveredPackets
- OverflowPackets
- RecoveredPackets
- RoundTripTime
- TotalPackets

Des métriques pour vérifier si votre source utilise le protocole SRT

Si le protocole de votre source est SRT (écouteur ou appelant), observez les indicateurs ci-dessous pour évaluer l'état de santé de votre source.

- ARQRecovered
- ARQRequests
- DroppedPackets
- NotRecoveredPackets
- OverflowPackets
- RecoveredPackets
- RoundTripTime
- TotalPackets

Des métriques pour vérifier si votre source utilise le protocole push Zixi

Si le protocole de votre source est Zixi Push, observez les indicateurs ci-dessous pour évaluer l'état de santé de votre source.

- ARQRecovered
- ARQRequests
- DroppedPackets
- FECPackets
- FECRecovered
- NotRecoveredPackets
- OverflowPackets

- RecoveredPackets
- RoundTripTime
- TotalPackets

Des indicateurs pour vérifier si votre source provient d'un droit

Si votre source provient d'un droit accordé à votre compte par un autre AWS compte, observez les statistiques ci-dessous pour évaluer l'état de santé de votre source.

- ARQRecovered
- ARQRequests
- DroppedPackets
- FECPackets
- FECRecovered
- NotRecoveredPackets
- OverflowPackets
- RecoveredPackets
- RoundTripTime
- TotalPackets

Indicateurs à surveiller si vous utilisez des passerelles

Consultez les indicateurs ci-dessous pour évaluer l'état de santé de votre passerelle.

Indicateurs à surveiller si vous utilisez une passerelle dotée d'un pont d'entrée

Consultez les indicateurs ci-dessous pour évaluer l'état du pont d'entrée de votre passerelle. Les mesures de résolution des problèmes de pont d'entrée recommandées sont séparées par protocole.

- RTP
  - IngressBridgeTotalPackets
  - IngressBridgeDroppedPackets
  - IngressBridgeSourceTotalPackets
  - IngressBridgeSourceDroppedPackets
  - IngressBridgeSourceOverflowPackets

  - IngressBridgeSourceRoundTripTime

- RTP-FEC
  - IngressBridgeTotalPackets
  - IngressBridgeDroppedPackets
  - IngressBridgeRecoveredPackets
  - IngressBridgeNotRecoveredPackets
  - IngressBridgeSourceTotalPackets
  - IngressBridgeSourceDroppedPackets
  - IngressBridgeSourceRecoveredPackets
  - IngressBridgeSourceNotRecoveredPackets
  - IngressBridgeSourceOverflowPackets
  - IngressBridgeSourceFECPackets
  - IngressBridgeSourceFECRecovered
  - IngressBridgeSourceRoundTripTime
- UDP
  - IngressBridgeTotalPackets
  - IngressBridgeSourceTotalPackets
  - IngressBridgeSourceOverflowPackets

Indicateurs à surveiller si vous utilisez une passerelle dotée d'un pont de sortie

Regardez les indicateurs ci-dessous pour évaluer l'état du pont de sortie de votre passerelle.

- EgressBridgeTotalPackets
- EgressBridgeDroppedPackets
- EgressBridgeRecoveredPackets
- EgressBridgeNotRecoveredPackets
- EgressBridgeSourceTotalPackets
- EgressBridgeSourceDroppedPackets
- EgressBridgeSourceRecoveredPackets
- EgressBridgeSourceNotRecoveredPackets

Surveillance à l'aide d' CloudWatch événements

Amazon CloudWatch Events vous permet d'automatiser vos AWS services et de répondre automatiquement aux événements du système tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements des AWS services sont fournis à CloudWatch Events en temps quasi réel. Vous pouvez écrire des règles simples pour indiquer quels événements vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle.

Les actions qui peuvent être déclenchées automatiquement à l'aide CloudWatch des événements sont les suivantes :

- Invoquer une fonction AWS Lambda
- Appel de la fonctionnalité Exécuter la commande d'Amazon EC2
- Relais de l'événement à Amazon Kinesis Data Streams
- Activation d'une machine à AWS Step Functions états
- Notification d'une rubrique Amazon SNS ou d'une file d'attente Amazon SQS

Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Events.

CloudWatch Evénements à MediaConnect

- Événement de changement d'état du MediaConnect flux AWS Elemental
- Événement de maintenance du MediaConnect flux AWS Elemental
- Événement relatif à l'état du MediaConnect flux AWS Elemental
- Événement d'alerte AWS Elemental MediaConnect
- Événement relatif à la santé des MediaConnect sources AWS Elemental
- Événement relatif à la santé des MediaConnect sorties AWS Elemental

Événement de changement d'état du MediaConnect flux AWS Elemental

Cet événement est publié lorsque l'état d'un flux passe ou passe à l'un des états suivants : veille, actif, mise à jour, suppression, démarrage, arrêt ou erreur.

Pour plus d'informations sur l'inscription à cet événement, consultez Amazon CloudWatch.

Le message suivant est un exemple de cet CloudWatch événement.

```
{
    "account": "111122223333",
    "detail": {
        "currentStatus": "STARTING",
        "previousStatus": "STANDBY"
    },
    "detail-type": "MediaConnect Flow Status Change",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "region": "us-east-1",
    "resources": ["arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow"],
    "source": "aws.mediaconnect",
    "time": "2022-01-06T00:45:47Z",
    "version": "0"
}
```

Événement de maintenance du MediaConnect flux AWS Elemental

Cet événement est publié lorsque l'état de maintenance d'un flux est modifié, que ce soit vers ou depuis l'un des états suivants :

- PLANIFIÉ - La maintenance est planifiée pour le flux.
- REPROGRAMMÉ : MediaConnect ne peut pas effectuer la maintenance à la date et à l'heure prévues précédemment. Une nouvelle date et heure ont été automatiquement attribuées par MediaConnect pour la maintenance de ce flux.
- ANNULÉ - La maintenance de ce flux est annulée par MediaConnect.
- EN COURS - La maintenance a commencé et est actuellement en cours pour ce flux.
- TERMINÉ - La maintenance s'est terminée avec succès pour ce flux.
- ÉCHEC - La maintenance ne s'est pas terminée correctement pour ce flux.

Pour plus d'informations sur l'inscription à cet événement, consultez Amazon CloudWatch.

Pour plus d'informations sur la MediaConnect maintenance, consultez la section Maintenance des MediaConnect flux.

Le message suivant est un exemple de cet CloudWatch événement.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "MediaConnect Flow Maintenance",
    "source": "aws.mediaconnect",
    "account": "111122223333",
    "time": "2022-02-14T00:45:47Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1:23aBC45dEF67hiJ8:12AbC34DE5fG:ExampleFlow"
    ],
    "detail": {
        "currentStatus": "FINISHED"
    }
}
```

Événement relatif à l'état du MediaConnect flux AWS Elemental

AWS Elemental MediaConnect publie les événements relatifs à l'état d'un flux lorsque l'état d'un indicateur d'état d'un flux change.

MediaConnect publie cet événement chaque fois qu'un changement d'état est apporté à un ou plusieurs des indicateurs de santé du flux suivants. Cet événement publie l'état actuel et précédent du flux.

Les indicateurs de santé du flux sont les suivants :

- État de la source
  - États possibles : `connectedreceiving`,`disconnected`, `idle`
- Commutateur Failover
  - États possibles :`true`, `false`
- TR-101 : La TR-101 est une recommandation technique standard de l'industrie pour la surveillance des flux de transport (TS). Les événements suivants sont publiés uniquement pour les protocoles basés sur TS.
  - La perte de synchronisation TS se `true` produit lorsque les charges utiles sources ne ressemblent pas à un flux de transport valide.
  - Une erreur de comptage de continuité se `true` produit lorsque la source détecte des erreurs de comptage de continuité.

- L'erreur de transport se `true` produit lorsque l'indicateur de transport est défini sur le TS.
- L'erreur de PCR se `true` produit lorsqu'il y a une discontinuité de la PCR ou un long intervalle dans la réception des paquets de PCR.

Pour plus d'informations sur l'inscription à cet événement, consultez Amazon CloudWatch.

Le message suivant est un exemple de cet CloudWatch événement.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "MediaConnect Flow Health",
  "source": "aws.mediaconnect",
  "account": "012345678901",
  "time": "2006-01-02T15:04:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediaconnect:us-
east-1:012345678901:flow:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleFlow"
  ],
  "detail": {
    "unhealthy": true,
    "current": {
      "failover_switch": false,
      "source_state": "CONNECTED",
      "tr101": {
        "ts_sync_loss": false,
        "continuity_count_error": true,
        "transport_error": true,
        "pcr_error": true
      }
    },
    "previous": {
      "failover_switch": false,
      "source_state": "CONNECTED",
      "tr101": {
        "ts_sync_loss": false,
        "continuity_count_error": false,
        "transport_error": false,
        "pcr_error": false
      }
    }
```

```
  }
}
```

Événement d'alerte AWS Elemental MediaConnect

MediaConnect publie un événement d'alerte lorsqu'une ressource rencontre une erreur. L'événement contient un code d'erreur et un message décrivant le problème. Ces alertes sont visibles sur la MediaConnect console ou à l'aide de la commande `describe-flow` AWS Command Line Interface (AWS CLI). Pour plus d'informations sur la commande `describe-flow`, consultez la AWS CLI Référence de commande de l'.

Pour plus d'informations sur l'inscription à cet événement, consultez Amazon CloudWatch.

Le message suivant est un exemple de cet CloudWatch événement.

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-0123456789ab",
 "detail-type": "MediaConnect Alert",
 "source": "aws.mediaconnect",
 "account": "111122223333",
 "time": "2022-01-06T00:45:47Z",
 "region": "us-east-1",
 "resources": [
 "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleFlow"
 ],
 "detail": {
 "errored": true,
 "error-code": "AccessDeniedException",
 "error-message": "Permission denied accessing encryption key for output
 Test. Removing output until it is fixed (secret arn:aws:secretsmanager:us-
east-1:111122223333:secret:ExampleSecret, role arn:aws:iam::111122223333:role/
ExampleKey)"
 }
}
```

Événement relatif à la santé des MediaConnect sources AWS Elemental

AWS Elemental MediaConnect publie les événements relatifs à l'état de santé de la source après le changement de l'état d'un indicateur de santé source.

MediaConnect publie cet événement chaque fois qu'un changement d'état est apporté à un ou plusieurs des indicateurs de santé de la source suivants. Cet événement publie l'état actuel et précédent du flux. Notez que l'événement d'état de la source répertorie le flux et la source concernés dans la `resources` section.

Les indicateurs de santé sources sont les suivants :

- État de la source
  - États possibles : `connectedreceiving`,`disconnected`, `idle`
- TR-101 : La TR-101 est une recommandation technique standard de l'industrie pour la surveillance des flux de transport (TS). Les événements suivants sont publiés uniquement pour les protocoles basés sur TS.
  - Perte de synchronisation TS : vrai lorsque les charges utiles sources ne ressemblent pas à un flux de transport valide.
  - Erreur de comptage de continuité : vrai lorsque la source détecte des erreurs de comptage de continuité.
  - Erreur de transport : vrai lorsque l'indicateur de transport est défini sur le TS.
  - Erreur PCR - vraie en cas de discontinuité de la PCR ou d'un long intervalle dans la réception des paquets PCR.

Pour plus d'informations sur l'inscription à cet événement, consultez Amazon CloudWatch.

Le message suivant est un exemple de cet CloudWatch événement.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "MediaConnect Source Health",
  "source": "aws.mediaconnect",
  "account": "012345678901",
  "time": "2006-01-02T15:04:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediaconnect:us-
east-1:012345678901:flow:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleFlow",
    "arn:aws:mediaconnect:us-
east-1:012345678901:source:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleSource"
  ],
  "detail": {
```

```
    "unhealthy": true,
    "current": {
      "state": "CONNECTED",
      "tr101": {
        "ts_sync_loss": false,
        "continuity_count_error": true,
        "transport_error": true,
        "pcr_error": true
      }
    },
    "previous": {
      "state": "CONNECTED",
      "tr101": {
        "ts_sync_loss": false,
        "continuity_count_error": false,
        "transport_error": false,
        "pcr_error": false
      }
    }
  }
}
```

Événement relatif à la santé des MediaConnect sorties AWS Elemental

AWS Elemental MediaConnect publie les événements de santé en sortie après que l'état d'un indicateur de santé en sortie change.

MediaConnect publie cet événement chaque fois que l'état d'un ou de plusieurs des indicateurs de santé des résultats suivants change. Cet événement publie l'état actuel et précédent du flux. Notez que l'événement d'état de la sortie répertorie le flux et la sortie concernés dans la `resources` section.

Les indicateurs de santé relatifs aux résultats sont les suivants :

- État de sortie
  - États possibles : `connectedreceiving`,`disconnected`, `idle`

Pour plus d'informations sur l'inscription à cet événement, consultez Amazon CloudWatch.

Le message suivant est un exemple de cet CloudWatch événement.

```
{
```

```
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "MediaConnect Output Health",
  "source": "aws.mediaconnect",
  "account": "012345678901",
  "time": "2006-01-02T15:04:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediaconnect:us-
east-1:012345678901:flow:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleFlow",
    "arn:aws:mediaconnect:us-
east-1:012345678901:output:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleOutput"
  ],
  "detail": {
    "current": {
      "state": "CONNECTED"
    },
    "previous": {
      "state": "DISCONNECTED"
    }
  }
}
```

Journalisation des appels d'MediaConnectAPI AWS Elemental avec AWS CloudTrail

AWS Elemental MediaConnect est intégré à AWS AWS MediaConnect Elemental. AWS CloudTrail CloudTrailcapture les appels d'API pour AWS Elemental MediaConnect en tant qu'événements. Les appels de code vers les opérations d'API AWS Elemental incluent MediaConnect des appels de code vers les opérations d'MediaConnectAPI AWS Elemental. Si vous créez un journal de suivi, vous pouvez diffuser en continu les CloudTrail événements sur un compartiment Amazon S3, y compris les événements pour AWS ElementalMediaConnect. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements. À l'aide des informations collectées parCloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS ElementalMediaConnect, l'adresse IP source à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour en savoir plus sur CloudTrail, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

MediaConnectInformations AWS Elemental dans CloudTrail

CloudTrail est activé sur votre compte AWS lorsque vous créez le compte. Quand une activité a lieu dans AWS ElementalMediaConnect, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements dans votre AWS compte, y compris les événements pour AWS ElementalMediaConnect, créez un journal de suivi. Un journal CloudTrail de suivi permet à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services supportés par CloudTrail
- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

Toutes les MediaConnect actions d'AWS Elemental sont enregistrées CloudTrail et documentées dans la référence de l'MediaConnectAPI AWS Elemental. À titre d'exemple, les appels aux opérations `CreateFlow`, `StartFlow` et `UpdateFlowOutput` génèrent des entrées dans les fichiers journaux CloudTrail.

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 effectuée avec les informations d'identification utilisateur racine ou AWS 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 requête a été effectuée par un autre service AWS.

Pour plus d'informations, consultez la section Élément userIdentity CloudTrail.

Présentation des entrées des fichiers MediaConnect journaux AWS Elemental

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. Les fichiers journaux CloudTrail contiennent une ou plusieurs entrées de journal. Une entrée de journal représente une demande individuelle à partir d'une source quelconque et comprend des informations sur l'opération demandée, y compris la date et l'heure de l'opération, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de journal CloudTrail qui illustre l'opération `DescribeFlow` :


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "ABCDEFGHIJKL123456789",
    "arn": "arn:aws:sts::111122223333:user/testUser",
    "accountId": "111122223333",
    "accessKeyId": "ABCDE12345EFGHIJKLMN",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-16T20:34:51Z",
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ABCDEFGHIJKL123456789",
        "arn": "arn:aws:iam::111122223333:role/Administrator",
        "accountId": "111122223333",
        "userName": "Administrator",
      },
    },
  },
  "eventTime": "2018-11-16T20:34:52Z",
  "eventSource": "mediaconnect.amazonaws.com",
  "eventName": "DescribeFlow",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.17",
```

```
  "userAgent": "aws-cli/1.15.40 Python/3.6.5 Darwin/16.7.0 botocore/1.10.40",
  "requestParameters": {
    "flowArn": "arn%3Aaws%3Amediaconnect%3Aus-west-2%111122223333%3Aflow
%3A1-23aBC45dEF67hiJ8-12AbC34DE5fG%3AAwardsShow",
  },
  "responseElements": {
  },
  "requestID": "1a2b3c4d-1234-5678-1234-1a2b3c4d5e6f",
  "eventID": "987abc65-1a2b-3c4d-5d6e-987abc654def",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333",
}
```


Surveillance du flux et de l'état de la source

Sur la AWS Elemental MediaConnect console, vous pouvez surveiller l'état de vos flux et de leurs sources.

L'état du flux indique si votre flux n'est pas connecté en raison d'un problème d'autorisation ou de chiffrement.

L'état de santé de la source indique si votre source est connectée. Si tel est le cas, la console affiche CloudWatch les métriques Amazon qui fournissent le statut de la source sur une période donnée.

Rubriques

- Surveillance de l'état d'un flux
- Surveillance de l'état de santé d'une source

Surveillance de l'état d'un flux

L'onglet Alertes de la MediaConnect console affiche la liste des alertes survenues lorsque vous avez démarré ou arrêté le flux en cours. Pour obtenir la liste complète des alertes relatives à un flux, consultez Amazon CloudWatch.

MediaConnect affiche les alertes suivantes dans l'onglet Alertes :

- Messages d'erreur contextuels concernant votre flux, appelés erreurs de flux.

- Le droit sur lequel repose ce flux est déjà utilisé. Cela se produit si vous créez plusieurs flux basés sur les mêmes droits. Si l'un de ces flux est déjà en cours d'exécution, MediaConnect affiche une alerte si vous essayez de démarrer le second flux.
- Le droit sur lequel repose ce flux n'existe plus. Cela se produit si le compte qui a accordé le droit (l'auteur du contenu) révoque le droit.
- Le droit sur lequel ce flux est basé n'a pas de source active. Cela se produit si le flux de l'expéditeur est supprimé ou arrêté. Lorsque vous démarrez votre flux sur la base de ce droit, aucun contenu ne provient du flux d'origine.
- Les informations de déchiffrement ou de chiffrement du flux ne sont pas valides. Cela peut se produire pour plusieurs raisons. Par exemple, la clé de déchiffrement ne correspond pas au type de l'algorithme spécifié. Ou bien, votre flux est basé sur un droit qui utilise le cryptage SPEKE et ne MediaConnect permet pas de contacter le fournisseur de clés de la plateforme d'accès conditionnel (CA).
- Votre flux est basé sur un droit, et le flux du créateur du contenu possède déjà le nombre maximum de sorties.

Erreurs de diffusion

MediaConnect Les alertes peuvent également contenir des erreurs contextuelles concernant les sources et les sorties du flux. Ces erreurs sont appelées erreurs de diffusion et suivent un format spécifique.

- *`Nom de la source`* Stream Error : *`message d'erreur`*. Vérifiez la source du flux.
- *`Nom de sortie`* Stream Error : *`message d'erreur`*. Vérifiez le débit sortant.

Le message d'erreur fournira plus de contexte pour le problème et vous pourrez l'utiliser comme indicateur pour savoir par où commencer le dépannage.

Exemple

Si vous avez reçu l'alerte suivante sur un flux nommé NationalBroadcast:

Erreur de flux source *`StudioFeed2`* : erreur de *`configuration CDI`*. Vérifiez la source du flux.

Cela indiquerait une erreur avec le CDI entrant à la source. Plus précisément, la prochaine étape devrait consister à vérifier les paramètres de la source StudioFeed2 sur le flux nommé

NationalBroadcast. Vous devez porter une attention particulière aux paramètres de source spécifiques au CDI, tels que le port entrant, l'interface VPC utilisée et les flux multimédias.

Afficher les alertes de flux

Pour consulter les alertes actives (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux.
3. Choisissez l'onglet Alertes.

   Le service affiche une liste des alertes, le cas échéant, sur le flux.

Surveillance de l'état de santé d'une source

Dans la AWS Elemental MediaConnect console, vous pouvez consulter CloudWatch les statistiques Amazon qui indiquent l'état de santé de la source sur une période donnée. L'état de santé de la source est indiqué à l'aide des indicateurs suivants :

- Débit source : débit de la vidéo entrante.
- Nombre total de paquets reçus : nombre total de paquets MediaConnect reçus.

Pour surveiller l'état d'une source (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Sur la page Flux, choisissez le nom du flux.
3. Choisissez l'onglet Source et consultez le statut de votre source. Cela consiste notamment à :
   - Le champ Santé de la source indique l'état actuel de la source.
     - Connecté indique que le flux est correctement connecté à sa source.
     - Déconnecté indique que le flux n'est pas connecté à sa source. Pour résoudre ce problème, vérifiez que la source envoie réellement du contenu. Vérifiez également les paramètres source du flux, tels que la liste d'autorisation CIDR et la configuration du protocole.
     - Le fait que le flux soit inactif indique qu'il n'a pas été démarré. Pour résoudre ce problème, lancez le flux.

- L'erreur indique qu' MediaConnect il n'est pas autorisé à communiquer avec CloudWatch. Pour résoudre l'erreur, vous devez vous connecter en AWS Management Console tant qu'entité permettant d'obtenir des statistiques métriques MediaConnect à partir de CloudWatch. Pour obtenir des conseils, consultez cet exemple.

- La section Mesures de santé de la source n'est visible que si l'état de santé de votre source est connecté. Les graphiques indiquent le débit source et le nombre total de paquets reçus au cours de la dernière heure. Vous pouvez choisir différentes périodes dans le menu déroulant situé dans le coin supérieur droit de la section.

> **Note**
>
> MediaConnect actualise CloudWatch automatiquement les données toutes les 1 minute, 5 minutes ou 30 minutes, selon la période que vous avez choisie. Lorsque les graphiques sont actualisés, les données sont en retard d'une minute sur le temps réel.

Balisage de ressources AWS Elemental MediaConnect

Une balise est un attribut personnalisé que vous conférez ou que AWS attribue à une ressource AWS. Chaque balise se compose de deux parties :

- Une clé de balise (par exemple, `CostCenter`, `Environment` ou `Project`). Les clés de balises sont sensibles à la casse.
- Un champ facultatif appelé valeur de balise (par exemple, `111122223333` ou `Production`). Si la valeur de balise est identique à l'utilisation d'une chaîne vide. Les valeurs de balise sont sensibles à la casse, tout comme les clés de balise.

Les balises vous permettent d'effectuer les actions suivantes :

- Identifier et organiser vos ressources AWS. De nombreux services AWS prennent en charge le balisage. Vous pouvez donc attribuer la même balise à des ressources à partir de différents services pour indiquer que les ressources sont liées. Par exemple, vous pouvez attribuer la même balise à un AWS Elemental MediaConnect flux que celle que vous attribuez à une sortie de AWS Elemental MediaLive canal.
- Suivre vos coûts AWS. Vous activez ces balises sur le tableau de bord AWS Billing and Cost Management. AWS utilise les balises pour classer vos coûts et pour vous fournir un rapport

mensuel d'allocation des coûts. Pour de plus amples informations, veuillez consulter Utilisation des balises d'allocation des coûts dans le Guide de l'utilisateur AWS Billing.

Les sections suivantes fournissent de plus amples informations sur les balises pour AWS Elemental MediaConnect.

Rubriques

- Ressources prises en charge dans AWS Elemental MediaConnect
- Conventions de dénomination et d'utilisation des balises
- Gestion des balises

Ressources prises en charge dans AWS Elemental MediaConnect

Les ressources suivantes de AWS Elemental MediaConnect prennent en charge le balisage :

- Flux
- Sources
- Outputs
- Droits

Pour obtenir des informations sur l'ajout et la gestion de balises, veuillez consulter Gestion des balises.

AWS Elemental MediaConnectne prend pas en charge la fonctionnalité de contrôle d'accès basée sur des balises de AWS Identity and Access Management (IAM).

Conventions de dénomination et d'utilisation des balises

Les conventions d'utilisation et d'attribution de noms de base suivantes s'appliquent à l'utilisation des balises avec les ressources AWS Elemental MediaConnect :

- Chaque ressource peut avoir un maximum de 50 balises.
- Pour chaque ressource, chaque clé de balise doit être unique, et chaque clé de balise peut avoir une seule valeur.
- La longueur maximale des clés de balise est de 128 caractères Unicode en UTF-8.
- La longueur maximale des valeurs de balise est de 256 caractères Unicode en UTF-8.

- Les caractères autorisés sont les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : . : + = @ _ / - (tiret). Les ressources Amazon EC2 autorisent tous les caractères.
- Les clés et valeurs de balise sont sensibles à la casse. La bonne pratique consiste à choisir une stratégie pour mettre des balises en majuscule et mettre en œuvre cette stratégie de manière cohérente sur tous les types de ressources. Par exemple, décidez si vous souhaitez utiliser `Costcenter`, `costcenter` ou `CostCenter`, et utilisez la même convention pour toutes les balises. Évitez d'utiliser des balises avec une incohérence de traitement de cas similaires.
- Le préfixe `aws:` est interdit pour les balises ; il est réservé à l'utilisation d'AWS. Vous ne pouvez pas modifier ni supprimer des clés ou valeurs de balise ayant ce préfixe. Les balises avec ce préfixe ne sont pas prises en comptes dans vos balises pour le quota de ressources.

Gestion des balises

Les balises sont constituées des propriétés `Key` et `Value` sur une ressource. Vous pouvez utiliser la console AWS Elemental MediaConnect, l'AWS CLI ou l'API AWS Elemental MediaConnect pour ajouter, modifier ou supprimer les valeurs de ces propriétés. Pour obtenir plus d'informations sur l'utilisation des balises, consultez ce qui suit :

- Ressources de la référence de l'API AWS Elemental MediaConnect.
- the section called “Gestion des balises dans un flux” dans ce guide
- the section called “Gestion des balises sur une source” dans ce guide
- the section called “Gestion des balises sur une sortie” dans ce guide
- the section called “Gestion des balises associées à un droit” dans ce guide

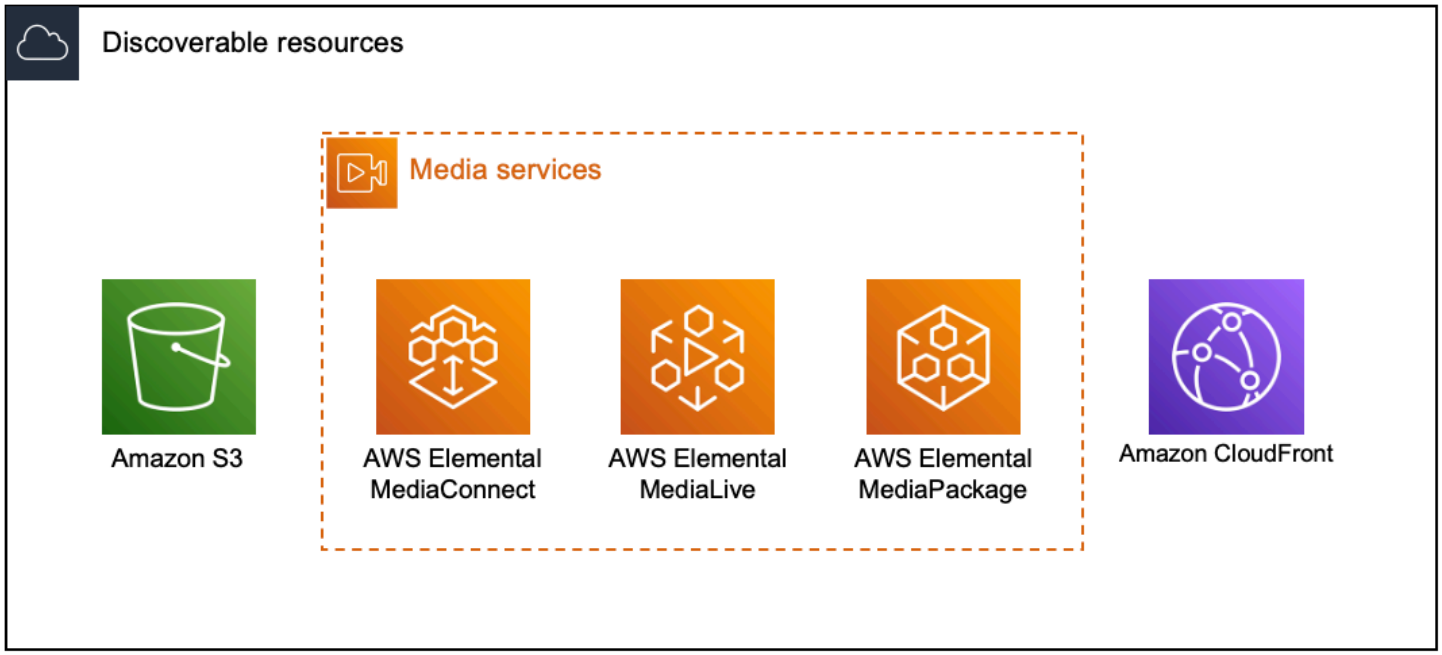
Surveillance des services AWS multimédias avec un moniteur de flux de travail

Le moniteur de flux de travail est un outil de découverte, de visualisation et de surveillance des flux de travail AWS multimédia. Le moniteur de flux de travail est disponible dans la AWS console et dans l'API. Vous pouvez utiliser le moniteur de flux de travail pour découvrir et créer des mappages visuels des ressources de votre flux de travail, appelés cartes de signaux. Vous pouvez créer et gérer des modèles CloudWatch d'alarme Amazon et de EventBridge règles Amazon pour surveiller les ressources mappées. Les modèles de surveillance que vous créez sont transformés en AWS

CloudFormation modèles déployables pour permettre la répétabilité. AWS-les modèles d'alarme recommandés fournissent une surveillance prédéfinie basée sur les meilleures pratiques.

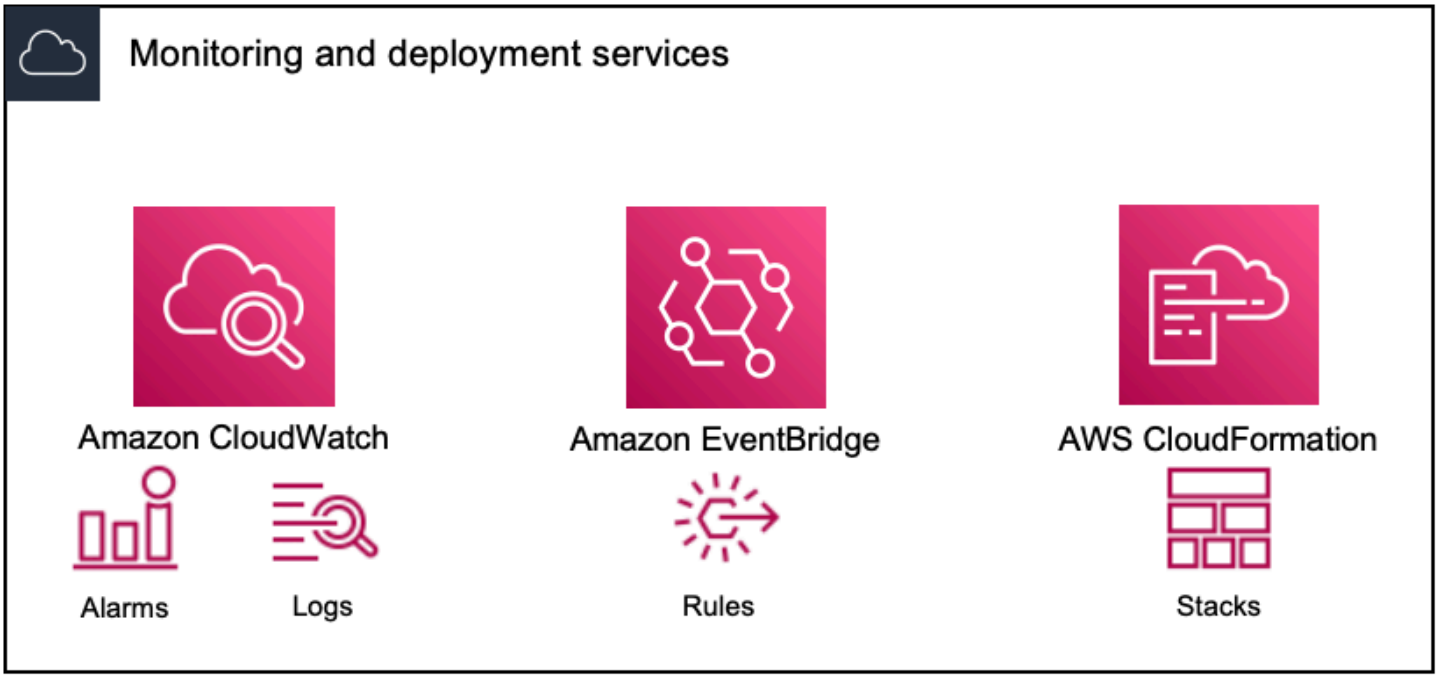
Découvrez

Utilisez des cartes de signaux pour découvrir automatiquement les AWS ressources interconnectées associées à votre flux de travail multimédia. La découverte peut commencer par n'importe quelle ressource de service prise en charge et crée un end-to-end mappage du flux de travail. Les cartes de signaux peuvent être utilisées comme outils de visualisation autonomes ou améliorées avec des modèles de surveillance.



Surveiller

Vous pouvez créer des modèles CloudWatch d'alarme et de EventBridge règles personnalisés pour surveiller l'état et l'état de vos flux de travail multimédia. Des modèles d'alarme conformes aux meilleures pratiques peuvent être importés dans votre environnement de surveillance des flux de travail. Vous pouvez utiliser les modèles d'alarme conformes aux meilleures pratiques tels quels ou les modifier pour mieux les adapter à votre flux de travail. Tous les modèles que vous créez sont transformés en AWS CloudFormation modèles pour un déploiement reproductible.



Note

L'utilisation du moniteur de flux de travail n'entraîne aucun coût direct. Cependant, les ressources créées et utilisées pour surveiller votre flux de travail entraînent des coûts. Lorsque la surveillance est déployée, Amazon CloudWatch et EventBridge des ressources Amazon sont créées. Lorsque vous utilisez la console de AWS gestion, avant de déployer la surveillance sur une carte de signaux, vous serez informé du nombre de ressources qui seront créées. Pour plus d'informations sur la tarification, voir : CloudWatchtarification et EventBridge tarification.

Workflow Monitor utilise des AWS CloudFormation modèles pour déployer les EventBridge ressources CloudWatch et. Ces modèles sont stockés dans un bucket Amazon Simple Storage Service de classe standard créé en votre nom, par Workflow Monitor, pendant le processus de déploiement et qui entraînera des frais de stockage d'objets et de rappel. Pour plus d'informations sur la tarification, consultez : Tarification Amazon S3.

Les aperçus générés dans la carte des signaux du moniteur de flux de travail pour les AWS Elemental MediaPackage canaux sont fournis depuis le point de terminaison MediaPackage Origin et entraînent des frais de transfert de données sortantes. Pour les tarifs, voir : MediaPackagetarification.

Composants du moniteur de flux de travail

Le moniteur de flux de travail comporte quatre composants principaux :

- CloudWatch modèles d'alarme - Définissez les conditions que vous souhaitez surveiller à l'aide CloudWatch. Vous pouvez créer vos propres modèles d'alarme ou importer des modèles prédéfinis créés par AWS. Pour plus d'informations, voir : CloudWatch groupes d'alarmes et modèles
- EventBridge modèles de règles - Définissez le mode d' EventBridge envoi des notifications lorsqu'une alarme est déclenchée. Pour plus d'informations, voir : EventBridge groupes de règles et modèles
- Cartes de signaux - Utilisez un processus automatisé pour créer des cartes de flux de travail AWS élémentaires à l'aide des AWS ressources existantes. Les cartes de signaux peuvent être utilisées pour découvrir les ressources de votre flux de travail et déployer une surveillance sur ces ressources. Pour plus d'informations, voir : Cartes des signaux du moniteur de flux de travail
- Vue d'ensemble - La page de présentation vous permet de surveiller directement l'état de plusieurs cartes de signaux à partir d'un seul endroit. Passez en revue les métriques, les journaux et les alarmes de vos flux de travail. Pour plus d'informations, voir : Présentation du moniteur de flux de travail

Services pris en charge

Le moniteur de flux de travail prend en charge la découverte automatique et le mappage des signaux des ressources associées aux services suivants :

- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaConnect
- Amazon S3
- Amazon CloudFront

Rubriques

- Configuration du moniteur de flux de travail
- Utilisation du moniteur de flux de travail

Configuration du moniteur de flux de travail

Pour configurer le moniteur de flux de travail pour la première fois, vous créez les modèles d'alarme et d'événement, et vous découvrez les cartes de signaux utilisées pour surveiller vos flux de travail multimédia. Le guide suivant décrit les étapes nécessaires pour configurer les rôles IAM de niveau administrateur et opérateur, créer des ressources de surveillance des flux de travail et déployer la surveillance dans vos flux de travail.

Rubriques

Commencer à utiliser le moniteur de flux de travail

Les étapes suivantes fournissent un aperçu de base de la première utilisation du moniteur de flux de travail.

1. Configurer les autorisations IAM de surveillance du flux de travail pour les rôles d'administrateur et d'opérateur : Politiques IAM de surveillance des flux de travail
2. Créez des modèles d'alarme ou importez des modèles prédéfinis créés par AWS : Alarmes CloudWatch
3. Créez des événements de notification qui seront diffusés par EventBridge : EventBridge règles
4. Découvrez des cartes de signalisation en utilisant vos ressources AWS élémentaires existantes : Cartes des signaux
5. Joignez les modèles d'alarme et les règles de notification à votre carte des signaux : Joindre des modèles
6. Déployez les modèles pour commencer à surveiller la carte des signaux : Déployer la surveillance
7. Surveillez et passez en revue les ressources de surveillance de votre flux de travail à l'aide de la section de présentation de la AWS console : Présentation

Politiques IAM de surveillance des flux de travail

Le moniteur de flux de travail interagit avec plusieurs AWS services pour créer des cartes de signaux, des builds, EventBridge des ressources CloudWatch et des AWS CloudFormation modèles. Étant donné que le moniteur de flux de travail interagit avec un large éventail de services, des politiques spécifiques AWS Identity and Access Management (IAM) doivent être attribuées à ces services. Les exemples suivants indiquent les politiques IAM nécessaires pour les rôles IAM d'administrateur et d'opérateur.

Politique IAM de l'administrateur

L'exemple de politique suivant concerne une stratégie IAM de surveillance des flux de travail au niveau de l'administrateur. Ce rôle permet de créer et de gérer les ressources du moniteur de flux de travail et les ressources de service prises en charge qui interagissent avec le moniteur de flux de travail.

```
                    {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "cloudwatch:List*",
      "cloudwatch:Describe*",
      "cloudwatch:Get*",
      "cloudwatch:PutAnomalyDetector",
      "cloudwatch:PutMetricData",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:PutCompositeAlarm",
      "cloudwatch:PutDashboard",
      "cloudwatch:DeleteAlarms",
      "cloudwatch:DeleteAnomalyDetector",
      "cloudwatch:DeleteDashboards",
      "cloudwatch:TagResource",
      "cloudwatch:UntagResource"
```

```
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:List*",
        "cloudformation:Describe*",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudfront:List*",
        "cloudfront:Get*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "events:List*",
        "events:Describe*",
        "events:CreateEventBus",
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:TagResource",
```

```
        "events:UntagResource"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:Describe*",
        "logs:Get*",
        "logs:TagLogGroup",
        "logs:TagResource",
        "logs:UntagLogGroup",
        "logs:UntagResource"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mediaconnect:List*",
        "mediaconnect:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "medialive:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mediapackage:List*",
        "mediapackage:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mediapackagev2:List*",
        "mediapackagev2:Get*"
```

```
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mediapackage-vod:List*",
        "mediapackage-vod:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mediatailor:List*",
        "mediatailor:Describe*",
        "mediatailor:Get*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:ListGroups",
        "resource-groups:GetGroup",
        "resource-groups:GetTags",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:CreateGroup",
        "resource-groups:UngroupResources",
        "resource-groups:GroupResources",
        "resource-groups:DeleteGroup",
        "resource-groups:UpdateGroupQuery",
        "resource-groups:UpdateGroup",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:*"
      ],
```

```
      "Resource": "arn:aws:s3:::workflow-monitor-templates*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:TagResource",
        "sns:UntagResource"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "tag:Get*",
        "tag:Describe*",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Politique IAM de l'opérateur

L'exemple de politique suivant concerne une stratégie IAM de surveillance des flux de travail au niveau de l'opérateur. Ce rôle permet un accès limité et en lecture seule aux ressources du moniteur de flux de travail et aux ressources de service prises en charge qui interagissent avec le moniteur de flux de travail.

```
                  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*"
```

```
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudfront:List*",
        "cloudfront:Get*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "events:List*",
        "events:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:Describe*",
        "logs:Get*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "mediaconnect:List*",
        "mediaconnect:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "medialive:List*",
        "medialive:Get*",
        "medialive:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mediapackage:List*",
        "mediapackage:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mediapackagev2:List*",
        "mediapackagev2:Get*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mediapackage-vod:List*",
        "mediapackage-vod:Describe*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mediatailor:List*",
        "mediatailor:Describe*",
```

```
        "mediatailor:Get*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::workflow-monitor-templates*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "tag:Get*",
        "tag:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Groupes et modèles de surveillance des flux de travail

Avant de déployer la surveillance du flux de travail sur une carte des signaux, vous devez créer les groupes et les modèles pour les CloudWatch alarmes et EventBridge les notifications. Les CloudWatch modèles définissent les scénarios et les seuils qui seront utilisés pour déclencher les alarmes. Les EventBridge modèles détermineront la manière dont ces alarmes vous seront signalées.

Si vous souhaitez uniquement des mappages de vos ressources connectées et que vous ne souhaitez pas utiliser les fonctionnalités des modèles de surveillance de Workflow Monitor, les cartes de signaux peuvent être utilisées sans CloudWatch les EventBridge modèles. Pour plus d'informations sur l'utilisation des cartes de signaux, voir : Cartes des signaux

Rubriques

- CloudWatch groupes d'alarmes et modèles
- EventBridge groupes de règles et modèles

CloudWatch groupes d'alarmes et modèles

Les alarmes de surveillance du flux de travail vous permettent d'utiliser CloudWatch les métriques existantes comme base des alarmes pour vos cartes de signaux. Vous pouvez créer un groupe de modèles d'alarmes pour trier et classer les types d'alarmes importants pour votre flux de travail. Au sein de chaque groupe de modèles d'alarme, vous créez des modèles d'alarme avec CloudWatch des mesures et des paramètres spécifiques que vous souhaitez surveiller. Vous pouvez créer vos propres modèles d'alarme ou importer des modèles d'alarme recommandés créés par AWS. Après avoir créé un groupe de modèles d'alarme et des modèles d'alarme au sein de ce groupe, vous pouvez associer un ou plusieurs de ces groupes de modèles d'alarme à une carte des signaux.

Vous devez d'abord créer un groupe de modèles d'alarmes. Après avoir créé un groupe de modèles d'alarme, vous pouvez créer vos propres modèles ou utiliser les modèles recommandés créés par AWS. Si vous souhaitez créer vos propres modèles d'alarme, continuez sur cette page. Pour plus d'informations sur l'importation de modèles recommandés, voir : Modèles recommandés

Cette section traite de la création d' CloudWatch alarmes à l'aide du moniteur de flux de travail. Pour plus d'informations sur la façon dont le CloudWatch service gère les alarmes et pour en savoir plus sur les composants des alarmes, consultez : Utilisation des CloudWatch alarmes dans le guide de CloudWatch l'utilisateur Amazon

Création de groupes de modèles d'alarmes

Pour créer un groupe de modèles d'alarmes

1. Dans le volet de navigation de la console Workflow Monitor, sélectionnez les modèles CloudWatch d'alarme.
2. Sélectionnez Créer un groupe de modèles d'alarme.
3. Donnez au groupe de modèles d'alarme un nom de groupe unique et une description facultative.
4. Sélectionnez Créer. Vous serez redirigé vers la page de détails du groupe de modèles d'alarmes nouvellement créé.

Création de modèles d'alarme

Pour créer un modèle d'alarme

1. Sur la page de détails du groupe de modèles d'alarme, sélectionnez Créer un modèle d'alarme.
2. Donnez au modèle d'alarme un nom de modèle unique et une description facultative.

3. Dans la section Choisir une métrique :

    1. Sélectionnez un type de ressource cible. Le type de ressource cible est une ressource pour le service concerné, telle qu'un canal pour MediaLive MediaPackage et/ou un flux pour MediaConnect.
    2. Sélectionnez un nom de métrique. Il s'agit de la CloudWatch métrique qui sert de base à l'alarme. La liste des mesures changera en fonction du type de ressource cible sélectionné.

4. Dans la section Paramètres de l'alarme :

    > **Note**
    >
    > Pour plus d'informations sur la façon dont le CloudWatch service gère les alarmes et pour en savoir plus sur les composants des alarmes, consultez : Utilisation des CloudWatch alarmes dans le guide de CloudWatch l'utilisateur Amazon

    1. Sélectionnez la statistique. Il s'agit d'une valeur telle qu'une somme ou une moyenne qui sera utilisée pour surveiller la métrique.
    2. Sélectionnez l'opérateur de comparaison. Ce champ fait référence au seuil que vous avez défini à l'étape suivante.
    3. Définissez un seuil. Il s'agit d'une valeur numérique que l'opérateur de comparaison utilise pour déterminer une valeur supérieure, inférieure ou égale au statut.
    4. Définissez une période. Il s'agit d'une valeur temporelle, en secondes. La période est la durée pendant laquelle la statistique, l'opérateur de comparaison et le seuil interagissent pour déterminer si l'alarme est déclenchée.
    5. Définissez les points de données. Cette valeur détermine le nombre de points de données nécessaires pour déclencher l'alarme.
    6. Sélectionnez le mode de traitement des données manquantes. Cette sélection détermine la façon dont cette alarme réagit aux données manquantes.

5. Sélectionnez Créer pour terminer le processus.

Un exemple de modèle d'alarme terminé peut comporter les paramètres suivants : Un type de ressource cible de MediaConnect flux est surveillé pour le nom de la métrique de déconnexions. La valeur statistique est définie sur Somme avec un opérateur de comparaison « supérieur ou égal à »

et un seuil de 10. La période est fixée à 60 secondes et ne nécessite qu'un point de données sur 1. Traiter les données manquantes est défini sur « ignorer ».

Le résultat de ces paramètres est le suivant : le moniteur du flux de travail surveillera les déconnexions sur le flux. Si 10 déconnexions ou plus se produisent dans les 60 secondes, l'alarme se déclenche. 10 déconnexions ou plus en 60 secondes ne doivent se produire qu'une seule fois pour que l'alarme se déclenche.

Modèles d'alarme recommandés

Les modèles recommandés par Workflow Monitor sont une sélection organisée de métriques de service AWS Elemental avec des paramètres d'alarme prédéfinis adaptés à la métrique. Si vous ne souhaitez pas créer de modèles d'alarme personnalisés, les modèles recommandés vous fournissent des modèles de surveillance conformes aux meilleures pratiques créés par AWS.

Le moniteur de flux de travail contient des groupes de modèles recommandés pour chaque service pris en charge. Ces groupes sont conçus pour appliquer la surveillance des meilleures pratiques à des types de flux de travail spécifiques. Chaque groupe de modèles contient une sélection organisée d'alarmes configurées à partir de métriques spécifiques au service. Par exemple, un groupe de modèles recommandé pour un flux de travail MediaLive multiplex comportera un ensemble de mesures préconfigurées différent de celui d'un flux de travail MediaConnect CDI.

Pour utiliser les modèles d'alarme recommandés

1. Suivez les étapes pour créer un groupe de modèles d'alarmes ou sélectionnez-en un existant.
2. Dans la section Modèles d'alarme, sélectionnez Importer. Vous devrez importer les modèles AWS recommandés dans votre groupe de modèles.
3. Utilisez le menu déroulant des groupes de modèles d'CloudWatch alarme pour sélectionner un groupe AWS recommandé. Ces groupes contiennent des alarmes sélectionnées pour des services spécifiques.
4. Sélectionnez les modèles à importer à l'aide des cases à cocher. Chaque modèle listera ses métriques, ses valeurs de surveillance préconfigurées et fournira une description de la métrique. Lorsque vous avez terminé de sélectionner les modèles, cliquez sur le bouton Ajouter.
5. Les modèles sélectionnés seront déplacés vers la section Modèles d'alarme à importer. Passez en revue vos choix et sélectionnez Importer.
6. Une fois l'importation terminée, les modèles sélectionnés seront ajoutés au groupe de modèles. Si vous souhaitez ajouter d'autres modèles, répétez le processus d'importation.

7. Les modèles importés peuvent être personnalisés après l'importation. Les paramètres d'alarme peuvent être modifiés pour répondre à vos besoins en matière d'alarme.

EventBridge groupes de règles et modèles

CloudWatch utilise les EventBridge règles d'Amazon pour envoyer des notifications. Vous pouvez envoyer des notifications en fonction des modèles d'événements que vous créez. Vous commencez par créer un groupe de modèles d'événements. Dans ce groupe de modèles d'événements, vous créez des modèles d'événements qui déterminent quelles conditions créent une notification et qui est averti.

Cette section traite de la création de EventBridge règles à l'aide du moniteur de flux de travail. Pour plus d'informations sur la manière dont le EventBridge service utilise les règles, consultez : EventBridge règles dans le guide de EventBridge l'utilisateur Amazon

Création de groupes de modèles d'événements

Pour créer un groupe de modèles d'événements

1. Dans le volet de navigation de la console Workflow Monitor, sélectionnez des modèles de EventBridge règles.
2. Sélectionnez Créer un groupe de modèles d'événements.
3. Donnez au groupe de modèles d'alarme un nom de groupe unique et une description facultative.
4. Sélectionnez Créer. Vous serez redirigé vers la page de détails du groupe de modèles d'alarmes nouvellement créé.

Création de modèles d'événements

Pour créer un modèle d'événement

1. Sur la page de détails du groupe de modèles d'événements, sélectionnez Créer un modèle d'événement.
2. Donnez au modèle d'événement un nom de modèle unique et une description facultative.
3. Dans la section Paramètres des règles :

1. Sélectionnez un type d'événement. Lorsque vous sélectionnez un type d'événement, vous pouvez choisir entre plusieurs événements créés par AWS ou sélectionner Signal map active alarm pour utiliser une alarme créée par un modèle d'alarme.
2. Sélectionnez un service cible. Cela détermine la manière dont vous souhaitez être informé de cet événement. Vous pouvez sélectionner Amazon Simple Notification Service ou CloudWatch les journaux.
3. Après avoir sélectionné un service cible, sélectionnez-en un. Il s'agira d'une rubrique Amazon SNS ou d'un groupe de CloudWatch journaux, selon le service cible que vous avez sélectionné.

4. Sélectionnez Créer pour terminer le processus.

Cartes des signaux du moniteur de flux de travail

Les cartes de signaux sont des mappages visuels des AWS ressources de votre flux de travail multimédia. Vous pouvez utiliser le moniteur de flux de travail pour démarrer la découverte de la carte des signaux sur tous les types de ressources pris en charge. Au cours du processus de découverte, le moniteur de flux de travail mappera automatiquement et récursivement toutes les AWS ressources connectées. Une fois la carte des signaux créée, vous pouvez utiliser la console de surveillance du flux de travail pour déployer des modèles de surveillance, consulter les métriques et afficher les détails des ressources mappées.

Rubriques

- Création de cartes de signalisation
- Visualisation des cartes de signalisation
- Joindre des modèles d'alarme et d'événement à votre carte des signaux
- Déploiement de modèles sur votre carte de signaux
- Mise à jour des cartes de signaux et des ressources sous-jacentes
- Supprimer des cartes de signaux

Création de cartes de signalisation

Pour créer une carte des signaux

1. Dans le volet de navigation de la console Workflow Monitor, sélectionnez Signal maps.

2. Sélectionnez Créer une carte des signaux.
3. Donnez un nom et une description à la carte des signaux.
4. Dans la section Découvrir une nouvelle carte des signaux, les ressources du compte courant et de la région sélectionnée sont affichées. Sélectionnez une ressource pour commencer la découverte de la carte des signaux. La ressource sélectionnée sera le point de départ de la découverte.
5. Sélectionnez Créer. Attendez quelques instants pour que le processus de découverte soit terminé. Une fois le processus terminé, la nouvelle carte des signaux vous sera présentée.

> **Note**
>
> Les aperçus générés dans la carte des signaux du moniteur de flux de travail pour les AWS Elemental MediaPackage canaux sont fournis depuis le point de terminaison MediaPackage Origin et entraînent des frais de transfert de données sortantes. Pour les tarifs, voir : MediaPackagetarification.

Visualisation des cartes de signalisation

Vues de la carte des signaux

Après avoir sélectionné une carte des signaux, vous disposez de deux vues qui peuvent être utilisées pour surveiller ou configurer la carte des signaux. Surveiller la carte des signaux et configurer la carte des signaux est un bouton contextuel situé dans le coin supérieur droit de la section console de la carte des signaux.

Si vous sélectionnez la carte des signaux à l'aide de la section Cartes des signaux du volet de navigation, votre carte des signaux sera affichée dans la vue de configuration. La vue de configuration vous permet d'apporter des modifications aux groupes de modèles attachés à cette carte de signaux, de déployer les modèles joints et d'afficher les détails de base et les balises de la carte de signaux.

Si vous sélectionnez la carte des signaux à l'aide de la section Vue d'ensemble du volet de navigation, votre carte des signaux sera affichée dans la vue de surveillance. La vue de surveillance affiche les CloudWatch alarmes, EventBridge les règles, les alertes, les journaux et les mesures de cette carte de signaux.

La vue peut être modifiée à tout moment en sélectionnant le bouton Monitor/Configure signal map en haut à droite. La vue de configuration nécessite des autorisations IAM de niveau administrateur. Les

autorisations IAM requises peuvent être consultées ici : Politiques IAM de surveillance des flux de travail

Naviguer sur la carte des signaux

Une carte des signaux contiendra des nœuds pour chaque ressource AWS prise en charge découverte par le moniteur de flux de travail. Certaines ressources, telles que les MediaLive chaînes et les MediaPackage points de terminaison, peuvent afficher des aperçus miniatures du contenu, si des aperçus miniatures sont disponibles.

En sélectionnant un nœud de ressource, puis en sélectionnant Afficher les détails des ressources sélectionnées dans le menu déroulant Actions, vous accédez à la page de détails du service associé. Par exemple, si vous sélectionnez un MediaLive canal et sélectionnez Afficher les détails des ressources sélectionnées, la page de détails de la MediaLive console correspondant à ce canal s'ouvre.

La sélection d'un nœud de ressource filtrera la liste des alarmes actives uniquement sur ce nœud. Si vous sélectionnez l'ARN cible de la ressource dans l'alarme active, vous serez redirigé vers la page de détails du service associé, avec la ressource sélectionnée ouverte.

Joindre des modèles d'alarme et d'événement à votre carte des signaux

Après avoir créé des modèles d'alarme et d'événement, vous devez les joindre à une carte des signaux. Tous les modèles d'alarme et d'événement que vous avez créés peuvent être joints à toutes les cartes de signaux découvertes.

Pour joindre des modèles d'alarme et d'événement à votre carte des signaux

1. Dans le volet de navigation de la console du moniteur de flux de travail, sélectionnez Signal maps et sélectionnez la carte des signaux avec laquelle vous souhaitez travailler.
2. Dans le coin supérieur droit de la page de carte des signaux, dans l'onglet Groupes de modèles CloudWatch d'alarmes, sélectionnez Joindre des groupes de modèles CloudWatch d'alarme.

    1. Dans la nouvelle section qui s'ouvre, choisissez tous les groupes de modèles d'alarme que vous souhaitez appliquer à cette carte de signaux, puis sélectionnez Ajouter. Cela entraînera le déplacement des groupes de modèles d'alarme sélectionnés vers la section Groupes de modèles CloudWatch d'alarme joints.
    2. Sélectionnez Enregistrer pour enregistrer vos modifications et revenir à la page de la carte des signaux.

3. À droite de la page de la carte des signaux, sélectionnez l'onglet Groupes de modèles de EventBridge règles, puis sélectionnez Attacher des groupes de modèles de EventBridge règles.

    1. Dans la nouvelle section qui s'ouvre, choisissez tous les groupes de modèles d'événements que vous souhaitez appliquer à cette carte de signaux, puis sélectionnez Ajouter. Cela entraînera le déplacement des groupes de modèles de règles sélectionnés vers la section Groupes de modèles de EventBridge règles attachés.
    2. Sélectionnez Enregistrer pour enregistrer vos modifications et revenir à la page de la carte des signaux.
4. Vous avez attribué des modèles CloudWatch d'alarme et de EventBridge règles à la carte des signaux, mais la surveillance n'est pas encore déployée. La section suivante traitera du déploiement des ressources de surveillance.

Déploiement de modèles sur votre carte de signaux

Après avoir joint les modèles d'alarme et d'événement à votre carte des signaux, vous devez déployer la surveillance. Tant que le déploiement n'est pas terminé, la surveillance de votre carte de signaux ne sera pas active.

Le moniteur de flux de travail ne déploie que les alarmes pertinentes pour la carte de signaux sélectionnée. Par exemple, le groupe de modèles d'alarme joint peut contenir des alarmes pour plusieurs services MediaLive, tels que MediaPackage, et MediaConnect. Si la carte de signal sélectionnée ne contient que des MediaLive ressources, aucune alarme ne sera déployée MediaPackage ou aucune MediaConnect alarme ne sera déployée.

Pour déployer les modèles de surveillance

1. Après avoir joint des groupes de modèles d'alarmes et d'événements à votre carte de signaux et enregistré vos modifications, sélectionnez Déployer le moniteur dans le menu déroulant Actions.
2. Il vous sera demandé de confirmer le déploiement et le nombre de ressources qui seront créées ainsi que le nombre CloudWatch de EventBridge ressources qui seront créées vous seront présentés. Si vous souhaitez continuer, sélectionnez Déployer.

> **Note**
>
> L'utilisation du moniteur de flux de travail n'entraîne aucun coût direct. Cependant, les ressources créées et utilisées pour surveiller votre flux de travail entraînent des coûts.

Lorsque la surveillance est déployée, Amazon CloudWatch et EventBridge des ressources Amazon sont créées. Lorsque vous utilisez la console de AWS gestion, avant de déployer la surveillance sur une carte de signaux, vous serez informé du nombre de ressources qui seront créées. Pour plus d'informations sur la tarification, voir : CloudWatchtarification et EventBridge tarification.
Workflow Monitor utilise des AWS CloudFormation modèles pour déployer les EventBridge ressources CloudWatch et. Ces modèles sont stockés dans un bucket Amazon Simple Storage Service de classe standard créé en votre nom, par Workflow Monitor, pendant le processus de déploiement et qui entraînera des frais de stockage d'objets et de rappel. Pour plus d'informations sur la tarification, consultez : Tarification Amazon S3.

3. L'état du déploiement est affiché à côté du nom de la carte des signaux. L'état du déploiement est également visible dans la section Stacks de la AWS CloudFormation console. Après quelques instants de création et de déploiement des ressources, la surveillance de votre carte des signaux commencera.

Mise à jour des cartes de signaux et des ressources sous-jacentes

Si une modification est apportée à votre flux de travail, vous devrez peut-être redécouvrir la carte des signaux et redéployer les ressources de surveillance. Le moniteur de flux de travail est un outil de visualisation et de surveillance qui n'est pas en mesure d'apporter des modifications à votre flux de travail. Les cartes de signaux représentent une point-in-time visualisation de votre flux de travail. Si vous ajoutez, supprimez ou modifiez de manière significative des parties de votre flux de travail multimédia, nous vous recommandons de redécouvrir la carte des signaux. Si des ressources de surveillance sont associées à la carte des signaux, nous vous recommandons de redéployer la surveillance après le processus de redécouverte.

Pour redécouvrir une carte des signaux

1. Dans le volet de navigation de la console du moniteur de flux de travail, sélectionnez Signal maps et sélectionnez la carte des signaux avec laquelle vous souhaitez travailler.
2. Vérifiez que vous êtes dans la vue de la carte de configuration des signaux. Pour plus d'informations sur la modification des vues, voir : Afficher les cartes des signaux
3. Dans le coin supérieur droit de la page de la carte des signaux, sélectionnez le menu déroulant Actions. Sélectionnez Redécouvrir.

4. L'écran de redécouverte vous sera présenté. Sélectionnez une ressource qui fait partie du flux de travail que vous êtes en train de redécouvrir. Cliquez sur le bouton Redécouvrir.
5. La carte des signaux sera reconstruite conformément au flux de travail actuel. Si vous devez redéployer des ressources de surveillance, restez sur la page de cette carte des signaux. Tous les modèles de surveillance précédemment joints resteront attachés, mais devront être redéployés.

Pour redéployer des modèles de surveillance après la redécouverte d'une carte de signaux

1. Après la redécouverte, vous serez dirigé vers la carte des signaux mise à jour. Pour redéployer les modèles de surveillance, sélectionnez Déployer le moniteur dans le menu déroulant Actions.
2. Il vous sera demandé de confirmer le déploiement et le nombre de EventBridge ressources qui seront créées vous sera présenté. CloudWatch Si vous souhaitez continuer, sélectionnez Déployer.
3. L'état du déploiement est affiché à côté du nom de la carte des signaux. Après quelques instants de création et de déploiement des ressources, la surveillance de votre carte des signaux commencera.

Supprimer des cartes de signaux

Si vous n'avez plus besoin d'une carte des signaux, elle peut être supprimée. Si vous avez déployé des modèles de surveillance sur la carte des signaux, le processus de suppression vous demandera de supprimer toutes CloudWatch les EventBridge ressources déployées sur cette carte des signaux. La suppression des ressources déployées n'affecte pas les modèles qui les ont créées. Cette suppression de ressources vise à garantir que vous ne disposez pas CloudWatch de EventBridge ressources déployées mais non utilisées.

Pour supprimer un mappage de signaux

1. Dans le volet de navigation de la console du moniteur de flux de travail, sélectionnez Signal maps et sélectionnez le bouton radio à côté de la carte des signaux que vous souhaitez supprimer.
2. Sélectionnez le bouton Supprimer. Il vous sera demandé de confirmer la suppression des ressources de surveillance. Sélectionnez Supprimer pour lancer le processus de suppression des ressources de surveillance.

3. La colonne Surveiller le déploiement affichera l'état actuel. Lorsque le statut est passé à DELETE_COMPLETE, sélectionnez à nouveau le bouton Supprimer.
4. Il vous sera demandé de confirmer la suppression de la carte des signaux. Sélectionnez Supprimer pour continuer et supprimer le mappage des signaux.

Quotas de surveillance des workflows

La section suivante contient les quotas pour les ressources de surveillance des flux de travail. Chaque quota est calculé « par compte ». Vous ne pouvez pas dépasser les quotas suivants sur un seul AWS compte. Ces quotas ne peuvent être augmentés.

Quotas

Type de ressource	Quota
CloudWatch groupes de modèles d'alarme	20
CloudWatch modèles d'alarme	200
EventBridge groupes de modèles de règles	20
EventBridge modèles de règles	200
Cartes des signaux	30
Cartes de signaux : nœuds de ressources dans une carte de signal unique	30
Cartes de signaux : groupes de modèles CloudWatch d'alarmes attachés à une seule carte de signaux	5
Cartes de signaux : groupes de modèles de EventBridge règles attachés à une seule carte de signaux	5

Utilisation du moniteur de flux de travail

Utilisez les sections de présentation et de cartographie des signaux de la console de surveillance des flux de travail pour consulter l'état actuel des flux de travail et les alarmes, mesures et journaux associés.

Rubriques

Présentation du moniteur de flux de travail

La section Vue d'ensemble de la console de surveillance du flux de travail est un tableau de bord qui fournit des at-a-glance informations sur vos cartes de signaux. Dans la section d'aperçu, vous pouvez voir l'état actuel de la surveillance de chaque carte de signaux, ainsi que CloudWatch les métriques et les CloudWatch journaux associés. Vous pouvez sélectionner n'importe quelle carte de signaux à afficher sur cette page de console de cartes de signaux.

Vue d'ensemble du filtrage

À l'aide de la barre de recherche dans la section d'aperçu, vous pouvez filtrer la liste des cartes de signaux à l'aide de contraintes contextuelles. Après avoir sélectionné la barre de recherche, une liste de propriétés à filtrer s'affichera. La sélection d'une propriété affichera des opérateurs tels que égal, contient, n'est pas égal et ne contient pas. La sélection d'un opérateur créera une liste de ressources à partir du type de propriété sélectionné. En sélectionnant l'une de ces ressources, la liste des cartes de signaux n'affichera que les cartes de signaux correspondant à la contrainte que vous avez définie.

Vue d'ensemble des journaux et des statistiques

Pour consulter CloudWatch les métriques et les journaux d'une carte de signaux, sélectionnez le bouton radio à côté du nom de la carte de signaux. Une interface à onglets pour les métriques et les journaux apparaîtra sous la liste de la carte des signaux.

CloudWatch Métriques

CloudWatch les métriques de la carte de signal sélectionnée seront sensibles au contexte et n'afficheront que les métriques associées aux services utilisés dans ce flux de travail de cartes

de signaux. Vous pouvez utiliser les outils de mesure à l'écran pour personnaliser les périodes métriques et les plages de temps affichées.

CloudWatch Journaux

Si vous avez associé un groupe de CloudWatch journaux à la carte des signaux, ce groupe sera affiché ici.

Utilisation des cartes de signaux du moniteur de flux de travail

Dans la section d'aperçu de la console, vous pouvez sélectionner une carte de signal spécifique pour afficher plus d'informations sur cette carte de signaux et les ressources de surveillance associées.

Après avoir sélectionné une carte des signaux, vous verrez apparaître la carte des signaux et un certain nombre de sections à onglets contenant plus d'informations :

- CloudWatch alarmes
- EventBridge règles
- AWS Alertes élémentaires
- Métriques
- Journaux
- Détails de base

Naviguer sur la carte des signaux

Une carte des signaux contiendra des nœuds pour chaque ressource AWS prise en charge découverte par le moniteur de flux de travail. Certaines ressources, telles que les MediaLive chaînes et les MediaPackage points de terminaison, peuvent afficher des aperçus miniatures du contenu, si des aperçus miniatures sont disponibles.

En sélectionnant un nœud de ressource, puis en sélectionnant Afficher les détails des ressources sélectionnées dans le menu déroulant Actions, vous accédez à la page de détails du service associé. Par exemple, si vous sélectionnez un MediaLive canal et sélectionnez Afficher les détails des ressources sélectionnées, la page de détails de la MediaLive console correspondant à ce canal s'ouvre.

La sélection d'un nœud de ressource filtrera la liste des alarmes actives uniquement sur ce nœud. Si vous sélectionnez l'ARN cible de la ressource dans l'alarme active, vous serez redirigé vers la page de détails du service associé, avec la ressource sélectionnée ouverte.

MediaConnect maintien du débit

AWS Elemental MediaConnect effectue régulièrement la maintenance des systèmes sous-jacents pour des raisons de sécurité, de fiabilité et de performance opérationnelle. Les activités de maintenance incluent des actions telles que l'application de correctifs au système d'exploitation, la mise à jour des pilotes ou l'installation de logiciels et de correctifs.

> **Note**
>
> Dans le cadre du processus de maintenance, votre flux doit être redémarré.

Vous pouvez sélectionner le jour et l'heure auxquels les événements de maintenance se produisent. C'est ce que l'on appelle une fenêtre de maintenance et elle est utilisée chaque fois qu'un événement de maintenance est requis. Si vous devez modifier le jour et l'heure, vous pouvez modifier la fenêtre de maintenance.

Lorsque la maintenance est requise pour votre flux, vous AWS attribuerez à votre flux une date de péremption obligatoire. Si aucune fenêtre de maintenance n'est configurée pour le flux, consultez la section Configuration des fenêtres de maintenance. Vous pouvez consulter les flux qui nécessitent une maintenance sur la MediaConnect console ou en utilisant la AWS CLI section Afficher les flux nécessitant une maintenance. Lorsqu'une date limite requise a été attribuée à votre flux, vous pouvez sélectionner une date précise pour que cette maintenance ait lieu. La date de maintenance sélectionnée ne s'appliquera qu'au prochain événement de maintenance.

Si vous ne configurez pas de fenêtre de maintenance, AWS sélectionnez-la automatiquement pour vous. Nous vous recommandons de définir une fenêtre de maintenance pour chaque flux et MediaConnect d'autoriser le redémarrage automatique pendant cette fenêtre. Le MediaConnect fait d'autoriser le redémarrage réduit les temps d'arrêt de votre flux. Si un flux nécessite une maintenance et que vous choisissez de le redémarrer manuellement, le statut de maintenance de ce flux passe à Annulé. Le flux redémarré manuellement appliquera toujours les mises à jour requises, mais vous ne recevrez pas le statut Terminé avec succès. Comme vous avez effectué le redémarrage manuellement, la maintenance est considérée comme annulée car MediaConnect aucune mise à jour n'est requise pour ce flux.

La durée de la fenêtre de maintenance est de deux heures.

> **Important**
>
> La durée de la fenêtre de deux heures ne signifie pas que le débit sera affecté pendant deux heures. Le flux s'arrêtera et redémarrera normalement à un moment donné dans la fenêtre de deux heures.

Exemple : si vous configurez l'heure de début de la fenêtre de maintenance d'un flux à 02h00, le flux redémarrera entre 02h00 et 04h00.

Si la maintenance n'a pas lieu à la date et à l'heure prévues, elle MediaConnect sera reprogrammée pour qu'elle ait lieu dans la fenêtre de maintenance de la semaine suivante ou définira automatiquement une nouvelle fenêtre si vous n'en avez pas configuré une.

Rubriques

Visualisation des flux nécessitant une maintenance

Vous pouvez consulter les flux qui nécessitent une maintenance dans la MediaConnect console ou en utilisant le AWS CLI.

> **Note**
>
> Si votre flux ne possède pas de date limite requise (console) ou de MaintenanceDeadline(AWS CLI), aucune maintenance n'est actuellement requise pour ce flux.

Pour afficher les flux nécessitant une maintenance (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Flux.
3. Dans la colonne de la fenêtre Maintenance, vous pouvez consulter la date limite requise. Vous pouvez également afficher la date limite requise sur la page de détails d'un flux individuel.
4. Tous les flux listés doivent être redémarrés avant la date indiquée.

Pour afficher les flux nécessitant une maintenance (AWS CLI)

- Dans le AWS CLI, vous pouvez utiliser la `list-flows` commande pour afficher tous les flux et leur statut de maintenance. En outre, vous pouvez consulter l'état de maintenance d'un flux spécifique à l'aide de la `describe-flow` commande :

```
aws mediaconnect list-flows
```

or

```
aws mediaconnect describe-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame
```

L'exemple suivant montre la valeur de retour de`list-flows`. La valeur de retour pour `describe-flow` utilise une structure similaire.

Dans cet exemple, le flux nommé BasketballGamepossède un MaintenanceDayet MaintenanceStartHourdéfini pour la maintenance récurrente. Le flux nommé AwardsShowpossède le MaintenanceStartHourset MaintenanceDayand, mais également un MaintenanceDeadline. MaintenanceDeadlineIl s'agit de la date d'échéance requise pour les redémarrages de maintenance sur ce flux. Le AwardsShowflux a également planifié une date spécifique pour les redémarrages de maintenance, indiquée dans la MaintenanceScheduledDatevaleur. Cela MaintenanceScheduledDatedoit se produire avant que MaintenanceDeadline:

```
{
    "Flows": [
        {
            "AvailabilityZone": "us-west-2d",
            "Description": "Example flow description",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
            "Name": "BasketballGame",
            "SourceType": "OWNED",
            "Status": "STANDBY",
            "Maintenance": {
                "MaintenanceDay": "Monday",
                "MaintenanceStartHour": "08:00"}
        },
        {
```

```
            "AvailabilityZone": "us-west-2b",
            "Description": "Example flow description",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:2-3aBC45dEF67hiJ8k-2AbC34DE5fGa6:AwardsShow",
            "Name": "AwardsShow",
            "SourceType": "OWNED",
            "Status": "ACTIVE",
            "Maintenance": {
                "MaintenanceDay": "Saturday",
                "MaintenanceDeadline": "2021-10-25T22:15:56Z",
                "MaintenanceScheduledDate": "2021-10-23",
                "MaintenanceStartHour": "23:00"}
        }
    ]
}
```


Configuration des fenêtres de maintenance

Vous pouvez sélectionner le jour et l'heure auxquels les événements de maintenance se produisent. C'est ce qu'on appelle une fenêtre de maintenance. Ces fenêtres permettent de minimiser l'impact de la maintenance sur votre production.

Une fenêtre de maintenance est utilisée chaque fois qu'un événement de maintenance est requis. Vous pouvez définir une fenêtre de maintenance lors de la création d'un flux ou ajouter la fenêtre à un flux existant. Pour modifier le jour et l'heure d'une fenêtre de maintenance, vous pouvez utiliser la MediaConnect console ou le AWS CLI. En outre, si une maintenance est requise, vous pouvez définir une date précise pour qu'elle ait lieu. La date que vous sélectionnez doit être antérieure à la date de maintenance requise.

Si vous ne définissez pas de fenêtre de maintenance, MediaConnect redémarrez les flux pour vous. Nous vous recommandons de définir une fenêtre de maintenance pour chaque flux nécessitant une maintenance.

Pour définir une fenêtre de maintenance (console)

1. Ouvrez la MediaConnect console à l'adresse https://console.aws.amazon.com/mediaconnect/.
2. Dans le volet de navigation, sélectionnez Flux. Lorsqu'un flux nécessite une maintenance, il affiche une date limite dans la colonne de la fenêtre Maintenance.

3. Sélectionnez le ou les flux. Vous pouvez définir une fenêtre de maintenance unique pour chaque flux. Vous pouvez également définir des fenêtres de maintenance en bloc en sélectionnant plusieurs flux.
4. Dans le menu déroulant Actions du flux, sélectionnez Modifier la fenêtre de maintenance du flux.
5.
   - Sélectionnez le jour de la semaine où la maintenance aura lieu dans le champ Jour de début.
   - Sélectionnez l'heure à laquelle la maintenance aura lieu dans le champ Heure de début. L'heure est présentée en UTC.
   - Si une maintenance est requise, vous avez la possibilité de sélectionner une date spécifique dans le champ Date de la fenêtre de maintenance. La date sélectionnée doit être antérieure à la date et à l'heure de maintenance requises.
   - Tâche de sélection Update (Mise à jour).
6. Vous pouvez vérifier la fenêtre en consultant la colonne Fenêtre de maintenance sur le tableau de bord Flows.

Pour définir une fenêtre de maintenance (AWS CLI)

1. Dans le AWS CLI, utilisez la `update-flow` commande avec l'`--maintenance`option. Vous devrez également utiliser l'`--flow-arn`option pour spécifier le flux avec lequel vous travaillez.

   L'`--maintenance`option accepte les arguments suivants :

   - `MaintenanceDay`
   - `MaintenanceStartHour`
   - `MaintenanceScheduleDate`- Cet argument n'est accepté que lorsqu'une date de maintenance requise est attribuée par AWS.
2. Utilisez la commande suivante pour mettre à jour le jour et l'heure de maintenance récurrente. Le jour et l'heure de maintenance peuvent être configurés à tout moment, quel que soit le statut de maintenance requis.

   ```
   aws mediaconnect update-flow --flow-arn arn:aws:mediaconnect:us-
   east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame --
   maintenance MaintenanceDay='Tuesday',MaintenanceStartHour='10:00'
   ```

   L'exemple suivant montre la valeur renvoyée lorsque vous définissez uniquement le MaintenanceDayet MaintenanceStartHour:

```
{
    "Flows": [
        {
            "AvailabilityZone": "us-west-2d",
            "Description": "Example flow description",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
            "Name": "BasketballGame",
            "SourceType": "OWNED",
            "Status": "STANDBY",
            "Maintenance": {
                "MaintenanceDay": "Tuesday",
                "MaintenanceStartHour": "10:00"}
        }
    ]
}
```

3. Utilisez la commande suivante pour définir une date de maintenance spécifique, en plus de définir le jour et l'heure de maintenance récurrente. La date planifiée de maintenance ne peut être définie que lorsqu'AWS a besoin d'une maintenance sur le flux.

```
aws mediaconnect update-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:2-3aBC45dEF67hiJ8k-2AbC34DE5fGa6:AwardsShow --maintenance
 MaintenanceDay='Saturday',MaintenanceStartHour='23:00',MaintenanceScheduledDate='2021-10-2
```

L'exemple suivant montre la valeur renvoyée lorsque vous définissez les valeurs MaintenanceDayMaintenanceStartHour, et MaintenanceScheduledDate:

```
{
    "Flows": [
        {
            "AvailabilityZone": "us-west-2b",
            "Description": "Example flow description",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:2-3aBC45dEF67hiJ8k-2AbC34DE5fGa6:AwardsShow",
            "Name": "AwardsShow",
            "SourceType": "OWNED",
            "Status": "ACTIVE",
            "Maintenance": {
                "MaintenanceDay": "Saturday",
                "MaintenanceDeadline": "2021-10-25T22:15:56Z",
```

```
                "MaintenanceScheduledDate": "2021-10-23",
                "MaintenanceStartHour": "23:00"}
        }
    ]
}
```

Le jour et l'heure sélectionnés sont utilisés pour tous les futurs événements de maintenance récurrents sur ce flux. Répétez ces étapes pour ajouter ou modifier des fenêtres de maintenance supplémentaires. Une fois la maintenance terminée, la colonne État de maintenance du tableau de bord Flows affiche Aucune maintenance requise.

Bonnes pratiques pour MediaConnect

Pour des performances et une disponibilité optimales, suivez les meilleures pratiques lorsque vous configurez vos MediaConnect flux AWS Elemental.

Performances

Les meilleures pratiques suivantes décrivent comment optimiser les performances des flux de transport :

- Assurez-vous d'avoir configuré vos flux de transport avec une bande passante de sortie agrégée allant jusqu'à 400 Mo/s. MediaConnectest conçu pour fonctionner avec une bande passante de sortie agrégée de 400 Mo/s.

  bande passante de sortie agrégée = (débit de la source) x (nombre de sorties)

  Par exemple, si votre flux possède une source avec un débit de 80 Mo/s et 5 sorties, la bande passante de sortie agrégée est de 400 Mo/s. De même, un flux qui possède une source avec un débit de 20 Mo/s et envoie du contenu vers 20 sorties possède également une bande passante de sortie agrégée de 400 Mo/s.

  > **Note**
  >
  > Comme vous pouvez spécifier deux destinations pour une seule sortie ST 2110 JPEG XS, ces sorties doivent être comptées deux fois dans ce calcul.

- Vous pouvez configurer des flux de transport avec des débits allant jusqu'à 120 mégabits par seconde (Mo/s) avec une vidéo en direct de qualité mezzanine.
- Vous pouvez utiliser jusqu'à 20 sorties Fujitsu. Outre les 20 sorties Fujitsu, vous pouvez utiliser jusqu'à 30 sorties autres que Fujitsu. La bande passante de sortie agrégée ne doit pas dépasser 400 Mo/s.

Les meilleures pratiques suivantes décrivent comment optimiser les performances des flux CDI :

- Vous pouvez utiliser jusqu'à 10 sorties pour les flux CDI. De plus, les flux CDI 4Kp60 prennent en charge 10 sorties ST 2110 JPEG XS, mais seulement 4 sorties CDI.

Les meilleures pratiques suivantes décrivent comment optimiser les performances des passerelles :

- L'API peut être utilisée pour démarrer plusieurs ponts à la fois. Si vous démarrez plusieurs ponts à l'aide de l'API, nous vous recommandons de ne pas en démarrer plus de 10 à la fois. Si vous devez démarrer plus de 10 ponts, utilisez plusieurs requêtes.

Disponibilité

- Pour minimiser les pertes de paquets, utilisez des protocoles basés sur la correction d'erreur directe (FEC) ou les protocoles ARQ (Automatic Repeat Request) tels que le protocole Zixi ou RTP-FEC. Ces protocoles sont conçus pour minimiser la perte de paquets entre les périphériques source et de destination.
- La perte de paquets étant présente sur tous les réseaux, même dans les réseaux entièrement gérés tels que le AWS Cloud, vous devez créer et gérer des connexions redondantes tout au long de vos flux de travail. DansMediaConnect, il existe plusieurs manières d'ajouter de la redondance à votre flux de travail :
  - Créez des flux dans au moins deux zones de disponibilité différentes.
  - Ajoutez une deuxième source à chaque flux. S'il y a des erreurs dans le flux, MediaConnect vous pouvez utiliser des paquets provenant d'une source redondante ou passer complètement à la source redondante.
- Nous recommandons que votre organisation crée un VPC spécifique pour tous les services multimédias AWS. Un VPC unique permet de garantir la disponibilité des adresses IP, de définir des règles appropriées dans les groupes de sécurité et de garantir qu'un administrateur réseau ne supprime pas accidentellement les interfaces réseau élastiques.

Fiabilité

- Configurez CloudWatch des métriques et des alarmes Amazon pour suivre l'état de santé de votre source. Pour en savoir plus sur les métriques à surveiller, consultezSurveillance et balisage.

Sécurité

- Le bloc CIDR sur la source de débit doit être aussi précis que possible. N'incluez que les adresses IP autorisées à apporter du contenu à votre flux. Si le bloc CIDR est trop large, il est possible que des tiers envoient du contenu à votre flux.

- Lorsque vous créez un nouveau mot de passe SRT pour chiffrer une sortie SRT, vous devez créer ce mot de passe dans. AWS Secrets Manager AWS Secrets Managern'applique pas de politique de mot de passe spécifique. Nous vous recommandons toutefois de respecter les points de passe suivants :
  - Longueur minimale du mot de passe de 10 caractères et longueur maximale de 80 caractères
  - Au minimum trois des types de caractères suivants : majuscules, minuscules, chiffres et les symboles **! @ # $ % ^ & * ( ) _ + - = [ ] { } | '**
  - Ne pas être identique au nom ou à l'adresse e-mail de votre compte AWS

Quotas dans AWS Elemental MediaConnect

Le tableau suivant décrit les quotas, anciennement appelés limites, dans AWS Elemental MediaConnect. Pour de plus amples informations sur les quotas qui peuvent être modifiés, veuillez consulter Quotas de service AWS.

Ressource	Quota par défaut	Commentaires
Droits	50 par flux	Le nombre maximal de droits que vous pouvez accordez par flux. Vous ne pouvez pas augmenter ce quota.
Flux	20 par AWS région	Le nombre maximum de flux que vous pouvez créer dans chaque AWS région. Vous pouvez demander une augmentation de quota.
Outputs	50 par flux de transport 10 par flux CDI	Le nombre maximal de sorties par flux. Vous ne pouvez pas augmenter ce quota.
Sources	2 par flux de transport 1 par flux CDI	Le nombre maximum de sources qu'un flux peut avoir. Vous ne pouvez pas augmenter ce quota.
Interfaces VPC	2 interfaces ENA et 1 interface EFA par flux	Nombre maximal d'interfaces VPC qu'un flux peut avoir. Vous ne pouvez pas augmenter ce quota.

> **Note**
>
> Pour optimiser les performances, nous vous recommandons de configurer votre flux de travail pour une bande passante de sortie cumulée inférieure ou égale à 400 Mo/s. Pour plus d'informations, veuillez consulter Bonnes pratiques.

Limites pour les demandes d'API

Le tableau suivant décrit les limites de fréquence des demandes d'API dans MediaConnect. Ces limites ne sont pas des quotas que vous pouvez augmenter. Si vous dépassez ces limites, MediaConnect renvoie une erreur HTTP 429 (`too many requests`).

Méthode API	Limite
Fréquence des demandes d'API : état d'équilibre	5 demandes par seconde pour chaque compte dans une région. Cette limite n'est pas un quota que vous pouvez augmenter.
Fréquence des demandes d'API - mode rafale Le mode Burst permet un dépassement temporaire de la limite d'état stable. Si les demandes d'API dépassent la limite du mode rafale, MediaConnect cela réduira la limite et renverra une erreur 429. La limite sera renouvelée à raison de 5 demandes par seconde.	30 demandes par seconde pour chaque compte dans une région. Cette limite n'est pas un quota que vous pouvez augmenter.

> **Note**
>
> Si votre application dépasse ces limites, nous vous recommandons d'implémenter un ralentissement exponentiel pour les nouvelles tentatives. Pour plus d'informations, consultez

Nouvelles tentatives après erreur et interruptions exponentielles dans AWS dans la Référence générale sur Amazon Web Services.

Référence : normes multimédia prises en charge

> **Important**
>
> MediaConnect respecte et met en œuvre de nombreuses normes du secteur des médias établies par différentes organisations. Cette référence n'est pas destinée à être une liste exhaustive, mais contient des normes mises en évidence par des organisations spécifiques.

Forum sur les services vidéo : recommandations techniques

AWS Elemental MediaConnect prend en charge les recommandations techniques (TR) du Video Services Forum (VSF) pour certaines fonctionnalités. Ce guide de référence peut être utilisé pour identifier les TR pris en charge MediaConnect. Pour plus d'informations sur les recommandations techniques, visitez le site Web de VSF : Recommandations techniques de VSF

Recommandations techniques VSF prises en charge

Recommandation technique	Description
TR-06-01 : Transport fiable de flux Internet (RIST) [profil simple]	Cette recommandation technique concerne uniquement le support RIST Simple Profile. MediaConnect ne prend pas en charge les profils principaux, améliorés ou évolutifs lors de l'utilisation de RIST.

TR-07 : Transport de vidéos JPEG XS dans un flux de transport MPEG-2 (TS) sur IP
 	
Important
Le TR-07 est automatiquement invoqué lorsque vous utilisez un protocole pris en charge et que le débit maximal est supérieur à 200 Mbits/s.
	MediaConnect prend en charge le transport JPEG XS au format MPEG-2 TS sur IP avec les exigences et limitations suivantes :
	• En tant que source :
	  • Seul un protocole RTP ou RTP-FEC redondant est pris en charge.
	  • Le débit source maximal est de 500 Mbits/s.
	• En sortie :

Recommandation technique	Description
	• Le protocole de sortie peut être RTP ou RTP-FEC. • Jusqu'à quatre sorties au total peuvent être utilisées, mais la bande passante totale ne doit pas dépasser 1 250 Mbits/s.

Recommandation technique	Description
TR-08 : Transport de vidéos JPEG XS dans ST 2110-22 **Note** Pour les flux directs JPEG XS dans lesquels les images vidéo ne sont pas codées par MediaConnect, les images vidéo ne sont pas décodées. Par conséquent, aucune validation de la conformité à la norme TR-08 n'est effectuée.	MediaConnect prend en charge le transport JPEG XS via le protocole SMPTE ST 2110-22 avec les exigences et limitations suivantes : • Un profil élevé est requis. L'utilisation du profil principal ne provoquera pas d'erreur, mais sera ignorée par MediaConnect. • Un mode entrelacé de 01 (champ supérieur en premier) est requis pour les signaux entrelacés. • Un sous-niveau de 3 bits-per-pixel ou 4 bits-per-pixel est requis. Le sous-niveau dépend du niveau de compression et de la profondeur de pixels que vous utilisez. • Description vidéo Les cases placées dans les images vidéo codées refléteront les valeurs conformes pour le profil, le mode entrelacé et le sous-niveau. • L'enregistrement de la spécification NMOS (Networked Media Open Specification) n'est pas pris en charge. • Mode de transmission de paquets séquentiel RTP (Real-Time Transport Protocol) uniquement. • Mode de mise en paquets Codestream uniquement. Le mode Slice n'est pas pris en charge. Configurations d'espace colorimétrique, de profondeur de bits et d'échantillonnage chromatique prises en charge : • Y CbCr 10 bits 4:2:2

Recommandation technique	Description
	• RGB 10 bits 4:4:4 • RGB 12 bits 4:4:4

SMPTE-2022

MediaConnect supporte de nombreuses normes de la SMPTE (Society of Motion Picture and Television Engineers). Le tableau suivant est spécifique au SMPTE-2022 et inclut une sélection de normes. Il ne s'agit pas d'une liste exhaustive de toutes les normes SMPTE prises en charge.

Normes SMPTE-2022 prises en charge

Standard	Description
SMPTE-2_7 : commutation de protection transparente du RTP	• Sources : MediaConnect prend en charge les sources RTP conformes à cette norme. Pour plus d'informations sur le basculement de source, voir Basculement de source • Sorties : Les sorties RTP et RTP-FEC sont conformes à la norme SMPTE 2_7. Si votre récepteur en aval prend en charge la fusion de sources en 7, les sorties RTP et RTP-FEC seront compatibles.

Ressources supplémentaires

Apprenez-en davantage sur les ressources AWS Elemental MediaConnect et sur d'autres AWS ressources.

Rubriques

Attributions open source d'AWS Elemental MediaConnect

Pour afficher les composants open source utilisés par MediaConnect, téléchargez le fichier suivant :

- MediaConnectOpenSourceAttributions.zip

Informations relatives à AWS Elemental MediaConnect

La liste suivante contient des ressources connexes qui vous seront utiles dans le cadre de votre utilisation d'AWS Elemental MediaConnect.

- Formations et ateliers : liens vers des formations spécialisées et basées sur les rôles, ainsi que des ateliers d'autoformation pour améliorer vos compétences AWS et acquérir une expérience pratique.
- Centre pour développeurs AWS : parcourez des didacticiels, téléchargez des outils et découvrez les événements pour les développeurs AWS.
- Outils pour développeur AWS : liens vers des outils pour développeur, kits SDK, boîtes à outils IDE et outils de ligne de commande pour développer et gérer des applications AWS.
- Centre de ressources pour la mise en route : découvrez comment configurer votre Compte AWS, rejoindre la communauté AWS et lancer votre première application.
- Tutoriels pratiques — Suivez les step-by-step didacticiels pour lancer votre première application surAWS.
- Livres blancs AWS : liens vers une liste complète des livres blancs techniques AWS couvrant des sujets tels que l'architecture, la sécurité et l'économie, créés par des architectes de solutions AWS ou d'autres experts techniques.

- AWS SupportCentre – Hub pour la création et la gestion de vos cas AWS Support. Inclut également des liens vers d'autres ressources utiles, telles que des forums, des FAQ techniques, l'état de santé d'un service et AWS Trusted Advisor.
- AWS Support— La principale page Web contenant des informations sur AWS Support un one-on-one canal d'assistance à réponse rapide pour vous aider à créer et à exécuter des applications dans le cloud.
- Contactez-nous : point de contact central pour toute question relative à la facturation AWS, à votre compte, aux événements, à des abus ou à d'autres problèmes.
- AWSConditions d'utilisation du site : informations détaillées sur nos droits d'auteur et notre marque, sur votre compte, votre licence et votre accès au site, et sur d'autres sujets.

Historique du document pour le guide de l'utilisateur

Le tableau suivant décrit la documentation de cette version d'AWS Elemental MediaConnect. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
moniteur de flux de travail	Analysez AWS les services multimédias et créez des cartes de signaux, des visualisations du flux de travail multimédia, entre ces services. Utilisez les cartes de signaux pour générer des alarmes et des notifications de surveillance à l'aide de CloudWatch EventBridge, et AWS CloudFormation.	11 avril 2024
Recommandation mise à jour du système d'exploitation MediaConnect Gateway	Le système d'exploitation recommandé pour MediaConnect Gateway a été mis à jour de RHEL 8 vers Ubuntu 20.04.	11 mars 2024
Surveillance du flux source : console	Des informations détaillées sur les MediaConnect flux de sources de flux peuvent être consultées à l'aide de la surveillance des métadonnées source dans la MediaConnect console. La surveillance des métadonnées source affiche des informations multimédia sur le flux de transport et ses programmes.	8 mars 2024

Surveillance du flux source : API	Des informations détaillées sur les MediaConnect flux de sources de flux peuvent être consultées à l'aide de l'API de surveillance des métadonnées sources. La surveillance des métadonnées source affiche des informations multimédia sur le flux de transport et ses programmes.	22 décembre 2023
Assistance VSF TR-07	La section de référence des normes multimédia prises en charge a été mise à jour pour refléter la mise en œuvre MediaConnect du TR-07 (transport de vidéos JPEG XS dans un flux de transport MPEG-2 sur IP) du Video Services Forum.	8 décembre 2023
Limites pour les demandes d'API	Le guide a été mis à jour pour inclure les limites des demandes d'API par seconde.	2 novembre 2023
AWS Elemental Link Appareils UHD avec MediaConnect	Vous pouvez désormais utiliser les appareils AWS Elemental Link UHD et le protocole push Zixi comme source de flux. MediaConnect	11 septembre 2023

MediaConnect métriques relatives aux médias	Le guide de l'utilisateur a été mis à jour pour inclure de nouvelles CloudWatch mesures permettant de surveiller l'état des médias transmis à l'aide de ce dernier MediaConnect.	7 septembre 2023
MediaConnect métriques à haute résolution	MediaConnect les métriques peuvent désormais être visualisées à des intervalles aussi courts qu'une seconde.	22 juin 2023
Référence aux normes multimédia prises en charge	Ce guide a été mis à jour pour inclure une liste de référence des normes du secteur des médias prises en charge par MediaConnect.	9 juin 2023
Basculement SRT	Vous pouvez désormais activer le basculement de source et ajouter une seconde source aux flux avec des sources SRT (écouteur ou appelant).	1er mai 2023
Table d'assistance en cas de basculement	Un nouveau tableau a été ajouté qui définit les protocoles sources qui peuvent prendre en charge le basculement.	1er mai 2023
MediaConnect Métriques de la passerelle	Le guide de l'utilisateur a été mis à jour pour inclure de nouvelles CloudWatch mesures relatives à la fonctionnalité MediaConnect Gateway.	13 avril 2023

Politique gérée par AWS - Nouvelle politique	Le MediaConnectGatewayInstanceRolePolicy a été créé.	13 avril 2023
Politique gérée par AWS - Nouvelle politique	Le AWSMediaConnectServicePolicy a été créé.	13 avril 2023
Passerelle AWS Elemental MediaConnect	Une nouvelle fonctionnalité appelée MediaConnect Gateway a été publiée. MediaConnect Gateway dans une implémentation sur site de. MediaConnect	13 avril 2023
AWS rôle lié à un service - Nouveau rôle	Le AWSServiceRoleForMediaConnect rôle a été créé.	13 avril 2023
Mise à jour des directives IAM pour MediaConnect	Mise à jour du guide s'aligner sur les bonnes pratiques IAM. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.	14 février 2023
CloudWatch Événements liés à la santé	De nouveaux CloudWatch événements de surveillance de l'état du flux, de la source et de la sortie ont été ajoutés MediaConnect.	8 février 2023
Support des couleurs pour les protocoles CDI	Un nouveau tableau a été ajouté qui définit l'espace colorimétrique, la profondeur de bits et la prise en charge de l'échantillonnage chromatique pour les protocoles CDI.	4 novembre 2022

MediaConnect Alertes : erreurs de diffusion	Le guide de l'utilisateur a été mis à jour pour inclure des informations sur les alertes d'erreur de diffusion.	27 octobre 2022
Sources et sorties de l'appelant SRT	Vous pouvez désormais utiliser le protocole d'appel SRT pour les sources et les sorties.	19 septembre 2022
Tableau des protocoles de source et de sortie	Une nouvelle table a été ajoutée qui définit les protocoles qui peuvent être utilisés pour les sources, les sorties ou les deux.	5 août 2022
CloudWatch Métriques de maintenance	Le guide de l'utilisateur a été mis à jour pour inclure de nouvelles CloudWatch mesures relatives à la MediaConnect maintenance.	1er août 2022
CloudWatch Événement de maintenance	Le guide de l'utilisateur a été mis à jour pour inclure un nouvel CloudWatch événement de MediaConnect maintenance.	1er août 2022
Chiffrement des mots de passe SRT	La documentation relative au chiffrement des mots de passe SRT a été ajoutée au guide.	31 mai 2022

Fenêtres de maintenance	Vous pouvez désormais planifier des fenêtres de maintenance MediaConnect pour effectuer la maintenance de vos flux. Vous pouvez planifier la maintenance à l'aide des nouveaux outils de planification de la console ou de l'API.	22 mars 2022
Sources et sorties Fujitsu-QOS	Vous pouvez désormais utiliser le protocole Fujitsu-QOS pour les sources et les sorties afin de transporter du contenu vers et depuis les appareils Fujitsu.	20 décembre 2021
Fenêtres de maintenance	Vous pouvez désormais planifier des fenêtres de maintenance MediaConnect pour effectuer la maintenance de vos flux en créant un dossier de support.	31 août 2021
Basculement à la source	Lorsque vous activez le basculement de source, vous pouvez désormais spécifier l'une des deux sources comme source principale. Vous pouvez choisir entre deux modes de basculement pour éviter toute interruption du flux vidéo.	11 juin 2021

Flux de travail CDI	MediaConnect prend désormais en charge le format JPEG XS pour les AWS flux de travail non compressé s avec interface numérique cloud (AWS CDI).	17 mai 2021
Adresse de l'auditeur	Pour les flux qui utilisent des protocoles d'écoute, vous pouvez désormais facilement localiser l'adresse IP sortante d'une sortie pour un Internet privé.	14 avril 2021
Sources et sorties de l'écouteu r SRT	Vous pouvez désormais utiliser le protocole SRT-Liste ner pour les sources et les sorties.	16 mars 2021
Réservations	Vous pouvez désormais acheter des réservations, qui offrent un tarif horaire réduit en échange de l'engagement à utiliser une quantité spécifiqu e de bande passante sortante chaque mois pendant une durée spécifiée.	30 septembre 2020
Désactivation des droits	Vous pouvez désormais désactiver le droit d'arrêter temporairement la diffusion de contenu sur le flux de l'abonné. Lorsque vous êtes prêt à rétablir l'accès, vous pouvez activer le droit.	24 juillet 2020

Indicateurs de santé de la source	Dans la MediaConnect console, vous pouvez consulter CloudWatch les statistiques Amazon qui indiquent l'état de santé de la source sur une période donnée.	11 mai 2020
Sorties VPC	Vous pouvez désormais ajouter une sortie pour envoyer du contenu depuis votre MediaConnect flux AWS Elemental vers votre VPC sans passer par Internet public.	7 avril 2020
Sources en VPC	Vous pouvez désormais connecter votre VPC à votre flux AWS MediaConnect Elemental et envoyer du contenu à votre flux sans passer par Internet public.	31 mars 2020
Basculement à la source	Vous pouvez désormais activer le basculement de source et ajouter une seconde source (redondante) à votre flux.	13 mars 2020
Quotas de service (sorties)	Vous pouvez désormais ajouter jusqu'à 50 sorties à chaque flux de transport.	7 février 2020

Partage des frais de transfert des données d'admissibilité avec l'abonné	Lorsque vous accordez un droit, vous pouvez désormais spécifier le pourcentage des frais de transfert de données d'accès que vous souhaitez que l'abonné soit responsable.	16 septembre 2019
Sources et sorties RIST	Vous pouvez désormais utiliser le protocole RIST pour les sources et les sorties.	11 septembre 2019
Sorties Zixi Pull	Vous pouvez désormais ajouter des sorties utilisant le protocole Zixi Pull.	26 juillet 2019
Support SPEKE	Vous pouvez désormais chiffrer le contenu de vos droits à l'aide de (SPEKE).	25 juin 2019
Quotas de service (flux)	Vous pouvez désormais demander une augmentation du quota de 20 flux par AWS région.	14 mars 2019
Nouveau guide et service	Il s'agit de la version initiale du service d'ingestion et de transport multimédia, AWS MediaConnect Elemental, et du guide de l'utilisateur AWS MediaConnect Elemental.	27 novembre 2018

Note

- Les services AWS multimédias ne sont pas conçus ou destinés à être utilisés avec des applications ou dans des situations nécessitant des performances fiables, telles que les opérations de sécurité des personnes, les systèmes de navigation ou de communication, le contrôle du trafic aérien ou les appareils de survie dans lesquels l'indisponibilité,

l'interruption ou la défaillance des services pourraient entraîner la mort, des blessures, des dommages matériels ou des dommages environnementaux.

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

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.