aws

Guide du développeur

Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka: Guide du développeur

Table of Contents

Bienvenue dans le Manuel du développeur Amazon MSK

Bienvenue dans le Manuel du développeur Amazon MSK. Les rubriques suivantes peuvent vous aider à démarrer avec ce guide, en fonction de ce que vous essayez de faire.

- Créez un cluster Amazon MSK en suivant le didacticiel Mise en route avec Amazon MSK.
- Approfondissez les fonctionnalités d'Amazon MSK dans Amazon MSK : comment ça marche.
- Exécutez Apache Kafka sans avoir à gérer ni à mettre à l'échelle la capacité du cluster avec MSK sans serveur.
- Utilisez MSK Connect pour diffuser des données vers et depuis votre cluster Apache Kafka.
- Réplicateur MSKÀ utiliser pour répliquer les données de manière fiable sur des clusters Amazon MSK situés dans des AWS régions différentes ou identiques.

Pour connaître les détails et les points forts du produit, ainsi que son coût, consultez la page consacrée à Amazon MSK.

Qu'est-ce qu'Amazon MSK ?

Amazon Managed Streaming for Apache Kafka (Amazon MSK) est un service entièrement géré qui vous permet de créer et d'exécuter des applications utilisant Apache Kafka pour traiter des données de diffusion. Amazon MSK fournit les opérations de plan de contrôle, telles que les opérations de création, de mise à jour et de suppression de clusters. Il vous permet d'utiliser les opérations de plan de données Apache Kafka, telles que celles pour la production et la consommation de données. Il exécute des versions open source d'Apache Kafka. Cela signifie que les applications, outils et plug-ins existants des partenaires et de la communauté Apache Kafka sont pris en charge sans nécessiter de modification du code d'application. Vous pouvez utiliser Amazon MSK pour créer des clusters utilisant n'importe quelle version Apache Kafka répertoriées sous the section called “Versions Apache Kafka prises en charge”.

Ces composants décrivent l'architecture d'Amazon MSK :

- Nœuds d'agent : lors de la création d'un cluster Amazon MSK, vous spécifiez le nombre de nœuds d'agent qu'Amazon MSK doit créer dans chaque zone de disponibilité. Le minimum est d'un courtier par zone de disponibilité. Chaque zone de disponibilité dispose de son propre sous-réseau VPC (Virtual Private Cloud).

- ZooKeeper nœuds — Amazon MSK crée également les ZooKeeper nœuds Apache pour vous. Apache ZooKeeper est un serveur open source qui permet une coordination distribuée très fiable.
- Contrôleurs KraFT — La communauté Apache Kafka a développé KraFT pour remplacer Apache ZooKeeper pour la gestion des métadonnées dans les clusters Apache Kafka. En mode KraFT, les métadonnées du cluster sont propagées au sein d'un groupe de contrôleurs Kafka, qui font partie du cluster Kafka, plutôt qu'entre les nœuds. ZooKeeper Les contrôleurs Kraft sont inclus sans frais supplémentaires pour vous et ne nécessitent aucune configuration ou gestion supplémentaire de votre part.

  > **Note**
  >
  > À partir de la version 3.7.x d'Apache Kafka sur MSK, vous pouvez créer des clusters utilisant le mode KraFT au lieu du mode. ZooKeeper

- Producteurs, consommateurs et créateurs de rubriques : Amazon MSK vous permet d'utiliser les opérations de plan de données Apache Kafka pour créer des rubriques ainsi que pour produire et consommer des données.
- Opérations de cluster Vous pouvez utiliser le AWS Management Console, le AWS Command Line Interface (AWS CLI) ou les API du SDK pour effectuer des opérations sur le plan de contrôle. Par exemple, vous pouvez créer ou supprimer un cluster Amazon MSK, répertorier tous les clusters d'un compte, consulter les propriétés d'un cluster et mettre à jour le nombre et le type d'agents dans un cluster.

Amazon MSK détecte et récupère automatiquement les scénarios de défaillance les plus courants pour les clusters. Ainsi, vos applications de producteurs et de consommateurs peuvent poursuivre leurs opérations d'écriture et de lecture avec un impact minimal. Lorsque Amazon MSK détecte une défaillance de l'agent, il l'atténue ou remplace l'agent malsain ou inaccessible par un nouveau. En outre, dans la mesure du possible, il réutilise le stockage de l'ancien agent pour réduire les données qu'Apache Kafka a besoin de répliquer. Votre impact sur la disponibilité est limité au temps nécessaire pour que Amazon MSK termine la détection et la récupération. Après une récupération, vos applications de producteurs et de consommateurs peuvent continuer à communiquer avec les mêmes adresses IP d'agent que celles utilisées avant l'échec.

Configuration d'Amazon MSK

Avant d'utiliser Amazon MSK pour la première fois, exécutez les tâches suivantes.

Tâches

- Inscrivez-vous pour AWS
- Téléchargez les bibliothèques et les outils

Inscrivez-vous pour AWS

Lorsque vous vous inscrivez AWS, votre compte Amazon Web Services est automatiquement connecté à tous les services AWS, y compris Amazon MSK. Seuls les services que vous utilisez vous sont facturés.

Si vous avez déjà un AWS compte, passez à la tâche suivante. Si vous n'avez pas de compte AWS , observez la procédure suivante pour en créer un.

Pour s'inscrire à un compte Amazon Web Services

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. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

Téléchargez les bibliothèques et les outils

Les bibliothèques et les outils suivants vous aident à utiliser Amazon MSK :

- L'AWS Command Line Interface (AWS CLI) prend en charge Amazon MSK. AWS CLI Cela vous permet de contrôler plusieurs Amazon Web Services à partir de la ligne de commande et de les

automatiser par le biais de scripts. Passez AWS CLI à la dernière version pour vous assurer qu'elle prend en charge les fonctionnalités Amazon MSK décrites dans ce guide de l'utilisateur. Pour de plus amples informations sur la mise à niveau de l' AWS CLI, consultez Installation de l' AWS Command Line Interface. Après l'avoir installé AWS CLI, vous devez le configurer. Pour plus d'informations sur la façon de configurer le AWS CLI, consultez aws configure.

- La référence d'API Amazon Managed Streaming for Kafka documente les opérations d'API prises en charge par Amazon MSK.
- Les kits SDK Amazon Web Services pour Go, Java, .NET JavaScript, Node.js, PHP, Python et Ruby incluent le support Amazon MSK et des exemples.

Mise en route avec Amazon MSK

Ce didacticiel présente un exemple de la manière dont vous pouvez créer un cluster MSK, produire et consommer des données et surveiller l'état de votre cluster à l'aide de métriques. Cet exemple ne représente pas toutes les options que vous pouvez choisir lorsque vous créez un cluster MSK. Dans ce didacticiel, nous choisissons à plusieurs reprises les options par défaut par souci de simplicité. Cela ne signifie pas qu'il s'agit des seules options qui fonctionnent pour configurer un cluster MSK ou des instances clients.

Rubriques

Étape 1 : créer un cluster Amazon MSK

Dans cette étape de mise en route avec Amazon MSK, vous créez un cluster Amazon MSK.

Pour créer un cluster Amazon MSK à l'aide du AWS Management Console

1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Choisissez Créer un cluster.
3. Dans Méthode de création, laissez l'option Création rapide sélectionnée. L'option Création rapide vous permet de créer un cluster avec les paramètres par défaut.
4. Dans Nom de cluster, saisissez un nom descriptif pour votre cluster. Par exemple, **`MSKTutorialCluster`**.
5. Dans Propriétés générales du cluster, choisissez Alloué comme type de cluster.
6. À partir du tableau situé sous Tous les paramètres du cluster, copiez les valeurs des paramètres suivants et enregistrez-les car vous en aurez besoin ultérieurement dans ce didacticiel :

- VPC
- Sous-réseaux
- Groupes de sécurité associés au VPC

7. Choisissez Créer un cluster.
8. Vérifiez le Statut du cluster sur la page Résumé du cluster. Le statut passe de Création à Actif à mesure qu'Amazon MSK alloue le cluster. Lorsque le statut est Actif, vous pouvez vous connecter au cluster. Pour de plus amples informations sur le statut des clusters, consultez États du cluster.

Étape suivante

Étape 2 : Créer un rôle IAM

Étape 2 : Créer un rôle IAM

Au cours de cette étape, vous effectuez deux tâches. La première tâche consiste à créer une politique IAM qui autorise l'accès à la création de rubriques sur le cluster et à l'envoi de données vers ces rubriques. La deuxième tâche consiste à créer un rôle IAM et à lui associer cette politique. À une étape ultérieure, vous créez un ordinateur client qui assume ce rôle et l'utilise pour créer une rubrique sur le cluster et pour envoyer des données à cette rubrique.

Pour créer une politique IAM permettant de créer des rubriques et d'y écrire

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Politiques.
3. Choisissez Create Policy (Créer une politique).
4. Choisissez l'onglet JSON, puis remplacez le JSON dans la fenêtre de l'éditeur par le JSON suivant.

   Remplacez *la région* par le code de la AWS région dans laquelle vous avez créé votre cluster. Remplacez *Account-ID* par votre ID de compte. Remplacez *MSK TutorialCluster* par le nom de votre cluster.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:AlterCluster",
                "kafka-cluster:DescribeCluster"
            ],
            "Resource": [
                "arn:aws:kafka:region:Account-ID:cluster/MSKTutorialCluster/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:*Topic*",
                "kafka-cluster:WriteData",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:region:Account-ID:topic/MSKTutorialCluster/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeGroup"
            ],
            "Resource": [
                "arn:aws:kafka:region:Account-ID:group/MSKTutorialCluster/*"
            ]
        }
    ]
}
```

Pour obtenir des instructions sur la rédaction de politiques sécurisées, consultez the section called “Contrôle d'accès IAM”.

5. Choisissez Suivant : Balises.
6. Choisissez Suivant : Vérification.
7. Pour le nom de la politique, entrez un nom descriptif, tel que msk-tutorial-policy.
8. Choisissez Créer une politique.

Pour créer un rôle IAM et lui attacher la politique

1. Dans le panneau de navigation, choisissez Rôles.
2. Sélectionnez Créer un rôle.
3. Sous Cas d'utilisation courants, choisissez EC2, puis Suivant : Autorisations.
4. Dans la zone de recherche, saisissez le nom de la politique que vous avez créée précédemment pour ce didacticiel. Ensuite, cochez la case située à gauche de la politique.
5. Choisissez Suivant : Balises.
6. Choisissez Suivant : Vérification.
7. Pour le nom du rôle, entrez un nom descriptif, tel que msk-tutorial-role.
8. Sélectionnez Créer un rôle.

Étape suivante

Étape 3 : Créer un ordinateur client

Étape 3 : Créer un ordinateur client

Lors de cette étape de Mise en route avec Amazon MSK, vous créez un ordinateur client. Vous utilisez cet ordinateur client pour créer une rubrique qui produit et consomme des données. Pour des raisons de simplicité, vous allez créer cet ordinateur client dans le VPC associé au cluster MSK afin que le client puisse facilement se connecter au cluster.

Pour créer un ordinateur client

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Sélectionnez Lancer des instances.
3. Saisissez un Nom pour votre ordinateur client, tel que **`MSKTutorialClient`**.
4. Laissez Amazon Linux 2 AMI (HVM) - Kernel 5.10, type de volume SSD sélectionné pour le type Amazon Machine Image (AMI).
5. Laissez le type d'instance t2.micro sélectionné.
6. Sous Paire de clés (connexion), choisissez Créer une nouvelle paire de clés. Saisissez **`MSKKeyPair`** dans Nom de la paire de clés, puis choisissez Télécharger la paire de clés. Vous pouvez utiliser également une paire de clés existante.

7. Développez la section Détails avancés et choisissez le rôle IAM que vous avez créé à l'étape 2 : créer un rôle IAM.
8. Choisissez Lancer l'instance.
9. Choisissez View Instances (Afficher les instances). Ensuite, dans la colonne Groupes de sécurité, choisissez le groupe de sécurité associé à votre nouvelle instance. Copiez l'ID du groupe de sécurité et enregistrez-le pour plus tard.
10. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
11. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité). Trouvez le groupe de sécurité dont vous avez enregistré l'identifiant dans the section called “Étape 1 : créer un cluster”.
12. Sous l'onglet Règles entrantes, choisissez Modifier les règles entrantes.
13. Choisissez Ajouter une règle.
14. Dans la nouvelle règle, choisissez Tout le trafic dans la colonne Type . Dans le deuxième champ de la colonne Source, sélectionnez le groupe de sécurité de votre ordinateur client. Il s'agit du groupe dont vous avez enregistré le nom après avoir lancé l'instance d'ordinateur client.
15. Sélectionnez Enregistrer les règles. Le groupe de sécurité du cluster peut désormais accepter le trafic provenant du groupe de sécurité de l'ordinateur client.

Étape suivante

Étape 4 : créer une rubrique

Étape 4 : créer une rubrique

Lors de cette étape de Mise en route avec Amazon MSK, vous installez les bibliothèques clientes et les outils Apache Kafka sur l'ordinateur client, puis vous créez une rubrique.

> ⚠ Warning
>
> Les numéros de version d'Apache Kafka utilisés dans ce didacticiel ne sont que des exemples. Nous vous recommandons d'utiliser la même version du client que votre version de cluster MSK. Certaines fonctionnalités et correctifs de bogues critiques peuvent être absents d'une ancienne version du client.

Pour rechercher la version de votre cluster MSK

1. Rendez-vous sur https://eu-west-2.console.aws.amazon.com/msk/
2. Sélectionnez le cluster MSK.
3. Notez la version d'Apache Kafka utilisée sur le cluster.
4. Remplacez les instances des numéros de version d'Amazon MSK dans ce didacticiel par la version obtenue à l'étape 3.

Pour créer une rubrique sur l'ordinateur client

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances. Ensuite, cochez la case en regard du nom de l'ordinateur client que vous avez créé dans Étape 3 : Créer un ordinateur client.
3. Choisissez Actions, puis Modifier. Suivez les instructions dans la console pour vous connecter à votre ordinateur client.
4. Installez Java sur l'ordinateur client en exécutant la commande suivante :

```
sudo yum -y install java-11
```

5. Exécutez la commande suivante pour télécharger Apache Kafka.

```
wget https://archive.apache.org/dist/kafka/{YOUR MSK VERSION}/kafka_2.13-{YOUR MSK
 VERSION}.tgz
```

> **Note**
>
> Si vous souhaitez utiliser un site miroir autre que celui utilisé dans cette commande, vous pouvez en choisir un autre sur le site web Apache.

6. Exécutez la commande suivante dans le répertoire où vous avez téléchargé le fichier TAR à l'étape précédente.

```
tar -xzf kafka_2.13-{YOUR MSK VERSION}.tgz
```

7. Accédez au répertoire `kafka_2.13-{YOUR MSK VERSION}/libs`, puis exécutez la commande suivante pour télécharger le fichier Amazon MSK IAM JAR. Le fichier Amazon MSK IAM JAR permet à l'ordinateur client d'accéder au cluster.

```
wget https://github.com/aws/aws-msk-iam-auth/releases/download/v1.1.1/aws-msk-iam-auth-1.1.1-all.jar
```

8. Accédez au répertoire `kafka_2.13-{YOUR MSK VERSION}/bin`. Copiez les paramètres de propriété suivants et collez-les dans un nouveau fichier. Nommez le fichier **`client.properties`** et enregistrez-le.

```
security.protocol=SASL_SSL
sasl.mechanism=AWS_MSK_IAM
sasl.jaas.config=software.amazon.msk.auth.iam.IAMLoginModule required;
sasl.client.callback.handler.class=software.amazon.msk.auth.iam.IAMClientCallbackHandler
```

9. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
10. Attendez que le statut de votre cluster devienne Actif. Cela peut prendre plusieurs minutes. Lorsque le statut devient Actif, choisissez le nom du cluster. Cela vous amène à une page contenant le récapitulatif du cluster.
11. Choisissez Afficher les informations sur le client.
12. Copiez la chaîne de connexion pour le point de terminaison privé.

    Vous obtiendrez trois points de terminaison pour chacun des agents. Vous n'avez besoin que d'un seul point de terminaison d'agent pour l'étape suivante.
13. Exécutez la commande suivante en remplaçant *`BootstrapServerString`* par l'un des points de terminaison du broker que vous avez obtenus à l'étape précédente.

```
<path-to-your-kafka-installation>/bin/kafka-topics.sh --create --bootstrap-server
 BootstrapServerString --command-config client.properties --replication-factor 3 --
partitions 1 --topic MSKTutorialTopic
```

    Si la commande réussit, le message suivant s'affiche : `Created topic MSKTutorialTopic.`

Étape suivante

Étape 5 : Produire et consommer des données

Étape 5 : Produire et consommer des données

Lors de cette étape de Mise en route avec Amazon MSK, vous produisez et consommez des données.

Pour produire et consommer des messages

1. Exécutez la commande suivante pour démarrer un producteur de console. Remplacez *BootstrapServerString* par la chaîne de connexion en texte brut que vous avez obtenue dans Créer un sujet. Pour obtenir des instructions sur la récupération de cette chaîne de connexion, consultez Obtention des agents d'amorçage pour un cluster Amazon MSK.

   ```
   <path-to-your-kafka-installation>/bin/kafka-console-producer.sh --
   broker-list BootstrapServerString --producer.config client.properties --
   topic MSKTutorialTopic
   ```

2. Saisissez le message souhaité, puis appuyez sur Entrée. Répétez cette étape deux ou trois fois. Chaque fois que vous entrez une ligne et appuyez sur Entrée, cette ligne est envoyée à votre cluster Apache Kafka sous forme de message distinct.
3. Gardez la connexion à l'ordinateur client ouverte, puis ouvrez une deuxième connexion séparée à cet ordinateur dans une nouvelle fenêtre.
4. Dans la commande suivante, remplacez *BootstrapServerString par la chaîne* de connexion en texte brut que vous avez enregistrée précédemment. Ensuite, pour créer un consommateur de console, exécutez la commande suivante avec votre deuxième connexion à l'ordinateur client.

   ```
   <path-to-your-kafka-installation>/bin/kafka-console-consumer.sh --bootstrap-
   server BootstrapServerString --consumer.config client.properties --
   topic MSKTutorialTopic --from-beginning
   ```

   Vous commencez à voir les messages que vous avez entrés plus tôt lorsque vous avez utilisé la commande du producteur de la console.
5. Entrez d'autres messages dans la fenêtre du producteur et regardez-les apparaître dans la fenêtre du consommateur.

Étape suivante

Étape 6 : Utiliser Amazon CloudWatch pour consulter les métriques Amazon MSK

Étape 6 : Utiliser Amazon CloudWatch pour consulter les métriques Amazon MSK

Dans cette étape de Getting Started Using Amazon MSK, vous examinez les métriques Amazon MSK sur Amazon. CloudWatch

Pour consulter les statistiques Amazon MSK dans CloudWatch

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Choisissez l'onglet Toutes les métriques, puis AWS/Kafka.
4. Pour afficher les métriques au niveau du broker, choisissez ID du broker, Nom du cluster. Pour les métriques au niveau du cluster, choisissez Nom du cluster.
5. (Facultatif) Dans le volet graphique, sélectionnez une statistique et une période, puis créez une CloudWatch alarme à l'aide de ces paramètres.

Étape suivante

Étape 7 : Supprimer les AWS ressources créées pour ce didacticiel

Étape 7 : Supprimer les AWS ressources créées pour ce didacticiel

À l'étape finale de Mise en route avec Amazon MSK, vous supprimez le cluster MSK et l'ordinateur client que vous avez créés pour ce didacticiel.

Pour supprimer les ressources à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez le nom de votre cluster. Par exemple, MSK TutorialCluster.
3. Choisissez Actions, puis Delete (Supprimer).
4. Ouvrez la console Amazon EC2 à l’adresse https://console.aws.amazon.com/ec2/.
5. Choisissez l'instance que vous avez créée pour votre ordinateur client, par exemple, **`MSKTutorialClient`**.
6. Choisissez État de l'instance, puis Résilier l'instance.

Pour supprimer la politique et le rôle IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Rôles.
3. Dans la zone de recherche, saisissez le nom du rôle IAM que vous avez créé pour ce didacticiel.
4. Choisissez le rôle. Ensuite, choisissez Supprimer le rôle et confirmez la suppression.
5. Dans le panneau de navigation, choisissez Politiques.
6. Dans la zone de recherche, saisissez le nom de la politique que vous avez créée pour ce didacticiel.
7. Choisissez la politique pour ouvrir sa page récapitulative. Sur la page Récapitulatif de la politique, choisissez Supprimer la politique.
8. Sélectionnez Supprimer.

Amazon MSK : comment ça marche

Un cluster Amazon MSK est la ressource Amazon MSK principale que vous pouvez créer dans votre compte. Les rubriques de cette section expliquent comment effectuer les opérations Amazon MSK courantes. Pour obtenir la liste de toutes les opérations que vous pouvez effectuer sur un cluster MSK, consultez les rubriques suivantes :

- L'interface AWS Management Console
- La référence de l'API Amazon MSK
- La référence des commandes de la CLI Amazon MSK

Rubriques

Création d'un cluster Amazon MSK

> **Important**
>
> Vous ne pouvez pas modifier le VPC d'un cluster Amazon MSK après avoir créé le cluster.

Avant de pouvoir créer un cluster Amazon MSK, vous devez posséder un Amazon Virtual Private Cloud (VPC) et configurer des sous-réseaux dans ce dernier.

Vous avez besoin de deux sous-réseaux situés dans deux zones de disponibilité différentes dans la région USA Ouest (Californie du Nord). Pour les autres régions où Amazon MSK est disponible, vous pouvez spécifier deux ou trois sous-réseaux. Vos sous-réseaux doivent être dans des zones de disponibilité différentes. Lorsque vous créez un cluster, Amazon MSK répartit les nœuds d'agent uniformément entre les sous-réseaux que vous spécifiez.

Tailles des courtiers

Lorsque vous créez un cluster Amazon MSK, vous spécifiez la taille des courtiers que vous souhaitez lui attribuer. Amazon MSK prend en charge les tailles de broker suivantes :

- kafka.t3.small
- kafka.m5.large, kafka.m5.xlarge, kafka.m5.2xlarge, kafka.m5.4xlarge, kafka.m5.8xlarge, kafka.m5.12xlarge, kafka.m5.16xlarge, kafka.m5.24xlarge
- kafka.m7g.large, kafka.m7g.xlarge, kafka.m7g.2xlarge, kafka.m7g.4xlarge, kafka.m7g.8xlarge, kafka.m7g.12xlarge, kafka.m7g.16xlarge

Les courtiers m7G utilisent des processeurs AWS Graviton (processeurs ARM personnalisés conçus par Amazon Web Services). Les courtiers M7g offrent une meilleure performance en termes de prix par rapport aux instances M5 comparables. Les courtiers M7g consomment moins d'énergie que les instances M5 comparables.

Les courtiers M7g Graviton ne sont pas disponibles dans les régions suivantes : CDG (Paris), CGK (Jakarta), CPT (Le Cap), DXB (Dubaï), HKG (Hong Kong), KIX (Osaka), LHR (Londres), MEL (Melbourne), MXP (Milan), OSU (États-Unis Est), PDT (États-Unis Ouest), TLV (Tel Aviv), YYC (Calgary), ZRH (Zürich).

MSK prend en charge les courtiers m7G sur les clusters exécutant l'une des versions de Kafka suivantes :

- 2.8.2. à plusieurs niveaux
- 3.3.2
- 3.4.0
- 3.5.1
- 3.6.0 avec stockage hiérarchisé
- 3,7. x
- 3.7.x.kraft

Les courtiers M7g et M5 présentent des performances de débit de référence supérieures à celles des courtiers T3 et sont recommandés pour les charges de travail de production. Les courtiers M7g et M5 peuvent également avoir plus de partitions par courtier que les courtiers T3. Utilisez les courtiers M7g ou M5 si vous exécutez des charges de travail de production plus importantes ou si vous avez besoin d'un plus grand nombre de partitions. Pour en savoir plus sur les tailles d'instance M7g et M5, consultez la section Instances à usage général Amazon EC2.

Les agents T3 ont la possibilité d'utiliser des crédits CPU pour augmenter temporairement les performances. Utilisez les agents T3 pour le développement à faible coût, si vous testez de petites ou de moyennes charges de travail de streaming ou si vous avez des charges de travail de streaming à faible débit qui peuvent connaître des pics. Nous vous recommandons d' proof-of-concept effectuer un test pour déterminer si les courtiers T3 sont suffisants pour la production ou pour une charge de travail critique. Pour en savoir plus sur la taille des courtiers T3, consultez Amazon EC2T3 Instances.

Pour plus d'informations sur le choix de la taille des courtiers, consultezBonnes pratiques.

Création d'un cluster à l'aide du AWS Management Console

Ce processus décrit la tâche courante qui consiste à créer un cluster provisionné à l'aide d'options de création personnalisées. Vous pouvez sélectionner d'autres options dans la console MSK pour créer un cluster sans serveur.

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez Créer un cluster.

3. Pour la méthode de création du cluster, choisissez Création personnalisée.
4. Spécifiez un nom de cluster unique ne comportant pas plus de 64 caractères.
5. Pour le type de cluster, choisissez Provisioned, qui vous permet de spécifier le nombre de courtiers, la taille du courtier et la capacité de stockage du cluster.
6. Sélectionnez la version d'Apache Kafka que vous souhaitez exécuter sur les courtiers. Pour voir une comparaison des fonctionnalités MSK prises en charge par chaque version d'Apache Kafka, sélectionnez Afficher la compatibilité des versions.
7. Selon la version d'Apache Kafka que vous sélectionnez, vous pouvez choisir le mode Metadata du cluster : ZooKeeper ou Kraft.
8. Sélectionnez la taille de courtier à utiliser pour le cluster en fonction des besoins de calcul, de mémoire et de stockage du cluster. Voir ???,
9. Sélectionnez le nombre de zones dans lesquelles les courtiers sont répartis.
10. Spécifiez le nombre de courtiers que vous souhaitez que MSK crée dans chaque zone de disponibilité. Le minimum est d'un courtier par zone de disponibilité et le maximum est de 30 courtiers par cluster pour les clusters ZooKeeper basés et de 60 courtiers par cluster pour les clusters basés sur Kraft.
11. Sélectionnez la quantité initiale de stockage que vous souhaitez attribuer à votre cluster. Vous ne pouvez pas réduire la capacité de stockage après avoir créé le cluster.
12. En fonction de la taille du courtier (taille de l'instance) que vous avez sélectionnée, vous pouvez spécifier le débit de stockage provisionné par courtier. Pour activer cette option, choisissez la taille du broker (taille de l'instance) kafka.m5.4xlarge ou supérieure pour x86, et kafka.m7g.2xlarge ou supérieure pour les instances basées sur Graviton. veuillez consulter ???.
13. Sélectionnez une option de mode de stockage en cluster, soit le stockage EBS uniquement, soit le stockage hiérarchisé et le stockage EBS.
14. Si vous souhaitez créer et utiliser une configuration de cluster personnalisée (ou si vous avez déjà enregistré une configuration de cluster), choisissez-en une. Sinon, vous pouvez créer le cluster en utilisant la configuration de cluster par défaut d'Amazon MSK. Pour de plus amples informations sur les configurations Amazon MSK, veuillez consulter Configuration.
15. Sélectionnez Suivant.
16. Pour les paramètres réseau, choisissez le VPC que vous souhaitez utiliser pour le cluster.
17. Sur la base du nombre de zones que vous avez précédemment sélectionné, spécifiez les zones de disponibilité et les sous-réseaux dans lesquels les courtiers seront déployés. Les sous-réseaux doivent se trouver dans des zones de disponibilité différentes.

18. Vous pouvez sélectionner un ou plusieurs groupes de sécurité auxquels vous souhaitez donner accès à votre cluster (par exemple, les groupes de sécurité des machines clientes). Si vous spécifiez des groupes de sécurité partagés avec vous, vous devez vous assurer que vous êtes autorisé à les utiliser. Vous devez disposer en particulier de l'autorisation `ec2:DescribeSecurityGroups`. Connexion à un cluster Amazon MSK.
19. Sélectionnez Suivant.
20. Sélectionnez les méthodes de contrôle d'accès et les paramètres de chiffrement du cluster pour chiffrer les données lors de leur transit entre les clients et les courtiers. Pour plus d'informations, consultez the section called "Chiffrement en transit".
21. Choisissez la clé KMS que vous souhaitez utiliser pour chiffrer les données au repos. Pour plus d'informations, consultez the section called "Chiffrement au repos".
22. Sélectionnez Suivant.
23. Choisissez le monitoring et les tags souhaités. Cela détermine l'ensemble de mesures que vous obtenez. Pour plus d'informations, consultez Surveillance d'un cluster. Amazon CloudWatch, Prometheus, Broker log delivery ou Cluster tags, puis sélectionnez Next.
24. Vérifiez les paramètres de votre cluster. Vous pouvez revenir en arrière et modifier les paramètres en sélectionnant Précédent pour revenir à l'écran de console précédent, ou Modifier pour modifier des paramètres de cluster spécifiques. Si les paramètres sont corrects, sélectionnez Créer un cluster.
25. Vérifiez le Statut du cluster sur la page Résumé du cluster. Le statut passe de Création à Actif à mesure qu'Amazon MSK alloue le cluster. Lorsque le statut est Actif, vous pouvez vous connecter au cluster. Pour de plus amples informations sur le statut des clusters, consultez États du cluster.

Création d'un cluster à l'aide du AWS CLI

1. Copiez le JSON suivant et enregistrez-le dans un fichier. Nommez le fichier `brokernodegroupinfo.json`. Remplacez les ID de sous-réseau dans le JSON par les valeurs correspondant à vos sous-réseaux. Les sous-réseaux doivent se trouver dans des zones de disponibilité différentes. Remplacez *« Security-Group-ID »* par l'ID d'un ou de plusieurs groupes de sécurité du VPC client. Les clients associés à ces groupes de sécurité ont accès au cluster. Si vous spécifiez des groupes de sécurité qui ont été partagés avec vous, vous devez vous assurer que vous disposez des autorisations pour ces groupes. Vous devez disposer en particulier de l'autorisation `ec2:DescribeSecurityGroups`. Par exemple, veuillez

consulter Amazon EC2 : permet la gestion des groupes de sécurité EC2 associés à un VPC spécifique, par programmation et dans la console. Enfin, enregistrez le fichier JSON mis à jour sur l'ordinateur sur lequel vous l'avez AWS CLI installé.

```
{
  "InstanceType": "kafka.m5.large",
  "ClientSubnets": [
    "Subnet-1-ID",
    "Subnet-2-ID"
  ],
  "SecurityGroups": [
    "Security-Group-ID"
  ]
}
```

> **Important**
>
> Spécifiez exactement deux sous-réseaux si vous utilisez la région USA Ouest (Californie du Nord). Pour les autres régions où Amazon MSK est disponible, vous pouvez spécifier deux ou trois sous-réseaux. Les sous-réseaux que vous spécifiez doivent se trouver dans des zones de disponibilité distinctes. Lorsque vous créez un cluster, Amazon MSK répartit les nœuds d'agent uniformément entre les sous-réseaux que vous spécifiez.

2. Exécutez la AWS CLI commande suivante dans le répertoire où vous avez enregistré le `brokernodegroupinfo.json` fichier, en remplaçant *« Your-Cluster-Name » par le nom* de votre choix. Pour *« Monitoring-Level »*, vous pouvez spécifier l'une des trois valeurs suivantes : `DEFAULT`, `PER_BROKER` ou `PER_TOPIC_PER_BROKER`. Pour de plus amples informations sur ces trois niveaux de surveillance, veuillez consulter ???. Le paramètre `enhanced-monitoring` est facultatif. Si vous ne le spécifiez pas dans la commande `create-cluster`, vous obtenez le niveau de surveillance `DEFAULT`.

```
aws kafka create-cluster --cluster-name "Your-Cluster-Name" --broker-node-group-
info file://brokernodegroupinfo.json --kafka-version "2.8.1" --number-of-broker-
nodes 3 --enhanced-monitoring "Monitoring-Level"
```

La sortie de la commande ressemble au JSON suivant :

```
{
    "ClusterArn": "...",
```

```
    "ClusterName": "AWSKafkaTutorialCluster",
    "State": "CREATING"
}
```

> **Note**
>
> La commande `create-cluster` peut renvoyer une erreur indiquant qu'un ou plusieurs sous-réseaux appartiennent à des zones de disponibilité non prises en charge. Lorsque cela se produit, l'erreur indique quelles zones de disponibilité ne sont pas prises en charge. Créez des sous-réseaux qui n'utilisent pas les zones de disponibilité non prises en charge et réessayez la commande `create-cluster`.

3. Enregistrez la valeur de la clé `ClusterArn` car vous en avez besoin pour effectuer d'autres actions sur votre cluster.
4. Exécutez la commande suivante pour vérifier votre cluster `STATE`. La valeur `STATE` passe de `CREATING` à `ACTIVE`, lorsqu'Amazon MSK approvisionne le cluster. Lorsque le statut est `ACTIVE`, vous pouvez vous connecter au cluster. Pour de plus amples informations sur le statut des clusters, consultez États du cluster.

```
aws kafka describe-cluster --cluster-arn <your-cluster-ARN>
```

Création d'un cluster avec une configuration Amazon MSK personnalisée à l'aide du AWS CLI

Pour de plus amples informations sur les configurations Amazon MSK personnalisées et sur la façon de les créer, veuillez consulter Configuration.

1. Enregistrez le JSON suivant dans un fichier, en remplaçant *`configuration-arn`* par l'ARN de la configuration que vous souhaitez utiliser pour créer le cluster.

```
{
    "Arn": configuration-arn,
    "Revision": 1
}
```

2. Exécutez la commande `create-cluster` et utilisez l'option `configuration-info` pour pointer vers le fichier JSON que vous avez enregistré à l'étape précédente. Voici un exemple.

```
aws kafka create-cluster --cluster-name ExampleClusterName --broker-node-group-
info file://brokernodegroupinfo.json --kafka-version "2.8.1" --number-of-broker-
nodes 3 --enhanced-monitoring PER_TOPIC_PER_BROKER --configuration-info file://
configuration.json
```

Voici un exemple de réponse réussie après l'exécution de cette commande.

```
{
    "ClusterArn": "arn:aws:kafka:us-east-1:123456789012:cluster/
CustomConfigExampleCluster/abcd1234-abcd-dcba-4321-a1b2abcd9f9f-2",
    "ClusterName": "CustomConfigExampleCluster",
    "State": "CREATING"
}
```

Création d'un cluster à l'aide de l'API

Pour créer un cluster à l'aide de l'API, consultez CreateCluster.

Suppression d'un cluster Amazon MSK

> **Note**
>
> Si votre cluster dispose d'une politique d'autoscaling, nous vous recommandons de supprimer cette politique avant de supprimer le cluster. Pour plus d'informations, consultez Dimensionnement automatique.

Suppression d'un cluster à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Sélectionnez le cluster MSK que vous souhaitez supprimer en cochant la case en regard de celui-ci.
3. Choisissez Supprimer et confirmez la suppression.

Suppression d'un cluster à l'aide du AWS CLI

Exécutez la commande suivante, en la *ClusterArn*remplaçant par le Amazon Resource Name (ARN) que vous avez obtenu lors de la création de votre cluster. Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d'informations, consultez the section called "Liste des clusters".

```
aws kafka delete-cluster --cluster-arn ClusterArn
```

Suppression d'un cluster à l'aide de l'API

Pour supprimer un cluster à l'aide de l'API, consultez DeleteCluster.

Obtention des agents d'amorçage pour un cluster Amazon MSK

Faire en sorte que les courtiers Bootstrap utilisent le AWS Management Console

Le terme agents d'amorçage désigne une liste d'agents qu'un client Apache Kafka peut utiliser comme point de départ pour se connecter au cluster. Cette liste n'inclut pas nécessairement tous les agents d'un cluster.

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Le tableau présente tous les clusters de la région actuelle sous ce compte. Choisissez le nom d'un cluster pour afficher sa description.
3. Sur la page de résumé du cluster, choisissez Voir les informations client. Cela vous montre les courtiers bootstrap, ainsi que la chaîne de ZooKeeper connexion Apache.

Faire en sorte que les courtiers Bootstrap utilisent le AWS CLI

Exécutez la commande suivante, en la *ClusterArn*remplaçant par le Amazon Resource Name (ARN) que vous avez obtenu lors de la création de votre cluster. Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d'informations, consultez the section called "Liste des clusters".

```
aws kafka get-bootstrap-brokers --cluster-arn ClusterArn
```

Pour un cluster MSK qui utilise the section called “Contrôle d'accès IAM”, la sortie de cette commande ressemble à l'exemple JSON suivant.

```
{
    "BootstrapBrokerStringSaslIam": "b-1.myTestCluster.123z8u.c2.kafka.us-
west-1.amazonaws.com:9098,b-2.myTestCluster.123z8u.c2.kafka.us-
west-1.amazonaws.com:9098"
}
```

L'exemple suivant montre les agents d'amorçage d'un cluster dont l'accès public est activé. Utilisez le `BootstrapBrokerStringPublicSaslIam` pour l'accès public et la `BootstrapBrokerStringSaslIam` chaîne pour l'accès depuis l'intérieur AWS.

```
{
    "BootstrapBrokerStringPublicSaslIam": "b-2-public.myTestCluster.v4ni96.c2.kafka-
beta.us-east-1.amazonaws.com:9198,b-1-public.myTestCluster.v4ni96.c2.kafka-
beta.us-east-1.amazonaws.com:9198,b-3-public.myTestCluster.v4ni96.c2.kafka-beta.us-
east-1.amazonaws.com:9198",
    "BootstrapBrokerStringSaslIam": "b-2.myTestCluster.v4ni96.c2.kafka-
beta.us-east-1.amazonaws.com:9098,b-1.myTestCluster.v4ni96.c2.kafka-beta.us-
east-1.amazonaws.com:9098,b-3.myTestCluster.v4ni96.c2.kafka-beta.us-
east-1.amazonaws.com:9098"
}
```

La chaîne des agents d'amorçage doit contenir trois agents issus des zones de disponibilité dans lesquelles votre cluster MSK est déployé (sauf si deux agents seulement sont disponibles).

Obtention des agents d'amorçage à l'aide de l'API

Pour que les courtiers bootstrap utilisent l'API, consultez GetBootstrapBrokers.

Liste des clusters Amazon MSK

Lister les clusters à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Le tableau présente tous les clusters de la région actuelle sous ce compte. Choisissez le nom d'un cluster pour afficher ses détails.

Lister les clusters à l'aide du AWS CLI

Exécutez la commande suivante.

```
aws kafka list-clusters
```

Liste des clusters à l'aide de l'API

Pour répertorier les clusters à l'aide de l'API, consultez ListClusters.

Gestion des métadonnées

Amazon MSK prend en charge les modes de gestion des métadonnées Apache ZooKeeper ou Kraft.

À partir de la version 3.7.x d'Apache Kafka sur Amazon MSK, vous pouvez créer des clusters utilisant le mode KraFT au lieu du mode. ZooKeeper Les clusters basés sur Kraft s'appuient sur des contrôleurs au sein de Kafka pour gérer les métadonnées.

Rubriques

- ZooKeeper mode
- Mode Kraft

ZooKeeper mode

Apache ZooKeeper est « un service centralisé permettant de gérer les informations de configuration, de nommer, de fournir une synchronisation distribuée et de fournir des services de groupe. Tous ces types de services sont utilisés sous une forme ou une autre par des applications distribuées », notamment Apache Kafka.

Si votre cluster utilise le ZooKeeper mode, vous pouvez suivre les étapes ci-dessous pour obtenir la chaîne de ZooKeeper connexion Apache. Cependant, nous vous recommandons d'utiliser le `BootstrapServerString` pour vous connecter à votre cluster et effectuer des opérations d'administration, car l'`--zookeeper`indicateur est devenu obsolète dans Kafka 2.5 et a été supprimé dans Kafka 3.0.

Obtenir la chaîne de ZooKeeper connexion Apache à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Le tableau présente tous les clusters de la région actuelle sous ce compte. Choisissez le nom d'un cluster pour afficher sa description.
3. Sur la page de résumé du cluster, choisissez Voir les informations client. Cela vous montre les courtiers bootstrap, ainsi que la chaîne de ZooKeeper connexion Apache.

Obtenir la chaîne de ZooKeeper connexion Apache à l'aide du AWS CLI

1. Si vous ne connaissez pas le nom Amazon Resource Name (ARN) de votre cluster, vous pouvez le trouver en listant tous les clusters de votre compte. Pour plus d'informations, consultez the section called "Liste des clusters".
2. Pour obtenir la chaîne de ZooKeeper connexion Apache, ainsi que d'autres informations sur votre cluster, exécutez la commande suivante, en la *ClusterArn*remplaçant par l'ARN de votre cluster.

```
aws kafka describe-cluster --cluster-arn ClusterArn
```

La sortie de cette commande `describe-cluster` ressemble à l'exemple JSON suivant.

```
{
    "ClusterInfo": {
        "BrokerNodeGroupInfo": {
            "BrokerAZDistribution": "DEFAULT",
            "ClientSubnets": [
                "subnet-0123456789abcdef0",
                "subnet-2468013579abcdef1",
                "subnet-1357902468abcdef2"
            ],
            "InstanceType": "kafka.m5.large",
            "StorageInfo": {
                "EbsStorageInfo": {
                    "VolumeSize": 1000
                }
            }
        },
```

```
        "ClusterArn": "arn:aws:kafka:us-east-1:111122223333:cluster/
testcluster/12345678-abcd-4567-2345-abcdef123456-2",
        "ClusterName": "testcluster",
        "CreationTime": "2018-12-02T17:38:36.75Z",
        "CurrentBrokerSoftwareInfo": {
            "KafkaVersion": "2.2.1"
        },
        "CurrentVersion": "K13V1IB3VIYZZH",
        "EncryptionInfo": {
            "EncryptionAtRest": {
                "DataVolumeKMSKeyId": "arn:aws:kms:us-
east-1:555555555555:key/12345678-abcd-2345-ef01-abcdef123456"
            }
        },
        "EnhancedMonitoring": "DEFAULT",
        "NumberOfBrokerNodes": 3,
        "State": "ACTIVE",
        "ZookeeperConnectString": "10.0.1.101:2018,10.0.2.101:2018,10.0.3.101:2018"
    }
}
```

L'exemple JSON précédent montre la clé `ZookeeperConnectString` dans la sortie de la commande `describe-cluster`. Copiez la valeur correspondant à cette clé et enregistrez-la pour pouvoir la réutiliser lorsque vous devrez créer une rubrique sur votre cluster.

> **Important**
>
> Votre cluster Amazon MSK doit être en bon `ACTIVE` état pour que vous puissiez obtenir la chaîne de ZooKeeper connexion Apache. Lorsqu'un cluster a toujours l'état `CREATING`, la sortie de la commande `describe-cluster` n'inclut pas `ZookeeperConnectString`. Si c'est le cas, attendez quelques minutes, puis exécutez à nouveau `describe-cluster` après que votre cluster a atteint l'état `ACTIVE`.

Obtenir la chaîne de ZooKeeper connexion Apache à l'aide de l'API

Pour obtenir la chaîne de ZooKeeper connexion Apache à l'aide de l'API, consultez DescribeCluster.

Mode Kraft

Amazon MSK a introduit la prise en charge de KraFT (Apache Kafka Raft) dans la version 3.7.x de Kafka. La communauté Apache Kafka a développé Kraft pour remplacer Apache ZooKeeper pour la gestion des métadonnées dans les clusters Apache Kafka. En mode KraFT, les métadonnées du cluster sont propagées au sein d'un groupe de contrôleurs Kafka, qui font partie du cluster Kafka, plutôt qu'entre les nœuds. ZooKeeper Les contrôleurs Kraft sont inclus sans frais supplémentaires pour vous et ne nécessitent aucune configuration ou gestion supplémentaire de votre part. Consultez KIP-500 pour plus d'informations sur KraFT.

Voici quelques points à noter concernant le mode KraFT sur MSK :

- Le mode KraFT n'est disponible que pour les nouveaux clusters. Vous ne pouvez pas changer de mode de métadonnées une fois le cluster créé.
- Sur la console MSK, vous pouvez créer un cluster basé sur Kraft en choisissant Kafka version 3.7.x et en cochant la case KraFT dans la fenêtre de création du cluster.
- Pour créer un cluster en mode KraFT à l'aide de l'API `CreateCluster`ou `CreateClusterV2`des opérations MSK, vous devez utiliser `3.7.x.kraft` comme version. À utiliser `3.7.x` comme version pour créer un cluster en ZooKeeper mode.
- Le nombre de partitions par broker est le même sur KraFT et sur les clusters ZooKeeper basés. Cependant, KraFT vous permet d'héberger un plus grand nombre de partitions par cluster en fournissant un plus grand nombre de courtiers dans un cluster.
- Aucune modification d'API n'est requise pour utiliser le mode Kraft sur Amazon MSK. Toutefois, si vos clients utilisent toujours la chaîne de `--zookeeper` connexion aujourd'hui, vous devez mettre à jour vos clients afin qu'ils utilisent la chaîne de `--bootstrap-server` connexion pour se connecter à votre cluster. L'`--zookeeper`indicateur est obsolète dans la version 2.5 d'Apache Kafka et est supprimé à partir de la version 3.0 de Kafka. Nous vous recommandons donc d'utiliser les versions récentes du client Apache Kafka et la chaîne de `--bootstrap-server` connexion pour toutes les connexions à votre cluster.
- ZooKeeper le mode continue d'être disponible pour toutes les versions publiées où zookeeper est également pris en charge par Apache Kafka. Consultez Versions Apache Kafka prises en charge pour plus de détails sur la fin du support pour les versions d'Apache Kafka et les futures mises à jour.
- Vous devez vérifier que tous les outils que vous utilisez sont capables d'utiliser les API Kafka Admin sans ZooKeeper connexion. Reportez-vous à Utilisation LinkedIn du régulateur de vitesse pour Apache Kafka avec Amazon MSK la section pour connaître les étapes mises à jour pour

connecter votre cluster au régulateur de vitesse. Le régulateur de vitesse contient également des instructions pour utiliser le régulateur de vitesse sans ZooKeeper.

- Vous n'avez pas besoin d'accéder directement aux contrôleurs KraFT de votre cluster pour effectuer des actions administratives. Toutefois, si vous utilisez la surveillance ouverte pour collecter des métriques, vous avez également besoin des points de terminaison DNS de vos contrôleurs afin de collecter des métriques non liées aux contrôleurs concernant votre cluster. Vous pouvez obtenir ces points de terminaison DNS à partir de la console MSK ou à l'aide de l'opération ListNodesAPI. Consultez Surveillance ouverte avec Prometheus les étapes mises à jour pour configurer la surveillance ouverte pour les clusters basés sur Kraft.
- Il n'y a aucune CloudWatch métrique supplémentaire à surveiller pour les clusters en mode Kraft par rapport aux clusters ZooKeeper en mode. MSK gère les contrôleurs KraFT utilisés dans vos clusters.
- Vous pouvez continuer à gérer les ACL à l'aide de clusters en mode KraFT à l'aide de la chaîne de `--bootstrap-server` connexion. Vous ne devez pas utiliser la chaîne de `--zookeeper` connexion pour gérer les ACL. veuillez consulter Listes de contrôle d'accès (ACL) Apache Kafka.
- En mode KraFT, les métadonnées de votre cluster sont stockées sur des contrôleurs KraFT au sein de Kafka et non sur des ZooKeeper nœuds externes. Par conséquent, il n'est pas nécessaire de contrôler l'accès aux nœuds de contrôleur séparément comme c'est le cas pour les ZooKeeper nœuds.

Gestion du stockage

Amazon MSK propose des fonctionnalités qui vous aident à gérer le stockage sur vos clusters MSK.

Rubriques

- Stockage hiérarchisé
- Mise à l'échelle du stockage des agents
- Provisionnement du débit de stockage

Stockage hiérarchisé

Le stockage hiérarchisé est un niveau de stockage peu coûteux pour Amazon MSK qui évolue vers un stockage pratiquement illimité, ce qui rend rentable le développement d'applications de streaming de données.

Vous pouvez créer un cluster Amazon MSK configuré avec un stockage hiérarchisé qui équilibre les performances et les coûts. Amazon MSK stocke les données de streaming dans un niveau de stockage principal optimisé pour les performances jusqu'à ce qu'elles atteignent les limites de conservation des rubriques Apache Kafka. Amazon MSK déplace ensuite automatiquement les données vers le nouveau niveau de stockage à faible coût.

Lorsque votre application commence à lire des données depuis le stockage hiérarchisé, vous pouvez vous attendre à une augmentation de la latence de lecture pour les premiers octets. Lorsque vous commencez à lire les données restantes de manière séquentielle à partir du niveau à faible coût, vous pouvez vous attendre à des latences similaires à celles du niveau de stockage principal. Vous n'avez pas besoin de provisionner de stockage pour le stockage hiérarchisé à faible coût ni de gérer l'infrastructure. Vous pouvez stocker n'importe quelle quantité de données et ne payer que ce que vous utilisez. Cette fonctionnalité est compatible avec les API introduites dans KIP-405 : stockage hiérarchisé de Kafka.

Certaines des fonctionnalités du stockage hiérarchisé sont décrites ci-dessous :

- Vous pouvez passer à un espace de stockage pratiquement illimité. Vous n'avez pas à deviner comment mettre à l'échelle votre infrastructure Apache Kafka.
- Vous pouvez conserver les données plus longtemps dans vos rubriques Apache Kafka ou augmenter le stockage de vos rubriques, sans avoir à augmenter le nombre d'agents.
- Il fournit un tampon de sécurité de plus longue durée pour gérer les retards imprévus dans le traitement.
- Vous pouvez retraiter les anciennes données dans leur ordre de production exact à l'aide de votre code de traitement des flux existant et des API Kafka.
- Les partitions se rééquilibrent plus rapidement car les données du stockage secondaire ne nécessitent pas de réplication sur les disques de l'agent.
- Les données entre les agents et le stockage hiérarchisé sont transférées au sein du VPC et ne transitent pas par Internet.
- Un ordinateur client peut utiliser le même processus pour se connecter à de nouveaux clusters avec le stockage hiérarchisé activé que pour se connecter à un cluster sans stockage hiérarchisé activé. Consultez la section Créer un ordinateur client.

Conditions préalables au stockage hiérarchisé

- Vous devez utiliser le client Apache Kafka version 3.0.0 ou supérieure pour créer une nouvelle rubrique avec le stockage hiérarchisé activé. Pour faire passer une rubrique existante au stockage hiérarchisé, vous pouvez reconfigurer un ordinateur client qui utilise une version du client Kafka antérieure à la version 3.0.0 (la version minimale d'Apache Kafka prise en charge est 2.8.2) pour activer le stockage hiérarchisé. veuillez consulter Étape 4 : créer une rubrique.
- Le cluster Amazon MSK sur lequel le stockage hiérarchisé est activé doit utiliser la version 3.6.0 ou supérieure, ou la version 2.8.2.

Contraintes et limites du stockage hiérarchisé

Le stockage hiérarchisé présente les contraintes et limites suivantes :

- Le stockage hiérarchisé s'applique uniquement aux clusters en mode provisionné.
- Le stockage hiérarchisé ne prend pas en charge la taille du broker t3.small.
- La période de conservation minimale dans le stockage à faible coût est de 3 jours. Il n'y a pas de durée de conservation minimale pour le stockage principal.
- Le stockage hiérarchisé ne prend pas en charge les répertoires de journaux multiples sur un agent (fonctionnalités liées au JBOD).
- Le stockage hiérarchisé ne prend pas en charge les rubriques compactées. Assurez-vous que le fichier cleanup.policy de toutes les rubriques pour lesquelles le stockage hiérarchisé est activé est configuré sur « SUPPRESSION » uniquement.
- Le stockage hiérarchisé peut être désactivé pour des rubriques individuelles, mais pas pour l’ensemble du cluster. Une fois désactivé, le stockage hiérarchisé ne peut pas être réactivé pour une rubrique.
- Si vous utilisez Amazon MSK version 2.8.2.tiered, vous ne pouvez migrer que vers une autre version d'Apache Kafka compatible avec le stockage hiérarchisé. Si vous ne souhaitez pas continuer à utiliser une version prise en charge par le stockage hiérarchisé, créez un nouveau cluster MSK et migrez vos données vers celui-ci.
- L' kafka-log-dirs outil ne peut pas indiquer la taille des données de stockage hiérarchisé. L'outil indique uniquement la taille des segments de journaux dans le stockage principal.

Comment les segments de journaux sont copiés vers le stockage hiérarchisé

Lorsque vous activez le stockage hiérarchisé pour une rubrique nouvelle ou existante, Apache Kafka copie les segments de journaux fermés du stockage principal vers le stockage hiérarchisé.

- Apache Kafka copie uniquement les segments de journaux fermés. Il copie tous les messages contenus dans le segment du journal vers un stockage hiérarchisé.
- Les segments actifs ne sont pas éligibles à la hiérarchisation. La taille du segment de journal (segment.bytes) ou le temps d'exécution du segment (segment.ms) contrôlent le taux de fermeture des segments, et le taux auquel Apache Kafka les copie ensuite vers un stockage hiérarchisé.

Les paramètres de conservation d'une rubrique pour laquelle le stockage hiérarchisé est activé sont différents des paramètres d'une rubrique sans stockage hiérarchisé activé. Les règles suivantes contrôlent la conservation des messages dans les rubriques pour lesquelles le stockage hiérarchisé est activé :

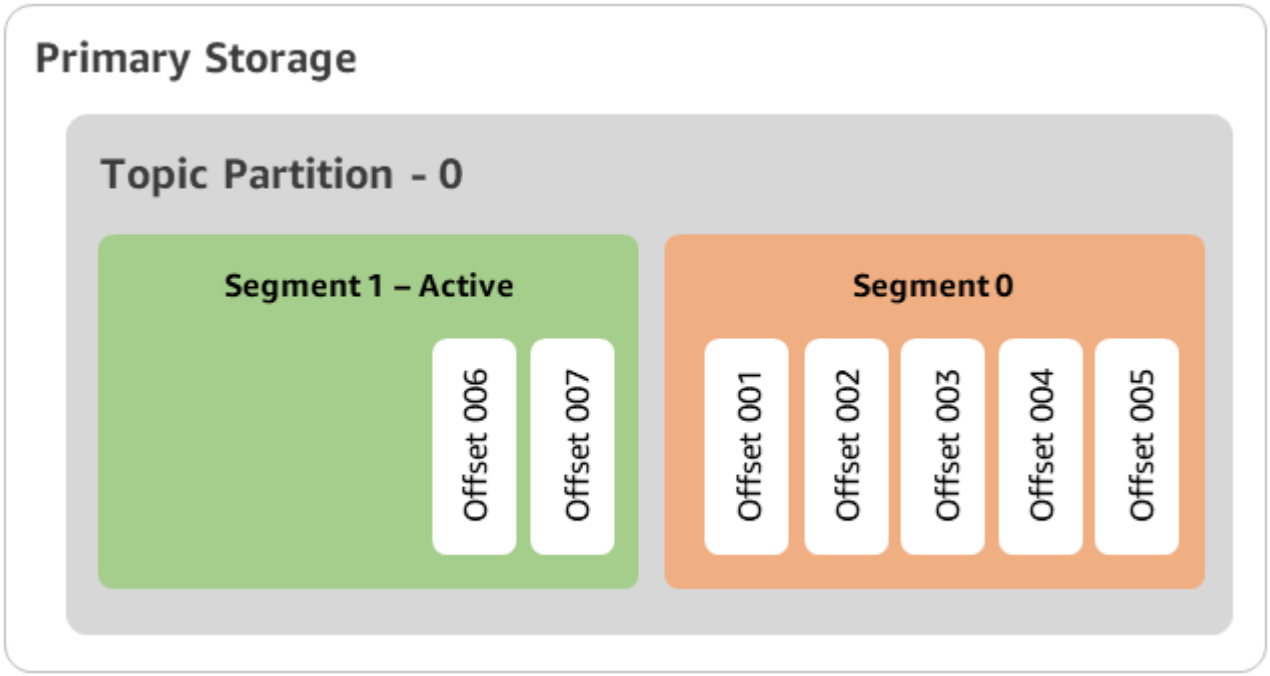
- Vous définissez la rétention dans Apache Kafka avec deux paramètres : log.retention.ms (heure) et log.retention.bytes (taille). Ces paramètres déterminent la durée totale et la taille des données conservées par Apache Kafka dans le cluster. Que vous activiez ou non le mode de stockage hiérarchisé, vous définissez ces configurations au niveau du cluster. Vous pouvez remplacer les paramètres au niveau de la rubrique par des configurations de rubrique.
- Lorsque vous activez le stockage hiérarchisé, vous pouvez également spécifier la durée pendant laquelle le niveau de stockage hautes performances principal stocke les données. Par exemple, si une rubrique possède un paramètre de conservation globale (log.retention.ms) de 7 jours et une rétention locale (local.retention.ms) de 12 heures, le stockage principal du cluster ne conserve les données que pendant les 12 premières heures. Le niveau de stockage à faible coût conserve les données pendant 7 jours complets.
- Les paramètres de conservation habituels s'appliquent à l'intégralité du journal. Cela inclut ses parties principales et hiérarchisées.
- Les paramètres local.retention.ms ou local.retention.bytes contrôlent la conservation des messages dans le stockage principal. Lorsque les données ont atteint les seuils de conservation du stockage principal (local.retention.ms/bytes) sur un journal complet, Apache Kafka copie les données du stockage principal vers un stockage hiérarchisé. Les données sont alors éligibles à l'expiration.
- Lorsqu'Apache Kafka copie un message d'un segment de journal vers un stockage hiérarchisé, il le supprime du cluster en fonction des paramètres retention.ms ou retention.bytes.

Exemple de scénario de stockage hiérarchisé

Ce scénario illustre le comportement d'une rubrique existante contenant des messages dans le stockage principal lorsque le stockage hiérarchisé est activé. Pour activer le stockage hiérarchisé sur ce sujet, vous devez définir remote.storage.enable sur `true`. Dans cet exemple, retention.ms est défini sur 5 jours et local.retention.ms est défini sur 2 jours. Voici la suite des événements lorsqu'un segment expire.

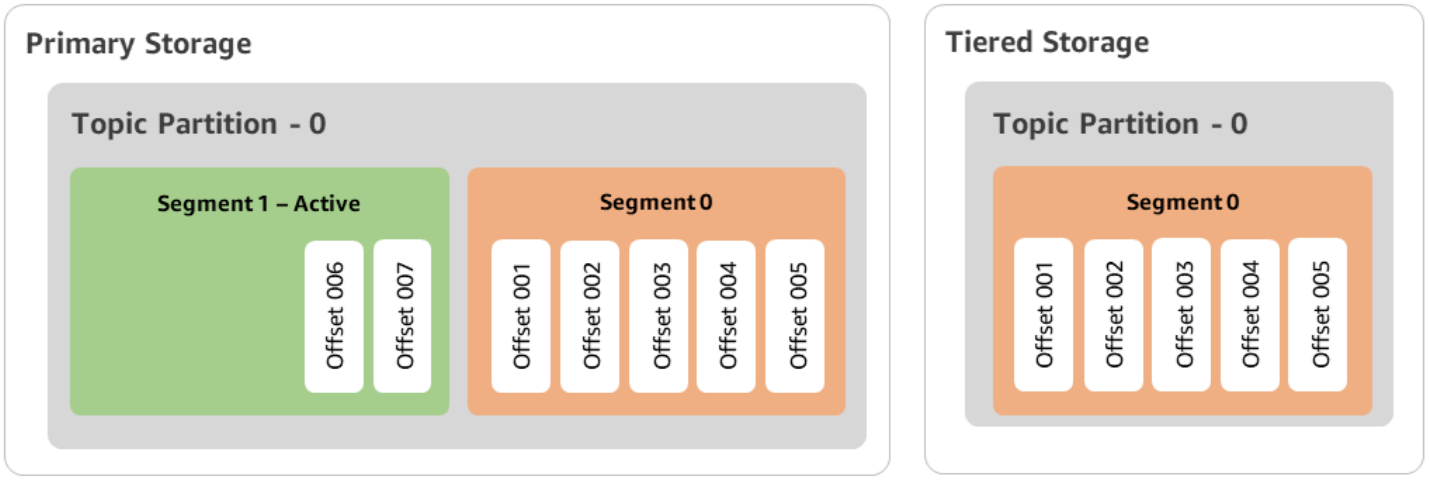
Temps T0 - Avant d'activer le stockage hiérarchisé.

Avant d'activer le stockage hiérarchisé pour cette rubrique, il existe deux segments de journal. L'un des segments est actif pour une partition de rubrique 0 existante.



Temps T1 (< 2 jours) - Stockage hiérarchisé activé. Segment 0 copié vers le stockage hiérarchisé.

Après avoir activé le stockage hiérarchisé pour cette rubrique, Apache Kafka copie le segment de journal 0 vers le stockage hiérarchisé une fois que le segment atteint les paramètres de conservation initiaux. Apache Kafka conserve également la copie de stockage principale du segment 0. Le segment 1 actif n'est pas encore éligible à la copie vers un stockage hiérarchisé. Dans cette chronologie, Amazon MSK n'applique encore aucun des paramètres de conservation pour les messages des segments 0 et 1. (local.retention.bytes/ms, retention.ms/bytes)



Temps T2 - Conservation locale en vigueur.

Après 2 jours, les paramètres de conservation principaux prennent effet pour le segment 0 qu'Apache Kafka a copié sur le stockage hiérarchisé. C'est le paramétrage de local.retention.ms sur 2 jours qui détermine cela. Le segment 0 expire désormais sur le stockage principal. Le segment 1 actif n'est pas encore éligible à l'expiration ni à la copie sur un stockage hiérarchisé.

Temps T3 - Conservation globale en vigueur.

Après 5 jours, les paramètres de conservation prennent effet et Kafka efface le segment 0 du journal et les messages associés du stockage hiérarchisé. Le segment 1 n'est pas encore éligible à l'expiration ni à la copie sur un stockage hiérarchisé, car il est actif. Le segment 1 n'est pas encore fermé, il n'est donc pas éligible au déploiement de segment.

Création d'un cluster Amazon MSK avec stockage hiérarchisé avec AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez Créer un cluster.
3. Choisissez Création personnalisée pour le stockage hiérarchisé.
4. Attribuez un nom au cluster.
5. Dans le type de cluster, sélectionnez Provisionné.
6. Choisissez une version d'Amazon Kafka prenant en charge le stockage hiérarchisé qu'Amazon MSK utilisera pour créer le cluster.
7. Spécifiez une taille de broker autre que kafka.t3.small.
8. Spécifiez le nombre d'agents qu'Amazon MSK doit créer dans chaque zone de disponibilité. Le minimum est d'un agent par zone de disponibilité et le maximum est de 30 agents par cluster.
9. Spécifiez le nombre de zones dans lesquelles les agents sont répartis.
10. Spécifiez le nombre d'agents Apache Kafka déployés par zone.
11. Sélectionnez Options de stockage. Cela inclut le stockage hiérarchisé et le stockage EBS pour activer le mode de stockage hiérarchisé.
12. Suivez les étapes restantes de l'assistant de création de cluster. Une fois l'opération terminée, le stockage hiérarchisé et le stockage EBS apparaissent comme mode de stockage du cluster dans la vue Vérifier et créer.
13. Sélectionnez Créer un cluster.

Création d'un cluster Amazon MSK avec stockage hiérarchisé avec AWS CLI

Pour activer le stockage hiérarchisé sur un cluster, créez le cluster avec la version et l'attribut Apache Kafka appropriés pour le stockage hiérarchisé. Suivez l'exemple de code ci-dessous. Suivez également les étapes décrites dans la prochaine section Création d'une rubrique Kafka avec le stockage hiérarchisé activé.

Voir create-cluster pour une liste complète des attributs pris en charge pour la création de clusters.

```
aws tiered-storage create-cluster \
 –cluster-name "MessagingCluster" \
 –broker-node-group-info file://brokernodegroupinfo.json \
 –number-of-broker-nodes 3 \
--kafka-version "3.6.0" \
--storage-mode "TIERED"
```

Création d'une rubrique Kafka avec le stockage hiérarchisé activé

Pour terminer le processus que vous avez entamé lorsque vous avez créé un cluster avec le stockage hiérarchisé activé, créez également une rubrique avec le stockage hiérarchisé activé avec les attributs du dernier exemple de code. Les attributs spécifiques au stockage hiérarchisé sont les suivants :

- `local.retention.ms` (par exemple, 10 minutes) pour les paramètres de conservation basés sur le temps ou `local.retention.bytes` pour les limites de taille des segments de journaux.
- `remote.storage.enable` défini sur `true` pour activer le stockage hiérarchisé.

La configuration suivante utilise local.retention.ms, mais vous pouvez remplacer cet attribut par local.retention.bytes. Cet attribut contrôle le temps qui peut s'écouler ou le nombre d'octets qu'Apache Kafka peut copier avant que ce dernier ne copie les données du stockage principal vers le stockage hiérarchisé. Voir Configuration au niveau des rubriques pour plus de détails sur les attributs de configuration pris en charge.

> **Note**
>
> Vous devez utiliser le client Apache Kafka version 3.0.0 ou supérieure. Ces versions prennent en charge un paramètre appelé `remote.storage.enable` uniquement dans les versions clientes de `kafka-topics.sh`. Pour activer le stockage hiérarchisé sur une rubrique

existante qui utilise une version antérieure d'Apache Kafka, consultez la section Activation du stockage hiérarchisé sur une rubrique existante.

```
bin/kafka-topics.sh --create --bootstrap-server $bs --replication-factor 2
 --partitions 6 --topic MSKTutorialTopic --config remote.storage.enable=true
 --config local.retention.ms=100000 --config retention.ms=604800000 --config
 segment.bytes=134217728
```

Activation et désactivation du stockage hiérarchisé sur une rubrique existante

Ces sections expliquent comment activer et désactiver le stockage hiérarchisé sur une rubrique que vous avez déjà créée. Pour créer un nouveau cluster et une nouvelle rubrique avec le stockage hiérarchisé activé, voir Création d'un cluster avec stockage hiérarchisé à l'aide d' AWS Management Console.

Activation du stockage hiérarchisé sur une rubrique existante

Pour activer le stockage hiérarchisé sur une rubrique existante, utilisez la syntaxe de commande `alter` de l'exemple suivant. Lorsque vous activez le stockage hiérarchisé sur une rubrique existante, vous n'êtes pas limité à une certaine version du client Apache Kafka.

```
bin/kafka-configs.sh --bootstrap-server $bsrv --alter --entity-type topics
 --entity-name msk-ts-topic --add-config 'remote.storage.enable=true,
 local.retention.ms=604800000, retention.ms=15550000000'
```

Désactivation du stockage hiérarchisé sur une rubrique existante

Pour désactiver le stockage hiérarchisé sur une rubrique existante, utilisez la syntaxe de commande `alter` dans le même ordre que lorsque vous activez le stockage hiérarchisé.

```
bin/kafka-configs.sh --bootstrap-server $bs --alter --entity-type topics --
entity-name MSKTutorialTopic --add-config 'remote.log.msk.disable.policy=Delete,
 remote.storage.enable=false'
```

> **Note**
>
> Lorsque vous désactivez le stockage hiérarchisé, vous supprimez complètement les données des rubriques dans le stockage hiérarchisé. Apache Kafka conserve les données de stockage

principales, mais applique toujours les règles de conservation principales basées sur `local.retention.ms`. Lorsque vous désactivez le stockage hiérarchisé sur une rubrique, vous ne pouvez pas le réactiver. Si vous souhaitez désactiver le stockage hiérarchisé sur une rubrique existante, vous n'êtes pas limité à une certaine version du client Apache Kafka.

Activation du stockage hiérarchisé sur un cluster existant à l'aide AWS de la CLI

> **Note**
>
> Vous ne pouvez activer le stockage hiérarchisé que si log.cleanup.policy de votre cluster est défini sur `delete`, car les rubriques compactées ne sont pas prises en charge sur le stockage hiérarchisé. Plus tard, vous pourrez configurer le log.cleanup.policy d'une rubrique individuelle sur `compact` si le stockage hiérarchisé n'est pas activé sur cette rubrique en particulier. Voir Configuration au niveau des rubriques pour plus de détails sur les attributs de configuration pris en charge.

1. Mettez à jour la version de Kafka : les versions de cluster ne sont pas de simples entiers. Pour trouver la version actuelle du cluster, utilisez l'`DescribeCluster`opération ou la commande `describe-cluster` AWS CLI. Voici un exemple de version : `KTVPDKIKX0DER`.

```
aws kafka update-cluster-kafka-version --cluster-arn ClusterArn --current-version
 Current-Cluster-Version --target-kafka-version 3.6.0
```

2. Modifiez le mode de stockage en cluster. L'exemple de code suivant montre comment modifier le mode de stockage du cluster en `TIERED` à l'aide de l'API `update-storage`.

```
aws kafka update-storage --current-version Current-Cluster-Version --cluster-arn
 Cluster-arn --storage-mode TIERED
```

Mise à jour du stockage hiérarchisé sur un cluster existant à l'aide de la console

> **Note**
>
> Vous ne pouvez activer le stockage hiérarchisé que si log.cleanup.policy de votre cluster est défini sur `delete`, car les rubriques compactées ne sont pas prises en charge sur le

stockage hiérarchisé. Plus tard, vous pourrez configurer le log.cleanup.policy d'une rubrique individuelle sur `compact` si le stockage hiérarchisé n'est pas activé sur cette rubrique en particulier. Voir Configuration au niveau des rubriques pour plus de détails sur les attributs de configuration pris en charge.

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Accédez à la page de résumé du cluster et choisissez Propriétés.
3. Accédez à la section Stockage et choisissez Modifier le mode de stockage du cluster.
4. Choisissez Stockage hiérarchisé et stockage EBS, puis Enregistrer les modifications.

Mise à l'échelle du stockage des agents

Vous pouvez augmenter la quantité de stockage EBS par agent. Vous ne pouvez pas réduire le stockage.

Les volumes de stockage restent disponibles pendant cette opération de mise à l'échelle.

Important

Lorsque le stockage est dimensionné pour un cluster MSK, le stockage supplémentaire est immédiatement disponible. Toutefois, le cluster a besoin d'une période de refroidissement après chaque événement de mise à l'échelle du stockage. Amazon MSK utilise cette période de refroidissement pour optimiser le cluster avant qu'il ne puisse être redimensionné. Cette période peut aller d'un minimum de 6 heures à plus de 24 heures, en fonction de la taille du stockage et de l'utilisation du cluster, ainsi que du trafic. Cela s'applique à la fois aux événements de dimensionnement automatique et au dimensionnement manuel à l'aide de l'opération UpdateBrokerde stockage. Pour plus d'informations sur la mise à l'échelle correcte de votre stockage, consultez Bonnes pratiques.

Vous pouvez utiliser le stockage hiérarchisé pour augmenter et passer en illimité le volume de stockage de votre agent. Consultez Stockage hiérarchisé.

Rubriques

- Dimensionnement automatique
- Mise à l'échelle manuelle

Dimensionnement automatique

Pour étendre automatiquement le stockage de votre cluster en réponse à une utilisation accrue, vous pouvez configurer une politique de mise à l'échelle automatique (autoscaling) des applications pour Amazon MSK. Dans une politique de type autoscaling, vous définissez l'utilisation du disque cible et la capacité de mise à l'échelle maximale.

Avant d'utiliser la mise à l'échelle automatique (autoscaling) pour Amazon MSK, vous devez tenir compte des points suivants :

- > **Important**
  >
  > Une action de mise à l'échelle du stockage ne peut avoir lieu qu'une fois toutes les six heures.

  Nous vous recommandons de commencer par un volume de stockage de taille adaptée à vos besoins de stockage. Pour obtenir des conseils sur la mise à l'échelle correcte de votre cluster, consultez Dimensionnez correctement votre cluster : nombre d'agents par cluster.
- Amazon MSK ne réduit pas le stockage de cluster en réponse à une utilisation réduite. Amazon MSK ne prend pas en charge la réduction de la taille des volumes de stockage. Si vous devez réduire la taille de votre stockage de cluster, vous devez migrer votre cluster existant vers un cluster ayant un espace de stockage plus petit. Pour en savoir plus sur la migration d'un cluster, consultez Migration.
- Amazon MSK ne prend pas en charge la mise à l'échelle automatique (autoscaling) dans les régions Asie-Pacifique (Osaka) et Afrique (Le Cap).
- Lorsque vous associez une politique d'auto-scaling à votre cluster, Amazon EC2 Auto Scaling crée automatiquement une alarme CloudWatch Amazon pour le suivi des cibles. Si vous supprimez un cluster doté d'une politique d'auto-scaling, cette CloudWatch alarme persiste. Pour supprimer l' CloudWatch alarme, vous devez supprimer une politique d'auto-scaling d'un cluster avant de le supprimer. Pour en savoir plus sur le suivi des cibles, consultez Politiques de mise à l'échelle de suivi des cibles pour Amazon EC2 Auto Scaling dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

Détails de la politique autoscaling

Votre politique autoscaling définit les paramètres suivants pour votre cluster :

- Cible d'utilisation du stockage : seuil d'utilisation du stockage utilisé par Amazon MSK pour déclencher une opération de mise à l'échelle automatique (autoscaling). Vous pouvez définir la cible d'utilisation entre 10 % et 80 % de la capacité de stockage actuelle. Nous vous recommandons de définir la cible d'utilisation du stockage entre 50 % et 60 %.
- Capacité de stockage maximale : limite de mise à l'échelle maximale qu'Amazon MSK peut définir pour le stockage de votre agent. Vous pouvez définir une capacité de stockage maximale de 16 TiO par agent. Pour plus d'informations, consultez Quota d'Amazon MSK.

Lorsqu'Amazon MSK détecte que votre métrique `Maximum Disk Utilization` est égale ou supérieure au paramètre `Storage Utilization Target`, il augmente votre capacité de stockage d'une quantité égale au plus grand des deux chiffres : 10 GiO ou 10 % du stockage actuel. Par exemple, si vous avez 1 000 GiO, cette quantité est de 100 GiO. Le service vérifie l'utilisation de votre stockage toutes les minutes. Les opérations de mise à l'échelle supplémentaires continuent d'augmenter le stockage d'une quantité égale au plus grand des deux nombres : 10 GiO ou 10 % du stockage actuel.

Pour déterminer si des opérations d'auto-scaling ont eu lieu, utilisez l' ListClusterOperationsopération.

Configuration de la fonction d'autoscaling pour votre cluster Amazon MSK

Vous pouvez utiliser la console Amazon MSK, l'API Amazon MSK ou AWS CloudFormation implémenter le dimensionnement automatique pour le stockage. CloudFormation le support est disponible via Application Auto Scaling.

> **Note**
>
> Vous ne pouvez pas implémenter de mécanisme d'autoscaling lorsque vous créez un cluster. Vous devez d'abord créer le cluster, puis créer et activer une politique d'autoscaling pour celui-ci. Toutefois, vous pouvez créer la politique pendant que le service Amazon MSK crée votre cluster.

Configuration de la fonction d'autoscaling à l'aide de la AWS Management Console

1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Dans la liste des clusters, choisissez votre cluster. Cela vous amène à une page répertoriant les détails du cluster.

3. Dans la section Autoscaling pour le stockage, choisissez Configurer.
4. Créez et nommez une politique d'autoscaling Spécifiez la cible d'utilisation du stockage, la capacité de stockage maximale et la métrique cible.
5. Sélectionnez `Save changes`.

Lorsque vous enregistrez et activez la nouvelle politique, celle-ci devient active pour le cluster. Amazon MSK étend ensuite le stockage du cluster une fois la cible d'utilisation du stockage atteinte.

Configuration de la fonction d'autoscaling à l'aide de l'interface de ligne de commande

1. Utilisez la RegisterScalableTargetcommande pour enregistrer un objectif d'utilisation du stockage.
2. Utilisez la PutScalingPolicycommande pour créer une politique d'extension automatique.

Configuration de la fonction d'autoscaling à l'aide de l'API

1. Utilisez l' RegisterScalableTargetAPI pour enregistrer un objectif d'utilisation du stockage.
2. Utilisez l' PutScalingPolicyAPI pour créer une politique d'extension automatique.

Mise à l'échelle manuelle

Pour augmenter le stockage, attendez que l'état du cluster soit `ACTIVE`. La mise à l'échelle du stockage est soumise à une période de refroidissement d'au moins six heures entre les événements. Même si l'opération met immédiatement à disposition du stockage supplémentaire, le service effectue des optimisations sur votre cluster qui peuvent prendre jusqu'à 24 heures ou plus. La durée de ces optimisations est proportionnelle à la taille de votre stockage.

Élargir le stockage des courtiers à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez le cluster MSK pour lequel vous souhaitez mettre à jour le stockage d'agent.
3. Dans la section Stockage, sélectionnez Modifier.
4. Spécifiez le volume de stockage souhaité. Vous pouvez uniquement augmenter la quantité de stockage, vous ne pouvez pas la diminuer.
5. Sélectionnez Enregistrer les modifications.

Élargir le stockage des courtiers à l'aide du AWS CLI

Exécutez la commande suivante, en la *ClusterArn*remplaçant par le Amazon Resource Name (ARN) que vous avez obtenu lors de la création de votre cluster. Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d'informations, consultez the section called "Liste des clusters".

Remplacez *Current-Cluster-Version* par la version actuelle du cluster.

> **Important**
>
> Les versions de cluster ne sont pas des entiers simples. Pour trouver la version actuelle du cluster, utilisez l'DescribeClusteropération ou la commande describe-cluster AWS CLI . Voici un exemple de version : `KTVPDKIKX0DER`.

Le paramètre *Target-volume-in-GIB* représente la quantité de stockage dont chaque agent doit disposer. Il est seulement possible de mettre à jour le stockage pour tous les agents. Vous ne pouvez pas spécifier d'agents individuels pour lesquels mettre à jour le stockage. La valeur que vous spécifiez pour le *volume cible en Gio* doit être un nombre entier supérieur à 100 Gio. Le stockage par agent après l'opération de mise à jour ne peut pas dépasser 16 384 Gio.

```
aws kafka update-broker-storage --cluster-arn ClusterArn --current-version Current-
Cluster-Version --target-broker-ebs-volume-info '{"KafkaBrokerNodeId": "All",
 "VolumeSizeGB": Target-Volume-in-GiB}'
```

Mise à l'échelle du stockage d'agent à l'aide de l'API

Pour mettre à jour le stockage d'un broker à l'aide de l'API, consultez la section UpdateBrokerStockage.

Provisionnement du débit de stockage

Les agents Amazon MSK conservent les données relatives sur des volumes de stockage. Les E/S de stockage sont consommées lorsque les producteurs écrivent dans le cluster, lorsque les données sont répliquées entre agents et lorsque les consommateurs lisent des données qui ne sont pas en mémoire. Le débit de stockage en volume est le taux auquel les données peuvent être écrites et lues sur un volume de stockage. Le débit de stockage provisionné est la capacité de spécifier ce taux pour les agents de votre cluster.

Vous pouvez spécifier le débit provisionné en Mio par seconde pour les clusters dont les courtiers sont de taille supérieure ou égale à 10 GiB et si le volume de stockage est supérieur `kafka.m5.4xlarge` ou égal à 10 GiB. Il est possible de spécifier le débit provisionné lors de la création du cluster. Vous pouvez également activer ou désactiver le débit provisionné pour un cluster qui est dans l'état `ACTIVE`.

Goulots d'étranglement du débit

Les goulots d'étranglement du débit des agents ont plusieurs causes : le débit du volume, le débit du réseau Amazon EC2 vers Amazon EBS et le débit de sortie d'Amazon EC2. Vous pouvez activer le débit de stockage provisionné pour ajuster le débit du volume. Cependant, les limites de débit des agents peuvent être causées par le débit du réseau Amazon EC2 vers Amazon EBS et le débit de sortie d'Amazon EC2.

Le débit de sortie d'Amazon EC2 dépend du nombre de groupes de consommateurs et du nombre de consommateurs par groupe de consommateurs. En outre, le débit du réseau Amazon EC2 vers Amazon EBS et le débit de sortie Amazon EC2 sont plus élevés pour les courtiers de grande taille.

Pour des volumes de 10 Go ou plus, vous pouvez provisionner un débit de stockage de 250 Mio par seconde ou plus. 250 Mio par seconde est la valeur par défaut. Pour provisionner le débit de stockage, vous devez choisir la taille du broker kafka.m5.4xlarge ou supérieure (ou kafka.m7g.2xlarge ou supérieure), et vous pouvez spécifier le débit maximal comme indiqué dans le tableau suivant.

taille du courtier	Débit de stockage maximal (Mio/s)
kafka.m5.4xlarge	593
kafka.m5.8xlarge	850
kafka.m5.12xlarge	1 000
kafka.m5.16xlarge	1 000
kafka.m5.24xlarge	1 000
kafka.m7g.2xlarge	312,5
kafka.m7g.4xlarge	625

taille du courtier	Débit de stockage maximal (Mio/s)
kafka.m7g.8xlarge	1 000
kafka.m7g, 12 x large	1 000
kafka.m7g, 16 x large	1 000

Mesure du débit de stockage

Vous pouvez utiliser les métriques `VolumeReadBytes` et `VolumeWriteBytes` pour mesurer le débit de stockage moyen d'un cluster. La somme de ces deux mesures donne le débit de stockage moyen en octets. Pour obtenir le débit de stockage moyen d'un cluster, définissez ces deux métriques sur SUM et sur la période 1 minute, puis utilisez la formule suivante.

```
Average storage throughput in MiB/s = (Sum(VolumeReadBytes) + Sum(VolumeWriteBytes)) /
 (60 * 1024 * 1024)
```

Pour obtenir des informations sur les métriques `VolumeReadBytes` et `VolumeWriteBytes`, consultez the section called “Surveillance de niveau PER_BROKER”.

Mise à jour de la configuration

Vous pouvez mettre à jour votre configuration Amazon MSK avant ou après avoir activé le débit provisionné. Toutefois, vous ne verrez pas le débit souhaité tant que vous n'aurez pas effectué les deux actions suivantes : mettre à jour le paramètre de configuration `num.replica.fetchers` et activer le débit provisionné.

Dans la configuration Amazon MSK par défaut, `num.replica.fetchers` a une valeur de 2. Pour mettre à jour votre `num.replica.fetchers`, vous pouvez utiliser les valeurs suggérées dans le tableau suivant. Ces valeurs sont fournies à titre indicatif. Nous vous recommandons d'ajuster ces valeurs en fonction de votre cas d'utilisation.

taille du courtier	num.replica.fetchers
kafka.m5.4xlarge	4
kafka.m5.8xlarge	8

taille du courtier	num.replica.fetchers
kafka.m5.12xlarge	14
kafka.m5.16xlarge	16
kafka.m5.24xlarge	16

Votre configuration mise à jour peut ne pas prendre effet avant 24 heures et peut prendre plus de temps lorsqu'un volume source n'est pas entièrement utilisé. Toutefois, les performances des volumes de transition sont au moins égales aux performances des volumes de stockage source pendant la période de migration. Un volume de 1 Tio entièrement utilisé prend généralement environ six heures pour migrer vers une configuration mise à jour.

Provisionnement du débit de stockage à l'aide du AWS Management Console

1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Choisissez Créer un cluster.
3. Choisissez Création personnalisée.
4. Attribuez un nom au cluster.
5. Dans la section Stockage, sélectionnez Activer.
6. Choisissez une valeur pour le débit de stockage par agent.
7. Choisissez un VPC, des zones, des sous-réseaux, ainsi qu'un groupe de sécurité.
8. Choisissez Suivant.
9. Au bas de l'étape Sécurité, choisissez Suivant.
10. Au bas de l'étape Surveillance et identifications, choisissez Suivant.
11. Vérifiez les paramètres du cluster, puis choisissez Créer un cluster.

Provisionnement du débit de stockage à l'aide du AWS CLI

Cette section montre un exemple de la façon dont vous pouvez utiliser le AWS CLI pour créer un cluster avec le débit provisionné activé.

1. Copiez le code JSON suivant dans un fichier et collez-le dans un fichier. Remplacez les espaces réservés des ID de sous-réseau et de groupes de sécurité par les valeurs de votre compte. Nommez le fichier `cluster-creation.json` et enregistrez-le.

```
{
    "Provisioned": {
        "BrokerNodeGroupInfo":{
            "InstanceType":"kafka.m5.4xlarge",
            "ClientSubnets":[
                "Subnet-1-ID",
                "Subnet-2-ID"
            ],
            "SecurityGroups":[
                "Security-Group-ID"
            ],
            "StorageInfo": {
                "EbsStorageInfo": {
                    "VolumeSize": 10,
                    "ProvisionedThroughput": {
                        "Enabled": true,
                        "VolumeThroughput": 250
                    }
                }
            }
        },
        "EncryptionInfo": {
            "EncryptionInTransit": {
                "InCluster": false,
                "ClientBroker": "PLAINTEXT"
            }
        },
        "KafkaVersion":"2.8.1",
        "NumberOfBrokerNodes": 2
    },
    "ClusterName": "provisioned-throughput-example"
}
```

2. Exécutez la AWS CLI commande suivante depuis le répertoire dans lequel vous avez enregistré le fichier JSON à l'étape précédente.

```
aws kafka create-cluster-v2 --cli-input-json file://cluster-creation.json
```

Provisionnement du débit de stockage à l'aide de l'API

Pour configurer le débit de stockage provisionné lors de la création d'un cluster, utilisez CreateCluster la version V2.

Mise à jour de la taille du courtier

Vous pouvez faire évoluer votre cluster MSK à la demande en modifiant la taille de vos courtiers sans réaffecter les partitions Apache Kafka. La modification de la taille de vos courtiers vous donne la possibilité d'ajuster la capacité de calcul de votre cluster MSK en fonction de l'évolution de vos charges de travail, sans interrompre les E/S de votre cluster. Amazon MSK utilise la même taille de courtier pour tous les courtiers d'un cluster donné.

Cette section explique comment mettre à jour la taille du broker pour votre cluster MSK. Vous pouvez mettre à jour la taille de votre courtier de cluster de M5 ou T3 à M7g, ou de M7g à M5. Sachez que la migration vers un courtier de plus petite taille peut diminuer les performances et réduire le débit maximal réalisable par courtier. La migration vers un courtier de plus grande taille peut améliorer les performances mais peut coûter plus cher.

La mise à jour de la taille du courtier s'effectue de manière continue lorsque le cluster est opérationnel. Cela signifie qu'Amazon MSK supprime un courtier à la fois pour effectuer la mise à jour de la taille du courtier. Pour plus d'informations sur la manière de rendre un cluster hautement disponible lors d'une mise à jour de la taille d'un courtier, consultez. the section called “Créer des clusters hautement disponibles” Pour réduire davantage tout impact potentiel sur la productivité, vous pouvez effectuer la mise à jour de la taille du courtier pendant une période de faible trafic.

Lors d'une mise à jour de la taille d'un courtier, vous pouvez continuer à produire et à consommer des données. Cependant, vous devez attendre que la mise à jour soit terminée avant de pouvoir redémarrer les agents ou invoquer l'une des opérations de mise à jour répertoriées sous les opérations Amazon MSK.

Si vous souhaitez mettre à jour votre cluster vers une taille de broker plus petite, nous vous recommandons d'essayer d'abord la mise à jour sur un cluster de test pour voir comment elle affecte votre scénario.

> **Important**
>
> Vous ne pouvez pas mettre à jour un cluster vers une taille de broker inférieure si le nombre de partitions par broker dépasse le nombre maximum spécifié dansthe section called “ Dimensionnez correctement votre cluster : nombre de partitions par agent”.

Mise à jour de la taille du courtier à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez le cluster MSK pour lequel vous souhaitez mettre à jour la taille du broker.
3. Sur la page de détails du cluster, recherchez la section Récapitulatif des courtiers, puis choisissez Modifier la taille du courtier.
4. Choisissez la taille de courtier que vous souhaitez dans la liste.
5. Enregistrez les modifications.

Mise à jour de la taille du courtier à l'aide du AWS CLI

1. Exécutez la commande suivante, en la *ClusterArn*remplaçant par le Amazon Resource Name (ARN) que vous avez obtenu lors de la création de votre cluster. Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d'informations, consultez the section called “Liste des clusters”.

   Remplacez *Current-Cluster-Version* par la version actuelle du cluster et *TargetType*par la nouvelle taille que vous souhaitez donner aux courtiers. Pour en savoir plus sur la taille des courtiers, consultezthe section called “Tailles des courtiers”.

   ```
   aws kafka update-broker-type --cluster-arn ClusterArn --current-version Current-Cluster-Version --target-instance-type TargetType
   ```

   Voici un exemple qui montre comment utiliser la commande :

   ```
   aws kafka update-broker-type --cluster-arn "arn:aws:kafka:us-east-1:0123456789012:cluster/exampleName/abcd1234-0123-abcd-5678-1234abcd-1" --current-version "K1X5R6FKA87" --target-instance-type kafka.m5.large
   ```

La sortie de cette commande ressemble à l'exemple JSON suivant.

```
{
    "ClusterArn": "arn:aws:kafka:us-east-1:0123456789012:cluster/exampleName/
abcd1234-0123-abcd-5678-1234abcd-1",
    "ClusterOperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef"
}
```

2. Pour obtenir le résultat de l'`update-broker-type`opération, exécutez la commande suivante en remplaçant *`ClusterOperationArn`* par l'ARN que vous avez obtenu dans le résultat de la `update-broker-type` commande.

```
aws kafka describe-cluster-operation --cluster-operation-arn ClusterOperationArn
```

La sortie de cette commande `describe-cluster-operation` ressemble à l'exemple JSON suivant.

```
{
  "ClusterOperationInfo": {
    "ClientRequestId": "982168a3-939f-11e9-8a62-538df00285db",
    "ClusterArn": "arn:aws:kafka:us-east-1:0123456789012:cluster/exampleName/
abcd1234-0123-abcd-5678-1234abcd-1",
    "CreationTime": "2021-01-09T02:24:22.198000+00:00",
    "OperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-operation/
exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef",
    "OperationState": "UPDATE_COMPLETE",
    "OperationType": "UPDATE_BROKER_TYPE",
    "SourceClusterInfo": {
      "InstanceType": "t3.small"
    },
    "TargetClusterInfo": {
      "InstanceType": "m5.large"
    }
  }
}
```

Si `OperationState` a la valeur `UPDATE_IN_PROGRESS`, attendez un moment, puis exécutez à nouveau la commande `describe-cluster-operation`.

Mise à jour de la taille du broker à l'aide de l'API

Pour mettre à jour la taille du broker à l'aide de l'API, consultez UpdateBrokerType.

Vous pouvez l'utiliser `UpdateBrokerType` pour mettre à jour la taille de votre courtier de cluster de M5 ou T3 à M7g, ou de M7g à M5.

Mise à jour de la configuration d'un cluster Amazon MSK

Pour mettre à jour la configuration d'un cluster, assurez-vous que l'état du cluster soit `ACTIVE`. Vous devez également veiller à ce que le nombre de partitions par agent sur votre cluster MSK est inférieur aux limites décrites dans the section called " Dimensionnez correctement votre cluster : nombre de partitions par agent". Vous ne pouvez pas mettre à jour la configuration d'un cluster qui dépasse ces limites.

Pour des informations sur la configuration MSK, notamment sur la création d'une configuration personnalisée, les propriétés que vous pouvez mettre à jour et ce qui se passe lorsque vous mettez à jour la configuration d'un cluster existant, veuillez consulter Configuration.

Mettre à jour la configuration d'un cluster à l'aide du AWS CLI

1. Copiez le JSON suivant et enregistrez-le dans un fichier. Nommez le fichier `configuration-info.json`. *`ConfigurationArn`*Remplacez-le par le Amazon Resource Name (ARN) de la configuration que vous souhaitez utiliser pour mettre à jour le cluster. La chaîne ARN doit être entre guillemets dans le JSON suivant.

   Remplacez *`Configuration-Revision`* par la révision de la configuration que vous souhaitez utiliser. Les révisions de configuration sont des entiers (nombres entiers) qui commencent à 1. Cet entier ne doit pas être entre guillemets dans le JSON suivant.

   ```
   {
        "Arn": ConfigurationArn,
        "Revision": Configuration-Revision
   }
   ```

2. Exécutez la commande suivante, en la *ClusterArn*remplaçant par l'ARN que vous avez obtenu lors de la création de votre cluster. Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d'informations, consultez the section called “Liste des clusters”.

   Remplacez *Path-to-Config-Info-file* par le chemin d'accès à votre fichier d'informations de configuration. Si vous avez nommé le fichier que vous avez créé à l'étape précédente `configuration-info.json` et que vous l'avez enregistré dans le répertoire courant, alors *Path-to-Config-info-file* est `configuration-info.json`.

   Remplacez *Current-Cluster-Version* par la version actuelle du cluster.

   > **Important**
   >
   > Les versions de cluster ne sont pas des entiers simples. Pour trouver la version actuelle du cluster, utilisez l'DescribeClusteropération ou la commande describe-cluster AWS CLI . Voici un exemple de version : `KTVPDKIKX0DER`.

   ```
   aws kafka update-cluster-configuration --cluster-arn ClusterArn --configuration-
   info file://Path-to-Config-Info-File --current-version Current-Cluster-Version
   ```

   Voici un exemple qui montre comment utiliser la commande :

   ```
   aws kafka update-cluster-configuration --cluster-arn "arn:aws:kafka:us-
   east-1:0123456789012:cluster/exampleName/abcd1234-0123-abcd-5678-1234abcd-1" --
   configuration-info file://c:\users\tester\msk\configuration-info.json --current-
   version "K1X5R6FKA87"
   ```

   La sortie de cette commande `update-cluster-configuration` ressemble à l'exemple JSON suivant.

   ```
   {
       "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/exampleClusterName/
   abcdefab-1234-abcd-5678-cdef0123ab01-2",
       "ClusterOperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
   operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
   abcd-4f7f-1234-9876543210ef"
   ```

```
}
```

3. Pour obtenir le résultat de l'`update-cluster-configuration`opération, exécutez la commande suivante en remplaçant *`ClusterOperationArn`* par l'ARN que vous avez obtenu dans le résultat de la `update-cluster-configuration` commande.

```
aws kafka describe-cluster-operation --cluster-operation-arn ClusterOperationArn
```

La sortie de cette commande `describe-cluster-operation` ressemble à l'exemple JSON suivant.

```
{
    "ClusterOperationInfo": {
        "ClientRequestId": "982168a3-939f-11e9-8a62-538df00285db",
        "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/
exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2",
        "CreationTime": "2019-06-20T21:08:57.735Z",
        "OperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef",
        "OperationState": "UPDATE_COMPLETE",
        "OperationType": "UPDATE_CLUSTER_CONFIGURATION",
        "SourceClusterInfo": {},
        "TargetClusterInfo": {
            "ConfigurationInfo": {
                "Arn": "arn:aws:kafka:us-east-1:123456789012:configuration/
ExampleConfigurationName/abcdabcd-abcd-1234-abcd-abcd123e8e8e-1",
                "Revision": 1
            }
        }
    }
}
```

Dans cette sortie, `OperationType` est `UPDATE_CLUSTER_CONFIGURATION`. Si `OperationState` a la valeur `UPDATE_IN_PROGRESS`, attendez un moment, puis exécutez à nouveau la commande `describe-cluster-operation`.

Mise à jour de la configuration d'un cluster à l'aide de l'API

Pour utiliser l'API afin de mettre à jour la configuration d'un cluster, consultez UpdateClusterConfiguration.

Expansion d'un cluster Amazon MSK

Utilisez cette opération Amazon MSK lorsque vous souhaitez augmenter le nombre d'agents dans votre cluster MSK. Pour développer un cluster, assurez-vous que son état soit `ACTIVE`.

> **Important**
>
> Si vous voulez étendre un cluster MSK, veillez à utiliser cette opération Amazon MSK. N'essayez pas d'ajouter d'agents à un cluster sans utiliser cette opération.

Pour de plus amples informations sur le rééquilibrage des partitions après avoir ajouté des agents à un cluster, veuillez consulter the section called “Réaffecter les partitions”.

Extension d'un cluster à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez le cluster MSK pour lequel vous souhaitez augmenter le nombre d'agents.
3. Sur la page des détails du cluster, cliquez sur le bouton Modifier en regard de l'en-tête Détails de l'agent au niveau du cluster.
4. Entrez le nombre d'agents dont le cluster doit disposer par zone de disponibilité, puis choisissez Enregistrer les modifications.

Extension d'un cluster à l'aide du AWS CLI

1. Exécutez la commande suivante, en la *`ClusterArn`*remplaçant par le Amazon Resource Name (ARN) que vous avez obtenu lors de la création de votre cluster. Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d’informations, consultez the section called “Liste des clusters”.

   Remplacez *`Current-Cluster-Version`* par la version actuelle du cluster.

> **Important**
>
> Les versions de cluster ne sont pas des entiers simples. Pour trouver la version actuelle du cluster, utilisez l'DescribeClusteropération ou la commande describe-cluster AWS CLI . Voici un exemple de version : `KTVPDKIKX0DER`.

Le paramètre *`Target-Number-of-Brokers`* représente le nombre total de nœuds d'agents que le cluster doit avoir une fois cette opération terminée avec succès. La valeur que vous spécifiez pour *`Target-Number-of-Brokers`* doit être un nombre entier supérieur au nombre actuel d'agents dans le cluster. Il doit également être un multiple du nombre de zones de disponibilité.

```
aws kafka update-broker-count --cluster-arn ClusterArn --current-version Current-
Cluster-Version --target-number-of-broker-nodes Target-Number-of-Brokers
```

La sortie de cette opération `update-broker-count` ressemble au JSON suivant.

```
{

    "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/exampleClusterName/
abcdefab-1234-abcd-5678-cdef0123ab01-2",
    "ClusterOperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef"
}
```

2. Pour obtenir le résultat de l'`update-broker-count`opération, exécutez la commande suivante en remplaçant *`ClusterOperationArn`* par l'ARN que vous avez obtenu dans le résultat de la `update-broker-count` commande.

```
aws kafka describe-cluster-operation --cluster-operation-arn ClusterOperationArn
```

La sortie de cette commande `describe-cluster-operation` ressemble à l'exemple JSON suivant.

```
{
    "ClusterOperationInfo": {
```

```
        "ClientRequestId": "c0b7af47-8591-45b5-9c0c-909a1a2c99ea",
        "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/
exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2",
        "CreationTime": "2019-09-25T23:48:04.794Z",
        "OperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef",
        "OperationState": "UPDATE_COMPLETE",
        "OperationType": "INCREASE_BROKER_COUNT",
        "SourceClusterInfo": {
            "NumberOfBrokerNodes": 9
        },
        "TargetClusterInfo": {
            "NumberOfBrokerNodes": 12
        }
    }
}
```

Dans cette sortie, `OperationType` est `INCREASE_BROKER_COUNT`. Si `OperationState` a la valeur `UPDATE_IN_PROGRESS`, attendez un moment, puis exécutez à nouveau la commande `describe-cluster-operation`.

Extension d'un cluster à l'aide de l'API

Pour augmenter le nombre de courtiers dans un cluster à l'aide de l'API, voir UpdateBrokerNombre.

Supprimer un courtier d'un cluster Amazon MSK

Utilisez cette opération Amazon MSK lorsque vous souhaitez supprimer des courtiers des clusters provisionnés par Amazon Managed Streaming for Apache Kafka (MSK). Vous pouvez réduire la capacité de stockage et de calcul de votre cluster en supprimant des ensembles de courtiers, sans impact sur la disponibilité, sans risque de durabilité des données ou sans interruption de vos applications de streaming de données.

Vous pouvez ajouter d'autres courtiers à votre cluster pour faire face à l'augmentation du trafic et supprimer des courtiers lorsque le trafic diminue. Grâce à la fonctionnalité d'ajout et de suppression de courtiers, vous pouvez utiliser au mieux la capacité de votre cluster et optimiser les coûts de votre infrastructure MSK. La suppression des courtiers vous permet de contrôler au niveau du courtier la capacité du cluster existant afin de répondre à vos besoins en matière de charge de travail et d'éviter la migration vers un autre cluster.

Utilisez la AWS console, l'interface de ligne de commande (CLI), le SDK ou AWS CloudFormation pour réduire le nombre de courtiers de votre cluster provisionné. MSK sélectionne les courtiers qui ne possèdent aucune partition (sauf pour Canary Topics) et empêche les applications de produire des données destinées à ces courtiers, tout en les retirant du cluster en toute sécurité.

Vous devez supprimer un courtier par zone de disponibilité si vous souhaitez réduire le stockage et le calcul d'un cluster. Par exemple, vous pouvez supprimer deux courtiers d'un cluster de deux zones de disponibilité ou trois courtiers d'un cluster de trois zones de disponibilité en une seule opération de suppression de courtiers.

Pour plus d'informations sur le rééquilibrage des partitions après avoir supprimé des courtiers d'un cluster, consultezthe section called “Réaffecter les partitions”.

Vous pouvez supprimer des courtiers de tous les clusters MSK provisionnés basés sur M5 et M7g, quelle que soit la taille de l'instance.

La suppression du broker est prise en charge sur les versions 2.8.1 et supérieures de Kafka, y compris sur les clusters en mode KraFT.

Rubriques

- Préparez-vous à supprimer les courtiers en supprimant toutes les partitions
- Supprimer un courtier à l'aide de la console AWS de gestion
- Supprimer un broker à l'aide de la AWS CLI
- Supprimer un courtier à l'aide de l' AWS API

Préparez-vous à supprimer les courtiers en supprimant toutes les partitions

Avant de commencer le processus de suppression des courtiers, déplacez d'abord toutes les partitions, à l'exception `__amazon_msk_canary_state` de celles relatives aux sujets `__amazon_msk_canary` et des courtiers que vous souhaitez supprimer. Il s'agit de rubriques internes créées par Amazon MSK pour les indicateurs de santé et de diagnostic du cluster.

Vous pouvez utiliser les API d'administration Kafka ou le régulateur de vitesse pour déplacer des partitions vers d'autres courtiers que vous souhaitez conserver dans le cluster. Consultez la section Réattribution de partitions.

Exemple de processus pour supprimer des partitions

Cette section est un exemple de la procédure à suivre pour supprimer des partitions du broker que vous souhaitez supprimer. Supposons que vous ayez un cluster composé de 6 courtiers, 2 courtiers dans chaque AZ, et qu'il comporte quatre sujets :

- `__amazon_msk_canary`
- `__consumer_offsets`
- `__amazon_msk_connect_offsets_my-mskc-connector_12345678-09e7-c657f7e4ff32-2`
- `msk-brk-rmv`

1. Créez un ordinateur client comme décrit dans Création d'un ordinateur client.
2. Après avoir configuré la machine cliente, exécutez la commande suivante pour répertorier toutes les rubriques disponibles dans votre cluster.

   ```
   ./bin/kafka-topics.sh --bootstrap-server “CLUSTER_BOOTSTRAP_STRING” --list
   ```

   Dans cet exemple, nous voyons quatre noms de rubrique`__amazon_msk_canary`,`__consumer_offsets`,`__amazon_msk_connect_offsets_my-mskc-connector_12345678-09e7-c657f7e4ff32-2`, et`msk-brk-rmv`.
3. Créez un fichier json appelé `topics.json` sur la machine cliente et ajoutez tous les noms de rubriques utilisateur comme dans l'exemple de code suivant. Il n'est pas nécessaire d'inclure le nom du `__amazon_msk_canary` sujet, car il s'agit d'un sujet géré par un service qui sera automatiquement déplacé si nécessaire.

   ```
   {
   "topics": [
   {"topic": "msk-brk-rmv"},
   {"topic": "__consumer_offsets"},
   {"topic": "__amazon_msk_connect_offsets_my-mskc-connector_12345678-09e7-c657f7e4ff32-2"}
   ],
   "version":1
   }
   ```
4. Exécutez la commande suivante pour générer une proposition visant à déplacer des partitions vers seulement 3 courtiers sur les 6 courtiers du cluster.

```
./bin/kafka-reassign-partitions.sh --bootstrap-server “CLUSTER_BOOTSTRAP_STRING” --
topics-to-move-json-file topics.json --broker-list 1,2,3 --generate
```

5. Créez un fichier appelé `reassignment-file.json` et copiez la commande `proposed partition reassignment configuration` que vous avez obtenue ci-dessus.
6. Exécutez la commande suivante pour déplacer les partitions que vous avez spécifiées dans le`reassignment-file.json`.

   ```
   ./bin/kafka-reassign-partitions.sh --bootstrap-server “CLUSTER_BOOTSTRAP_STRING” --
   reassignment-json-file reassignment-file.json --execute
   ```

   La sortie ressemble à ce qui suit:

   ```
   Successfully started partition reassignments for morpheus-test-topic-1-0,test-
   topic-1-0
   ```

7. Exécutez la commande suivante pour vérifier que toutes les partitions ont été déplacées.

   ```
   ./bin/kafka-reassign-partitions.sh --bootstrap-server “CLUSTER_BOOTSTRAP_STRING” --
   reassignment-json-file reassignment-file.json --verify
   ```

   La sortie ressemble à ce qui suit. Surveillez l'état jusqu'à ce que toutes les partitions des sujets que vous avez demandés aient été réattribuées avec succès :

   ```
   Status of partition reassignment:
   Reassignment of partition msk-brk-rmv-0 is completed.
   Reassignment of partition msk-brk-rmv-1 is completed.
   Reassignment of partition __consumer_offsets-0 is completed.
   Reassignment of partition __consumer_offsets-1 is completed.
   ```

8. Lorsque le statut indique que la réaffectation de partition pour chaque partition est terminée, surveillez les `UserPartitionExists` métriques pendant 5 minutes pour vous assurer qu'elles s'affichent `0` pour les courtiers à partir desquels vous avez déplacé les partitions. Après avoir confirmé cela, vous pouvez procéder à la suppression du courtier du cluster.

Supprimer un courtier à l'aide de la console AWS de gestion

Pour supprimer des courtiers à l'aide de la console AWS de gestion

1. Ouvrez la console Amazon MSK sur https://console.aws.amazon.com/msk/.
2. Choisissez le cluster MSK qui contient les courtiers que vous souhaitez supprimer.
3. Sur la page des détails du cluster, cliquez sur le bouton Actions et sélectionnez l'option Modifier le nombre de courtiers.
4. Entrez le nombre de courtiers que vous souhaitez attribuer au cluster par zone de disponibilité. La console récapitule le nombre de courtiers qui seront supprimés dans les zones de disponibilité. Assurez-vous que c'est ce que vous voulez.
5. Sélectionnez Enregistrer les modifications.

Pour éviter la suppression accidentelle de courtiers, la console vous demande de confirmer que vous souhaitez supprimer des courtiers.

Supprimer un broker à l'aide de la AWS CLI

Exécutez la commande suivante, en la `ClusterArn` remplaçant par le Amazon Resource Name (ARN) que vous avez obtenu lors de la création de votre cluster. Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d'informations, consultez Listing Amazon MSK clusters. Remplacez `Current-Cluster-Version` par la version actuelle du cluster.

> **Important**
>
> Les versions de cluster ne sont pas des entiers simples. Pour trouver la version actuelle du cluster, utilisez l'DescribeClusteropération ou la commande describe-cluster AWS CLI . Voici un exemple de version : `KTVPDKIKX0DER`.

Le paramètre *`Target-Number-of-Brokers`* représente le nombre total de nœuds d'agents que le cluster doit avoir une fois cette opération terminée avec succès. La valeur que vous spécifiez pour le *`nombre cible de courtiers`* doit être un nombre entier inférieur au nombre actuel de courtiers dans le cluster. Il doit également être un multiple du nombre de zones de disponibilité.

```
aws kafka update-broker-count --cluster-arn ClusterArn --current-version Current-
Cluster-Version --target-number-of-broker-nodes Target-Number-of-Brokers
```

La sortie de cette opération `update-broker-count` ressemble au JSON suivant.

```
{
"ClusterOperationInfo": {
"ClientRequestId": "c0b7af47-8591-45b5-9c0c-909a1a2c99ea",
        "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/exampleClusterName/
abcdefab-1234-abcd-5678-cdef0123ab01-2",
        "CreationTime": "2019-09-25T23:48:04.794Z",
        "OperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef",
        "OperationState": "UPDATE_COMPLETE",
        "OperationType": "DECREASE_BROKER_COUNT",
        "SourceClusterInfo": {
"NumberOfBrokerNodes": 12
        },
        "TargetClusterInfo": {
"NumberOfBrokerNodes": 9
        }
    }
}
```

Dans cette sortie, `OperationType` est `DECREASE_BROKER_COUNT`. Si `OperationState` a la valeur `UPDATE_IN_PROGRESS`, attendez un moment, puis exécutez à nouveau la commande `describe-cluster-operation`.

Supprimer un courtier à l'aide de l' AWS API

Pour supprimer les courtiers d'un cluster à l'aide de l'API, consultez UpdateBrokerCount dans le manuel Amazon Managed Streaming for Apache Kafka API Reference.

Mise à jour des paramètres de sécurité d'un cluster

Utilisez cette opération Amazon MSK pour mettre à jour les paramètres d'authentification et de chiffrement client-agent de votre cluster MSK. Vous pouvez également mettre à jour l'autorité de sécurité privée utilisée pour signer les certificats pour l'authentification TLS mutuelle. Vous ne pouvez pas modifier le paramètre de chiffrement intégré au cluster (agent à agent).

Le cluster doit être dans l'état `ACTIVE` pour que vous puissiez mettre à jour ses paramètres de sécurité.

Si vous activez l'authentification via IAM, SASL ou TLS, vous devez également activer le chiffrement entre les clients et les agents. Le tableau suivant présente les combinaisons possibles.

Authentification	Options de chiffrement client-agent	Chiffrement agent-agent
Unauthenticated	TLS, PLAINTEXT, TLS_PLAINTEXT	Peut être activé ou désactivé.
mTLS	TLS, TLS_PLAINTEXT	Doit être activé.
SASL/SCRAM	TLS	Doit être activé.
SASL/IAM	TLS	Doit être activé.

Lorsque le chiffrement client-agent est défini sur `TLS_PLAINTEXT` et que l'authentification client est définie sur `mTLS`, Amazon MSK crée deux types d'écouteurs auxquels les clients peuvent se connecter : un écouteur permettant aux clients de se connecter à l'aide de l'authentification mTLS avec chiffrement TLS, et un autre permettant aux clients de se connecter sans authentification ni chiffrement (texte en clair).

Pour plus d'informations sur les paramètres de sécurité, consultez la section Sécurité.

Mettre à jour les paramètres de sécurité d'un cluster à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez le cluster MSK que vous voulez mettre à jour.
3. Dans la section Paramètres, choisissez Modifier.
4. Choisissez les paramètres d'authentification et de chiffrement que vous souhaitez pour le cluster, puis sélectionnez Enregistrer les modifications.

Mettre à jour les paramètres de sécurité d'un cluster à l'aide du AWS CLI

1. Créez un fichier JSON qui contient les paramètres de chiffrement que vous souhaitez attribuer au cluster. Voici un exemple.

> **Note**
>
> Vous pouvez uniquement mettre à jour le paramètre de chiffrement client-agent. Vous ne pouvez pas mettre à jour le paramètre de chiffrement intégré au cluster (agent à agent).

```
{"EncryptionInTransit":{"ClientBroker": "TLS"}}
```

2. Créez un fichier JSON qui contient les paramètres d'authentification que vous souhaitez attribuer au cluster. Voici un exemple.

```
{"Sasl":{"Scram":{"Enabled":true}}}
```

3. Exécutez la AWS CLI commande suivante :

```
aws kafka update-security --cluster-arn ClusterArn --current-version Current-Cluster-Version --client-authentication file://Path-to-Authentication-Settings-JSON-File --encryption-info file://Path-to-Encryption-Settings-JSON-File
```

La sortie de cette opération `update-security` ressemble au JSON suivant.

```
{

    "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2",
    "ClusterOperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-abcd-4f7f-1234-9876543210ef"
}
```

4. Pour connaître l'état de l'`update-security`opération, exécutez la commande suivante en remplaçant *`ClusterOperationArn`* par l'ARN que vous avez obtenu dans le résultat de la `update-security` commande.

```
aws kafka describe-cluster-operation --cluster-operation-arn ClusterOperationArn
```

La sortie de cette commande `describe-cluster-operation` ressemble à l'exemple JSON suivant.

```
{
    "ClusterOperationInfo": {
        "ClientRequestId": "c0b7af47-8591-45b5-9c0c-909a1a2c99ea",
        "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/
exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2",
        "CreationTime": "2021-09-17T02:35:47.753000+00:00",
        "OperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef",
        "OperationState": "PENDING",
        "OperationType": "UPDATE_SECURITY",
        "SourceClusterInfo": {},
        "TargetClusterInfo": {}
    }
}
```

Si `OperationState` a la valeur `PENDING` ou `UPDATE_IN_PROGRESS`, attendez un moment, puis exécutez à nouveau la commande `describe-cluster-operation`.

Mise à jour des paramètres de sécurité d'un cluster à l'aide de l'API

Pour mettre à jour les paramètres de sécurité d'un cluster à l'aide de l'API, consultez UpdateSecurity.

> **Note**
>
> Les opérations d'API AWS CLI et destinées à mettre à jour les paramètres de sécurité d'un cluster sont idempotentes. Cela signifie que si vous invoquez l'opération de mise à jour de sécurité et que vous spécifiez un paramètre d'authentification ou de chiffrement identique à celui du cluster, ce paramètre ne changera pas.

Redémarrage d'un agent pour un cluster Amazon MSK

Utilisez cette opération Amazon MSK lorsque vous souhaitez redémarrer un agent pour votre cluster MSK. Pour redémarrer un agent pour un cluster, assurez-vous que le cluster est dans l'état `ACTIVE`.

Le service Amazon MSK peut redémarrer les agents de votre cluster MSK pendant la maintenance du système, telle que l'application de correctifs ou les mises à niveau de version. Le redémarrage

manuel d'un agent vous permet de tester la résilience de vos clients Kafka afin de déterminer comment ils répondent à la maintenance du système.

Redémarrer un courtier à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez le cluster MSK dont vous souhaitez redémarrer l'agent.
3. Faites défiler la page jusqu'à la section Informations de l'agent et choisissez l'agent que vous souhaitez redémarrer.
4. Cliquez sur le bouton Redémarrer l'agent.

Redémarrer un courtier à l'aide du AWS CLI

1. Exécutez la commande suivante, en la *ClusterArn*remplaçant par le Amazon Resource Name (ARN) que vous avez obtenu lors de la création de votre cluster, puis *BrokerId*par l'ID du broker que vous souhaitez redémarrer.

   > **Note**
   >
   > L'opération `reboot-broker` prend uniquement en charge le redémarrage d'un agent à la fois.

   Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d'informations, consultez the section called “Liste des clusters”.

   Si vous ne disposez pas d'identifiants d'agent pour votre cluster, vous pouvez les trouver en répertoriant les nœuds d'agents. Pour plus d'informations, consultez list-nodes.

   ```
   aws kafka reboot-broker --cluster-arn ClusterArn --broker-ids BrokerId
   ```

   La sortie de cette opération `reboot-broker` ressemble au JSON suivant.

   ```
   {

       "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/exampleClusterName/
   abcdefab-1234-abcd-5678-cdef0123ab01-2",
   ```

```
    "ClusterOperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef"
}
```

2. Pour obtenir le résultat de l'`reboot-broker`opération, exécutez la commande suivante en la *`ClusterOperationArn`*remplaçant par l'ARN que vous avez obtenu dans le résultat de la `reboot-broker` commande.

```
aws kafka describe-cluster-operation --cluster-operation-arn ClusterOperationArn
```

La sortie de cette commande `describe-cluster-operation` ressemble à l'exemple JSON suivant.

```
{
    "ClusterOperationInfo": {
        "ClientRequestId": "c0b7af47-8591-45b5-9c0c-909a1a2c99ea",
        "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/
exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2",
        "CreationTime": "2019-09-25T23:48:04.794Z",
        "OperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef",
        "OperationState": "REBOOT_IN_PROGRESS",
        "OperationType": "REBOOT_NODE",
        "SourceClusterInfo": {},
        "TargetClusterInfo": {}
    }
}
```

Lorsque l'opération de redémarrage est terminée, l'opération `OperationState` devient `REBOOT_COMPLETE`.

Redémarrage d'un agent à l'aide de l'API

Pour redémarrer un courtier dans un cluster à l'aide de l'API, consultez RebootBroker.

Impact du redémarrage du broker lors de l'application de correctifs et d'autres opérations de maintenance

Amazon MSK met régulièrement à jour le logiciel de vos courtiers. Ces mises à jour n'ont aucun impact sur les écritures et les lectures de vos applications si vous suivez les meilleures pratiques.

Amazon MSK utilise des mises à jour logicielles continues afin de maintenir la haute disponibilité de vos clusters. Au cours de ce processus, les courtiers sont redémarrés un par un et Kafka transfère automatiquement le leadership à un autre courtier en ligne. Les clients Kafka disposent de mécanismes intégrés pour détecter automatiquement le changement de direction des partitions et continuer à écrire et à lire des données dans un cluster MSK.

Lorsqu'un courtier se déconnecte, il est normal de constater des erreurs de déconnexion transitoires chez vos clients. Vous observerez également pendant une brève période (jusqu'à 2 minutes, généralement moins) des pics de latence de lecture et d'écriture de p99 (généralement des millisecondes élevées, jusqu'à environ 2 secondes). Ces pics sont attendus et sont causés par le fait que le client se reconnecte à un nouveau courtier leader ; cela n'a aucun impact sur vos produits ou votre consommation et se résorbera après la reconnexion.

Vous observerez également une augmentation de la métrique`UnderReplicatedPartitions`, ce qui est attendu car les partitions du broker qui a été arrêté ne répliquent plus les données. Cela n'a aucun impact sur les écritures et les lectures des applications, car les répliques de ces partitions hébergées sur d'autres courtiers répondent désormais aux demandes.

Après la mise à jour logicielle, lorsque le courtier revient en ligne, il doit « rattraper » les messages produits alors qu'il était hors ligne. Pendant le catch up, vous pouvez également observer une augmentation de l'utilisation du débit du volume et du processeur. Cela ne devrait pas avoir d'impact sur les écritures et les lectures dans le cluster si vos courtiers disposent de suffisamment de ressources en termes de processeur, de mémoire, de réseau et de volume.

Balisage d'un cluster Amazon MSK

Vous pouvez affecter vos propres métadonnées sous la forme de balises à une ressource Amazon MSK, telle qu'un cluster MSK. Une balise est une paire clé-valeur que vous définissez pour la ressource. L'utilisation de balises est un moyen simple mais puissant de gérer les AWS ressources et d'organiser les données, y compris les données de facturation.

Rubriques

Principes de base des étiquettes

Vous pouvez utiliser l'API Amazon MSK pour effectuer les tâches suivantes :

- Ajouter des balises à une ressource Amazon MSK.
- Répertorier les balises pour une ressource Amazon MSK.
- Supprimer les balises d'une ressource Amazon MSK.

Vous pouvez également utiliser des balises pour classer vos ressources Amazon MSK par catégorie. Par exemple, vous pouvez classer les clusters Amazon MSK par objectif, propriétaire ou environnement. Dans la mesure où vous avez défini la clé et la valeur de chaque balise, vous pouvez créer un ensemble personnalisé de catégories répondant à vos besoins spécifiques. Par exemple, vous pouvez définir un ensemble de balises vous permettant de suivre les clusters par propriétaire et application associée.

Voici plusieurs exemples de balises :

- `Project: Project name`
- `Owner: Name`
- `Purpose: Load testing`
- `Environment: Production`

Suivi des coûts à l'aide d'étiquettes

Vous pouvez utiliser des balises pour classer et suivre vos AWS coûts. Lorsque vous appliquez des balises à vos AWS ressources, notamment aux clusters Amazon MSK, votre rapport de répartition des AWS coûts inclut l'utilisation et les coûts agrégés par balises. Vous pouvez organiser vos coûts entre plusieurs services en appliquant des balises qui représentent des catégories métier (telles que les centres de coûts, les noms d'applications ou les propriétaires). Pour plus d'informations, consultez

Utilisation des identifications de répartition des coûts pour les rapports de facturation personnalisés dans le Guide de l'utilisateur AWS Billing .

Restrictions liées aux étiquettes

Les restrictions suivantes s'appliquent aux balises dans Amazon MSK.

Restrictions de base

- Le nombre maximum d'identifications par ressource est de 50.
- Les clés et valeurs d'étiquette sont sensibles à la casse.
- Vous ne pouvez pas changer ou modifier les balises d'une ressource supprimée.

Restrictions relatives aux clés de balise

- Chaque clé de balise doit être unique. Si vous ajoutez une balise avec une clé qui est déjà en cours d'utilisation, la nouvelle balise remplacera la paire clé-valeur existante.
- Vous ne pouvez pas démarrer une clé de balise avec, `aws:` car ce préfixe est réservé à une utilisation par AWS. AWS crée des balises qui commencent par ce préfixe en votre nom, mais vous ne pouvez pas les modifier ou les supprimer.
- Les clés de balise doivent comporter entre 1 et 128 caractères Unicode.
- Les clés de balise doivent comporter les caractères suivants : lettres Unicode, chiffres, espaces et les caractères spéciaux suivants : `_ . / = + - @`.

Restrictions relatives à la valeur de balise

- Les valeurs de balise doivent comporter entre 0 et 255 caractères Unicode.
- Les valeurs de balise peuvent être vides. Si tel n'est pas le cas, elles doivent être composées des caractères suivants : lettres Unicode, chiffres, espaces et les caractères spéciaux suivants : `_ . / = + - @`.

Balisage des ressources à l'aide de l'API Amazon MSK

Vous pouvez utiliser les opérations suivantes pour marquer ou annuler les balises d'une ressource Amazon MSK ou pour répertorier l'ensemble actuel de balises pour une ressource :

- ListTagsForResource

- TagResource
- UntagResource

Configuration d’Amazon MSK

Amazon Managed Streaming for Apache Kafka fournit une configuration par défaut pour les courtiers, les topics et les nœuds Apache ZooKeeper . Vous pouvez également créer des configurations personnalisées et les utiliser pour créer de nouveaux clusters MSK ou pour mettre à jour des clusters existants. Une configuration MSK consiste en un ensemble de propriétés et leurs valeurs correspondantes.

Rubriques

Configurations MSK personnalisées

Vous pouvez utiliser Amazon MSK pour créer une configuration MSK personnalisée dans laquelle vous définissez les propriétés suivantes. Les propriétés que vous ne définissez pas obtiennent explicitement les valeurs qu'elles ont dans the section called “Configuration par défaut”. Pour de plus amples informations sur les propriétés de configuration, veuillez consulter Configuration d'Apache Kafka.

Propriétés de configuration d'Apache Kafka

Name (Nom)	Description
allow.everyone.if.no.acl.found	Si vous souhaitez définir cette propriété sur `false`, assurez-vous d'abord de définir des listes de contrôle d'accès (ACL) Apache Kafka pour votre cluster. Si vous définissez cette propriété sur `false` et que vous ne définissez pas d'abord les listes de contrôle d'accès (ACL) Apache Kafka, vous perdez l'accès au cluster. Dans ce cas, vous pouvez à nouveau mettre à jour la configuration et définir cette propriété sur `true` pour accéder de nouveau au cluster.

Name (Nom)	Description
auto.create.topics.enable	Active la création automatique de rubriques sur le serveur.
compression.type	Type de compression final pour une rubrique donnée. Vous pouvez définir cette propriété sur les codecs de compression standard (`gzip`, `snappy`, `lz4` et `zstd`). Il accepte en outre `uncompressed` . Cette valeur équivaut à l'absence de compression. Si vous définissez la valeur sur `producer`, cela implique de retenir le codec de compression d'origine défini par le producteur.
connections.max.idle.ms	Délai d'expiration des connexions inactives en millisecondes. Les threads du processeu r de socket de serveur ferment les connexion s inactives pendant une durée supérieure à la valeur que vous avez définie pour cette propriété.
default.replication.factor	Facteur de réplication par défaut pour les rubriques créées automatiquement.
delete.topic.enable	Active l'opération de suppression de rubrique. Si vous désactivez cette configuration, vous ne pouvez pas supprimer une rubrique via l'outil d'administration.
group.initial.rebalance.delay.ms	Temps pendant lequel le coordinateur du groupe attend que davantage de consommat eurs de données rejoignent un nouveau groupe avant d'effectuer le premier rééquilibrage. Un délai plus long signifie potentiellement moins de rééquilibrages, mais augmente le temps jusqu'au début du traitement.

Name (Nom)	Description
group.max.session.timeout.ms	Délai maximal de session pour les consommateurs enregistrés. Les délais d'expiration plus longs donnent aux consommateurs plus de temps pour traiter les messages entre les battements de cœur, au prix d'un délai plus long pour détecter les défaillances.
group.min.session.timeout.ms	Délai d'expiration minimum de session pour les consommateurs enregistrés. Des délais d'expiration plus courts entraînent une détection plus rapide des défaillances, au prix des battements de cœur plus fréquents des consommateurs. Cela peut surcharger les ressources des agents.
leader.imbalance.per.broker.pourcentage	Ratio de déséquilibre de leader autorisé par courtier. Le contrôleur déclenche un équilibrage de leader s'il dépasse cette valeur par agent. Cette valeur est spécifiée en pourcentage.
log.cleaner.delete.retention.ms	Durée pendant laquelle vous souhaitez qu'Apache Kafka conserve les enregistrements supprimés. La valeur minimale est 0.

Name (Nom)	Description
log.cleaner.min.cleanable.ratio	Cette propriété de configuration peut avoir des valeurs comprises entre 0 et 1. Cette valeur détermine la fréquence à laquelle le compacteur de journal tente de nettoyer le journal (si le compactage du journal est activé). Par défaut, Apache Kafka évite de nettoyer un journal si plus de 50 % du journal a été compacté. Ce ratio limite l'espace maximal que le journal gaspille avec des doublons (à 50 %, cela signifie que le journal peut contenir tout au plus 50 % de doublons). Un ratio plus élevé signifie moins de nettoyages, plus efficaces, mais aussi plus d'espace perdu dans le journal.
log.cleanup.policy	Stratégie de nettoyage par défaut pour les segments au-delà de la fenêtre de rétention. Liste de stratégies valides séparées par des virgules. Les stratégies valides sont `delete` et `compact`. Pour les clusters compatibles avec le stockage hiérarchisé, la politique valide est `delete` uniquement.
log.flush.interval.messages	Nombre de messages accumulés sur une partition de journal avant que les messages ne soient vidés sur le disque.
log.flush.interval.ms	Durée maximale en millisecondes pendant laquelle un message dans une rubrique est conservé en mémoire avant d'être vidé sur le disque. Si vous ne définissez pas cette valeur, la valeur de log.flush.scheduler.interval.ms est utilisée. La valeur minimale est 0.

Name (Nom)	Description
log.message.timestamp.difference.max.ms	Différence de temps maximale autorisée entre l'horodatage lorsqu'un agent reçoit un message et l'horodatage spécifié dans le message. Si log.message.timestamp.type=CreateTime, un message est rejeté si la différence d'horodat age dépasse ce seuil. Cette configuration est ignorée si LogAppend log.message.timest amp.type= Time.
log.message.timestamp.type	Spécifie si l'horodatage du message est l'heure de création du message ou l'heure d'ajout du journal. Les valeurs autorisées sont `CreateTime` et `LogAppendTime` .
log.retention.bytes	Taille maximale du journal avant de le supprimer.
log.retention.hours	Nombre d'heures pour conserver un fichier journal avant de le supprimer, tertiaire à la propriété log.retention.ms.
log.retention.minutes	Nombre de minutes de conservation d'un fichier journal avant de le supprimer, secondaire à la propriété log.retention.ms. Si vous ne définisse z pas cette valeur, la valeur de log.reten tion.hours est utilisée.
log.retention.ms	Nombre de millisecondes pour conserver un fichier journal avant de le supprimer (en millisecondes), si ce n'est pas défini, la valeur dans log.retention.minutes est utilisée.

Name (Nom)	Description
log.roll.ms	Durée maximale avant le déploiement d'un nouveau segment de journal (en milliseco ndes). Si vous ne définissez pas cette valeur, la valeur de log.roll.hours est utilisée. La valeur minimale possible pour cette propriété est 1.
log.segment.bytes	Taille maximale d'un seul fichier journal.
max.incremental.fetch.session.cache.slots	Nombre maximal de sessions d'extraction incrémentielle qui sont maintenues.
message.max.octets	La plus grande taille de lot d'enregistrement autorisée par Kafka. Si vous augmentez la valeur et qu'il y a des consommateurs plus anciens que 0.10.2, vous devez aussi augmenter la taille d'extraction des consommat eurs afin qu'ils puissent récupérer des lots d'enregistrements aussi volumineux. La dernière version de format de message regroupe toujours les massages en lots pour plus d'efficacité. Les versions de format de message précédentes ne regroupent pas les enregistrements non compressés en lots et dans ce cas, cette limite ne s'applique qu'à un seul enregistrement. Vous pouvez définir cette valeur par rubrique avec le niveau de rubrique max.message.bytes config.

Name (Nom)	Description
min.insync.replicas	Lorsqu'un producteur définit acks sur `"all"` (ou `"-1"`), la valeur de min.insync.replicas spécifie le nombre minimum de réplicas qui doivent reconnaître une écriture pour que celle-ci soit considérée comme réussie. Si ce minimum ne peut être atteint, le producteur émet une exception (NotEnoughReplicas ou NotEnoughReplicasAfterAppend). Vous pouvez utiliser des valeurs dans min.insync.replicas et acks pour appliquer de meilleures garanties de durabilité. Par exemple, vous pouvez créer une rubrique avec un facteur de réplication de 3, définir min.insync.replica s sur 2 et produire avec des acks de `"all"`. Cela garantit que le producteur déclenche une exception si la majorité des réplicas ne reçoivent pas d'écriture.
num.io.threads	Nombre de threads utilisés par le serveur pour le traitement des demandes, qui peuvent inclure des E/S de disque.
num.network.threads	Nombre de threads que le serveur utilise pour recevoir des demandes du réseau et lui envoyer des réponses.
num.partitions	Nombre par défaut de partitions de journal par rubrique.
num.recovery.threads.per.data.dir	Nombre de threads par répertoire de données à utiliser pour récupérer des journaux au démarrage et pour leur vidage lors de l'arrêt.

Name (Nom)	Description
num.replica.fetchers	Nombre de threads de récupération utilisés pour répliquer les messages d'un broker source. Si vous augmentez cette valeur, vous pouvez augmenter le degré de parallélisme d'E/S dans l'agent suiveur.
offsets.retention.minutes	Lorsqu'un groupe de consommateurs perd tous ses consommateurs (c'est-à-dire qu'il devient vide), ses compensations sont conservées pour cette période de rétention avant d'être jetées. Pour les consommateurs autonomes (c'est-à-dire ceux qui utilisent l'affectation manuelle), les décalages expirent après l'heure de la dernière validation plus cette période de conservation.
offsets.topic.replication.factor	Facteur de réplication de la rubrique des décalages. Définissez cette valeur à un niveau supérieur pour garantir la disponibilité. La création de rubrique interne échoue jusqu'à ce que la taille du cluster réponde à cette exigence de facteur de réplication.
réplica.fetch.max.bytes	Nombre d'octets de messages à essayer de récupérer pour chaque partition. Ce n'est pas un maximum absolu. Si le premier lot d'enregis trements de la première partition non vide de l'extraction est supérieur à cette valeur, le lot d'enregistrements est renvoyé pour assurer la progression. Les message.max.bytes (broker config) ou max.message.bytes (topic config) définissent la taille maximale du lot d'enregis trements que l'agent accepte.

Name (Nom)	Description
replica.fetch.response.max.bytes	Nombre maximal d'octets attendu pour l'ensemble de la réponse de récupération. Les enregistrements sont récupérés par lots, et si le premier lot d'enregistrements de la première partition non vide de l'extraction est supérieur à cette valeur, le lot d'enregistrements sera toujours renvoyé pour assurer la progressi on. Ce n'est pas un maximum absolu. Les propriétés message.max.bytes (broker config) ou max.message.bytes (topic config) spécifient la taille maximale du lot d'enregistrements que le broker accepte.
replica.lag.time.max.ms	Si un suiveur n'a envoyé aucune demande d'extraction ou n'a pas consommé le décalage de fin existant avec le journal du leader pendant au moins ce nombre de millisecondes, le leader supprime le suiveur de l'ISR. MinValue: 10000 MaxValue = 30000
replica.selector.class	Le nom de classe complet qui implémente ReplicaSelector. L'agent utilise cette valeur pour trouver le réplica en lecture préféré. Si vous utilisez Apache Kafka, version 2.4.1 ou supérieure, et que vous souhaitez permettre aux consommateurs de récupérer le réplica le plus proche, définissez cette propriété sur `org.apache.kafka.common.rep lica.RackAwareReplicaSelector` . Pour plus d'informations, consultez the section called “Apache Kafka version 2.4.1 (utilisez plutôt 2.4.1.1)”.

Name (Nom)	Description
replica.socket.receive.buffer.bytes	Tampon de réception du socket pour les demandes réseau.
socket.receive.buffer.bytes	Tampon SO_RCVBUF des sockets de serveur de socket. La valeur minimale que vous pouvez définir pour cette propriété est -1. Si la valeur est -1, Amazon MSK utilise le système d'exploit ation par défaut.
socket.request.max.octets	Nombre maximal d'octets dans une requête socket.
socket.send.buffer.bytes	Tampon SO_SNDBUF des sockets de serveur de socket. La valeur minimale que vous pouvez définir pour cette propriété est -1. Si la valeur est -1, Amazon MSK utilise le système d'exploit ation par défaut.
transaction.max.timeout.ms	Délai maximal pour les transactions. Si le temps de transaction demandé à un client dépasse cette valeur, le courtier renvoie une erreur InitProducerIdRequest. Cela évite au client un délai d'expiration trop important et cela peut empêcher les consommateurs de lire des rubriques incluses dans la transaction.
transaction.state.log.min.isr	Configuration min.insync.replicas remplacée pour la rubrique de la transaction.
transaction.state.log.replication.factor	Facteur de réplication de la rubrique de la transaction. Configurez cette propriété sur une valeur plus élevée pour augmenter la disponibi lité. La création de rubrique interne échoue jusqu'à ce que la taille du cluster réponde à cette exigence de facteur de réplication.

Name (Nom)	Description
transactional.id.expiration.ms	Durée en millisecondes pendant laquelle le coordinateur de transactions attend de recevoir les mises à jour du statut de la transaction en cours avant que l'ID transactionnel du coordinateur n'expire. Ce paramètre influence également l'expiration de l'ID de producteur, car il entraîne l'expiration de ce dernier lorsque ce délai est écoulé après la dernière écriture avec l'ID de producteur donné. Les ID de producteur peuvent expirer plus tôt si la dernière écriture à partir de l'ID de producteur est supprimée en raison des paramètres de conservation de la rubrique. La valeur minimale pour cette propriété est 1 milliseconde.
unclean.leader.election.enable	Indique si les réplicas ne figurant pas dans l'ensemble ISR doivent servir de leader en dernier recours, même si cela peut entraîner une perte de données.
zookeeper.connection.timeout.ms	ZooKeeper clusters de modes. Durée maximale pendant laquelle le client attend avant d'établir une connexion. ZooKeeper Si vous ne définissez pas cette valeur, la valeur de zookeeper.session.timeout.ms est utilisée. MinValue = 6000 MaxValue (inclus) = 18000

Name (Nom)	Description
zookeeper.session.timeout.ms	ZooKeeper clusters de modes. Le délai d'expiration de ZooKeeper la session Apache en millisecondes. MinValue = 6000 MaxValue (inclus) = 18000

Pour savoir comment créer une configuration MSK personnalisée, dresser une liste de toutes les configurations ou les décrire, veuillez consulter the section called “Opérations de configuration”. Pour créer un cluster MSK à l'aide d'une configuration MSK personnalisée ou pour mettre à jour un cluster avec une nouvelle configuration personnalisée, consultez Comment ça marche.

Lorsque vous mettez à jour votre cluster MSK existant avec une configuration MSK personnalisée, Amazon MSK redémarre la propagation lorsque nécessaire et utilise les bonnes pratiques pour limiter les temps d'arrêt du client. Par exemple, après qu'Amazon MSK a redémarré chaque agent, il essaie de laisser l'agent rattraper les données que l'agent a pu manquer lors de la mise à jour de la configuration avant de passer à l'agent suivant.

Configuration dynamique

Outre les propriétés de configuration fournies par Amazon MSK, vous pouvez définir dynamiquement les propriétés de configuration au niveau du cluster et de l'agent qui ne nécessitent pas de redémarrage de l'agent. Vous pouvez définir certaines propriétés de configuration de manière dynamique. Il s'agit des propriétés qui ne sont pas marquées en lecture seule dans la table sous Configurations de l'agent dans la documentation Apache Kafka. Pour de plus amples informations sur la configuration dynamique et les exemples de commandes, consultez Mise à jour des configurations de l'agent dans la documentation Apache Kafka.

> **Note**
>
> Vous pouvez définir la propriété `advertised.listeners`, mais pas la propriété `listeners`.

Configuration au niveau de la rubrique

Vous pouvez utiliser les commandes Apache Kafka pour définir ou modifier les propriétés de configuration au niveau des rubriques nouvelles et existantes. Pour de plus amples informations sur les propriétés de configuration au niveau de la rubrique et pour obtenir des exemples de définition, consultez Configurations au niveau de la rubrique dans la documentation Apache Kafka.

États de configuration

Une configuration Amazon MSK peut avoir l'un des états suivants. Pour effectuer une opération sur une configuration, celle-ci doit être à l'état `ACTIVE` ou `DELETE_FAILED` :

- `ACTIVE`
- `DELETING`
- `DELETE_FAILED`

Configuration Amazon MSK par défaut

Lorsque vous créez un cluster MSK et que vous ne spécifiez pas de configuration MSK personnalisée, Amazon MSK crée et utilise une configuration par défaut avec les valeurs indiquées dans le tableau suivant. Pour les propriétés qui ne figurent pas dans cette table, Amazon MSK utilise les valeurs par défaut associées à votre version d'Apache Kafka. Pour obtenir la liste de ces valeurs par défaut, consultez Apache Kafka Configuration.

Valeurs de la configuration par défaut

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
allow.everyone.if.no.acl.found	Si aucun modèle de ressource ne correspond à une ressource spécifique, la ressource n'a aucune ACL associée. Dans ce cas, si vous	`true`	`true`

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
	définissez cette propriété sur `true`, tous les utilisateurs peuvent accéder à la ressource, et pas seulement les super utilisateurs.		
auto.create.topics.enable	Active la création automatique d'une rubrique sur le serveur.	`false`	`false`
auto.leader.rebalance.enable	Active l'équilibrage automatique du leader. Un thread d'arrière-plan vérifie et lance un équilibrage de leader si nécessaire à intervalles réguliers.	`true`	`true`
default.replication.factor	Facteurs de réplication par défaut pour les rubriques créées automatiquement.	3 pour les clusters situés dans 3 zones de disponibilité et 2 pour les clusters situés dans 2 zones de disponibilité.	3 pour les clusters situés dans 3 zones de disponibilité et 2 pour les clusters situés dans 2 zones de disponibilité.

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
local.retention.bytes	Taille maximale des segments de journal locaux pour une partition avant la suppression des anciens segments. Si vous ne définissez pas cette valeur, la valeur de log.retention.bytes est utilisée. La valeur effective doit toujours être inférieure ou égale à la valeur de log.retention.bytes. Une valeur par défaut de -2 signifie qu'aucune limite n'est appliquée à la conservation locale. Cela correspond au paramètre retention.ms/bytes de -1. Les propriétés local.retention.ms et local.retention.bytes sont similaires à log.retention, car elles sont utilisées pour déterminer la durée pendant laquelle les segments de journal doivent	-2 pour un nombre illimité	-2 pour un nombre illimité

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
	être conservés dans le stockage local. Les configurations log.retention.* existantes sont des configurations de conservation pour la partition de la rubrique. Cela inclut le stockage local et distant. Valeurs valides : nombres entiers compris entre [-2 ; +Inf]		

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
local.retention.ms	Nombre de millisecondes pour retenir le segment de journal local avant sa suppression. Si vous ne définissez pas cette valeur, Amazon MSK utilise la valeur de log.retention.ms. La valeur effective doit toujours être inférieure ou égale à la valeur de log.retention.bytes. Une valeur par défaut de -2 signifie qu'aucune limite n'est appliquée à la conservation locale. Cela correspond au paramètre retention.ms/bytes de -1. Les valeurs local.retention.ms et local.retention.bytes sont similaires à celles de log.retention. MSK utilise cette configuration pour déterminer la durée pendant laquelle les segments de journal doivent	-2 pour un nombre illimité	-2 pour un nombre illimité

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
	être conservés dans le stockage local. Les configurations log.retention.* existantes sont des configurations de conservation pour la partition de la rubrique. Cela inclut le stockage local et distant. Les valeurs valides sont des nombres entiers supérieurs à 0.		

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
log.message.timestamp.difference.max.ms	Différence maximale autorisée entre l'horodatage lorsqu'un broker reçoit un message et l'horodatage spécifié dans le message. Si log.message.timestamp.type=CreateTime, un message sera rejeté si la différence d'horodatage dépasse ce seuil. Cette configuration est ignorée si LogAppend log.message.timestamp.type=Time. La différence d'horodatage maximale autorisée ne doit pas être supérieure à log.retention.ms afin d'éviter la propagation de journaux inutilement fréquente.	9223372036854775807	86400000 pour Kafka 2.8.2.tiered
log.segment.bytes	Taille maximale d'un seul fichier journal.	1073741824	134217728

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
min.insync.replicas	Lorsqu'un producteur définit la valeur de acks (accusé de réception reçu par le producteur de l'agent Kafka) sur `"all"` (ou `"-1"`), la valeur de min.insync.replicas spécifie le nombre minimum de réplicas qui doivent reconnaître une écriture pour que celle-ci soit considérée comme réussie. Si cette valeur n'atteint pas ce minimum, le producteur déclenche une exception (NotEnoughReplicas ou NotEnoughReplicasAfterAppend). Lorsque vous utilisez les valeurs de min.insync.replicas et acks ensemble, vous pouvez appliquer de meilleures garanties de durabilité. Par exemple, vous pouvez créer une rubrique	2 pour les clusters situés dans 3 zones de disponibilité et 1 pour les clusters situés dans 2 zones de disponibilité.	2 pour les clusters situés dans 3 zones de disponibilité et 1 pour les clusters situés dans 2 zones de disponibilité.

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
	avec un facteur de réplication de 3, définir min.insyn c.replicas sur 2 et produire avec des acks de `"all"`. Cela garantit que le producteur déclenche une exception si la majorité des réplicas ne reçoivent pas d'écriture.		
num.io.threads	Nombre de threads utilisés par le serveur pour produire des demandes, qui peuvent inclure des E/S de disque.	8	max (8, vCPU) où les vCPU dépendent de la taille d'instance de l'agent
num.network.threads	Nombre de threads que le serveur utilise pour recevoir des demandes du réseau et lui envoyer des réponses.	5	max (5, vCPU / 2) où les vCPU dépendent de la taille d'instance de l'agent
num.partitions	Nombre par défaut de partitions de journal par rubrique.	1	1

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
num.replica.fetchers	Nombre de threads de récupération utilisés pour répliquer les messages provenant d'un agent source. Si vous augmentez cette valeur, vous pouvez augmenter le degré de parallélisme des E/S dans l'agent suiveur.	2	max (2, vCPU / 4) où les vCPU dépendent de la taille d'instance de l'agent
remote.log.msk.disable.policy	Utilisé avec remote.storage.enable pour désactiver le stockage hiérarchisé. Définissez cette politique sur Supprimer, pour indiquer que les données du stockage hiérarchisé sont supprimées lorsque vous définissez remote.storage.enable sur false.	N/A	DELETE

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
remote.log.reader.threads	Taille du pool de threads du lecteur de journaux distant, qui est utilisée pour planifier des tâches visant à récupérer des données à partir d'un stockage distant.	N/A	max (10, vCPU * 0,67) où les vCPU dépendent de la taille d'instance de l'agent
remote.storage.enable	Active le stockage (distant) hiérarchisé pour une rubrique s'il est défini sur true. Désactive le stockage hiérarchisé au niveau de la rubrique s'il est défini sur false et remote.log.msk.disable.policy est défini sur Supprimer. Lorsque vous désactivez le stockage hiérarchisé, vous supprimez les données du stockage distant. Lorsque vous désactivez le stockage hiérarchisé pour une rubrique, vous ne pouvez pas le réactiver.	false	true

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
replica.lag.time.max.ms	Si un suiveur n'a envoyé aucune demande d'extraction ou n'a pas consommé le décalage de fin existant avec le journal du leader pendant au moins ce nombre de millisecondes, le leader supprime le suiveur de l'ISR.	30 000	30 000

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
retention.ms	Champ obligatoire. La durée minimale est de 3 jours. Le paramètre étant obligatoire, il n'y a pas de valeur par défaut. Amazon MSK utilise la valeur retention.ms avec local.retention.ms pour déterminer à quel moment les données sont transférées du stockage local vers le stockage hiérarchisé. La valeur local.retention.ms indique quand déplacer les données du stockage local vers le stockage hiérarchisé. La valeur retention.ms indique à quel moment les données doivent être supprimées du stockage hiérarchisé (c'est-à-dire lorsqu'elles sont supprimées du cluster). Valeurs valides : nombres	Minimum 259 200 000 millisecondes (3 jours). -1 pour une conservation illimitée.	Minimum 259 200 000 millisecondes (3 jours). -1 pour une conservation illimitée.

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
	entiers compris entre [-1 ; +Inf]		
socket.receive.buffer.bytes	Tampon SO_RCVBUF tampon des sockets de serveur de socket. Si la valeur est -1, le système d'exploitation par défaut est utilisé.	102400	102400
socket.request.max.octets	Nombre maximal d'octets dans une requête socket.	104857600	104857600
socket.send.buffer.bytes	Tampon SO_SNDBUF des sockets de serveur de socket. Si la valeur est -1, le système d'exploitation par défaut est utilisé.	102400	102400
unclean.leader.election.enable	Indique si vous souhaiter que les réplicas ne figurant pas dans l'ensemble ISR servent de leader en dernier recours, même si cela peut entraîner une perte de données.	vrai	false

Name (Nom)	Description	Valeur par défaut d'un cluster de stockage non hiérarchisé	Valeur par défaut d'un cluster de stockage hiérarchisé
zookeeper.session.timeout.ms	Le délai d'expiration de ZooKeeper la session Apache en millisecondes.	18000	18000
zookeeper.set.acl	Client défini pour utiliser des listes de contrôle d'accès (ACL) sécurisées.	false	false

Pour de plus amples informations sur la définition de valeurs de configuration personnalisées, consultez the section called “Configurations personnalisées”.

Directives relatives à la configuration du stockage hiérarchisé au niveau de la rubrique

Vous trouverez ci-dessous les paramètres et les limites par défaut lorsque vous configurez le stockage hiérarchisé au niveau de la rubrique.

- Amazon MSK ne prend pas en charge les segments de journal de plus petite taille pour les rubriques pour lesquelles le stockage hiérarchisé est activé. Si vous souhaitez créer un segment, la taille minimale du segment de journal est de 48 Mio, ou le temps d'exécution des segments est d'au moins 10 minutes. Ces valeurs correspondent aux propriétés segment.bytes et segment.ms.
- La valeur de local.retention.ms/bytes ne peut pas être égale ou supérieure à retention.ms/bytes. Il s'agit du paramètre de conservation du stockage hiérarchisé.
- La valeur par défaut de local.retention.ms/bytes est -2. Cela signifie que la valeur retention.ms est utilisée pour local.retention.ms/bytes. Dans ce cas, les données restent à la fois dans le stockage local et dans le stockage hiérarchisé (une copie dans chaque cas), et elles expirent en même temps. Pour cette option, une copie des données locales est conservée sur le stockage distant. Dans ce cas, les données lues à partir du trafic de consommation proviennent du stockage local.

- La valeur par défaut de retention.ms est de 7 jours. Il n'existe aucune limite de taille par défaut pour retention.bytes.
- La valeur minimale de retention.ms/bytes est -1. Cela signifie une conservation infinie.
- La valeur minimale de local.retention.ms/bytes est -2. Cela signifie une conservation infinie pour le stockage local. Il correspond au paramètre retention.ms/bytes égal à -1.
- La configuration retention.ms au niveau de la rubrique est obligatoire pour les rubriques pour lesquelles le stockage hiérarchisé est activé. La valeur minimale de retention.ms est de 3 jours.

Opérations de configuration d'Amazon MSK

Cette rubrique décrit comment créer des configurations MSK personnalisées et effectuer des opérations sur celles-ci. Pour de plus amples informations sur l'utilisation des configurations MSK pour créer ou mettre à jour des clusters, reportez-vous à la section Comment ça marche.

Cette rubrique contient les sections suivantes :

Pour créer une configuration MSK

1. Créez un fichier dans lequel vous spécifiez les propriétés de configuration à définir et les valeurs que vous souhaitez leur attribuer. Voici le contenu d'un exemple de fichier de configuration.

   ```
   auto.create.topics.enable = true

   log.roll.ms = 604800000
   ```

2. Exécutez la AWS CLI commande suivante et remplacez *config-file-path* par le chemin du fichier dans lequel vous avez enregistré votre configuration à l'étape précédente.

> **Note**
>
> Le nom que vous choisissez pour votre configuration doit correspondre à la regex suivante : « ^[0-9A-Za-z][0-9A-Za-z-]{0,}$ ».

```
aws kafka create-configuration --name "ExampleConfigurationName" --description
 "Example configuration description." --kafka-versions "1.1.1" --server-properties
 fileb://config-file-path
```

Voici un exemple de réponse réussie après l'exécution de cette commande.

```
{
    "Arn": "arn:aws:kafka:us-east-1:123456789012:configuration/SomeTest/
abcdabcd-1234-abcd-1234-abcd123e8e8e-1",
    "CreationTime": "2019-05-21T19:37:40.626Z",
    "LatestRevision": {
        "CreationTime": "2019-05-21T19:37:40.626Z",
        "Description": "Example configuration description.",
        "Revision": 1
    },
    "Name": "ExampleConfigurationName"
}
```

3. La commande précédente renvoie un Amazon Resource Name (ARN) pour votre nouvelle configuration. Enregistrez cet ARN car vous en avez besoin pour faire référence à cette configuration dans d'autres commandes. Si vous perdez votre ARN de configuration, vous pouvez répertorier toutes les configurations de votre compte pour le retrouver.

Pour mettre à jour une configuration MSK

1. Créez un fichier dans lequel vous spécifiez les propriétés de configuration que vous souhaitez mettre à jour et les valeurs que vous souhaitez leur attribuer. Voici le contenu d'un exemple de fichier de configuration.

```
auto.create.topics.enable = true

min.insync.replicas = 2
```

2. Exécutez la commande AWS CLI suivante et remplacez *config-file-path* par le chemin d'accès au fichier dans lequel vous avez enregistré votre configuration à l'étape précédente.

   Remplacez *configuration-arn* par l'ARN obtenu lors de la création de la configuration. Si vous n'avez pas enregistré l'ARN lorsque vous avez créé la configuration, vous pouvez utiliser la commande `list-configurations` pour répertorier toutes les configurations de votre compte. La configuration que vous souhaitez voir figurer dans la liste apparaît dans la réponse. L'ARN de la configuration apparaît également dans cette liste.

   ```
   aws kafka update-configuration --arn configuration-arn --description "Example
    configuration revision description." --server-properties fileb://config-file-path
   ```

3. Voici un exemple de réponse réussie après l'exécution de cette commande.

   ```
   {
       "Arn": "arn:aws:kafka:us-east-1:123456789012:configuration/SomeTest/
   abcdabcd-1234-abcd-1234-abcd123e8e8e-1",
       "LatestRevision": {
           "CreationTime": "2020-08-27T19:37:40.626Z",
           "Description": "Example configuration revision description.",
           "Revision": 2
       }
   }
   ```

Pour supprimer une configuration MSK

La procédure suivante explique comment supprimer une configuration qui n'est pas attachée à un cluster. Vous ne pouvez pas supprimer une configuration attachée à un cluster.

1. Pour exécuter cet exemple, remplacez *configuration-arn* par l'ARN obtenu lors de la création de la configuration. Si vous n'avez pas enregistré l'ARN lorsque vous avez créé la configuration, vous pouvez utiliser la commande `list-configurations` pour répertorier toutes les configurations de votre compte. La configuration que vous souhaitez voir figurer dans la liste apparaît dans la réponse. L'ARN de la configuration apparaît également dans cette liste.

   ```
   aws kafka delete-configuration --arn configuration-arn
   ```

2. Voici un exemple de réponse réussie après l'exécution de cette commande.

```
{
    "arn": " arn:aws:kafka:us-east-1:123456789012:configuration/SomeTest/
abcdabcd-1234-abcd-1234-abcd123e8e8e-1",
    "state": "DELETING"
}
```

Pour décrire une configuration MSK

1. La commande suivante renvoie les métadonnées relatives à la configuration. Pour obtenir une description détaillée de la configuration, exécutez le `describe-configuration-revision`.

   Pour exécuter cet exemple, remplacez *`configuration-arn`* par l'ARN obtenu lors de la création de la configuration. Si vous n'avez pas enregistré l'ARN lorsque vous avez créé la configuration, vous pouvez utiliser la commande `list-configurations` pour répertorier toutes les configurations de votre compte. La configuration que vous souhaitez voir figurer dans la liste apparaît dans la réponse. L'ARN de la configuration apparaît également dans cette liste.

   ```
   aws kafka describe-configuration --arn configuration-arn
   ```

2. Voici un exemple de réponse réussie après l'exécution de cette commande.

   ```
   {
       "Arn": "arn:aws:kafka:us-east-1:123456789012:configuration/SomeTest/abcdabcd-
   abcd-1234-abcd-abcd123e8e8e-1",
       "CreationTime": "2019-05-21T00:54:23.591Z",
       "Description": "Example configuration description.",
       "KafkaVersions": [
           "1.1.1"
       ],
       "LatestRevision": {
           "CreationTime": "2019-05-21T00:54:23.591Z",
           "Description": "Example configuration description.",
           "Revision": 1
       },
       "Name": "SomeTest"
   }
   ```

Pour décrire une révision de configuration MSK

Si vous utilisez la commande `describe-configuration` pour décrire une configuration MSK, vous voyez les métadonnées de la configuration. Pour obtenir une description de la configuration, utilisez la commande `describe-configuration-revision`.

- Exécutez la commande suivante et remplacez *`configuration-arn`* par l'ARN obtenu lors de la création de la configuration. Si vous n'avez pas enregistré l'ARN lorsque vous avez créé la configuration, vous pouvez utiliser la commande `list-configurations` pour répertorier toutes les configurations de votre compte. La configuration que vous souhaitez voir figurer dans la liste apparaît dans la réponse. L'ARN de la configuration apparaît également dans cette liste.

```
aws kafka describe-configuration-revision --arn configuration-arn --revision 1
```

Voici un exemple de réponse réussie après l'exécution de cette commande.

```
{
    "Arn": "arn:aws:kafka:us-east-1:123456789012:configuration/SomeTest/abcdabcd-
abcd-1234-abcd-abcd123e8e8e-1",
    "CreationTime": "2019-05-21T00:54:23.591Z",
    "Description": "Example configuration description.",
    "Revision": 1,
    "ServerProperties":
 "YXV0by5jcmVhdGUudG9waWNzLmVuYWJsZSA9IHRydWUKCgp6b29rZWVwZXIuY29ubmVjdGlvbi50aW1lb3V0Lm1zI
}
```

La valeur de `ServerProperties` est codée à l'aide de base64. Si vous utilisez un décodeur base64 (par exemple, https://www.base64decode.org/) pour le décoder manuellement, vous obtenez le contenu du fichier de configuration d'origine utilisé pour créer la configuration personnalisée. Dans ce cas, vous obtenez ce qui suit :

```
auto.create.topics.enable = true

log.roll.ms = 604800000
```

Pour répertorier toutes les configurations MSK de votre compte pour la région actuelle

- Exécutez la commande suivante.

```
aws kafka list-configurations
```

Voici un exemple de réponse réussie après l'exécution de cette commande.

```
{
    "Configurations": [
        {
            "Arn": "arn:aws:kafka:us-east-1:123456789012:configuration/SomeTest/
abcdabcd-abcd-1234-abcd-abcd123e8e8e-1",
            "CreationTime": "2019-05-21T00:54:23.591Z",
            "Description": "Example configuration description.",
            "KafkaVersions": [
                "1.1.1"
            ],
            "LatestRevision": {
                "CreationTime": "2019-05-21T00:54:23.591Z",
                "Description": "Example configuration description.",
                "Revision": 1
            },
            "Name": "SomeTest"
        },
        {
            "Arn": "arn:aws:kafka:us-east-1:123456789012:configuration/SomeTest/
abcdabcd-1234-abcd-1234-abcd123e8e8e-1",
            "CreationTime": "2019-05-03T23:08:29.446Z",
            "Description": "Example configuration description.",
            "KafkaVersions": [
                "1.1.1"
            ],
            "LatestRevision": {
                "CreationTime": "2019-05-03T23:08:29.446Z",
                "Description": "Example configuration description.",
                "Revision": 1
            },
            "Name": "ExampleConfigurationName"
        }
    ]
```

```
}
```

MSK sans serveur

> **Note**
>
> MSK sans serveur est disponible dans les régions : USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon), Canada (Centre), Asie-Pacifique (Mumbai), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), Asie-Pacifique (Tokyo), Asie-Pacifique (Séoul), Europe (Francfort), Europe (Stockholm), Europe (Irlande), Europe (Paris) et Europe (Londres).

MSK sans serveur est un type de cluster pour Amazon MSK qui vous permet d'exécuter Apache Kafka sans avoir à gérer ni à mettre à l'échelle la capacité du cluster. Il provisionne et met à l'échelle automatiquement la capacité tout en gérant les partitions de votre rubrique, afin que vous puissiez diffuser des données sans devoir vous soucier de la bonne taille ou de la mise à l'échelle des clusters. MSK sans serveur propose un modèle de tarification basé sur le débit, de sorte que vous ne payez que ce que vous utilisez. Envisagez d'utiliser un cluster sans serveur si vos applications ont besoin d'une capacité de streaming à la demande qui augmente ou diminue automatiquement.

MSK sans serveur est entièrement compatible avec Apache Kafka. Vous pouvez donc utiliser n'importe quelle application client compatible pour produire et consommer des données. Il intègre également les services suivants :

- AWS PrivateLink pour fournir une connectivité privée
- AWS Identity and Access Management (IAM) pour l'authentification et l'autorisation à l'aide de langages Java et non-Java. Pour obtenir des instructions sur la configuration des clients pour IAM, consultez Configurer les clients pour le contrôle d'accès IAM.
- AWS Glue Registre des schémas pour la gestion des schémas
- Service géré Amazon pour Apache Flink pour le traitement de flux basé sur Apache Flink
- AWS Lambda pour le traitement des événements

> **Note**
>
> MSK sans serveur nécessite un contrôle d'accès IAM pour tous les clusters. Les listes de contrôle d'accès (listes ACL) Apache Kafka ne sont pas prises en charge. Pour plus d'informations, consultez the section called “Contrôle d'accès IAM”.

Pour obtenir des informations sur les quotas de service qui s'appliquent à MSK sans serveur, veuillez consulter the section called “Quota pour les clusters sans serveur”.

Pour vous aider à démarrer avec les clusters sans serveur et pour en savoir plus sur leurs options de configuration et de surveillance, consultez ce qui suit.

Rubriques

- Premiers pas avec les clusters sans serveur MSK
- Configuration des clusters sans serveur
- Surveillance des clusters sans serveur

Premiers pas avec les clusters sans serveur MSK

Ce didacticiel présente un exemple de la manière dont vous pouvez créer un cluster MSK sans serveur, créer une machine cliente pouvant y accéder et utiliser le client pour créer des rubriques sur le cluster et pour écrire des données dans ces rubriques. Cet exercice ne représente pas toutes les options que vous pouvez choisir lorsque vous créez un cluster sans serveur. Dans les différentes parties de cet exercice, nous choisissons les options par défaut par souci de simplicité. Cela ne signifie pas qu'il s'agit des seules options qui fonctionnent pour configurer un cluster sans serveur. Vous pouvez également utiliser l'API AWS CLI ou l'API Amazon MSK. Pour plus d'informations, consultez la Référence 2.0 d'API Amazon MSK.

Rubriques

- Étape 1 : Créer un cluster MSK sans serveur
- Étape 2 : Créer un rôle IAM
- Étape 3 : Créer un ordinateur client
- Étape 4 : Créer une rubrique Apache Kafka
- Étape 5 : Produire et consommer des données
- Étape 6 : Supprimer des ressources

Étape 1 : Créer un cluster MSK sans serveur

Au cours de cette étape, vous effectuez deux tâches. Vous devez d'abord créer un cluster MSK sans serveur avec les paramètres par défaut. Ensuite, vous collectez des informations sur le cluster. Il

s'agit d'informations dont vous aurez besoin ultérieurement lorsque vous créerez un client capable d'envoyer des données au cluster.

Pour créer un cluster sans serveur

1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home.
2. Choisissez Créer un cluster.
3. Dans Méthode de création, laissez l'option Création rapide sélectionnée. L'option Création rapide vous permet de créer un cluster sans serveur avec les paramètres par défaut.
4. Pour Nom du cluster, entrez un nom descriptif, tel que **`msk-serverless-tutorial-cluster`**.
5. Dans Propriétés générales du cluster, choisissez Sans serveur comme Type de cluster. Utilisez les valeurs par défaut pour les autres propriétés générales du cluster.
6. Notez le tableau sous Tous les paramètres du cluster. Ce tableau répertorie les valeurs par défaut pour les paramètres importants tels que le réseau et la disponibilité, et indique si vous pouvez modifier chaque paramètre après avoir créé le cluster. Pour modifier un paramètre avant de créer le cluster, vous devez choisir l'option Création personnalisée sous Méthode de création.

   > **Note**
   >
   > Vous pouvez connecter des clients provenant d'un maximum de cinq VPC différents grâce à des clusters MSK sans serveur. Pour aider les applications clientes à basculer vers une autre zone de disponibilité en cas de panne, vous devez spécifier au moins deux sous-réseaux dans chaque VPC.

7. Choisissez Créer un cluster.

Pour recueillir des informations sur le cluster

1. Dans la section Résumé du cluster, choisissez Voir les informations client. Ce bouton reste grisé tant qu'Amazon MSK n'a pas fini de créer le cluster. Vous devrez peut-être attendre quelques minutes avant que le bouton soit actif pour pouvoir l'utiliser.
2. Copiez la chaîne sous le libellé Point de terminaison. Il s'agit de la chaîne de votre serveur d'amorçage.
3. Choisissez l’onglet Propriétés.

4. Dans la section Paramètres réseau, copiez les identifiants des sous-réseaux et du groupe de sécurité et enregistrez-les, car vous aurez besoin de ces informations ultérieurement pour créer un ordinateur client.
5. Choisissez l'un des sous-réseaux. Cela ouvre la console Amazon VPC. Recherchez l'identifiant de l'Amazon VPC associé au sous-réseau. Enregistrez l'ID de cet Amazon VPC pour une utilisation ultérieure.

Étape suivante

Étape 2 : Créer un rôle IAM

Étape 2 : Créer un rôle IAM

Au cours de cette étape, vous effectuez deux tâches. La première tâche consiste à créer une politique IAM qui autorise l'accès à la création de rubriques sur le cluster et à l'envoi de données vers ces rubriques. La deuxième tâche consiste à créer un rôle IAM et à lui associer cette politique. À une étape ultérieure, nous créons un ordinateur client qui assume ce rôle et l'utilise pour créer une rubrique sur le cluster et pour envoyer des données à cette rubrique.

Pour créer une politique IAM permettant de créer des rubriques et d'y écrire

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Politiques.
3. Choisissez Create Policy (Créer une politique).
4. Choisissez l'onglet JSON, puis remplacez le JSON dans la fenêtre de l'éditeur par le JSON suivant.

   Remplacez *région* par le code de la Région AWS dans laquelle vous avez créé votre cluster. Remplacez *Account-ID* par votre ID de compte. *msk-serverless-tutorial-cluster*Remplacez-le par le nom de votre cluster sans serveur.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
```

```
                "kafka-cluster:AlterCluster",
                "kafka-cluster:DescribeCluster"
            ],
            "Resource": [
                "arn:aws:kafka:region:Account-ID:cluster/msk-serverless-tutorial-
cluster/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:*Topic*",
                "kafka-cluster:WriteData",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:region:Account-ID:topic/msk-serverless-tutorial-
cluster/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeGroup"
            ],
            "Resource": [
                "arn:aws:kafka:region:Account-ID:group/msk-serverless-tutorial-
cluster/*"
            ]
        }
    ]
}
```

Pour obtenir des instructions sur la rédaction de politiques sécurisées, consultez the section called “Contrôle d'accès IAM”.

5. Choisissez Suivant : Balises.
6. Choisissez Suivant : Vérification.
7. Pour le nom de politique, entrez un nom descriptif, tel que **`msk-serverless-tutorial-policy`**.
8. Choisissez Créer une politique.

Pour créer un rôle IAM et lui attacher la politique

1. Dans le panneau de navigation, choisissez Rôles.
2. Sélectionnez Créer un rôle.
3. Sous Cas d'utilisation courants, choisissez EC2, puis Suivant : Autorisations.
4. Dans la zone de recherche, saisissez le nom de la politique que vous avez créée précédemment pour ce didacticiel. Ensuite, cochez la case située à gauche de la politique.
5. Choisissez Suivant : Balises.
6. Choisissez Suivant : Vérification.
7. Pour le nom de rôle, entrez un nom descriptif, tel que **`msk-serverless-tutorial-role`**.
8. Sélectionnez Créer un rôle.

Étape suivante

Étape 3 : Créer un ordinateur client

Étape 3 : Créer un ordinateur client

Au cours de cette étape, vous effectuez deux tâches. La première tâche consiste à créer une instance Amazon EC2 à utiliser comme ordinateur client Apache Kafka. La deuxième tâche consiste à installer les outils Java et Apache Kafka sur l'ordinateur.

Pour créer un ordinateur client

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Lancer l'instance.
3. Saisissez un nom descriptif pour votre ordinateur client, tel que **`msk-serverless-tutorial-client`**.
4. Laissez Amazon Linux 2 AMI (HVM) - Kernel 5.10, type de volume SSD sélectionné pour le type Amazon Machine Image (AMI).
5. Laissez le type d'instance t2.micro sélectionné.
6. Sous Paire de clés (connexion), choisissez Créer une nouvelle paire de clés. Saisissez **`MSKServerlessKeyPair`** pour Nom de la paire de clés. Puis choisissez Télécharger la paire de clés. Vous pouvez utiliser également une paire de clés existante.
7. Sous Paramètres réseau, choisissez Modifier.

8. Dans VPC, saisissez l'ID du cloud privé virtuel (VPC) pour votre cluster sans serveur. Il s'agit du VPC basé sur le service Amazon VPC dont vous avez enregistré l'ID après avoir créé le cluster.
9. Pour Sous-réseau, choisissez le sous-réseau dont vous avez enregistré l'ID après avoir créé le cluster.
10. Pour Pare-feu (groupes de sécurité), sélectionnez le groupe de sécurité associé au cluster. Cette valeur fonctionne si ce groupe de sécurité possède une règle d'entrée qui autorise le trafic provenant du groupe de sécurité à se diriger vers lui-même. Avec une telle règle, les membres d'un même groupe de sécurité peuvent communiquer entre eux. Pour de plus amples informations, veuillez consulter Règles des groupes de sécurité dans le Manuel du développeur Amazon VPC.
11. Développez la section Détails avancés et choisissez le rôle IAM que vous avez créé dans la section Étape 2 : Créer un rôle IAM.
12. Choisissez Lancer.
13. Dans le panneau de navigation de gauche, sélectionnez Instances. Cochez ensuite la case dans la ligne qui représente votre instance Amazon EC2 nouvellement créée. À partir de maintenant, nous appelons cette instance l'ordinateur client.
14. Choisissez Connexion et suivez les instructions pour vous connecter à l'ordinateur client.

Pour configurer les outils client Apache Kafka sur l'ordinateur client

1. Pour installer Java, exécutez la commande suivante sur l'ordinateur client :

```
sudo yum -y install java-11
```

2. Pour obtenir les outils Apache Kafka dont nous avons besoin pour créer des rubriques et envoyer des données, exécutez les commandes suivantes :

```
wget https://archive.apache.org/dist/kafka/2.8.1/kafka_2.12-2.8.1.tgz
```

```
tar -xzf kafka_2.12-2.8.1.tgz
```

3. Accédez au répertoire `kafka_2.12-2.8.1/libs`, puis exécutez la commande suivante pour télécharger le fichier Amazon MSK IAM JAR. Le fichier Amazon MSK IAM JAR permet à l'ordinateur client d'accéder au cluster.

```
wget https://github.com/aws/aws-msk-iam-auth/releases/download/v1.1.1/aws-msk-iam-auth-1.1.1-all.jar
```

4. Accédez au répertoire `kafka_2.12-2.8.1/bin`. Copiez les paramètres de propriété suivants et collez-les dans un nouveau fichier. Nommez le fichier `client.properties` et enregistrez-le.

```
security.protocol=SASL_SSL
sasl.mechanism=AWS_MSK_IAM
sasl.jaas.config=software.amazon.msk.auth.iam.IAMLoginModule required;
sasl.client.callback.handler.class=software.amazon.msk.auth.iam.IAMClientCallbackHandler
```

Étape suivante

Étape 4 : Créer une rubrique Apache Kafka

Étape 4 : Créer une rubrique Apache Kafka

Dans cette étape, vous utilisez l'ordinateur client créé précédemment pour créer une rubrique sur le cluster sans serveur.

Pour créer une rubrique et y écrire des données

1. Dans la commande `export` suivante, remplacez *`my-endpoint`* par la chaîne bootstrap-server que vous avez enregistrée après avoir créé le cluster. Accédez ensuite au répertoire `kafka_2.12-2.8.1/bin` de l'ordinateur client et exécutez la commande `export`.

```
export BS=my-endpoint
```

2. Exécutez la commande suivante pour créer une rubrique appelée `msk-serverless-tutorial`.

```
<path-to-your-kafka-installation>/bin/kafka-topics.sh --bootstrap-server $BS
 --command-config client.properties --create --topic msk-serverless-tutorial --
partitions 6
```

Étape suivante

Étape 5 : Produire et consommer des données

Étape 5 : Produire et consommer des données

Dans cette étape, vous produisez et consommez des données à l'aide de la rubrique que vous avez créée à l'étape précédente.

Pour produire et consommer des messages

1. Exécutez la commande suivante pour créer un producteur de console.

```
<path-to-your-kafka-installation>/bin/kafka-console-producer.sh --broker-list $BS
 --producer.config client.properties --topic msk-serverless-tutorial
```

2. Saisissez le message souhaité, puis appuyez sur Entrée. Répétez cette étape deux ou trois fois. Chaque fois que vous entrez une ligne et appuyez sur Entrée, cette ligne est envoyée à votre cluster sous forme de message distinct.
3. Gardez la connexion à l'ordinateur client ouverte, puis ouvrez une deuxième connexion séparée à cet ordinateur dans une nouvelle fenêtre.
4. Utilisez votre deuxième connexion à l'ordinateur client pour créer un consommateur de console avec la commande suivante. Remplacez *my-endpoint* par la chaîne du serveur d'amorçage que vous avez enregistrée après avoir créé le cluster.

```
<path-to-your-kafka-installation>/bin/kafka-console-consumer.sh --bootstrap-
server my-endpoint --consumer.config client.properties --topic msk-serverless-
tutorial --from-beginning
```

   Vous commencez à voir les messages que vous avez entrés plus tôt lorsque vous avez utilisé la commande du producteur de la console.
5. Entrez d'autres messages dans la fenêtre du producteur et regardez-les apparaître dans la fenêtre du consommateur.

Étape suivante

Étape 6 : Supprimer des ressources

Étape 6 : Supprimer des ressources

Dans cette étape, vous supprimez les ressources que vous avez créées dans ce didacticiel.

Pour supprimer le cluster

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/home.
2. Dans la liste des clusters, choisissez le cluster que vous avez créé pour ce didacticiel.
3. Pour Actions, choisissez Supprimer le cluster.
4. Saisissez `delete` dans le champ, puis choisissez Supprimer.

Pour arrêter l'ordinateur client

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la liste des instances Amazon EC2, choisissez l'ordinateur client que vous avez créé pour ce didacticiel.
3. Choisissez État de l'instance, puis Résilier l'instance.
4. Sélectionnez Résilier.

Pour supprimer la politique et le rôle IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Rôles.
3. Dans la zone de recherche, saisissez le nom du rôle IAM que vous avez créé pour ce didacticiel.
4. Choisissez le rôle. Ensuite, choisissez Supprimer le rôle et confirmez la suppression.
5. Dans le panneau de navigation, choisissez Politiques.
6. Dans la zone de recherche, saisissez le nom de la politique que vous avez créée pour ce didacticiel.
7. Choisissez la politique pour ouvrir sa page récapitulative. Sur la page Récapitulatif de la politique, choisissez Supprimer la politique.
8. Sélectionnez Supprimer.

Configuration des clusters sans serveur

Amazon MSK définit les propriétés de configuration des agents pour les clusters sans serveur. Vous ne pouvez pas modifier les paramètres des propriétés de configuration de ces agents. Toutefois, vous pouvez définir les propriétés de configuration des rubriques suivantes.

Propriété de configuration	Par défaut	Modifiable	Valeur maximale autorisée
cleanup.policy	Suppression	Oui, mais uniquement au moment de la création de la rubrique	
compression.type	Producer	Oui	
max.message.bytes	1048588	Oui	8 Mio
message.timestamp.difference.max.ms	long.max	Oui	
message.timestamp.type	CreateTime	Oui	
retention.bytes	250 Gio	Oui	250 Gio
retention.ms	7 jours	Oui	Illimité

Vous pouvez également utiliser les commandes Apache Kafka pour définir ou modifier les propriétés de configuration au niveau des rubriques pour des rubriques nouvelles et existantes. Pour de plus amples informations sur les propriétés de configuration au niveau des rubriques et savoir comment les définir, veuillez consulter Configurations au niveau des rubriques dans la documentation Apache Kafka.

Surveillance des clusters sans serveur

Amazon MSK s'intègre à Amazon CloudWatch afin que vous puissiez collecter, consulter et analyser les métriques de votre cluster MSK Serverless. Les métriques indiquées dans le tableau suivant sont disponibles pour tous les clusters sans serveur. Comme ces métriques sont publiées sous forme de points de données individuels pour chaque partition de la rubrique, nous vous recommandons de les consulter sous forme de statistiques « SUM » pour obtenir une vue au niveau de la rubrique.

Amazon MSK publie `PerSec` des statistiques CloudWatch à une fréquence d'une fois par minute. Cela signifie que la statistique « SUM » pour une période d'une minute représente avec précision les données par seconde pour les métriques `PerSec`. Pour collecter des données par seconde pendant

une période de plus d'une minute, utilisez l'expression CloudWatch mathématique suivante :`m1 * 60/PERIOD(m1)`.

Métriques disponibles au niveau de la surveillance DEFAULT

Nom	Lorsqu'il est visible	Dimensions	Description
`BytesInPerSec`	Après qu'un producteur a écrit dans une rubrique	Nom du cluster, rubrique	Nombre d'octets par seconde reçus des clients. Cette métrique est disponible pour chaque rubrique.
`BytesOutPerSec`	Après qu'un groupe de consommateurs a consommé à partir d'une rubrique	Nom du cluster, rubrique	Nombre d'octets par seconde envoyés aux clients. Cette métrique est disponible pour chaque rubrique.
`FetchMessageConversionsPerSec`	Après qu'un groupe de consommateurs a consommé à partir d'une rubrique	Nom du cluster, rubrique	Nombre de conversions de messages d'extraction par seconde pour la rubrique.
`EstimatedMaxTimeLag`	Après qu'un groupe de consommateurs a consommé à partir d'une rubrique	Nom du cluster, groupe de consommateurs, rubrique	Une estimation temporelle de la MaxOffsetLag métrique.
`MaxOffsetLag`	Après qu'un groupe de consommateurs a consommé	Nom du cluster, groupe de consommateurs, rubrique	Décalage maximal entre toutes les partitions d'une rubrique.

Nom	Lorsqu'il est visible	Dimensions	Description
	à partir d'une rubrique		
`MessagesInPerSec`	Après qu'un producteur a écrit dans une rubrique	Nom du cluster, rubrique	Nombre de messages entrants par seconde pour la rubrique.
`ProduceMessageConversionsPerSec`	Après qu'un producteur a écrit dans une rubrique	Nom du cluster, rubrique	Nombre de conversions de messages de production par seconde pour la rubrique.
`SumOffsetLag`	Après qu'un groupe de consommateurs a consommé à partir d'une rubrique	Nom du cluster, groupe de consommateurs, rubrique	Décalage agrégé pour toutes les partitions d'une rubrique.

Pour consulter les métriques MSK sans serveur

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sous Métriques, sélectionnez Toutes les métriques.
3. Dans les métriques, recherchez le terme **`kafka`**.
4. Choisissez AWS/Kafka/ Nom du cluster, rubrique ou AWS/Kafka/ Nom du cluster, groupe de consommateurs, rubrique pour voir les différentes métriques.

MSK Connect

Qu'est-ce que MSK Connect ?

MSK Connect est une fonctionnalité d'Amazon MSK qui permet aux développeurs de diffuser facilement des données vers et depuis leurs clusters Apache Kafka. MSK Connect utilise Kafka Connect 2.7.1, un framework open source permettant de connecter les clusters Apache Kafka à des systèmes externes tels que des bases de données, des index de recherche et des systèmes de fichiers. Avec MSK Connect, vous pouvez déployer des connecteurs entièrement gérés conçus pour Kafka Connect qui transfèrent des données vers ou extraient des données depuis des magasins de données populaires tels qu'Amazon S3 et Amazon OpenSearch Service. Vous pouvez déployer des connecteurs développés par des tiers comme Debezium pour diffuser les journaux des modifications des bases de données vers un cluster Apache Kafka ou déployer un connecteur existant sans modification de code. Les connecteurs sont automatiquement mis à l'échelle pour s'adapter à l'évolution de la charge et vous ne payez que pour les ressources que vous utilisez.

Utilisez des connecteurs sources pour importer des données provenant de systèmes externes dans vos rubriques. Grâce aux connecteurs récepteurs, vous pouvez exporter les données de vos rubriques vers des systèmes externes.

MSK Connect prend en charge les connecteurs pour tout cluster Apache Kafka connecté à un Amazon VPC, qu'il s'agisse d'un cluster MSK ou d'un cluster Apache Kafka hébergé indépendamment.

MSK Connect surveille en permanence l'état de santé et l'état de livraison des connecteurs, applique les correctifs et gère le matériel sous-jacent, et adapte automatiquement les connecteurs en fonction de l'évolution du débit.

Pour commencer à utiliser la console, consultez the section called “Premiers pas”.

Pour en savoir plus sur les AWS ressources que vous pouvez créer avec MSK Connect, consultez the section called “Connecteurs”the section called “Plugins”, etthe section called “Workers”.

Pour plus d'informations sur l'API MSK Connect, consultez le manuel Référence de l'API Amazon MSK Connect.

Premiers pas avec MSK Connect

Il s'agit d'un step-by-step didacticiel qui utilise le AWS Management Console pour créer un cluster MSK et un connecteur récepteur qui envoie des données du cluster vers un compartiment S3.

Rubriques

Étape 1 : Configurer les ressources requises

Au cours de cette étape, vous créez les ressources suivantes dont vous avez besoin pour ce scénario de mise en route :

- Un compartiment S3 destiné à servir de destination pour recevoir les données du connecteur.
- Un cluster MSK auquel vous allez envoyer des données. Le connecteur lira ensuite les données de ce cluster et les enverra au compartiment S3 de destination.
- Un rôle IAM qui permet au connecteur d'écrire dans le compartiment S3 de destination.
- Le point de terminaison d'un VPC Amazon permettant d'envoyer des données depuis le VPC Amazon qui possède le cluster et le connecteur vers Amazon S3.

Pour créer le compartiment S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.
3. Pour le nom du compartiment, entrez un nom descriptif, tel que `mkc-tutorial-destination-bucket`.
4. Faites défiler l'écran vers le bas et choisissez Créer un compartiment.
5. Dans la liste des compartiments, choisissez le compartiment que vous venez de créer.
6. Choisissez Créer un dossier.

7. Entrez `tutorial` comme nom de dossier, puis faites défiler l'écran vers le bas et choisissez Créer un dossier.

Pour créer le cluster

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Dans le volet de gauche, sous Clusters MSK, sélectionnez Clusters.
3. Choisissez Créer un cluster.
4. Choisissez Création personnalisée.
5. Comme nom de cluster, saisissez `mkc-tutorial-cluster`.
6. Dans Propriétés générales du cluster, choisissez Provisionné comme type de cluster.
7. Sous Mise en réseau, choisissez un VPC Amazon. Sélectionnez ensuite les zones de disponibilité et les sous-réseaux que vous voulez utiliser. N'oubliez pas les identifiants du VPC Amazon et des sous-réseaux que vous avez sélectionnés, car vous en aurez besoin plus tard dans ce didacticiel.
8. Sous Méthodes de contrôle d'accès, assurez-vous que seul l'accès non authentifié est sélectionné.
9. Sous Chiffrement, assurez-vous que seul le texte brut est sélectionné.
10. Continuez à utiliser l'assistant, puis choisissez Créer un cluster. Vous accédez alors à la page Détails du cluster. Sur cette page, sous Groupes de sécurité appliqués, recherchez l'ID du groupe de sécurité. N'oubliez pas cet ID, car vous en aurez besoin ultérieurement dans ce didacticiel.

Pour créer le rôle IAM capable d'écrire dans le compartiment de destination

1. Ouvrez la console IAM à l’adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de gauche, sous Gestion des accès, sélectionnez Rôles.
3. Sélectionnez Créer un rôle.
4. Sous Ou sélectionnez un service pour afficher ses cas d'utilisation, choisissez S3.
5. Faites défiler l'écran vers le bas et sous Sélectionnez votre cas d'utilisation, choisissez à nouveau S3.
6. Sélectionnez Suivant : autorisations.

7. Choisissez Créer une politique. Cette action ouvre un nouvel onglet de votre navigateur dans lequel vous allez créer la politique. Laissez l'onglet de création de rôles d'origine ouvert, car nous y reviendrons plus tard.
8. Choisissez l'onglet JSON, puis remplacez le texte de la fenêtre par la politique suivante.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::<my-tutorial-destination-bucket>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": "*"
    }
  ]
}
```

9. Choisissez Suivant : Balises.
10. Choisissez Suivant : Vérification.
11. Entrez `mkc-tutorial-policy` comme nom de politique, puis faites défiler l'écran vers le bas et choisissez Créer une politique.

12. De retour dans l'onglet du navigateur dans lequel vous étiez en train de créer le rôle, cliquez sur le bouton d'actualisation.
13. Recherchez `mkc-tutorial-policy` et sélectionnez-le en cliquant sur le bouton situé à sa gauche.
14. Choisissez Suivant : Balises.
15. Choisissez Suivant : Vérification.
16. Entrez `mkc-tutorial-role` comme nom de rôle et supprimez le texte dans la zone de description.
17. Sélectionnez Créer un rôle.

Pour autoriser MSK Connect à assumer le rôle

1. Dans le volet gauche de la console IAM, sous Gestion des accès, sélectionnez Rôles.
2. Recherchez `mkc-tutorial-role` et choisissez-le.
3. Sur la page Récapitulatif du rôle, choisissez l'onglet Relations d'approbation.
4. Choisissez Modifier la relation d’approbation.
5. Remplacez la politique d'approbation existante par le code JSON suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "kafkaconnect.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. Choisissez Mettre à jour la politique d'approbation.

Pour créer un point de terminaison d'un VPC Amazon à partir du VPC du cluster vers Amazon S3

1. Ouvrez la console Amazon VPC à l’adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet gauche, sélectionnez Points de terminaison.

3. Choisissez Créer un point de terminaison.
4. Sous Nom du service, sélectionnez le service com.amazonaws.us-east-1.s3 et le type de passerelle.
5. Choisissez le VPC du cluster, puis cochez la case située à gauche de la table de routage associée aux sous-réseaux du cluster.
6. Choisissez Créer un point de terminaison.

Étape suivante

Étape 2 : Créer un plugin personnalisé

Étape 2 : Créer un plugin personnalisé

Un plugin contient le code qui définit la logique du connecteur. Au cours de cette étape, vous allez créer un plugin personnalisé contenant le code du connecteur récepteur Lenses Amazon S3. Dans une étape ultérieure, lorsque vous créerez le connecteur MSK, vous spécifierez que son code se trouve dans ce plugin personnalisé. Vous pouvez utiliser le même plugin pour créer plusieurs connecteurs MSK avec des configurations différentes.

Pour créer le connecteur personnalisé

1. Téléchargez le connecteur S3.
2. Chargez le fichier ZIP vers un compartiment S3 auquel vous avez accès. Pour plus d'informations sur le chargement de fichiers sur Amazon S3, consultez la section Chargement d'objets dans le guide de l'utilisateur d'Amazon S3.
3. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
4. Dans le volet de gauche, développez MSK Connect, puis choisissez Plugins personnalisés.
5. Choisissez Créer un plugin personnalisé.
6. Choisissez Parcourir S3.
7. Dans la liste des compartiments, recherchez le compartiment dans lequel vous avez chargé le fichier ZIP, puis sélectionnez-le.
8. Dans la liste des objets du compartiment, sélectionnez le bouton radio situé à gauche du fichier ZIP, puis cliquez sur le bouton intitulé Choisir.
9. Entrez `mkc-tutorial-plugin` comme nom de plugin personnalisé, puis choisissez Créer un plugin personnalisé.

La création du plugin personnalisé peut prendre AWS quelques minutes. Une fois le processus de création terminé, le message suivant apparaît dans une bannière en haut de la fenêtre du navigateur.

```
Custom plugin mkc-tutorial-plugin was successfully created
The custom plugin was created. You can now create a connector using this custom plugin.
```

Étape suivante

Étape 3 : Créer un ordinateur client et une rubrique Apache Kafka

Étape 3 : Créer un ordinateur client et une rubrique Apache Kafka

Dans cette étape, vous créez une instance Amazon EC2 à utiliser comme instance de client Apache Kafka. Vous utilisez ensuite cette instance pour créer une rubrique sur le cluster.

Pour créer un ordinateur client

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Sélectionnez Lancer des instances.
3. Saisissez un Nom pour votre ordinateur client, tel que **mkc-tutorial-client**.
4. Laissez Amazon Linux 2 AMI (HVM) - Kernel 5.10, type de volume SSD sélectionné pour le type Amazon Machine Image (AMI).
5. Choisissez le type d'instance t2.xlarge.
6. Sous Paire de clés (connexion), choisissez Créer une nouvelle paire de clés. Saisissez **mkc-tutorial-key-pair** dans Nom de la paire de clés, puis choisissez Télécharger la paire de clés. Vous pouvez utiliser également une paire de clés existante.
7. Choisissez Lancer l'instance.
8. Choisissez View Instances (Afficher les instances). Ensuite, dans la colonne Groupes de sécurité, choisissez le groupe de sécurité associé à votre nouvelle instance. Copiez l'ID du groupe de sécurité et enregistrez-le pour plus tard.

Pour autoriser le client nouvellement créé à envoyer des données au cluster

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de gauche, sélectionnez Groupes de sécurité sous l'onglet SÉCURITÉ. Dans la colonne ID du groupe de sécurité), recherchez le groupe de sécurité du cluster. Vous avez enregistré l'ID de ce groupe de sécurité lorsque vous avez créé le cluster dans the section called

"Étape 1 : Configurer les ressources requises". Choisissez ce groupe de sécurité en cochant la case située à gauche de sa ligne. Assurez-vous qu'aucun autre groupe de sécurité n'est sélectionné simultanément.

3. Dans la moitié inférieure de l'écran, choisissez l'onglet Règles entrantes.
4. Choisissez Modifier les règles entrantes.
5. Dans le coin inférieur gauche de l'écran, choisissez Ajouter une règle.
6. Dans la nouvelle règle, choisissez Tout le trafic dans la colonne Type . Dans le champ à droite de la colonne Source, entrez l'ID du groupe de sécurité de l'ordinateur client. Il s'agit de l'ID du groupe de sécurité que vous avez enregistré après avoir créé l'ordinateur client.
7. Sélectionnez Enregistrer les règles. Votre cluster MSK accepte désormais tout le trafic provenant du client que vous avez créé dans la procédure précédente.

Pour créer une rubrique

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le tableau des instances, sélectionnez `mkc-tutorial-client`.
3. En haut de l'écran, choisissez Connexion, puis suivez les instructions pour vous connecter à l'instance.
4. Installez Java sur l'instance client en exécutant la commande suivante :

```
sudo yum install java-1.8.0
```

5. Exécutez la commande suivante pour télécharger Apache Kafka.

```
wget https://archive.apache.org/dist/kafka/2.2.1/kafka_2.12-2.2.1.tgz
```

> **Note**
>
> Si vous souhaitez utiliser un site miroir autre que celui utilisé dans cette commande, vous pouvez en choisir un autre sur le site web Apache.

6. Exécutez la commande suivante dans le répertoire où vous avez téléchargé le fichier TAR à l'étape précédente.

```
tar -xzf kafka_2.12-2.2.1.tgz
```

7. Accédez au répertoire kafka_2.12-2.2.1.
8. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
9. Dans le volet de gauche, choisissez Clusters, puis choisissez le nom`mkc-tutorial-cluster`.
10. Choisissez Afficher les informations sur le client.
11. Copiez la chaîne de connexion en texte brut.
12. Sélectionnez Exécuté.
13. Exécutez la commande suivante sur l'instance cliente (`mkc-tutorial-client`), en la *`bootstrapServerString`*remplaçant par la valeur que vous avez enregistrée lorsque vous avez consulté les informations client du cluster.

```
<path-to-your-kafka-installation>/bin/kafka-topics.sh --create --bootstrap-
server bootstrapServerString --replication-factor 2 --partitions 1 --topic mkc-
tutorial-topic
```

Si la commande réussit, le message suivant s'affiche : `Created topic mkc-tutorial-topic.`

Étape suivante

Étape 4 : Créer un connecteur

Étape 4 : Créer un connecteur

Pour créer le connecteur

1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Dans le volet gauche, développez MSK Connect, puis choisissez Connecteurs.
3. Sélectionnez Créer un connecteur.
4. Dans la liste des plugins, choisissez `mkc-tutorial-plugin`, puis Suivant.
5. Pour le nom du connecteur, entrez `mkc-tutorial-connector`.
6. Dans la liste des clusters, choisissez `mkc-tutorial-cluster`.
7. Copiez la configuration suivante et collez-la dans le champ de configuration du connecteur.

```
connector.class=io.confluent.connect.s3.S3SinkConnector
s3.region=us-east-1
format.class=io.confluent.connect.s3.format.json.JsonFormat
flush.size=1
schema.compatibility=NONE
tasks.max=2
topics=mkc-tutorial-topic
partitioner.class=io.confluent.connect.storage.partitioner.DefaultPartitioner
storage.class=io.confluent.connect.s3.storage.S3Storage
s3.bucket.name=<my-tutorial-destination-bucket>
topics.dir=tutorial
```

8. Sous Autorisations d'accès, choisissez `mkc-tutorial-role`.
9. Choisissez Suivant. Sur la page Sécurité, sélectionnez à nouveau Suivant.
10. Sur la page Journaux, choisissez Suivant.
11. Sous Vérifier et créer, choisissez Créer un connecteur.

Étape suivante

Étape 5 : Envoyer des données

Étape 5 : Envoyer des données

Au cours de cette étape, vous envoyez des données à la rubrique Apache Kafka que vous avez créée précédemment, puis vous recherchez ces mêmes données dans le compartiment S3 de destination.

Pour envoyer des données au cluster MSK

1. Dans le dossier `bin` de l'installation d'Apache Kafka sur l'instance cliente, créez un fichier texte nommé `client.properties` avec le contenu suivant.

```
security.protocol=PLAINTEXT
```

2. Exécutez la commande suivante pour créer un producteur de console. Remplacez *`BootstrapBrokerString`* par la valeur que vous avez obtenue lors de l'exécution de la commande précédente.

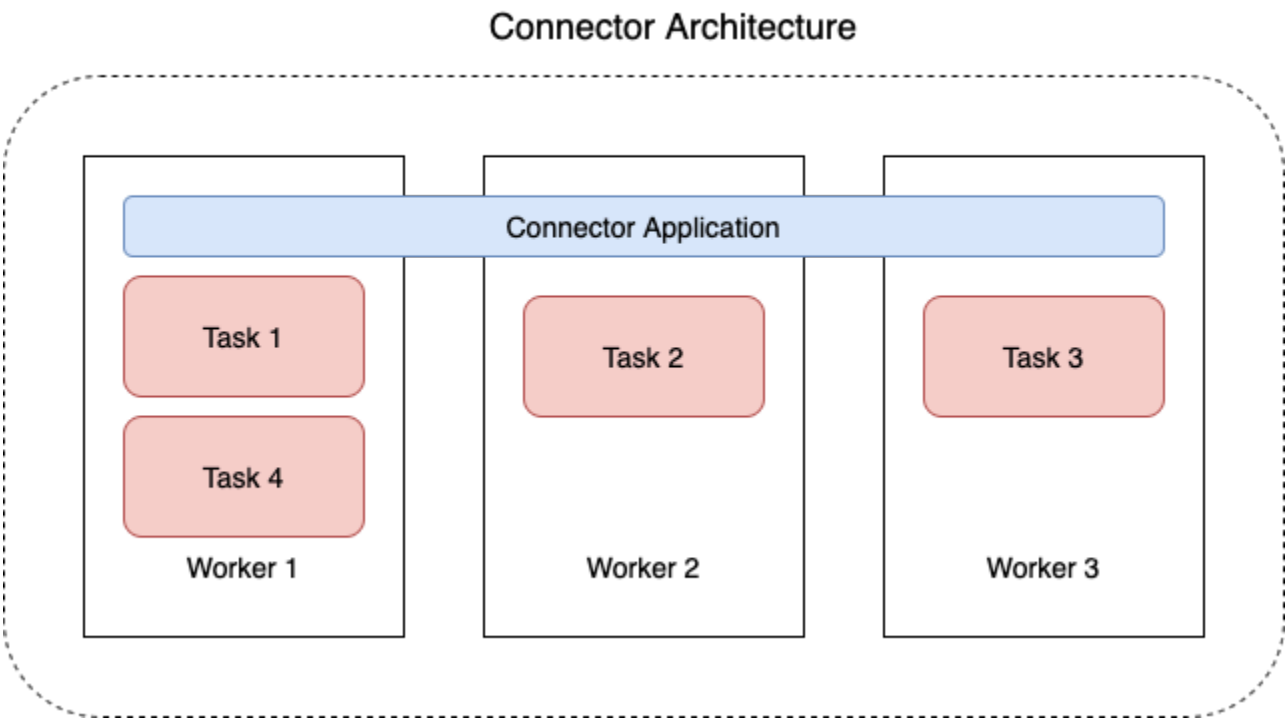
```
<path-to-your-kafka-installation>/bin/kafka-console-producer.sh --broker-
list BootstrapBrokerString --producer.config client.properties --topic mkc-
tutorial-topic
```

3. Saisissez le message souhaité, puis appuyez sur Entrée. Répétez cette étape deux ou trois fois. Chaque fois que vous entrez une ligne et appuyez sur Entrée, cette ligne est envoyée à votre cluster Apache Kafka sous forme de message distinct.
4. Recherchez dans le compartiment Amazon S3 de destination les messages que vous avez envoyés à l'étape précédente.

Connecteurs

Un connecteur intègre des systèmes externes et des services Amazon à Apache Kafka en copiant en continu les données de streaming d'une source de données vers votre cluster Apache Kafka, ou en copiant en continu les données de votre cluster vers un récepteur de données. Un connecteur peut également exécuter une logique légère telle que la transformation, la conversion de format ou le filtrage des données avant de les livrer à une destination. Les connecteurs source extraient les données d'une source de données et les transmettent au cluster, tandis que les connecteurs récepteurs extraient les données du cluster et les transfèrent vers un récepteur de données.

Le diagramme suivant illustre l'architecture d'un connecteur. Un worker est un processus de machine virtuelle Java (JVM) qui exécute la logique du connecteur. Chaque worker crée un ensemble de tâches qui s'exécutent dans des threads parallèles et se chargent de copier les données. Les tâches ne stockent pas l'état et peuvent donc être démarrées, arrêtées ou redémarrées à tout moment afin de fournir un pipeline de données résilient et évolutif.



Capacité du connecteur

La capacité totale d'un connecteur dépend du nombre de workers qu'il possède, ainsi que du nombre d'unités MSK Connect (MCU) par worker. Chaque MCU représente 1 vCPU de calcul et 4 Gio de mémoire. La mémoire MCU correspond à la mémoire totale d'une instance de worker et non à la mémoire de tas utilisée.

Les employés de MSK Connect utilisent les adresses IP des sous-réseaux fournis par le client. Chaque travailleur utilise une adresse IP provenant de l'un des sous-réseaux fournis par le client. Vous devez vous assurer que vous disposez d'un nombre suffisant d'adresses IP disponibles dans les sous-réseaux fournis à une CreateConnector demande pour tenir compte de leur capacité spécifiée, en particulier lors du dimensionnement automatique des connecteurs où le nombre de travailleurs peut fluctuer.

Pour créer un connecteur, vous devez choisir l'un des deux modes de capacité suivants.

- Provisionné : choisissez ce mode si vous connaissez les exigences de capacité de votre connecteur. Vous spécifiez deux valeurs :
  - Le nombre de workers.
  - Le nombre de MCU par worker.

- Mis à l'échelle automatiquement : choisissez ce mode si les exigences de capacité de votre connecteur sont variables ou si vous ne les connaissez pas à l'avance. Lorsque vous utilisez le mode de mise à l'échelle automatique, Amazon MSK Connect remplace la propriété `tasks.max` de votre connecteur par une valeur proportionnelle au nombre de workers s'exécutant dans le connecteur et au nombre de MCU par worker.

  Vous spécifiez trois ensembles de valeurs :

  - Le nombre minimal et maximal de workers.
  - Les pourcentages d'utilisation de la mise à l'échelle horizontale et de la montée en charge du processeur, qui sont déterminés par la métrique `CpuUtilization`. Lorsque la métrique `CpuUtilization` du connecteur dépasse le pourcentage de montée en charge, MSK Connect augmente le nombre de workers qui utilisent le connecteur. Lorsque la métrique `CpuUtilization` passe en dessous du pourcentage de la mise à l'échelle horizontale, MSK Connect réduit le nombre de workers. Le nombre de workers reste toujours dans les limites des nombres minimum et maximum que vous spécifiez lors de la création du connecteur.
  - Le nombre de MCU par worker.

Pour de plus amples informations sur les workers, consultez the section called “Workers”. Pour en savoir plus sur les métriques MSK Connect, consultez the section called “Surveillance”.

Création d'un connecteur

Création d'un connecteur à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Dans le volet gauche, sous MSK Connect, choisissez Connecteurs.
3. Sélectionnez Créer un connecteur.
4. Vous pouvez choisir entre utiliser un plugin personnalisé existant pour créer le connecteur ou créer d'abord un nouveau plugin personnalisé. Pour plus d'informations sur les plugins personnalisés et sur la façon de les créer, consultez the section called “Plugins”. Dans cette procédure, supposons que vous souhaitez utiliser un plugin personnalisé. Dans la liste des plugins personnalisés, recherchez celui que vous souhaitez utiliser, cochez la case située à gauche, puis choisissez Suivant.
5. Entrez un nom et, éventuellement, une description.
6. Choisissez le cluster auquel vous souhaitez vous connecter.

7. Spécifiez la configuration du connecteur. Les paramètres de configuration que vous devez spécifier dépendent du type de connecteur que vous souhaitez créer. Cependant, certains paramètres sont communs à tous les connecteurs, par exemple les paramètres `connector.class` et `tasks.max`. Voici un exemple de configuration pour le connecteur récepteur Confluent Amazon S3.

   ```
   connector.class=io.confluent.connect.s3.S3SinkConnector
   tasks.max=2
   topics=my-example-topic
   s3.region=us-east-1
   s3.bucket.name=my-destination-bucket
   flush.size=1
   storage.class=io.confluent.connect.s3.storage.S3Storage
   format.class=io.confluent.connect.s3.format.json.JsonFormat
   partitioner.class=io.confluent.connect.storage.partitioner.DefaultPartitioner
   key.converter=org.apache.kafka.connect.storage.StringConverter
   value.converter=org.apache.kafka.connect.storage.StringConverter
   schema.compatibility=NONE
   ```

8. Vous configurez ensuite la capacité de votre connecteur. Vous pouvez choisir entre deux modes de capacité : provisionné et mis à l'échelle automatiquement. Pour plus d'informations sur ces deux options, consultez la section the section called “Capacité”.
9. Choisissez la configuration de worker par défaut ou une configuration de worker personnalisée. Pour plus d'informations sur la création des configurations de worker par défaut, consultez the section called “Workers”.
10. Vous spécifiez ensuite le rôle d'exécution du service. Il doit s'agir d'un rôle IAM que MSK Connect peut assumer et qui accorde au connecteur toutes les autorisations dont il a besoin pour accéder aux ressources nécessaires AWS . Ces autorisations dépendent de la logique du connecteur. Pour plus d'informations sur la création de ce rôle, consultez the section called “Rôles d'exécution du service”.
11. Choisissez Suivant, passez en revue les informations de sécurité, puis choisissez à nouveau Suivant.
12. Définissez les options de journalisation souhaitées, puis sélectionnez Suivant. Pour de plus amples informations sur la journalisation, veuillez consulter the section called “Journalisation”.
13. Sélectionnez Créer un connecteur.

Pour utiliser l'API MSK Connect afin de créer un connecteur, consultez CreateConnector.

Plugins

Un plugin est une AWS ressource qui contient le code qui définit la logique de votre connecteur. Vous chargez un fichier JAR (ou un fichier ZIP contenant un ou plusieurs fichiers JAR) dans un compartiment S3 et vous spécifiez l'emplacement du compartiment lorsque vous créez le plugin. Lorsque vous créez un connecteur, vous spécifiez le plugin que MSK Connect doit utiliser. La relation entre les plugins et les connecteurs est la suivante one-to-many : vous pouvez créer un ou plusieurs connecteurs à partir du même plugin.

Pour plus d'informations sur le développement du code d'un connecteur, consultez le Guide de développement des connecteurs dans la documentation d'Apache Kafka.

Création d'un plugin personnalisé à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Dans le volet de gauche, sous MSK Connect, choisissez Plugins personnalisés.
3. Choisissez Créer un plugin personnalisé.
4. Choisissez Parcourir S3.
5. Dans la liste des compartiments S3, choisissez le compartiment contenant le fichier JAR ou ZIP du plugin.
6. Dans la liste des objets, cochez la case située à gauche du fichier JAR ou ZIP du plugin, puis sélectionnez Choisir.
7. Choisissez Créer un plugin personnalisé.

Pour utiliser l'API MSK Connect afin de créer un plugin personnalisé, consultez CreateCustomPlugin.

Workers

Un worker est un processus de machine virtuelle Java (JVM) qui exécute la logique du connecteur. Chaque worker crée un ensemble de tâches qui s'exécutent dans des threads parallèles et se chargent de copier les données. Les tâches ne stockent pas l'état et peuvent donc être démarrées, arrêtées ou redémarrées à tout moment afin de fournir un pipeline de données résilient et évolutif. Les modifications du nombre de workers, qu'elles soient dues à un événement de mise à l'échelle ou à des défaillances inattendues, sont automatiquement détectées par les autres workers. Ils se coordonnent pour rééquilibrer les tâches entre les workers restants. Les workers de Connect utilisent les groupes de consommateurs d'Apache Kafka pour coordonner et rééquilibrer leurs tâches.

Si les exigences de capacité de votre connecteur sont variables ou difficiles à estimer, vous pouvez laisser MSK Connect ajuster le nombre de workers selon vos besoins entre une limite inférieure et une limite supérieure que vous spécifiez. Vous pouvez également spécifier le nombre exact de workers que vous souhaitez exécuter sur votre logique de connecteur. Pour plus d'informations, consultez the section called “Capacité”.

Les employés de MSK Connect consomment des adresses IP

Les employés de MSK Connect consomment des adresses IP dans les sous-réseaux fournis par le client. Chaque travailleur utilise une adresse IP provenant de l'un des sous-réseaux fournis par le client. Vous devez vous assurer que vous disposez d'un nombre suffisant d'adresses IP disponibles dans les sous-réseaux fournis à une CreateConnector demande pour tenir compte de leur capacité spécifiée, en particulier lors du dimensionnement automatique des connecteurs où le nombre de travailleurs peut fluctuer.

Rubriques

Configuration du processus worker par défaut

MSK Connect fournit la configuration de worker par défaut suivante :

```
key.converter=org.apache.kafka.connect.storage.StringConverter
value.converter=org.apache.kafka.connect.storage.StringConverter
```

Propriétés de configuration de l'environnement de worker compatibles

MSK Connect fournit une configuration de worker par défaut. Vous avez également la possibilité de créer une configuration de worker personnalisée à utiliser avec vos connecteurs. La liste suivante inclut des informations sur les propriétés de configuration de worker prises en charge ou non par Amazon MSK Connect.

- Seules les propriétés `key.converter` et `value.converter` sont obligatoires.
- MSK Connect prend en charge les propriétés de configuration `producer.` suivantes.

```
producer.acks
producer.batch.size
producer.buffer.memory
producer.compression.type
producer.enable.idempotence
producer.key.serializer
producer.max.request.size
producer.metadata.max.age.ms
producer.metadata.max.idle.ms
producer.partitioner.class
producer.reconnect.backoff.max.ms
producer.reconnect.backoff.ms
producer.request.timeout.ms
producer.retry.backoff.ms
producer.value.serializer
```

- MSK Connect prend en charge les propriétés de configuration `consumer.` suivantes.

```
consumer.allow.auto.create.topics
consumer.auto.offset.reset
consumer.check.crcs
consumer.fetch.max.bytes
consumer.fetch.max.wait.ms
consumer.fetch.min.bytes
consumer.heartbeat.interval.ms
consumer.key.deserializer
consumer.max.partition.fetch.bytes
consumer.max.poll.records
consumer.metadata.max.age.ms
consumer.partition.assignment.strategy
consumer.reconnect.backoff.max.ms
consumer.reconnect.backoff.ms
consumer.request.timeout.ms
consumer.retry.backoff.ms
consumer.session.timeout.ms
consumer.value.deserializer
```

- Toutes les autres propriétés de configuration qui ne commencent pas par les préfixes `producer.` ou sont `consumer.` prises en charge, sauf les propriétés suivantes.

```
access.control.
admin.
```

```
admin.listeners.https.
client.
connect.
inter.worker.
internal.
listeners.https.
metrics.
metrics.context.
rest.
sasl.
security.
socket.
ssl.
topic.tracking.
worker.
bootstrap.servers
config.storage.topic
connections.max.idle.ms
connector.client.config.override.policy
group.id
listeners
metric.reporters
plugin.path
receive.buffer.bytes
response.http.headers.config
scheduled.rebalance.max.delay.ms
send.buffer.bytes
status.storage.topic
```

Pour plus d'informations sur les propriétés de configuration de worker et ce qu'elles représentent, consultez Kafka Connect Configs dans la documentation Apache Kafka.

Création d'une configuration de worker personnalisée

Création d'une configuration de travail personnalisée à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Dans le volet gauche, sous MSK Connect, choisissez Configurations de worker.
3. Choisissez Créer une configuration de worker.
4. Entrez un nom et une description facultative, puis ajoutez les propriétés et les valeurs que vous souhaitez leur attribuer.

5. Choisissez Créer une configuration de worker.

Pour utiliser l'API MSK Connect afin de créer une configuration de travail, consultez CreateWorkerConfiguration.

Gestion des décalages du connecteur source en utilisant `offset.storage.topic`

Cette section fournit des informations qui vous aideront à gérer les décalages des connecteurs source à l'aide de la rubrique Stockage des décalages. La rubrique du stockage des décalages est une rubrique interne que Kafka Connect utilise pour stocker les décalages de configuration des connecteurs et des tâches.

Utilisation de la rubrique de stockage des décalages par défaut

Par défaut, Amazon MSK Connect génère une nouvelle rubrique de stockage des décalages sur votre cluster Kafka pour chaque connecteur que vous créez. MSK construit le nom de rubrique par défaut en utilisant des parties de l'ARN du connecteur. Par exemple, `__amazon_msk_connect_offsets_my-mskc-connector_12345678-09e7-4abc-8be8-c657f7e4ff32-2`.

Spécification de votre propre rubrique de stockage des décalages

Pour assurer la continuité des décalages entre les connecteurs source, vous pouvez utiliser une rubrique de stockage des décalages de votre choix au lieu de la rubrique par défaut. La spécification d'une rubrique de stockage des décalages vous aide à accomplir des tâches telles que la création d'un connecteur source qui reprend la lecture à partir du dernier décalage d'un connecteur précédent.

Pour spécifier une rubrique de stockage des décalages, vous devez fournir une valeur pour la propriété `offset.storage.topic` dans votre configuration de worker avant de créer un connecteur. Si vous souhaitez réutiliser la rubrique de stockage des décalages pour utiliser les décalages d'un connecteur créé précédemment, vous devez donner au nouveau connecteur le même nom que l'ancien connecteur. Si vous créez une rubrique de stockage de décalages personnalisée, vous devez définir `cleanup.policy` sur `compact` dans la configuration de votre rubrique.

> **Note**
>
> Si vous spécifiez une rubrique de stockage des décalages lorsque vous créez un connecteur récepteur, MSK Connect crée la rubrique si elle n'existe pas déjà. Toutefois, cette rubrique ne sera pas utilisée pour enregistrer les décalages du connecteur.
> Les décalages du connecteur récepteur sont plutôt gérés à l'aide du protocole de groupe de consommateurs Kafka. Chaque connecteur récepteur crée un groupe nommé `connect-{CONNECTOR_NAME}`. Tant que le groupe de consommateurs existe, tous les connecteurs récepteurs successifs que vous créez avec la même valeur `CONNECTOR_NAME` seront maintenus à partir du dernier décalage validé.

Example Spécification d'une rubrique de stockage des décalages pour recréer un connecteur source avec une configuration mise à jour

Supposons que vous disposiez d'un connecteur CDC (Change Data Capture) et que vous souhaitiez modifier la configuration du connecteur sans perdre votre place dans le flux CDC. Vous ne pouvez pas mettre à jour la configuration de connecteur existante, mais vous pouvez supprimer le connecteur et en créer un autre portant le même nom. Pour indiquer au nouveau connecteur par où commencer à lire dans le flux CDC, vous pouvez spécifier la rubrique de stockage des décalages de l'ancien connecteur dans votre configuration de worker. Les étapes suivantes expliquent comment effectuer cette tâche.

1. Sur votre machine cliente, exécutez la commande suivante pour trouver le nom de la rubrique de stockage des décalages de votre connecteur. Remplacez *<bootstrapBrokerString>* par la chaîne de l'agent d'amorçage de votre cluster. Pour obtenir des instructions sur l'obtention de votre chaîne de l'agent d'amorçage, consultez Obtention des agents d'amorçage pour un cluster Amazon MSK.

   ```
   <path-to-your-kafka-installation>/bin/kafka-topics.sh --list --bootstrap-
   server <bootstrapBrokerString>
   ```

   La sortie suivante présente une liste de toutes les rubriques du cluster, y compris les rubriques du connecteur interne par défaut. Dans cet exemple, le connecteur CDC existant utilise la rubrique de stockage des décalages par défaut créée par MSK Connect. C'est pourquoi la rubrique de stockage des décalages est appelée `__amazon_msk_connect_offsets_my-mskc-connector_12345678-09e7-4abc-8be8-c657f7e4ff32-2`.

```
__consumer_offsets
__amazon_msk_canary
__amazon_msk_connect_configs_my-mskc-connector_12345678-09e7-4abc-8be8-
c657f7e4ff32-2
__amazon_msk_connect_offsets_my-mskc-connector_12345678-09e7-4abc-8be8-
c657f7e4ff32-2
__amazon_msk_connect_status_my-mskc-connector_12345678-09e7-4abc-8be8-
c657f7e4ff32-2
my-msk-topic-1
my-msk-topic-2
```

2. Ouvrez la console Amazon MSK sur https://console.aws.amazon.com/msk/.
3. Choisissez votre connecteur dans la liste des connecteurs. Copiez et enregistrez le contenu du champ de configuration du connecteur afin de pouvoir le modifier et l'utiliser pour créer le nouveau connecteur.
4. Pour supprimer la connecteur, choisissez Supprimer. Puis saisissez le nom du connecteur dans le champ d'entrée du texte pour confirmer la suppression.
5. Créez une configuration de worker personnalisée avec des valeurs adaptées à votre scénario. Pour obtenir des instructions, veuillez consulter Création d'une configuration de worker personnalisée.

   Dans votre configuration de worker, vous devez spécifier le nom de la rubrique de stockage des décalages que vous avez précédemment récupérée en tant que valeur pour `offset.storage.topic` comme dans la configuration suivante.

```
config.providers.secretManager.param.aws.region=us-east-1
key.converter=<org.apache.kafka.connect.storage.StringConverter>
value.converter=<org.apache.kafka.connect.storage.StringConverter>
config.providers.secretManager.class=com.github.jcustenborder.kafka.config.aws.SecretsManag
config.providers=secretManager
offset.storage.topic=__amazon_msk_connect_offsets_my-mskc-
connector_12345678-09e7-4abc-8be8-c657f7e4ff32-2
```

6. **Important**

   Vous devez donner à votre nouveau connecteur le même nom que l'ancien connecteur.

Créez un nouveau connecteur à l'aide de la configuration de worker que vous avez configurée à l'étape précédente. Pour obtenir des instructions, veuillez consulter Création d'un connecteur.

Considérations

Tenez compte des éléments suivants lorsque vous gérez les décalages du connecteur source.

- Pour spécifier une rubrique de stockage des décalages, indiquez le nom de la rubrique Kafka dans lequel les décalages des connecteurs sont stockés en tant que valeur pour `offset.storage.topic` dans votre configuration de worker.
- Soyez prudent lorsque vous modifiez la configuration d'un connecteur. La modification des valeurs de configuration peut entraîner un comportement involontaire du connecteur si un connecteur source utilise les valeurs de la configuration pour saisir des enregistrements de décalage. Pour plus d'informations, nous vous recommandons de consulter la documentation de votre plugin.
- Personnaliser le nombre de partitions par défaut : en plus de personnaliser la configuration de worker en ajoutant `offset.storage.topic`, vous pouvez personnaliser le nombre de partitions pour les rubriques de stockage des décalages et des statuts. Les partitions par défaut pour les rubriques internes sont les suivantes.
  - `config.storage.topic` : 1, non configurable, doit être une rubrique à partition unique
  - `offset.storage.topic` : 25, configurable en fournissant `offset.storage.partitions`
  - `status.storage.topic` : 5, configurable en fournissant `status.storage.partitions`
- Suppression manuelle des rubriques : Amazon MSK Connect crée de nouvelles rubriques internes à Kafka Connect (le nom de la rubrique commence par `__amazon_msk_connect`) à chaque déploiement de connecteurs. Les anciennes rubriques attachées à des connecteurs supprimés ne sont pas automatiquement supprimées car les rubriques internes, telles que `offset.storage.topic`, peuvent être réutilisées entre les connecteurs. Cependant, vous pouvez supprimer manuellement les rubriques internes non utilisées créées par MSK Connect. Les rubriques internes sont nommées selon le format `__amazon_msk_connect_<offsets|status|configs>_`*`connector_name_connector_id`*.

  L'expression régulière `__amazon_msk_connect_<offsets|status|configs>_`*`connector_name_connector_id`* peut être utilisée pour supprimer les rubriques internes. Vous ne devez pas supprimer une rubrique interne actuellement utilisée par un connecteur en cours d'exécution.

- Utilisation du même nom pour les rubriques internes créées par MSK Connect : si vous souhaitez réutiliser la rubrique de stockage des décalages pour utiliser les décalages d'un connecteur créé précédemment, vous devez donner au nouveau connecteur le même nom que l'ancien connecteur. La propriété `offset.storage.topic` peut être définie à l'aide de la configuration de worker pour attribuer le même nom à `offset.storage.topic` et réutilisée entre différents connecteurs. Cette configuration est décrite dans Gestion des décalages de connecteurs. MSK Connect n'autorise pas que les différents connecteurs partagent `config.storage.topic` et`status.storage.topic`. Ces rubriques sont créées chaque fois que vous créez un nouveau connecteur dans MSKC. Ils sont automatiquement nommés selon le format `__amazon_msk_connect_<status|configs>_`*`connector_name_connector_id`* et sont donc différents selon les connecteurs que vous créez.

Externalisation d'informations sensibles à l'aide des fournisseurs de configuration

Cet exemple montre comment externaliser des informations sensibles pour Amazon MSK Connect à l'aide d'un fournisseur de configuration open source. Un fournisseur de configuration vous permet de spécifier des variables plutôt que du texte brut dans une configuration de connecteur ou de worker, et les workers exécutés dans votre connecteur résolvent ces variables au moment de l'exécution. Cela empêche le stockage d'informations d'identification et d'autres secrets en texte brut. Dans cet exemple, le fournisseur de configuration prend en charge la récupération des paramètres de configuration depuis AWS Secrets Manager, Amazon S3 et Systems Manager (SSM). À l'étape 2, vous pouvez voir comment configurer le stockage et la récupération d'informations sensibles pour le service que vous souhaitez configurer.

Rubriques

- Étape 1 : Créer un plugin personnalisé et le charger sur S3
- Étape 2 : Configurer les paramètres et les autorisations pour différents fournisseurs
- Étape 3 : Créer une configuration de worker personnalisée avec des informations sur votre fournisseur de configuration
- Étape 4 : Créer un connecteur
- Considérations

Étape 1 : Créer un plugin personnalisé et le charger sur S3

Pour créer un plugin personnalisé, créez un fichier zip contenant le connecteur msk-config-provider en exécutant les commandes suivantes sur votre machine locale.

Pour créer un plugin personnalisé en utilisant une fenêtre de terminal et Debezium comme connecteur

Utilisez la AWS CLI pour exécuter des commandes en tant que superutilisateur avec des informations d'identification vous permettant d'accéder à votre compartiment AWS S3. Pour plus d'informations sur l'installation et la configuration de la AWS CLI, consultez la section Getting started with the AWS CLI dans le guide de AWS Command Line Interface l'utilisateur. Pour plus d'informations sur l'utilisation de l' AWS interface de ligne de commande avec Amazon S3, consultez la section Utilisation d'Amazon S3 avec l' AWS interface de ligne de commande dans le guide de AWS Command Line Interface l'utilisateur.

1. Dans une fenêtre de terminal, créez un dossier nommé `custom-plugin` dans votre espace de travail à l'aide de la commande suivante.

   ```
   mkdir custom-plugin && cd custom-plugin
   ```

2. Téléchargez la dernière version stable du plug-in du connecteur MySQL depuis le site Debezium à l'aide de la commande suivante.

   ```
   wget https://repo1.maven.org/maven2/io/debezium/debezium-connectormysql/
   2.2.0.Final/debezium-connector-mysql-2.2.0.Final-plugin.tar.gz
   ```

   Extrayez le fichier gzip téléchargé dans le dossier `custom-plugin` à l'aide de la commande suivante.

   ```
   tar xzf debezium-connector-mysql-2.2.0.Final-plugin.tar.gz
   ```

3. Téléchargez le fichier zip du fournisseur de configuration MSK à l'aide de la commande suivante.

   ```
   wget https://github.com/aws-samples/msk-config-providers/releases/download/r0.1.0/
   msk-config-providers-0.1.0-with-dependencies.zip
   ```

   Extrayez le fichier zip téléchargé dans le dossier `custom-plugin` à l'aide de la commande suivante.

```
unzip msk-config-providers-0.1.0-with-dependencies.zip
```

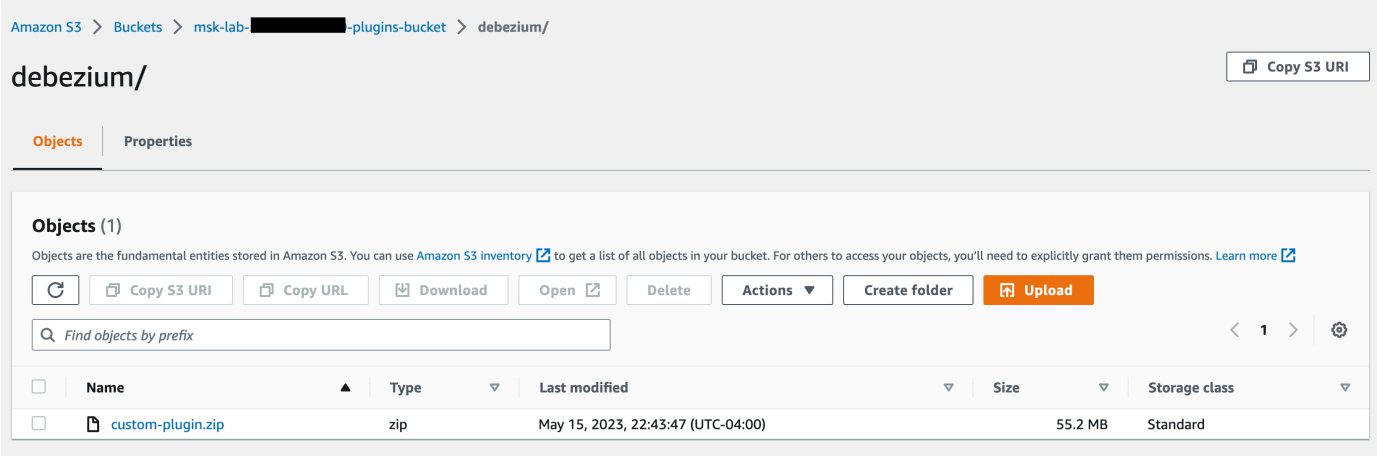
4. Compressez le contenu du fournisseur de configuration MSK à partir de l'étape ci-dessus et du connecteur personnalisé dans un seul fichier nommé `custom-plugin.zip`.

```
zip -r ../custom-plugin.zip *
```

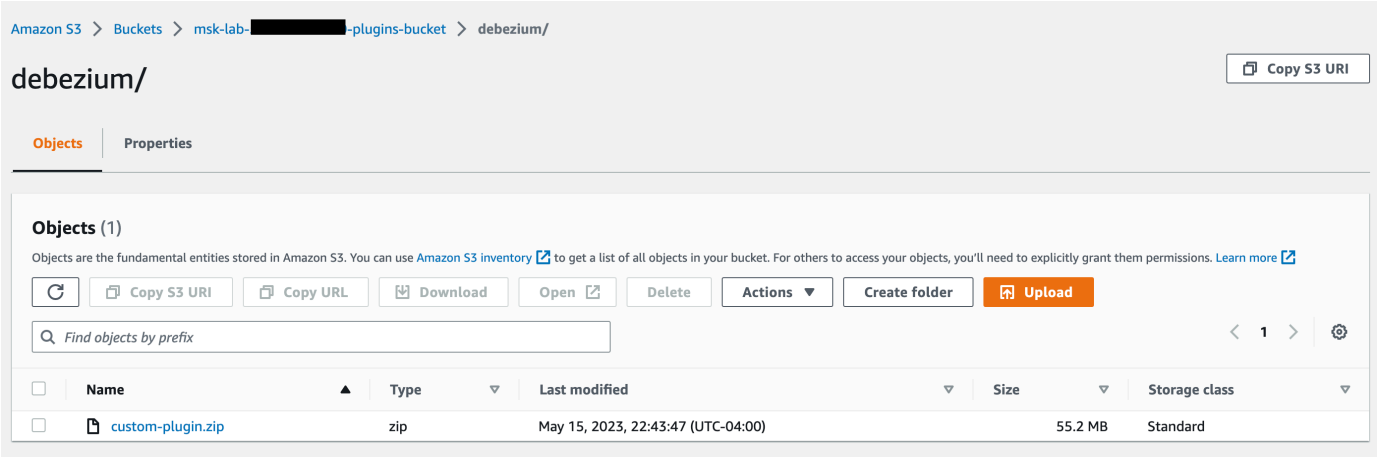
5. Chargez le fichier sur S3 pour référence ultérieure.

```
aws s3 cp ../custom-plugin.zip s3:<S3_URI_BUCKET_LOCATION>
```

6. Sur la console Amazon MSK, dans la section MSK Connect, choisissez Plugin personnalisé, puis choisissez Créer un plugin personnalisé et parcourez le compartiment S3 s3:<***S3_URI_BUCKET_LOCATION***> pour sélectionner le fichier ZIP du plugin personnalisé que vous venez de télécharger.



7. Entrez **`debezium-custom-plugin`** comme nom du plugin. Si vous le souhaitez, saisissez une description et choisissez Créer un plugin personnalisé.



Étape 2 : Configurer les paramètres et les autorisations pour différents fournisseurs

Vous pouvez configurer les valeurs des paramètres dans les trois services suivants :

- Secrets Manager
- Systems Manager Parameter Store
- S3 - Simple Storage Service

Sélectionnez l'un des onglets ci-dessous pour obtenir des instructions sur la configuration des paramètres et des autorisations pertinentes pour ce service.

Configure in Secrets Manager

Pour configurer les valeurs de paramètres dans Secrets Manager

1. Ouvrez la console Secrets Manager.
2. Créez un nouveau secret pour stocker vos informations d'identification ou vos secrets. Pour obtenir des instructions, voir Création d'un AWS Secrets Manager secret dans le guide de AWS Secrets Manager l'utilisateur.
3. Copiez l'ARN de votre secret.
4. Ajoutez les autorisations Secrets Manager de l'exemple de politique suivant à votre rôle d'exécution du service. Remplacez *<arn:aws:secretsmanager:us-east-1:123456789000:secret* : -1234> par l'ARN de votre secret. MySecret
5. Ajoutez la configuration du worker et les instructions relatives au connecteur.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Action": [
                    "secretsmanager:GetResourcePolicy",
                    "secretsmanager:GetSecretValue",
                    "secretsmanager:DescribeSecret",
                    "secretsmanager:ListSecretVersionIds"
                ],
                "Resource": [
```

```
                "<arn:aws:secretsmanager:us-
east-1:123456789000:secret:MySecret-1234>"
                ]
            }
        ]
    }
```

6. Pour utiliser le fournisseur de configuration Secrets Manager, copiez les lignes de code suivantes dans la zone de texte de configuration du worker à l'étape 3 :

```
# define name of config provider:

config.providers = secretsmanager

# provide implementation classes for secrets manager:

config.providers.secretsmanager.class =
 com.amazonaws.kafka.config.providers.SecretsManagerConfigProvider

# configure a config provider (if it needs additional initialization), for
 example you can provide a region where the secrets or parameters are located:

config.providers.secretsmanager.param.region = us-east-1
```

7. Pour utiliser le fournisseur de configuration Secrets Manager, copiez les lignes de code suivantes dans la zone de texte de configuration du worker à l'étape 4.

```
#Example implementation for secrets manager variable
database.hostname=${secretsmanager:MSKAuroraDBCredentials:username}

database.password=${secretsmanager:MSKAuroraDBCredentials:password}
```

Vous pouvez également utiliser l'étape ci-dessus avec d'autres fournisseurs de configuration.

Configure in Systems Manager Parameter Store

Pour configurer et utiliser des valeurs de paramètres dans Systems Manager Parameter Store

1. Ouvrez la console Systems Manager.
2. Dans le panneau de navigation, choisissez Stockage de paramètres.

3. Créez un nouveau paramètre à stocker dans le Systems Manager. Pour obtenir des instructions, reportez-vous à la section Créer un paramètre Systems Manager (console) dans le Guide de AWS Systems Manager l'utilisateur.
4. Copiez l'ARN de votre paramètre.
5. Ajoutez les autorisations Systems Manager de l'exemple de politique suivant à votre rôle d'exécution du service. Remplacez *<arn:aws:ssm:us-east- MyParameterName 1:123456789000:parameter/* > par l'ARN de votre paramètre.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "ssm:GetParameterHistory",
                    "ssm:GetParametersByPath",
                    "ssm:GetParameters",
                    "ssm:GetParameter"
                ],
                "Resource": "arn:aws:ssm:us-east-1:123456789000:parameter/
MyParameterName"
            }
        ]
    }
```

6. Pour utiliser le fournisseur de configuration Parameter Store, copiez les lignes de code suivantes dans la zone de texte de configuration du worker à l'étape 3 :

```
# define name of config provider:

config.providers = ssm

# provide implementation classes for parameter store:

config.providers.ssm.class =
 com.amazonaws.kafka.config.providers.SsmParamStoreConfigProvider

# configure a config provider (if it needs additional initialization), for
 example you can provide a region where the secrets or parameters are located:
```

```
config.providers.ssm.param.region = us-east-1
```

7. Pour utiliser le fournisseur de configuration Parameter Store, copiez les lignes de code suivantes dans la zone de texte de configuration du worker à l'étape 5.

```
#Example implementation for parameter store variable
schema.history.internal.kafka.bootstrap.servers=
${ssm::MSKBootstrapServerAddress}
```

Vous pouvez également grouper les deux étapes ci-dessus avec d'autres fournisseurs de configuration.

Configure in Amazon S3

Pour configurer des objets/fichiers dans Amazon S3

1. Ouvrez la console Amazon S3.
2. Chargez votre objet dans un compartiment dans S3. Pour obtenir des instructions, consultez Chargement d'objets.
3. Copiez l'ARN de votre objet.
4. Ajoutez les autorisations de lecture d'objets Amazon S3 de l'exemple de politique suivant à votre rôle d'exécution du service. Remplacez *<arn:aws:s3:::MY_S3_BUCKET/path/to/custom-plugin.zip>* par l'ARN de votre objet.

```
{
    "Version": "2012-10-17",
    "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": "s3:GetObject",
                "Resource": "<arn:aws:s3:::MY_S3_BUCKET/path/to/custom-
plugin.zip>"
            }
        ]
    }
```

5. Pour utiliser le fournisseur de configuration Amazon S3, copiez les lignes de code suivantes dans la zone de texte de configuration du worker à l'étape 3 :

```
# define name of config provider:

config.providers = s3import
# provide implementation classes for S3:

config.providers.s3import.class =
 com.amazonaws.kafka.config.providers.S3ImportConfigProvider
```

6. Pour utiliser le fournisseur de configuration Amazon S3, copiez les lignes de code suivantes dans la zone de texte de configuration du worker à l'étape 4.

```
#Example implementation for S3 object

database.ssl.truststore.location = ${s3import:us-west-2:my_cert_bucket/path/to/
trustore_unique_filename.jks}
```

Vous pouvez également grouper les deux étapes ci-dessus avec d'autres fournisseurs de configuration.

Étape 3 : Créer une configuration de worker personnalisée avec des informations sur votre fournisseur de configuration

1. Sélectionnez Configurations de worker dans la section Amazon MSK Connect.
2. Sélectionnez Créer une configuration de worker.
3. Entrez `SourceDebeziumCustomConfig` dans la zone de texte Nom de la configuration du worker. La description est facultative.
4. Copiez le code de configuration approprié en fonction des fournisseurs souhaités, puis collez-le dans la zone de texte Configuration du worker.
5. Voici un exemple de configuration de worker pour les trois fournisseurs :

```
key.converter=org.apache.kafka.connect.storage.StringConverter
key.converter.schemas.enable=false
value.converter=org.apache.kafka.connect.json.JsonConverter
value.converter.schemas.enable=false
offset.storage.topic=offsets_my_debezium_source_connector
```

```
# define names of config providers:

config.providers=secretsmanager,ssm,s3import

# provide implementation classes for each provider:

config.providers.secretsmanager.class    =
 com.amazonaws.kafka.config.providers.SecretsManagerConfigProvider
config.providers.ssm.class               =
 com.amazonaws.kafka.config.providers.SsmParamStoreConfigProvider
config.providers.s3import.class          =
 com.amazonaws.kafka.config.providers.S3ImportConfigProvider

# configure a config provider (if it needs additional initialization), for example
 you can provide a region where the secrets or parameters are located:


config.providers.secretsmanager.param.region = us-east-1
config.providers.ssm.param.region = us-east-1
```

6. Cliquez sur Créer une configuration de worker.

Étape 4 : Créer un connecteur

1. Créez un nouveau connecteur en suivant les instructions de la section Créer un nouveau connecteur.
2. Choisissez le fichier `custom-plugin.zip` que vous avez chargé dans votre compartiment S3 dans la section ??? comme source du plugin personnalisé.
3. Copiez le code de configuration approprié en fonction des fournisseurs souhaités, puis collez-le dans le champ Configuration du connecteur.
4. Voici un exemple de configuration de connecteur pour les trois fournisseurs :

```
#Example implementation for parameter store variable
schema.history.internal.kafka.bootstrap.servers=${ssm::MSKBootstrapServerAddress}

#Example implementation for secrets manager variable
database.hostname=${secretsmanager:MSKAuroraDBCredentials:username}

database.password=${secretsmanager:MSKAuroraDBCredentials:password}

#Example implementation for Amazon S3 file/object
```

```
database.ssl.truststore.location = ${s3import:us-west-2:my_cert_bucket/path/to/
trustore_unique_filename.jks}
```

5. Sélectionnez Utiliser une configuration personnalisée et choisissez dans le SourceDebeziumCustomConfigmenu déroulant Configuration du travailleur.
6. Suivez les étapes restantes indiquées dans les instructions de la section Créer un connecteur.

Considérations

Tenez compte des points suivants lorsque vous utilisez le fournisseur de configuration MSK avec Amazon MSK Connect :

- Attribuez les autorisations appropriées lors de l'utilisation des fournisseurs de configuration au rôle d'exécution du service IAM.
- Définissez les fournisseurs de configuration dans les configurations du worker et leur implémentation dans la configuration du connecteur.
- Des valeurs de configuration sensibles peuvent apparaître dans les journaux des connecteurs si un plugin ne définit pas ces valeurs comme secrètes. Kafka Connect traite les valeurs de configuration non définies de la même manière que toute autre valeur en texte brut. Pour en savoir plus, veuillez consulter la section Empêcher l'apparition de secrets dans les journaux des connecteurs.
- Par défaut, MSK Connect redémarre fréquemment un connecteur lorsque celui-ci utilise un fournisseur de configuration. Pour désactiver ce comportement de redémarrage, vous pouvez définir la valeur `config.action.reload` sur `none` dans la configuration de votre connecteur.

Rôles et politiques IAM pour MSK Connect

Rubriques

- Rôles d'exécution du service
- Exemples de politiques IAM pour MSK Connect
- Prévention du problème de l’adjoint confus entre services
- AWS politiques gérées pour MSK Connect
- Utilisation des rôles liés à un service pour MSK Connect

Rôles d'exécution du service

> **Note**
>
> Amazon MSK Connect ne prend pas en charge l'utilisation du rôle lié au service comme rôle d'exécution du service. Vous devez créer un rôle d'exécution de service distinct. Pour savoir comment créer un rôle IAM personnalisé, consultez la section Création d'un rôle pour déléguer des autorisations à un AWS service dans le Guide de l'utilisateur IAM.

Lorsque vous créez un connecteur avec MSK Connect, vous devez spécifier un rôle AWS Identity and Access Management (IAM) à utiliser avec celui-ci. Votre rôle d'exécution du service doit avoir la politique d'approbation suivante pour que MSK Connect puisse l'assumer. Pour plus d'informations sur les clés de contexte de condition de cette politique, veuillez consulter the section called "Prévention du problème de l'adjoint confus entre services".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "kafkaconnect.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "Account-ID"
        },
        "ArnLike": {
          "aws:SourceArn": "MSK-Connector-ARN"
        }
      }
    }
  ]
}
```

Si le cluster Amazon MSK que vous souhaitez utiliser avec votre connecteur est un cluster qui utilise l'authentification IAM, vous devez ajouter la politique d'autorisation suivante au rôle d'exécution du

service du connecteur. Pour plus d'informations sur la façon de trouver l'UUID de votre cluster et sur la façon de construire des ARN de rubrique, consultez the section called “Ressources”.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:DescribeCluster"
            ],
            "Resource": [
                "cluster-arn"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:ReadData",
                "kafka-cluster:DescribeTopic"
            ],
            "Resource": [
                "ARN of the topic that you want a sink connector to read from"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:WriteData",
                "kafka-cluster:DescribeTopic"
            ],
            "Resource": [
                "ARN of the topic that you want a source connector to write to"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:CreateTopic",
                "kafka-cluster:WriteData",
                "kafka-cluster:ReadData",
                "kafka-cluster:DescribeTopic"
```

```
            ],
            "Resource": [
                "arn:aws:kafka:region:account-id:topic/cluster-name/cluster-uuid/
__amazon_msk_connect_*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeGroup"
            ],
            "Resource": [
                "arn:aws:kafka:region:account-id:group/cluster-name/cluster-uuid/
__amazon_msk_connect_*",
                "arn:aws:kafka:region:account-id:group/cluster-name/cluster-uuid/
connect-*"
            ]
        }
    ]
}
```

Selon le type de connecteur, vous devrez peut-être également associer au rôle d'exécution du service une politique d'autorisation lui permettant d'accéder aux AWS ressources. Par exemple, si votre connecteur doit envoyer des données à un compartiment S3, le rôle d'exécution du service doit disposer d'une politique d'autorisations autorisant l'écriture dans ce compartiment. À des fins de test, vous pouvez utiliser l'une des politiques IAM prédéfinies qui offrent un accès complet, comme `arn:aws:iam::aws:policy/AmazonS3FullAccess`. Toutefois, pour des raisons de sécurité, nous vous recommandons d'utiliser la politique la plus restrictive qui permette à votre connecteur de lire depuis la AWS source ou d'écrire sur le AWS récepteur.

Exemples de politiques IAM pour MSK Connect

Pour donner à un utilisateur non administrateur un accès complet à toutes les fonctionnalités de MSK Connect, associez une politique telle que la suivante au rôle IAM de l'utilisateur.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "kafkaconnect:*",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeSecurityGroups",
                "logs:CreateLogDelivery",
                "logs:GetLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
kafkaconnect.amazonaws.com/AWSServiceRoleForKafkaConnect*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "kafkaconnect.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
kafkaconnect.amazonaws.com/AWSServiceRoleForKafkaConnect*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "delivery.logs.amazonaws.com"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketPolicy",
                "s3:GetBucketPolicy"
            ],
            "Resource": "ARN of the Amazon S3 bucket to which you want MSK Connect to
 deliver logs"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "ARN of the service execution role"
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "ARN of the Amazon S3 object that corresponds to the custom
 plugin that you want to use for creating connectors"
        },
        {
            "Effect": "Allow",
            "Action": "firehose:TagDeliveryStream",
            "Resource": "ARN of the Firehose delivery stream to which you want MSK
 Connect to deliver logs"
        }
    ]
}
```

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. En AWS, l'usurpation d'identité interservices peut entraîner un problème de confusion chez les adjoints. 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 de contexte de condition globale `aws:SourceArn` et `aws:SourceAccount` dans les politiques de ressources afin de limiter les autorisations à la ressource octroyées par MSK Connect à un autre service. Si la valeur `aws:SourceArn` ne contient pas l'ID de compte (par exemple, un Amazon Resource Name (ARN) d'un compartiment Amazon S3 ne contient pas l'ID de compte), vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations. Si vous utilisez les deux clés de contexte de condition globale et que la valeur `aws:SourceArn` contient l'ID de compte, la valeur `aws:SourceAccount` et le compte dans la valeur `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'ils sont utilisés dans la même instruction de politique. Utilisez `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.

Dans le cas de MSK Connect, la valeur de `aws:SourceArn` doit être un connecteur MSK.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, *`arn:aws:kafkaconnect:us-east-1:123456789012:connector/*`* représente tous les connecteurs appartenant au compte portant l'ID 123456789012 dans la région USA Est (Virginie du Nord).

L'exemple suivant montre comment utiliser les clés de contexte de condition globale `aws:SourceArn` et `aws:SourceAccount` dans MSK Connect afin d'éviter le problème de l'adjoint confus. Remplacez *`Account-ID`* et *`MSK-Connector-ARN`* par vos informations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": " kafkaconnect.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "Account-ID"
        },
        "ArnLike": {
```

```
          "aws:SourceArn": "MSK-Connector-ARN"
        }
      }
    }
  ]
}
```

AWS politiques gérées pour MSK Connect

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les 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.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonMSK ConnectReadOnlyAccess

Cette politique accorde à l'utilisateur les autorisations nécessaires pour répertorier et décrire les ressources MSK Connect.

Vous pouvez associer la politique `AmazonMSKConnectReadOnlyAccess` à vos identités IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "kafkaconnect:ListConnectors",
                "kafkaconnect:ListCustomPlugins",
                "kafkaconnect:ListWorkerConfigurations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafkaconnect:DescribeConnector"
            ],
            "Resource": [
                "arn:aws:kafkaconnect:*:*:connector/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafkaconnect:DescribeCustomPlugin"
            ],
            "Resource": [
                "arn:aws:kafkaconnect:*:*:custom-plugin/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafkaconnect:DescribeWorkerConfiguration"
            ],
            "Resource": [
                "arn:aws:kafkaconnect:*:*:worker-configuration/*"
            ]
        }
    ]
}
```

AWS politique gérée : KafkaConnectServiceRolePolicy

Cette politique accorde au service Connect les autorisations nécessaires pour créer et gérer les interfaces réseau dotées de la balise `AmazonMSKConnectManaged:true`. Ces interfaces réseau donnent à MSK Connect l'accès réseau aux ressources de votre VPC Amazon, telles qu'un cluster Apache Kafka, une source ou un récepteur.

Vous ne pouvez pas vous associer KafkaConnectServiceRolePolicy à vos entités IAM. Cette politique est attachée à un rôle lié au service qui permet à MSK Connect d'effectuer des actions en votre nom.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:CreateNetworkInterface"
   ],
   "Resource": "arn:aws:ec2:*:*:network-interface/*",
   "Condition": {
    "StringEquals": {
     "aws:RequestTag/AmazonMSKConnectManaged": "true"
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": "AmazonMSKConnectManaged"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:CreateNetworkInterface"
   ],
   "Resource": [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:CreateTags"
   ],
   "Resource": "arn:aws:ec2:*:*:network-interface/*",
   "Condition": {
    "StringEquals": {
     "ec2:CreateAction": "CreateNetworkInterface"
    }
   }
  },
```

```
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeNetworkInterfaces",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:AttachNetworkInterface",
    "ec2:DetachNetworkInterface",
    "ec2:DeleteNetworkInterface"
   ],
   "Resource": "arn:aws:ec2:*:*:network-interface/*",
   "Condition": {
    "StringEquals": {
     "ec2:ResourceTag/AmazonMSKConnectManaged": "true"
    }
   }
  }
 ]
}
```

Mises à jour des politiques AWS gérées par MSK Connect

Consultez les détails des mises à jour apportées aux politiques AWS gérées pour MSK Connect depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
Mise à jour de la politique en lecture seule de MSK Connect	MSK Connect a mis à jour la ConnectReadOnlyAccess politique d'AmazonMSK afin de supprimer les restrictions relatives aux opérations de mise en vente.	13 octobre 2021
MSK Connect a commencé à suivre les modifications	MSK Connect a commencé à suivre les modifications apportées à ses politiques AWS gérées.	14 septembre 2021

Utilisation des rôles liés à un service pour MSK Connect

Amazon MSK Connect utilise des rôles liés à un service AWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à MSK Connect. Les rôles liés au service sont prédéfinis par MSK Connect et incluent toutes les autorisations dont le service a besoin pour appeler AWS d'autres services en votre nom.

Un rôle lié à un service simplifie la configuration de MSK Connect, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. MSK Connect définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul MSK Connect 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.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle lié à un service pour MSK Connect

MSK Connect utilise le rôle lié au service nommé — AWSServiceRoleForKafkaConnectAutorise Amazon MSK Connect à accéder aux ressources Amazon en votre nom.

Le rôle AWSServiceRoleForKafkaConnect lié au service fait confiance au `kafkaconnect.amazonaws.com` service pour assumer le rôle.

Pour obtenir des informations sur la politique d'autorisations utilisé par le rôle, consultez the section called “KafkaConnectServiceRolePolicy”.

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 du rôle lié à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour MSK Connect

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un connecteur dans le AWS Management Console, le ou l' AWS API AWS CLI, MSK Connect crée le rôle lié au service pour vous.

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 un connecteur, MSK Connect recrée automatiquement le rôle lié au service.

Modification d'un rôle lié à un service pour MSK Connect

MSK Connect ne vous permet pas de modifier le rôle lié au AWSServiceRoleForKafkaConnect service. 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 au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, 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 MSK Connect

Vous pouvez utiliser la console IAM, AWS CLI ou l' AWS API pour supprimer manuellement le rôle lié à un service. Pour ce faire, vous devez d'abord supprimer manuellement tous vos connecteurs MSK Connect, puis supprimer manuellement le rôle. Pour plus d'informations, veuillez consulter 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 MSK Connect

MSK Connect 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 AWS.

Activation de l'accès à Internet pour Amazon MSK Connect

Si votre connecteur pour Amazon MSK Connect a besoin d'un accès à Internet, nous vous recommandons d'utiliser les paramètres Amazon Virtual Private Cloud (VPC) suivants pour activer cet accès.

- Configurez votre connecteur avec des sous-réseaux privés.
- Créez une passerelle NAT publique ou une instance NAT pour votre VPC dans un sous-réseau public. Pour plus d'informations, consultez la page Connecter des sous-réseaux à Internet ou à d'autres VPC à l'aide de périphériques NAT dans le Guide de l'utilisateur Amazon Virtual Private Cloud.
- Autorisez le trafic sortant de vos sous-réseaux privés vers votre passerelle ou instance NAT.

Configuration d'une passerelle NAT pour Amazon MSK Connect

Les étapes suivantes vous montrent comment configurer une passerelle NAT pour permettre à un connecteur d'accéder à Internet. Vous devez effectuer ces étapes avant de créer un connecteur dans un sous-réseau privé.

Prérequis

Vérifiez que vous avez les éléments suivants.

- L'ID du Amazon Virtual Private Cloud (VPC) associé à votre cluster. Par exemple, vpc-123456ab.
- L'ID des sous-réseaux privés de votre VPC. Par exemple, subnet-a1b2c3de, subnet-f4g5h6ij, etc. Vous devez configurer votre connecteur avec des sous-réseaux privés.

Pour activer l'accès à Internet pour votre connecteur

1. Ouvrez la Amazon Virtual Private Cloud console à l'adresse https://console.aws.amazon.com/vpc/.
2. Créez un sous-réseau public pour votre passerelle NAT avec un nom descriptif et notez l'ID du sous-réseau. Pour obtenir des informations détaillées, veuillez consulter Créer un sous-réseau dans votre VPC.
3. Créez une passerelle Internet afin que votre VPC puisse communiquer avec Internet et notez l'ID de passerelle. Attachez la passerelle Internet à votre VPC. Pour de plus amples informations, consultez Créer et attacher une passerelle Internet.
4. Provisionnez une passerelle NAT publique afin que les hôtes de vos sous-réseaux privés puissent accéder à votre sous-réseau public. Lorsque vous créez la passerelle NAT, sélectionnez le sous-réseau public que vous avez créé précédemment. Pour obtenir des informations, consultez Créer une passerelle NAT.
5. Configurez vos tables de routage. Vous devez disposer de deux tables de routage au total pour terminer cette configuration. Vous devriez déjà avoir une table de routage principale créée automatiquement en même temps que votre VPC. Au cours de cette étape, vous créez une table de routage supplémentaire pour votre sous-réseau public.

    a. Utilisez les paramètres suivants pour modifier la table de routage principale de votre VPC afin que vos sous-réseaux privés acheminent le trafic vers votre passerelle NAT. Pour obtenir des informations, consultez la section Utiliser des tables de routage dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Table de routage MSKC privée

Propriété	Valeur
Identification de nom	Nous vous recommandons de donner à cette table de routage un nom descriptif pour vous aider à l'identifier. Par exemple, MSKC privé.
Sous-réseaux associés	Vos sous-réseaux privés
Une route pour permettre l'accès à Internet pour MSK Connect	• Destination : 0.0.0.0/0 • Cible : votre identifiant de passerelle NAT. Par exemple, nat-12a345bc6789efg1h.
Une route pour l'ensemble du trafic local	• Destination : 10.0.0.0/16. Cette valeur peut varier en fonction du bloc d'adresse CIDR de votre VPC. • Cible : locale

b. Suivez les instructions de la section Créer une table de routage personnalisée pour créer une table de routage pour votre sous-réseau public. Lorsque vous créez la table, entrez un nom descriptif dans le champ Identification de nom pour vous aider à identifier le sous-réseau auquel la table est associée. Par exemple, MSKC public.

c. Configurez votre table de routage MSKC public à l'aide des paramètres suivants.

Propriété	Valeur
Identification de nom	MSKC public ou un autre nom descriptif que vous choisissez
Sous-réseaux associés	Votre sous-réseau public avec passerelle NAT

Propriété	Valeur
Une route pour permettre l'accès à Internet pour MSK Connect	• Destination : 0.0.0.0/0 • Cible : votre identifiant de passerelle Internet. Par exemple, igw-1a234bc5.
Une route pour l'ensemble du trafic local	• Destination : 10.0.0.0/16. Cette valeur peut varier en fonction du bloc d'adresse CIDR de votre VPC. • Cible : locale

Noms d'hôtes DNS privés

Grâce à la prise en charge des noms d'hôte DNS privés dans MSK Connect, vous pouvez configurer des connecteurs pour référencer des noms de domaine publics ou privés. Cette prise en charge dépend des serveurs DNS spécifiés dans le jeu d'options DHCP du VPC.

Un jeu d'options DHCP est un groupe de configurations réseau utilisé par les instances EC2 dans un VPC pour communiquer sur votre réseau VPC. Chaque VPC possède un jeu d'options DHCP par défaut, mais vous pouvez créer un jeu d'options DHCP personnalisé si, par exemple, vous souhaitez que les instances d'un VPC utilisent un serveur DNS différent pour la résolution des noms de domaine plutôt que le serveur DNS fourni par Amazon. Voir Jeux d'options DHCP dans le VPC Amazon.

Avant que la capacité/fonctionnalité de résolution DNS privée ne soit incluse dans MSK Connect, les connecteurs utilisaient les résolveurs DNS du VPC de service pour les requêtes DNS provenant d'un connecteur client. Les connecteurs n'utilisaient pas les serveurs DNS définis dans les jeux d'options DHCP du VPC du client pour la résolution DNS.

Les connecteurs pouvaient uniquement faire référence à des noms d'hôtes dans des configurations de connecteurs clients ou à des plugins pouvant être résolus publiquement. Ils ne pouvaient pas résoudre les noms d'hôtes privés définis dans une zone hébergée en privé ou utiliser les serveurs DNS d'un autre réseau client.

Sans le DNS privé, les clients qui choisissaient de rendre leurs bases de données, leurs entrepôts de données et leurs systèmes tels que le Secrets Manager dans leur propre VPC inaccessibles à

Internet ne pouvaient pas utiliser les connecteurs MSK. Les clients utilisent souvent des noms d'hôte DNS privés pour se conformer à la politique de sécurité de l'entreprise.

Rubriques

Configuration d'un jeu d'options DHCP du VPC pour votre connecteur

Les connecteurs utilisent automatiquement les serveurs DNS définis dans leur jeu d'options DHCP du VPC lors de la création du connecteur. Avant de créer un connecteur, assurez-vous de configurer l'option DHCP du VPC définie pour les exigences de résolution du nom d'hôte DNS de votre connecteur.

Les connecteurs que vous avez créés avant que la fonctionnalité de nom d'hôte DNS privé ne soit disponible dans MSK Connect continuent d'utiliser la configuration de résolution DNS précédente sans qu'aucune modification ne soit requise.

Si vous avez uniquement besoin d'une résolution de nom d'hôte DNS pouvant être résolue publiquement dans votre connecteur, pour faciliter la configuration, nous vous recommandons d'utiliser le VPC par défaut de votre compte lorsque vous créez le connecteur. Consultez Serveur Amazon DNS dans le Guide de l'utilisateur du VPC Amazon pour plus d'informations sur le serveur DNS fourni par Amazon ou Amazon Route 53 Resolver.

Si vous devez résoudre des noms d'hôtes DNS privés, assurez-vous que les options DHCP du VPC transmis lors de la création du connecteur sont correctement configurées. Pour plus d'informations, consultez Travailler avec des jeux d'options DHCP dans le Guide de l'utilisateur du VPC Amazon.

Lorsque vous configurez un jeu d'options DHCP pour la résolution de noms d'hôtes DNS privés, assurez-vous que le connecteur peut atteindre les serveurs DNS personnalisés que vous configurez dans le jeu d'options DHCP. Dans le cas contraire, la création de votre connecteur échouera.

Après avoir personnalisé le jeu d'options DHCP du VPC, les connecteurs créés ultérieurement dans ce VPC utilisent les serveurs DNS que vous avez spécifiés dans le jeu d'options. Si vous modifiez le jeu d'options après avoir créé un connecteur, le connecteur adopte les paramètres du nouveau jeu d'options en quelques minutes.

Attributs DNS pour votre VPC

Assurez-vous que les attributs DNS du VPC sont correctement configurés, comme décrit dans la section Attributs DNS de votre VPC et Noms d'hôte DNS dans le Guide de l'utilisateur du VPC Amazon.

Consultez la section Résolution des requêtes DNS entre les VPC et votre réseau dans le Guide du développeur Amazon Route 53 pour obtenir plus d'informations sur l'utilisation des points de terminaison de résolution entrants et sortants pour connecter d'autres réseaux à votre VPC afin de les utiliser avec votre connecteur.

Gestion des défaillances

Cette section décrit les échecs éventuels de création de connecteurs associés à la résolution DNS et les actions suggérées pour résoudre les problèmes.

Échec	Action suggérée
La création du connecteur échoue si une requête de résolution DNS échoue ou si les serveurs DNS sont inaccessibles depuis le connecteur.	Vous pouvez voir des échecs de création de connecteurs dus à des requêtes de résolution DNS infructueuses dans vos CloudWatch journaux, si vous avez configuré ces journaux pour votre connecteur. Vérifiez les configurations des serveurs DNS et assurez-vous de la connectivité réseau avec les serveurs DNS à partir du connecteur.
Si vous modifiez la configuration des serveurs DNS dans votre jeu d'options DHCP du VPC alors qu'un connecteur est en cours d'exécution, les requêtes de résolution DNS provenant du connecteur peuvent échouer. Si la résolution DNS échoue, certaines tâches du connecteur peuvent passer à l'état d'échec.	Vous pouvez voir des échecs de création de connecteurs dus à des requêtes de résolution DNS infructueuses dans vos CloudWatch journaux, si vous avez configuré ces journaux pour votre connecteur. Les tâches ayant échoué devraient redémarrer automatiquement pour rétablir le connecteur. Si cela ne se produit pas, vous pouvez contacter le support pour redémarrer les tâches ayant

Échec	Action suggérée
	échoué pour leur connecteur ou vous pouvez recréer le connecteur.

Journalisation pour MSK Connect

MSK Connect peut écrire des événements de journal que vous pouvez utiliser pour déboguer votre connecteur. Lorsque vous créez un connecteur, vous pouvez spécifier aucune ou plusieurs des destinations de journal suivantes :

- Amazon CloudWatch Logs : vous spécifiez le groupe de journaux auquel vous souhaitez que MSK Connect envoie les événements de journal de votre connecteur. Pour plus d'informations sur la création d'un groupe de journaux, voir Création d'un groupe de journaux dans le Guide de l'utilisateur CloudWatch des journaux.
- Amazon S3 : vous spécifiez le compartiment S3 auquel vous souhaitez que MSK Connect envoie les événements de journal de votre connecteur. Pour plus d'informations sur la façon de créer un compartiment S3, consultez Création d'un compartiment dans le Guide de l'utilisateur Amazon S3.
- Amazon Data Firehose : vous spécifiez le flux de diffusion vers lequel vous souhaitez que MSK Connect envoie les événements du journal de votre connecteur. Pour plus d'informations sur la création d'un flux de diffusion, consultez la section Création d'un flux de diffusion Amazon Data Firehose dans le guide de l'utilisateur de Firehose.

Pour en savoir plus sur la configuration de la journalisation, consultez la section Activation de la journalisation à partir de certains services AWS dans le Guide de l'utilisateur Amazon CloudWatch Logs .

MSK Connect émet les types d'événements de journal suivants :

Niveau	Description
`INFO`	Événements d'exécution présentant un intérêt au démarrage et à l'arrêt.

Niveau	Description
WARN	Situations d'exécution qui ne sont pas des erreurs mais qui sont indésirables ou inattendues.
FATAL	Erreurs graves entraînant un arrêt prématuré.
ERROR	Conditions inattendues et erreurs d'exécution qui ne sont pas fatales.

Voici un exemple d'événement de journal envoyé à CloudWatch Logs :

```
[Worker-0bb8afa0b01391c41] [2021-09-06 16:02:54,151] WARN [Producer
 clientId=producer-1] Connection to node 1 (b-1.my-test-cluster.twwhtj.c2.kafka.us-
east-1.amazonaws.com/INTERNAL_IP) could not be established. Broker may not be
 available. (org.apache.kafka.clients.NetworkClient:782)
```

Empêcher l'apparition de secrets dans les journaux des connecteurs

> **Note**
>
> Des valeurs de configuration sensibles peuvent apparaître dans les journaux des connecteurs si un plugin ne définit pas ces valeurs comme secrètes. Kafka Connect traite les valeurs de configuration non définies de la même manière que toute autre valeur en texte brut.

Si votre plugin définit une propriété comme secrète, Kafka Connect supprime la valeur de la propriété des journaux du connecteur. Par exemple, les journaux du connecteur suivants montrent que si un plugin définit `aws.secret.key` comme un type `PASSWORD`, sa valeur est alors remplacée par **`[hidden]`**.

```
   2022-01-11T15:18:55.000+00:00    [Worker-05e6586a48b5f331b] [2022-01-11
15:18:55,150] INFO SecretsManagerConfigProviderConfig values:
   2022-01-11T15:18:55.000+00:00    [Worker-05e6586a48b5f331b] aws.access.key =
my_access_key
   2022-01-11T15:18:55.000+00:00    [Worker-05e6586a48b5f331b] aws.region = us-east-1
```

```
    2022-01-11T15:18:55.000+00:00    [Worker-05e6586a48b5f331b] aws.secret.key
= [hidden]
    2022-01-11T15:18:55.000+00:00    [Worker-05e6586a48b5f331b] secret.prefix =
    2022-01-11T15:18:55.000+00:00    [Worker-05e6586a48b5f331b] secret.ttl.ms = 300000
    2022-01-11T15:18:55.000+00:00    [Worker-05e6586a48b5f331b]
(com.github.jcustenborder.kafka.config.aws.SecretsManagerConfigProviderConfig:361)
```

Pour éviter que des secrets n'apparaissent dans les fichiers journaux du connecteur, le développeur d'un plugin doit utiliser la constante d'énumération de Kafka Connect `ConfigDef.Type.PASSWORD` pour définir les propriétés sensibles. Lorsqu'une propriété est du type `ConfigDef.Type.PASSWORD`, Kafka Connect exclut sa valeur des journaux du connecteur, même si la valeur est envoyée sous forme de texte brut.

Surveillance de MSK Connect

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de MSK Connect et de vos autres AWS solutions. 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 l'utilisation du processeur ou d'autres mesures de votre connecteur, afin de pouvoir augmenter sa capacité si nécessaire. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Le tableau suivant indique les métriques que MSK Connect envoie CloudWatch sous la `ConnectorName` dimension. MSK Connect fournit ces métriques par défaut et sans frais supplémentaires. CloudWatch conserve ces indicateurs pendant 15 mois, afin que vous puissiez accéder aux informations historiques et avoir une meilleure idée des performances de vos connecteurs. 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.

Métriques MSK Connect

Nom des métriques	Description
`BytesInPerSec`	Nombre total d'octets reçus par le connecteur.
`BytesOutPerSec`	Nombre total d'octets fournis par le connecteur.

Nom des métriques	Description
CpuUtilization	Pourcentage de la consommation du processeur par système et par utilisateur.
ErroredTaskCount	Nombre de tâches qui ont des erreurs.
MemoryUtilization	Pourcentage de la mémoire totale d'une instance de worker, et pas seulement la mémoire de tas de la machine virtuelle Java (JVM) actuellement utilisée. La JVM ne restitue généralement pas de mémoire au système d'exploitation. Ainsi, la taille de tas de la JVM (MemoryUtilization) commence généralement par une taille de tas minimale qui augmente progressivement jusqu'à un maximum stable d'environ 80 à 90 %. L'utilisation du tas de mémoire de la JVM peut augmenter ou diminuer à mesure que l'utilisation réelle de la mémoire du connecteur change.
RebalanceCompletedTotal	Nombre total de rééquilibres effectués par ce connecteur.
RebalanceTimeAvg	Durée moyenne (en millisecondes) que le connecteur consacre au rééquilibrage.
RebalanceTimeMax	Durée maximale (en millisecondes) que le connecteur consacre au rééquilibrage.
RebalanceTimeSinceLast	Durée (en millisecondes) écoulée depuis que ce connecteur a effectué le dernier rééquilibrage.
RunningTaskCount	Nombre de tâches en cours d'exécution dans le connecteur.

Nom des métriques	Description
SinkRecordReadRate	Nombre moyen (par seconde) d'enregis trements lus depuis le cluster Apache Kafka ou Amazon MSK.
SinkRecordSendRate	Nombre moyen (par seconde) d'enregis trements générés par les transformations et envoyés à la destination. Ce nombre n'inclut pas les enregistrements filtrés.
SourceRecordPollRate	Nombre moyen (par seconde) d'enregis trements produits ou interrogés.
SourceRecordWriteRate	Nombre moyen (par seconde) d'enregis trements générés par les transformations et écrits sur le cluster Apache Kafka ou Amazon MSK.
TaskStartupAttemptsTotal	Nombre total de démarrages de tâches que le connecteur a tentés. Vous pouvez utiliser cette métrique pour identifier les anomalies lors des tentatives de démarrage de tâches.
TaskStartupSuccessPercentage	Pourcentage moyen de démarrages de tâches réussis pour le connecteur. Vous pouvez utiliser cette métrique pour identifier les anomalies lors des tentatives de démarrage de tâches.
WorkerCount	Nombre de workers en cours d'exécution dans le connecteur.

Exemples

Cette section contient des exemples destinés à vous aider à configurer les ressources Amazon MSK Connect, comme les connecteurs tiers et les fournisseurs de configuration courants.

Rubriques

Connecteur récepteur Amazon S3

Cet exemple montre comment utiliser le connecteur récepteur Amazon S3 Confluent et comment AWS CLI créer un connecteur récepteur Amazon S3 dans MSK Connect.

1. Copiez le code JSON et collez-le dans un nouveau fichier. Remplacez les chaînes d'espace réservé par des valeurs correspondant à la chaîne de connexion des serveurs d'amorçage de votre cluster Amazon MSK et aux identifiants de sous-réseau et de groupe de sécurité du cluster. Pour plus d'informations sur la configuration d'un rôle d'exécution de service, consultez the section called “Rôles et politiques IAM”.

```
{
    "connectorConfiguration": {
        "connector.class": "io.confluent.connect.s3.S3SinkConnector",
        "s3.region": "us-east-1",
        "format.class": "io.confluent.connect.s3.format.json.JsonFormat",
        "flush.size": "1",
        "schema.compatibility": "NONE",
        "topics": "my-test-topic",
        "tasks.max": "2",
        "partitioner.class":
 "io.confluent.connect.storage.partitioner.DefaultPartitioner",
        "storage.class": "io.confluent.connect.s3.storage.S3Storage",
        "s3.bucket.name": "my-test-bucket"
    },
    "connectorName": "example-S3-sink-connector",
    "kafkaCluster": {
        "apacheKafkaCluster": {
            "bootstrapServers": "<cluster-bootstrap-servers-string>",
            "vpc": {
                "subnets": [
                    "<cluster-subnet-1>",
                    "<cluster-subnet-2>",
                    "<cluster-subnet-3>"
                ],
                "securityGroups": ["<cluster-security-group-id>"]
            }
```

```
        }
    },
    "capacity": {
        "provisionedCapacity": {
            "mcuCount": 2,
            "workerCount": 4
        }
    },
    "kafkaConnectVersion": "2.7.1",
    "serviceExecutionRoleArn": "<arn-of-a-role-that-msk-connect-can-assume>",
    "plugins": [
        {
            "customPlugin": {
                "customPluginArn": "<arn-of-custom-plugin-that-contains-connector-
code>",
                "revision": 1
            }
        }
    ],
    "kafkaClusterEncryptionInTransit": {"encryptionType": "PLAINTEXT"},
    "kafkaClusterClientAuthentication": {"authenticationType": "NONE"}
}
```

2. Exécutez la AWS CLI commande suivante dans le dossier où vous avez enregistré le fichier JSON à l'étape précédente.

```
aws kafkaconnect create-connector --cli-input-json file://connector-info.json
```

Voici un exemple du résultat que vous obtenez lorsque vous exécutez la commande.

```
{
    "ConnectorArn": "arn:aws:kafkaconnect:us-east-1:123450006789:connector/example-
S3-sink-connector/abc12345-abcd-4444-a8b9-123456f513ed-2",
    "ConnectorState": "CREATING",
    "ConnectorName": "example-S3-sink-connector"
}
```

Connecteur source Debezium avec fournisseur de configuration

Cet exemple explique comment utiliser le plugin du connecteur Debezium MySQL avec une base de données Amazon Aurora compatible avec MySQL comme source. Dans cet exemple, nous

avons également configuré le fournisseur de configuration AWS Secrets Manager open source pour externaliser les informations d'identification de la base de données dans AWS Secrets Manager. Pour en savoir plus sur les fournisseurs de configuration, consultez Externalisation d'informations sensibles à l'aide des fournisseurs de configuration.

> **Important**
>
> Le plugin du connecteur Debezium MySQL ne prend en charge qu'une seule tâche et ne fonctionne pas avec le mode de capacité de mise à l'échelle automatique pour Amazon MSK Connect. Vous devez plutôt utiliser le mode de capacité provisionné et définir la valeur de `workerCount` égale à un dans la configuration de votre connecteur. Pour en savoir plus sur les modes de capacité de MSK Connect, consultez Capacité du connecteur.

Avant de commencer

Votre connecteur doit être en mesure d'accéder à Internet afin de pouvoir interagir avec des services extérieurs au vôtre Amazon Virtual Private Cloud. AWS Secrets Manager Les étapes décrites dans cette section vous aident à effectuer les tâches suivantes pour activer l'accès à Internet.

- Configurez un sous-réseau public qui héberge une passerelle NAT et achemine le trafic vers une passerelle Internet dans votre VPC.
- Créez une route par défaut qui dirige le trafic de votre sous-réseau privé vers votre passerelle NAT.

Pour plus d'informations, consultez Activation de l'accès à Internet pour Amazon MSK Connect.

Prérequis

Avant de pouvoir activer l'accès à Internet, vous devez disposer des éléments suivants :

- L'ID du Amazon Virtual Private Cloud (VPC) associé à votre cluster. Par exemple, vpc-123456ab.
- L'ID des sous-réseaux privés de votre VPC. Par exemple, subnet-a1b2c3de, subnet-f4g5h6ij, etc. Vous devez configurer votre connecteur avec des sous-réseaux privés.

Pour activer l'accès à Internet pour votre connecteur

1. Ouvrez la Amazon Virtual Private Cloud console à l'adresse https://console.aws.amazon.com/vpc/.

2. Créez un sous-réseau public pour votre passerelle NAT avec un nom descriptif et notez l'ID du sous-réseau. Pour obtenir des informations détaillées, veuillez consulter Créer un sous-réseau dans votre VPC.
3. Créez une passerelle Internet afin que votre VPC puisse communiquer avec Internet et notez l'ID de passerelle. Attachez la passerelle Internet à votre VPC. Pour de plus amples informations, consultez Créer et attacher une passerelle Internet.
4. Provisionnez une passerelle NAT publique afin que les hôtes de vos sous-réseaux privés puissent accéder à votre sous-réseau public. Lorsque vous créez la passerelle NAT, sélectionnez le sous-réseau public que vous avez créé précédemment. Pour obtenir des informations, consultez Créer une passerelle NAT.
5. Configurez vos tables de routage. Vous devez disposer de deux tables de routage au total pour terminer cette configuration. Vous devriez déjà avoir une table de routage principale créée automatiquement en même temps que votre VPC. Au cours de cette étape, vous créez une table de routage supplémentaire pour votre sous-réseau public.

   a. Utilisez les paramètres suivants pour modifier la table de routage principale de votre VPC afin que vos sous-réseaux privés acheminent le trafic vers votre passerelle NAT. Pour obtenir des informations, consultez la section Utiliser des tables de routage dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

      Table de routage MSKC privée

Propriété	Valeur
Identification de nom	Nous vous recommandons de donner à cette table de routage un nom descriptif pour vous aider à l'identifier. Par exemple, MSKC privé.
Sous-réseaux associés	Vos sous-réseaux privés
Une route pour permettre l'accès à Internet pour MSK Connect	• Destination : 0.0.0.0/0 • Cible : votre identifiant de passerelle NAT. Par exemple, nat-12a345bc6789efg1h.

Propriété	Valeur
Une route pour l'ensemble du trafic local	• Destination : 10.0.0.0/16. Cette valeur peut varier en fonction du bloc d'adresse CIDR de votre VPC. • Cible : locale

b. Suivez les instructions de la section Créer une table de routage personnalisée pour créer une table de routage pour votre sous-réseau public. Lorsque vous créez la table, entrez un nom descriptif dans le champ Identification de nom pour vous aider à identifier le sous-réseau auquel la table est associée. Par exemple, MSKC public.

c. Configurez votre table de routage MSKC public à l'aide des paramètres suivants.

Propriété	Valeur
Identification de nom	MSKC public ou un autre nom descriptif que vous choisissez
Sous-réseaux associés	Votre sous-réseau public avec passerelle NAT
Une route pour permettre l'accès à Internet pour MSK Connect	• Destination : 0.0.0.0/0 • Cible : votre identifiant de passerelle Internet. Par exemple, igw-1a234bc5.
Une route pour l'ensemble du trafic local	• Destination : 10.0.0.0/16. Cette valeur peut varier en fonction du bloc d'adresse CIDR de votre VPC. • Cible : locale

Maintenant que vous avez activé l'accès à Internet pour Amazon MSK Connect, vous êtes prêt à créer un connecteur.

Création d'un connecteur source Debezium

1. Créez un plugin personnalisé

   a. Téléchargez la dernière version stable du plugin du connecteur MySQL depuis le site Debezium. Notez la version de Debezium que vous téléchargez (version 2.x ou ancienne série 1.x). Vous allez créer ultérieurement un connecteur basé sur votre version de Debezium.

   b. Téléchargez et extrayez le fournisseur de configuration AWS Secrets Manager.

   c. Placez les archives suivantes dans le même répertoire :

   - Le dossier `debezium-connector-mysql`
   - Le dossier `jcusten-border-kafka-config-provider-aws-0.1.1`

   d. Compressez le répertoire que vous avez créé à l'étape précédente dans un fichier ZIP, puis chargez ce dernier dans un compartiment S3. Pour obtenir des informations, consultez Chargement d'objets dans le Guide de l'utilisateur Amazon S3.

   e. Copiez le code JSON et collez-le dans un fichier. Par exemple, `debezium-source-custom-plugin.json`. Remplacez *< example-custom-plugin-name >* par le nom que vous souhaitez attribuer au plugin, *< arn-of-your-s 3-bucket>* par l'ARN du compartiment S3 dans lequel vous avez chargé le fichier ZIP et *<file-key-of-ZIP-object>* par la clé de fichier de l'objet ZIP que vous avez chargé sur S3.

```
{
    "name": "<example-custom-plugin-name>",
    "contentType": "ZIP",
    "location": {
        "s3Location": {
            "bucketArn": "<arn-of-your-s3-bucket>",
            "fileKey": "<file-key-of-ZIP-object>"
        }
    }
}
```

   f. Exécutez la AWS CLI commande suivante depuis le dossier dans lequel vous avez enregistré le fichier JSON pour créer un plugin.

```
aws kafkaconnect create-custom-plugin --cli-input-json file://<debezium-source-custom-plugin.json>
```

Vous devez voir un résultat similaire à ce qui suit.

```
{
    "CustomPluginArn": "arn:aws:kafkaconnect:us-east-1:012345678901:custom-
plugin/example-custom-plugin-name/abcd1234-a0b0-1234-c1-12345678abcd-1",
    "CustomPluginState": "CREATING",
    "Name": "example-custom-plugin-name",
    "Revision": 1
}
```

g. Exécutez la commande suivante pour vérifier le statut du plugin. Le statut doit passer de `CREATING` à `ACTIVE`. Remplacez l'espace réservé de l'ARN par l'ARN que vous avez obtenu dans le résultat de la commande précédente.

```
aws kafkaconnect describe-custom-plugin --custom-plugin-arn "<arn-of-your-
custom-plugin>"
```

2. Configurer AWS Secrets Manager et créer un secret pour les informations d'identification de votre base de données

   a. Ouvrez la console Secrets Manager en suivant le lien https://console.aws.amazon.com/secretsmanager/.

   b. Créez un nouveau secret pour stocker les informations d'identification de connexion à votre base de données. Pour obtenir des informations, consultez la section Créer un secret dans le Guide de l'utilisateur AWS Secrets Manager.

   c. Copiez l'ARN de votre secret.

   d. Ajoutez les autorisations Secrets Manager de l'exemple de politique suivant à votre Rôles d'exécution du service. Remplacez *<arn:aws:secretsmanager:us-east-1:123456789000:secret* : -1234> par l'ARN de votre secret. MySecret

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource": [
        "<arn:aws:secretsmanager:us-east-1:123456789000:secret:MySecret-1234>"
      ]
    }
  ]
}
```

Pour obtenir des informations sur la façon d'ajouter des autorisations IAM, consultez Ajout et suppression d'autorisations basées sur l'identité IAM dans le Guide d'utilisateur IAM.

3. Créez une configuration de worker personnalisée avec des informations sur votre fournisseur de configuration

   a. Copiez les propriétés de configuration du worker suivantes dans un fichier, en remplaçant les chaînes d'espace réservé par des valeurs correspondant à votre scénario. Pour en savoir plus sur les propriétés de configuration du fournisseur de configuration AWS Secrets Manager, consultez SecretsManagerConfigProviderla documentation du plugin.

```
key.converter=<org.apache.kafka.connect.storage.StringConverter>
value.converter=<org.apache.kafka.connect.storage.StringConverter>
config.providers.secretManager.class=com.github.jcustenborder.kafka.config.aws.SecretsM
config.providers=secretManager
config.providers.secretManager.param.aws.region=<us-east-1>
```

   b. Exécutez la AWS CLI commande suivante pour créer votre configuration de travail personnalisée.

      Remplacez les valeurs suivantes :

      - *< my-worker-config-name >* - un nom descriptif pour votre configuration de travail personnalisée
      - *< encoded-properties-file-content -string>* - une version codée en base64 des propriétés en texte brut que vous avez copiées à l'étape précédente

```
aws kafkaconnect create-worker-configuration --name <my-worker-config-name> --
properties-file-content <encoded-properties-file-content-string>
```

4. Créez un connecteur

   a. Copiez le code JSON suivant qui correspond à votre version de Debezium (2.x ou 1.x) et collez-le dans un nouveau fichier. Remplacez les chaînes *<placeholder>* par des valeurs correspondant à votre scénario. Pour plus d'informations sur la configuration d'un rôle d'exécution de service, consultez the section called “Rôles et politiques IAM”.

   Notez que la configuration utilise des variables comme `${secretManager:MySecret-1234:dbusername}` plutôt que du texte brut pour spécifier les informations d'identification de la base de données. Remplacez *MySecret-1234* par le nom de votre secret, puis indiquez le nom de la clé que vous souhaitez récupérer. Vous devez également remplacer *<arn-of-config-provider-worker-configuration>* par l'ARN de votre configuration de worker personnalisée.

   Debezium 2.x

   Pour les versions 2.x de Debezium, copiez le code JSON suivant et collez-le dans un nouveau fichier. Remplacez les chaînes *<espace réservé>* par des valeurs correspondant à votre scénario.

```
{
 "connectorConfiguration": {
  "connector.class": "io.debezium.connector.mysql.MySqlConnector",
  "tasks.max": "1",
  "database.hostname": "<aurora-database-writer-instance-endpoint>",
  "database.port": "3306",
  "database.user": "<${secretManager:MySecret-1234:dbusername}>",
  "database.password": "<${secretManager:MySecret-1234:dbpassword}>",
  "database.server.id": "123456",
  "database.include.list": "<list-of-databases-hosted-by-specified-server>",
  "topic.prefix": "<logical-name-of-database-server>",
  "schema.history.internal.kafka.topic": "<kafka-topic-used-by-debezium-to-track-schema-changes>",
  "schema.history.internal.kafka.bootstrap.servers": "<cluster-bootstrap-servers-string>",
  "schema.history.internal.consumer.security.protocol": "SASL_SSL",
  "schema.history.internal.consumer.sasl.mechanism": "AWS_MSK_IAM",
  "schema.history.internal.consumer.sasl.jaas.config":
 "software.amazon.msk.auth.iam.IAMLoginModule required;",
  "schema.history.internal.consumer.sasl.client.callback.handler.class":
 "software.amazon.msk.auth.iam.IAMClientCallbackHandler",
```

```
  "schema.history.internal.producer.security.protocol": "SASL_SSL",
  "schema.history.internal.producer.sasl.mechanism": "AWS_MSK_IAM",
  "schema.history.internal.producer.sasl.jaas.config":
 "software.amazon.msk.auth.iam.IAMLoginModule required;",
  "schema.history.internal.producer.sasl.client.callback.handler.class":
 "software.amazon.msk.auth.iam.IAMClientCallbackHandler",
  "include.schema.changes": "true"
 },
 "connectorName": "example-Debezium-source-connector",
 "kafkaCluster": {
  "apacheKafkaCluster": {
   "bootstrapServers": "<cluster-bootstrap-servers-string>",
   "vpc": {
    "subnets": [
     "<cluster-subnet-1>",
     "<cluster-subnet-2>",
     "<cluster-subnet-3>"
    ],
    "securityGroups": ["<id-of-cluster-security-group>"]
   }
  }
 },
 "capacity": {
  "provisionedCapacity": {
   "mcuCount": 2,
   "workerCount": 1
  }
 },
 "kafkaConnectVersion": "2.7.1",
 "serviceExecutionRoleArn": "<arn-of-service-execution-role-that-msk-
connect-can-assume>",
 "plugins": [{
  "customPlugin": {
   "customPluginArn": "<arn-of-msk-connect-plugin-that-contains-connector-
code>",
   "revision": 1
  }
 }],
 "kafkaClusterEncryptionInTransit": {
  "encryptionType": "TLS"
 },
 "kafkaClusterClientAuthentication": {
  "authenticationType": "IAM"
 },
```

```
 "workerConfiguration": {
  "workerConfigurationArn": "<arn-of-config-provider-worker-configuration>",
  "revision": 1
 }
}
```

Debezium 1.x

Pour les versions 1.x de Debezium, copiez le code JSON suivant et collez-le dans un nouveau fichier. Remplacez les chaînes *<espace réservé>* par des valeurs correspondant à votre scénario.

```
{
 "connectorConfiguration": {
  "connector.class": "io.debezium.connector.mysql.MySqlConnector",
  "tasks.max": "1",
  "database.hostname": "<aurora-database-writer-instance-endpoint>",
  "database.port": "3306",
  "database.user": "<${secretManager:MySecret-1234:dbusername}>",
  "database.password": "<${secretManager:MySecret-1234:dbpassword}>",
  "database.server.id": "123456",
  "database.server.name": "<logical-name-of-database-server>",
  "database.include.list": "<list-of-databases-hosted-by-specified-server>",
  "database.history.kafka.topic": "<kafka-topic-used-by-debezium-to-track-
schema-changes>",
  "database.history.kafka.bootstrap.servers": "<cluster-bootstrap-servers-
string>",
  "database.history.consumer.security.protocol": "SASL_SSL",
  "database.history.consumer.sasl.mechanism": "AWS_MSK_IAM",
  "database.history.consumer.sasl.jaas.config":
 "software.amazon.msk.auth.iam.IAMLoginModule required;",
  "database.history.consumer.sasl.client.callback.handler.class":
 "software.amazon.msk.auth.iam.IAMClientCallbackHandler",
  "database.history.producer.security.protocol": "SASL_SSL",
  "database.history.producer.sasl.mechanism": "AWS_MSK_IAM",
  "database.history.producer.sasl.jaas.config":
 "software.amazon.msk.auth.iam.IAMLoginModule required;",
  "database.history.producer.sasl.client.callback.handler.class":
 "software.amazon.msk.auth.iam.IAMClientCallbackHandler",
  "include.schema.changes": "true"
 },
 "connectorName": "example-Debezium-source-connector",
 "kafkaCluster": {
```

```
  "apacheKafkaCluster": {
   "bootstrapServers": "<cluster-bootstrap-servers-string>",
   "vpc": {
    "subnets": [
     "<cluster-subnet-1>",
     "<cluster-subnet-2>",
     "<cluster-subnet-3>"
    ],
    "securityGroups": ["<id-of-cluster-security-group>"]
   }
  }
 },
 "capacity": {
  "provisionedCapacity": {
   "mcuCount": 2,
   "workerCount": 1
  }
 },
 "kafkaConnectVersion": "2.7.1",
 "serviceExecutionRoleArn": "<arn-of-service-execution-role-that-msk-
connect-can-assume>",
 "plugins": [{
  "customPlugin": {
   "customPluginArn": "<arn-of-msk-connect-plugin-that-contains-connector-
code>",
   "revision": 1
  }
 }],
 "kafkaClusterEncryptionInTransit": {
  "encryptionType": "TLS"
 },
 "kafkaClusterClientAuthentication": {
  "authenticationType": "IAM"
 },
 "workerConfiguration": {
  "workerConfigurationArn": "<arn-of-config-provider-worker-configuration>",
  "revision": 1
 }
}
```

b. Exécutez la AWS CLI commande suivante dans le dossier où vous avez enregistré le fichier JSON à l'étape précédente.

```
aws kafkaconnect create-connector --cli-input-json file://connector-info.json
```

Voici un exemple du résultat que vous obtenez lorsque vous exécutez la commande.

```
{
    "ConnectorArn": "arn:aws:kafkaconnect:us-east-1:123450006789:connector/
example-Debezium-source-connector/abc12345-abcd-4444-a8b9-123456f513ed-2",
    "ConnectorState": "CREATING",
    "ConnectorName": "example-Debezium-source-connector"
}
```

Pour avoir un exemple de connecteur Debezium avec des étapes détaillées, consultez Présentation d'Amazon MSK Connect - Diffusez des données vers et depuis vos clusters Apache Kafka à l'aide de connecteurs gérés.

Bonnes pratiques

Utilisez ces informations comme référence pour trouver rapidement des recommandations sur l'optimisation des performances avec Amazon MSK Connect.

Rubriques

- Connexion à partir de connecteurs

Connexion à partir de connecteurs

Les bonnes pratiques suivantes peuvent améliorer les performances de votre connectivité à Amazon MSK Connect.

Ne superposez pas les adresses IP pour l'appairage Amazon VPC ou la passerelle de transit

Si vous utilisez l'appairage Amazon VPC ou la passerelle de transit avec Amazon MSK Connect, ne configurez pas votre connecteur pour accéder aux ressources des VPC appairés dont les adresses IP se situent dans les plages CIDR :

- "10.99.0.0/16"

- "192.168.0.0/16"
- "172.21.0.0/16"

Guide de migration vers Amazon MSK Connect

Cette section explique comment migrer votre application de connecteur Apache Kafka vers Amazon Managed Streaming for Apache Kafka Connect (Amazon MSK Connect).

Rubriques

Avantages de l'utilisation d'Amazon MSK Connect

Apache Kafka est l'une des plateformes de streaming open source les plus largement adoptées pour l'ingestion et le traitement de flux de données en temps réel. Avec Apache Kafka, vous pouvez dissocier et dimensionner indépendamment vos applications productrices et consommatrices de données.

Kafka Connect est un élément important de la création et de l'exécution d'applications de streaming avec Apache Kafka. Kafka Connect fournit un moyen standardisé de transférer des données entre Kafka et des systèmes externes. Kafka Connect est hautement évolutif et peut gérer de gros volumes de données Kafka Connect fournit un ensemble puissant d'opérations d'API et d'outils pour configurer, déployer et surveiller les connecteurs qui déplacent les données entre les sujets Kafka et les systèmes externes. Vous pouvez utiliser ces outils pour personnaliser et étendre les fonctionnalités de Kafka Connect afin de répondre aux besoins spécifiques de votre application de streaming.

Vous pouvez rencontrer des difficultés lorsque vous exploitez des clusters Apache Kafka Connect de manière autonome ou lorsque vous essayez de migrer des applications Apache Kafka Connect open source vers. AWS Ces défis incluent le temps nécessaire à la configuration de l'infrastructure et au déploiement des applications, les obstacles techniques liés à la configuration de clusters Apache Kafka Connect autogérés et les frais administratifs opérationnels.

Pour relever ces défis, nous vous recommandons d'utiliser Amazon Managed Streaming for Apache Kafka Connect (Amazon MSK Connect) pour migrer vos applications open source Apache Kafka

Connect vers. AWS Amazon MSK Connect simplifie l'utilisation de Kafka Connect pour diffuser des données depuis et vers des clusters Apache Kafka et des systèmes externes, tels que des bases de données, des index de recherche et des systèmes de fichiers.

Voici certains des avantages de la migration vers Amazon MSK Connect :

- Élimination de la charge opérationnelle : Amazon MSK Connect allège la charge opérationnelle associée à l'application de correctifs, au provisionnement et à la mise à l'échelle des clusters Apache Kafka Connect. Amazon MSK Connect surveille en permanence l'état de vos clusters Connect et automatise les correctifs et les mises à niveau de version sans perturber vos charges de travail.
- Redémarrage automatique des tâches Connect : Amazon MSK Connect peut récupérer automatiquement les tâches ayant échoué afin de réduire les interruptions de production. Les échecs de tâches peuvent être provoqués par des erreurs temporaires, telles que le dépassement de la limite de connexion TCP pour Kafka ou le rééquilibrage des tâches lorsque de nouveaux collaborateurs rejoignent le groupe de consommateurs pour les connecteurs récepteurs.
- Mise à l'échelle horizontale et verticale automatique : Amazon MSK Connect permet à l'application du connecteur de s'adapter automatiquement pour prendre en charge des débits plus élevés. Amazon MSK Connect gère le dimensionnement pour vous. Il vous suffit de spécifier le nombre de travailleurs dans le groupe de mise à l'échelle automatique et les seuils d'utilisation. Vous pouvez utiliser le fonctionnement de l'`UpdateConnector`API Amazon MSK Connect pour augmenter ou diminuer verticalement les vCPU entre 1 et 8 vCPU afin de prendre en charge un débit variable.
- Connectivité réseau privée — Amazon MSK Connect se connecte de manière privée aux systèmes source et récepteur en utilisant AWS PrivateLink des noms DNS privés.

Migration vers Amazon MSK Connect

Cette section décrit brièvement les rubriques relatives à la gestion des états utilisées par Kafka Connect et Amazon MSK Connect. Cette section couvre également les procédures de migration des connecteurs source et récepteur.

Rubriques

- Sujets internes utilisés par Kafka Connect
- Gestion de l'état des applications Amazon MSK Connect
- Migration des connecteurs source vers Amazon MSK Connect
- Migration des connecteurs récepteurs vers Amazon MSK Connect

Sujets internes utilisés par Kafka Connect

Une application Apache Kafka Connect qui s'exécute en mode distribué mémorise son état en utilisant des rubriques internes du cluster Kafka et l'appartenance à un groupe. Les valeurs de configuration suivantes correspondent aux rubriques internes utilisées pour les applications Kafka Connect :

- Rubrique de configuration, spécifiée par `config.storage.topic`

  Dans la rubrique consacrée à la configuration, Kafka Connect enregistre la configuration de tous les connecteurs et tâches lancés par les utilisateurs. Chaque fois que les utilisateurs mettent à jour la configuration d'un connecteur ou lorsqu'un connecteur demande une reconfiguration (par exemple, le connecteur détecte qu'il peut démarrer d'autres tâches), un enregistrement est envoyé à cette rubrique. Cette rubrique est activée pour le compactage, elle conserve donc toujours le dernier état de chaque entité.

- Rubrique sur les décalages, spécifiée par `offset.storage.topic`

  Dans la rubrique sur les décalages, Kafka Connect enregistre les décalages des connecteurs source. Tout comme le sujet de configuration, le sujet des décalages est activé pour le compactage. Cette rubrique est utilisée pour écrire les positions des sources uniquement pour les connecteurs sources qui produisent des données destinées à Kafka à partir de systèmes externes. Les connecteurs Sink, qui lisent les données de Kafka et les envoient à des systèmes externes, stockent leurs offsets en utilisant les groupes de consommateurs Kafka habituels.

- Sujet de statut, spécifié par `status.storage.topic`

  Dans la rubrique consacrée à l'état, Kafka Connect enregistre l'état actuel des connecteurs et des tâches. Cette rubrique est utilisée comme emplacement central pour les données demandées par les utilisateurs de l'API REST. Cette rubrique permet aux utilisateurs d'interroger n'importe quel worker tout en obtenant l'état de tous les plugins en cours d'exécution. Tout comme les rubriques relatives à la configuration et aux décalages, la rubrique d'état est également activée pour le compactage.

Outre ces sujets, Kafka Connect utilise largement l'API d'adhésion aux groupes de Kafka. Les groupes sont nommés d'après le nom du connecteur. Par exemple, pour un connecteur nommé file-sink, le groupe est nommé. connect-file-sink Chaque consommateur du groupe fournit des enregistrements pour une seule tâche. Ces groupes et leurs compensations peuvent être récupérés à l'aide d'outils classiques de groupes de consommateurs, tels que`Kafka-consumer-`

`group.sh`. Pour chaque connecteur récepteur, le moteur d'exécution Connect exécute un groupe de consommateurs normal qui extrait les enregistrements de Kafka.

Gestion de l'état des applications Amazon MSK Connect

Par défaut, Amazon MSK Connect crée trois rubriques distinctes dans le cluster Kafka pour chaque connecteur Amazon MSK afin de stocker la configuration, le décalage et l'état du connecteur. Les noms des rubriques par défaut sont structurés comme suit :

- *__msk_connect_configs_ nom du connecteur _ identifiant du connecteur*
- *__msk_connect_status_ nom du connecteur _ identifiant du connecteur*
- *__msk_connect_offsets_ nom du connecteur _ identifiant du connecteur*

> **Note**
>
> Pour assurer la continuité du décalage entre les connecteurs source, vous pouvez utiliser une rubrique de stockage de décalage de votre choix au lieu de la rubrique par défaut. La spécification d'une rubrique de stockage des décalages vous aide à accomplir des tâches telles que la création d'un connecteur source qui reprend la lecture à partir du dernier décalage d'un connecteur précédent. Pour spécifier un sujet de stockage offset, entrez une valeur pour la offset.storage.topicpropriété dans la configuration du worker Amazon MSK Connect avant de créer le connecteur.

Migration des connecteurs source vers Amazon MSK Connect

Les connecteurs source sont des applications Apache Kafka Connect qui importent des enregistrements depuis des systèmes externes dans Kafka. Cette section décrit le processus de migration des applications du connecteur source Apache Kafka Connect qui exécutent des clusters Kafka Connect sur site ou des clusters Kafka Connect autogérés qui s'exécutent sur AWS Amazon MSK Connect.

L'application du connecteur source Kafka Connect stocke les décalages dans une rubrique nommée avec la valeur définie pour la propriété de configuration. `offset.storage.topic` Voici des exemples de messages de décalage pour un connecteur JDBC exécutant deux tâches qui importent des données à partir de deux tables différentes nommées `movies` et. `shows` La dernière ligne importée depuis le tableau des films possède un identifiant principal de`18343`. La dernière ligne importée depuis le tableau des shows possède un ID principal de`732`.

```
["jdbcsource",{"protocol":"1","table":"sample.movies"}] {"incrementing":18343}
["jdbcsource",{"protocol":"1","table":"sample.shows"}] {"incrementing":732}
```

Pour migrer les connecteurs source vers Amazon MSK Connect, procédez comme suit :

1. Créez un plugin personnalisé Amazon MSK Connect en extrayant les bibliothèques de connecteurs de votre cluster Kafka Connect sur site ou autogéré.
2. Créez les propriétés du worker Amazon MSK Connect et définissez les propriétés `key.converter`, `value.converter`, avec les mêmes valeurs que celles définies pour le connecteur Kafka qui s'exécute dans votre cluster Kafka Connect existant. `offset.storage.topic`
3. Suspendez l'application du connecteur sur le cluster existant en effectuant une `PUT /connectors/`*`connector-name`*`/pause` demande sur le cluster Kafka Connect existant.
4. Assurez-vous que toutes les tâches de l'application du connecteur sont complètement arrêtées. Vous pouvez arrêter les tâches soit en faisant une `GET /connectors/`*`connector-name`*`/status` demande sur le cluster Kafka Connect existant, soit en consommant les messages du nom de rubrique défini pour la propriété`status.storage.topic`.
5. Obtenez la configuration du connecteur à partir du cluster existant. Vous pouvez obtenir la configuration du connecteur soit en faisant une `GET /connectors/`*`connector-name`*`/config/` demande sur le cluster existant, soit en consommant les messages du nom de rubrique défini pour la propriété`config.storage.topic`.
6. Créez un nouveau connecteur Amazon MSK portant le même nom qu'un cluster existant. Créez ce connecteur à l'aide du plug-in personnalisé que vous avez créé à l'étape 1, des propriétés de travail que vous avez créées à l'étape 2 et de la configuration du connecteur que vous avez extraite à l'étape 5.
7. Lorsque le statut du connecteur Amazon MSK est défini`active`, consultez les journaux pour vérifier que le connecteur a commencé à importer des données depuis le système source.
8. Supprimez le connecteur du cluster existant en effectuant une `DELETE /connectors/`*`connector-name`* demande.

Migration des connecteurs récepteurs vers Amazon MSK Connect

Les connecteurs Sink sont des applications Apache Kafka Connect qui exportent des données de Kafka vers des systèmes externes. Cette section décrit le processus de migration des applications du

connecteur récepteur Apache Kafka Connect qui exécutent des clusters Kafka Connect sur site ou des clusters Kafka Connect autogérés qui s'exécutent sur AWS Amazon MSK Connect.

Les connecteurs de réception Kafka Connect utilisent l'API d'adhésion au groupe Kafka et stockent les offsets dans les mêmes `__consumer_offset` rubriques qu'une application grand public classique. Ce comportement simplifie la migration du connecteur récepteur d'un cluster autogéré vers Amazon MSK Connect.

Pour migrer les connecteurs récepteurs vers Amazon MSK Connect, procédez comme suit :

1. Créez un plugin personnalisé Amazon MSK Connect en extrayant les bibliothèques de connecteurs de votre cluster Kafka Connect sur site ou autogéré.
2. Créez les propriétés du worker Amazon MSK Connect et définissez les propriétés `key.converter` et `value.converter` les mêmes valeurs que celles définies pour le connecteur Kafka qui s'exécute dans votre cluster Kafka Connect existant.
3. Suspendez l'application du connecteur sur votre cluster existant en effectuant une `PUT /connectors/`*`connector-name`*`/pause` demande sur le cluster Kafka Connect existant.
4. Assurez-vous que toutes les tâches de l'application du connecteur sont complètement arrêtées. Vous pouvez arrêter les tâches soit en faisant une `GET /connectors/`*`connector-name`*`/status` demande sur le cluster Kafka Connect existant, soit en consommant les messages du nom de rubrique défini pour la propriété`status.storage.topic`.
5. Obtenez la configuration du connecteur à partir du cluster existant. Vous pouvez obtenir la configuration du connecteur soit en faisant une `GET /connectors/`*`connector-name`*`/config` demande sur le cluster existant, soit en consommant les messages du nom de rubrique défini pour la propriété`config.storage.topic`.
6. Créez un nouveau connecteur Amazon MSK portant le même nom que le cluster existant. Créez ce connecteur à l'aide du plug-in personnalisé que vous avez créé à l'étape 1, des propriétés de travail que vous avez créées à l'étape 2 et de la configuration du connecteur que vous avez extraite à l'étape 5.
7. Lorsque le statut du connecteur Amazon MSK est défini`active`, consultez les journaux pour vérifier que le connecteur a commencé à importer des données depuis le système source.
8. Supprimez le connecteur du cluster existant en effectuant une `DELETE /connectors/`*`connector-name`* demande.

Résolution des problèmes liés à Amazon MSK Connect

La documentation suivante peut vous aider à résoudre les problèmes que vous pouvez rencontrer lors de l'utilisation de MSK Connect. Vous pouvez également publier votre problème sur AWS re:Post.

Le connecteur ne parvient pas à accéder aux ressources hébergées sur l'Internet public

Consultez Activation de l'accès à Internet pour Amazon MSK Connect.

Le nombre de tâches en cours d'exécution du connecteur n'est pas égal au nombre de tâches spécifié dans tasks.max

Voici quelques raisons pour lesquelles un connecteur peut utiliser moins de tâches que la configuration tasks.max spécifiée :

- Certaines implémentations de connecteurs limitent le nombre de tâches pouvant être utilisées. Par exemple, le connecteur Debezium pour MySQL est limité à l'utilisation d'une seule tâche.
- Lorsque vous utilisez le mode de capacité mise à l'échelle automatiquement, Amazon MSK Connect remplace la propriété tasks.max d'un connecteur par une valeur proportionnelle au nombre de workers exécutant le connecteur et au nombre de MCU par worker.
- Pour les connecteurs récepteurs, le niveau de parallélisme (nombre de tâches) ne peut pas être supérieur au nombre de partitions de rubrique. Bien que vous puissiez définir une valeur supérieure à tasks.max, une seule partition n'est jamais traitée par plus d'une tâche à la fois.
- Dans Kafka Connect 2.7.x, l'assignateur de partition client par défaut est `RangeAssignor`. Le comportement de cet assignateur consiste à donner la première partition de chaque rubrique à un seul consommateur, la deuxième partition de chaque rubrique à un seul consommateur, etc. Cela signifie que le nombre maximum de tâches actives utilisées par un connecteur récepteur `RangeAssignor` est égal au nombre maximal de partitions utilisées dans un même sujet. Si cela ne fonctionne pas pour votre cas d'utilisation, vous devez créer une configuration de worker dans laquelle la propriété `consumer.partition.assignment.strategy` est définie sur un assignateur de partition consommateur plus approprié. Voir Interface Kafka 2.7 ConsumerPartitionAssignor : toutes les classes d'implémentation connues.

Réplicateur MSK

Qu'est-ce que le réplicateur Amazon MSK ?

Amazon MSK Replicator est une fonctionnalité Amazon MSK qui vous permet de répliquer de manière fiable des données entre des clusters Amazon MSK situés dans des régions différentes ou identiques AWS . Le réplicateur MSK vous permet de créer facilement des applications de streaming résilientes au niveau régional pour une disponibilité et une continuité des activités accrues. Le réplicateur MSK fournit une réplication asynchrone automatique sur les clusters MSK, éliminant ainsi le besoin d'écrire du code personnalisé, de gérer l'infrastructure ou de configurer un réseau entre régions.

Le réplicateur MSK adapte automatiquement les ressources sous-jacentes afin que vous puissiez répliquer les données à la demande sans avoir à surveiller ou à mettre à l'échelle la capacité.
Le réplicateur MSK reproduit également les métadonnées Kafka nécessaires, notamment les configurations de rubriques, les listes de contrôle d'accès (ACL) et les décalages de groupes de consommateurs. Si un événement inattendu se produit dans une région, vous pouvez basculer vers l'autre AWS région et reprendre le traitement en toute simplicité.

Le réplicateur MSK prend en charge à la fois la réplication entre régions (CRR) et la réplication dans une même région (SRR). Lors de la réplication entre régions, les clusters MSK source et cible se trouvent dans des régions différentes AWS . Dans la réplication dans la même région, les clusters MSK source et cible se trouvent dans la même région. AWS Vous devez créer des clusters MSK source et cible avant de les utiliser avec le réplicateur MSK.

> **Note**
>
> MSK Replicator prend en charge les AWS régions suivantes : USA Est (us-east-1, Virginie du Nord) ; USA Est (us-east-2, Ohio) ; USA Ouest (us-west-2, Oregon) ; Europe (eu-west-1, Irlande) ; Europe (eu-central-1, Francfort) ; Asie-Pacifique (ap-southeast-1) Asie-Pacifique (ap-southeast-2, Singapour) ; Asie-Pacifique (ap-southeast-2, Sydney), Europe (eu-north-1, Stockholm), Asie-Pacifique (ap-south-1, Mumbai), Europe (eu-west-3, Paris), Amérique du Sud (sa-east-1, São Paulo), Asie-Pacifique (ap-northeast-1) ap-northeast-2, Séoul), Europe (eu-west-2, Londres), Asie-Pacifique (ap-northeast-1, Tokyo), ouest des États-Unis (us-west-1, Californie du Nord), Canada (ca-central-1, Central).

Voici quelques utilisations courantes du réplicateur Amazon MSK.

- Création d'applications de streaming multirégionales : créez des applications de streaming hautement disponibles et tolérantes aux pannes pour une résilience accrue sans avoir à configurer de solutions personnalisées.
- Accès aux données à faible latence : offrez un accès aux données à faible latence aux consommateurs de différentes régions géographiques.
- Distribution de données à vos partenaires : copiez les données d'un cluster Apache Kafka vers plusieurs clusters Apache Kafka, afin que les différentes équipes/partenaires disposent de leurs propres copies des données.
- Agrégation des données à des fins d'analyse : copiez les données de plusieurs clusters Apache Kafka dans un seul cluster pour générer facilement des informations sur des données agrégées en temps réel.
- Écrivez localement, accédez à vos données dans le monde entier : configurez la réplication multiactive pour propager automatiquement les écritures effectuées dans une AWS région vers d'autres régions afin de fournir des données à moindre latence et à moindre coût.

Fonctionnement du réplicateur Amazon MSK

Pour commencer à utiliser MSK Replicator, vous devez créer un nouveau réplicateur dans la région de votre cluster cible. AWS MSK Replicator copie automatiquement toutes les données du cluster de la AWS région principale appelée source vers le cluster de la région de destination appelée cible. Les clusters source et cible peuvent se trouver dans la même région ou dans des AWS régions différentes. Vous devez créer le cluster cible s'il n'existe pas déjà.

Lorsque vous créez un réplicateur, MSK Replicator déploie toutes les ressources requises dans la AWS région du cluster cible afin d'optimiser la latence de réplication des données. La latence de réplication varie en fonction de nombreux facteurs, notamment la distance réseau entre AWS les régions de vos clusters MSK, la capacité de débit de vos clusters source et cible, et le nombre de partitions sur vos clusters source et cible. Le réplicateur MSK met automatiquement à l'échelle les ressources sous-jacentes afin que vous puissiez répliquer les données à la demande sans avoir à surveiller ou à mettre à l'échelle la capacité.

Réplication des données

Par défaut, MSK Replicator copie toutes les données de manière asynchrone depuis le dernier décalage des partitions thématiques du cluster source vers le cluster cible. Si le paramètre « Détecter

et copier les nouveaux sujets » est activé, MSK Replicator détecte et copie automatiquement les nouveaux sujets ou partitions de sujets dans le cluster cible. Cependant, le réplicateur peut prendre jusqu'à 30 secondes pour détecter et créer les nouveaux sujets ou partitions de sujets sur le cluster cible. Les messages envoyés au sujet source avant sa création sur le cluster cible ne seront pas répliqués. Vous pouvez également configurer votre réplicateur lors de la création pour démarrer la réplication à partir du premier décalage dans les partitions des rubriques du cluster source si vous souhaitez répliquer les messages existants sur vos sujets vers le cluster cible.

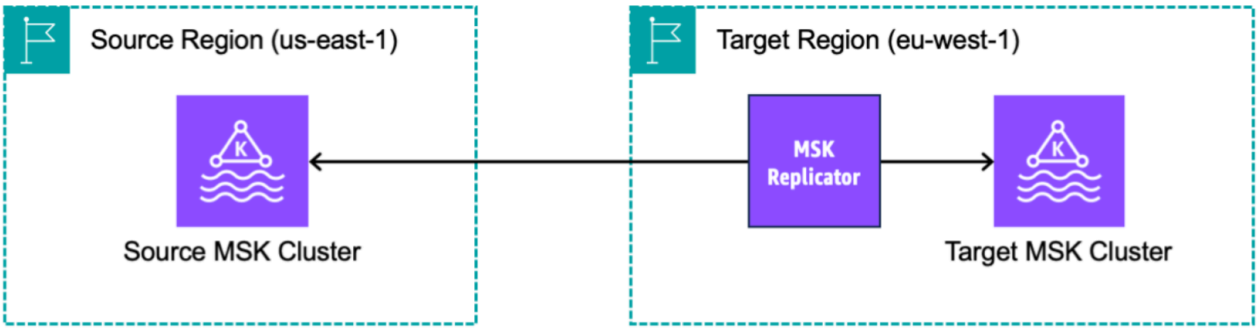
MSK Replicator ne stocke pas vos données. Les données sont consommées à partir de votre cluster source, mises en mémoire tampon et écrites dans le cluster cible. La mémoire tampon est automatiquement effacée lorsque les données sont écrites avec succès ou échouent après de nouvelles tentatives. Toutes les communications et les données entre MSK Replicator et vos clusters sont toujours chiffrées en transit. Tous les appels d'API MSK Replicator tels que`DescribeClusterV2`,`CreateTopic`, `DescribeTopicDynamicConfiguration` sont capturés dans. AWS CloudTrail Les journaux de votre courtier MSK refléteront également la même chose.

MSK Replicator crée des sujets dans le cluster cible avec un facteur de réplication de 3. Si nécessaire, vous pouvez modifier le facteur de réplication directement sur le cluster cible.

Réplication des métadonnées

MSK Replicator prend également en charge la copie des métadonnées du cluster source vers le cluster cible. Les métadonnées incluent la configuration des rubriques, les listes de contrôle d'accès (ACL) en lecture et les décalages des groupes de consommateurs. Tout comme la réplication des données, la réplication des métadonnées s'effectue également de manière asynchrone. Pour de meilleures performances, MSK Replicator donne la priorité à la réplication des données plutôt qu'à la réplication des métadonnées.

Dans le cadre de la synchronisation des offsets des groupes de consommateurs, MSK Replicator est optimisé pour les clients du cluster source qui lisent à une position plus proche de la pointe du flux (fin de la partition thématique). Si vos groupes de consommateurs sont en retard sur le cluster source, vous constaterez peut-être un retard plus important pour ces groupes de consommateurs sur le cluster cible par rapport à la source. Cela signifie qu'après le basculement vers le cluster cible, vos clients retraiteront un plus grand nombre de messages dupliqués. Pour réduire ce décalage, vos clients du cluster source devraient rattraper leur retard et commencer à consommer dès le début du stream (fin de la partition thématique). Au fur et à mesure que vos clients rattrapent leur retard, MSK Replicator réduira automatiquement le décalage.



Exigences et considérations relatives à la création d'un réplicateur Amazon MSK

Notez ces exigences relatives au cluster MSK pour exécuter un réplicateur Amazon MSK.

Rubriques

- Autorisations requises pour créer un réplicateur MSK
- Types et versions de clusters pris en charge
- Configuration du cluster MSK sans serveur
- Modifications dans la configurations des clusters

Autorisations requises pour créer un réplicateur MSK

Voici un exemple de la politique IAM requise pour créer un réplicateur MSK. L'action `kafka:TagResource` n'est nécessaire que si des balises sont fournies lors de la création du réplicateur MSK.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:PassRole",
                "iam:CreateServiceLinkedRole",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeVpcs",
                "kafka:CreateReplicator",
                "kafka:TagResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Voici un exemple de politique IAM pour décrire le réplicateur. L'action `kafka:DescribeReplicator` ou l'action `kafka:ListTagsForResource` est nécessaire, pas les deux.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "kafka:DescribeReplicator",
                "kafka:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Types et versions de clusters pris en charge

Il s'agit des exigences relatives aux types d'instances pris en charge, aux versions de Kafka et aux configurations réseau.

- Le réplicateur MSK prend en charge à la fois les clusters provisionnés MSK et les clusters MSK sans serveur dans n'importe quelle combinaison en tant que clusters source et cible. Les autres types de clusters Kafka ne sont pas pris en charge pour le moment par le réplicateur MSK.

- Les clusters MSK sans serveur nécessitent un contrôle d'accès IAM, ne prennent pas en charge la réplication ACL d'Apache Kafka et, avec une prise en charge limitée, la réplication de configuration sur site. veuillez consulter MSK sans serveur.
- MSK Replicator n'est pris en charge que sur les clusters exécutant Apache Kafka 2.7.0 ou une version ultérieure, que vos clusters source et cible se trouvent dans la même région ou dans des régions différentes. AWS
- Le réplicateur MSK prend en charge les clusters utilisant des types d'instance de type m5.large ou supérieur. Les clusters t3.small ne sont pas pris en charge.
- Si vous utilisez le réplicateur MSK avec un cluster MSK provisionné, vous avez besoin d'un minimum de trois agents dans les clusters source et cible. Vous pouvez répliquer les données entre des clusters situés dans deux zones de disponibilité, mais vous aurez besoin d'un minimum de quatre agents dans ces clusters.
- Vos clusters MSK source et cible doivent se trouver dans le même AWS compte. La réplication entre clusters appartenant à différents comptes n'est pas prise en charge.
- Si les clusters MSK source et cible se trouvent dans des AWS régions différentes (entre régions), MSK Replicator exige que la connectivité privée multi-VPC du cluster source soit activée pour sa méthode de contrôle d'accès IAM. La connectivité multi-VPC n'est pas requise pour les autres méthodes d'authentification sur le cluster source. Le multi-VPC n'est pas nécessaire si vous répliquez des données entre des clusters d'une même région. AWS veuillez consulter the section called “Connectivité privée à plusieurs VPC dans une seule région”.

Configuration du cluster MSK sans serveur

- MSK sans serveur prend en charge la réplication de ces configurations de rubriques pour les clusters cibles MSK sans serveur lors de la création de rubriques : `cleanup.policy`, `compression.type`, `max.message.bytes`, `retention.bytes`, `retention.ms`.
- MSK sans serveur prend uniquement en charge les configurations de rubriques suivantes lors de la synchronisation des configurations de rubriques : `compression.type`, `max.message.bytes`, `retention.bytes`, `retention.ms`.
- Le réplicateur utilise 83 partitions compactées sur les clusters MSK sans serveur cibles. Assurez-vous que les clusters MSK sans serveur cibles disposent d'un nombre suffisant de partitions compactées. veuillez consulter Quota de MSK sans serveur.

Modifications dans la configurations des clusters

- Il est recommandé de ne pas activer ou désactiver le stockage hiérarchisé après la création du réplicateur MSK. Si votre cluster cible n'est pas hiérarchisé, MSK ne copiera pas les configurations de stockage hiérarchisé, que votre cluster source soit hiérarchisé ou non. Si vous activez le stockage hiérarchisé sur le cluster cible après la création du réplicateur, celui-ci doit être recréé. Si vous souhaitez copier des données d'un cluster non hiérarchisé vers un cluster hiérarchisé, vous ne devez pas copier les configurations des rubriques. Consultez la section Activation et désactivation du stockage hiérarchisé sur une rubrique existante.
- Ne modifiez pas les paramètres de configuration du cluster après la création du réplicateur MSK. Les paramètres de configuration du cluster sont validés lors de la création du réplicateur MSK. Pour éviter tout problème avec le réplicateur MSK, ne modifiez pas les paramètres suivants une fois le réplicateur MSK créé.
  - Changez le cluster MSK en type d'instance t3.
  - Modifiez les autorisations de rôle d'exécution de service.
  - Désactivez la connectivité privée MSK multi-VPC.
  - Modifiez la politique basée sur les ressources du cluster attachée.
  - Modifiez les règles de groupe de sécurité du cluster.

Mise en route avec le réplicateur Amazon MSK

Ce didacticiel explique comment configurer un cluster source et un cluster cible dans la même AWS région ou dans différentes AWS régions. Ensuite, vous utilisez ces clusters pour créer un réplicateur Amazon MSK.

Étape 1 : Préparer le cluster source Amazon MSK

Si vous avez déjà créé un cluster source MSK pour le réplicateur MSK, assurez-vous qu'il répond aux exigences décrites dans cette section. Dans le cas contraire, suivez ces étapes pour créer un cluster source provisionné par MSK ou sans serveur.

Le processus de création d'un cluster source de réplicateur MSK entre régions et mêmes régions est similaire. Les différences sont mises en évidence dans les procédures suivantes.

1. Créez un cluster MSK provisionné ou sans serveur avec le contrôle d'accès IAM activé dans la région source. Votre cluster source doit avoir au moins trois agents.

2. Pour un réplicateur MSK entre régions, si la source est un cluster provisionné, configurez-le avec la connectivité privée multi-VPC activée pour les schémas de contrôle d'accès IAM. Notez que le type d'authentification non authentifié n'est pas pris en charge lorsque la connectivité multi-VPC est activée. Il n'est pas nécessaire d'activer la connectivité privée multi-VPC pour les autres schémas d'authentification (mTLS ou SASL/SCRAM). Vous pouvez utiliser simultanément des schémas d'authentification mTLS ou SASL/SCRAM pour vos autres clients qui se connectent à votre cluster MSK. Vous pouvez configurer la connectivité privée multi-VPC dans les détails du cluster de consoles, dans les paramètres réseau ou avec l'API `UpdateConnectivity`. Voir Le propriétaire du cluster active le multi-VPC. Si votre cluster source est un cluster MSK sans serveur, vous n'avez pas besoin d'activer la connectivité privée multi-VPC.

   Pour un réplicateur MSK de même région, le cluster source MSK ne nécessite pas de connectivité privée multi-VPC et les autres clients peuvent toujours accéder au cluster en utilisant le type d'authentification non authentifié.

3. Pour les réplicateurs MSK entre régions, vous devez attacher une politique d'autorisations basée sur les ressources au cluster source. Cela permet à MSK de se connecter à ce cluster pour répliquer les données. Vous pouvez le faire à l'aide de la CLI ou des procédures de AWS console ci-dessous. Consultez également les politiques basées sur les ressources d'Amazon MSK. Vous n'avez pas besoin d'effectuer cette étape pour les réplicateurs MSK de la même région.

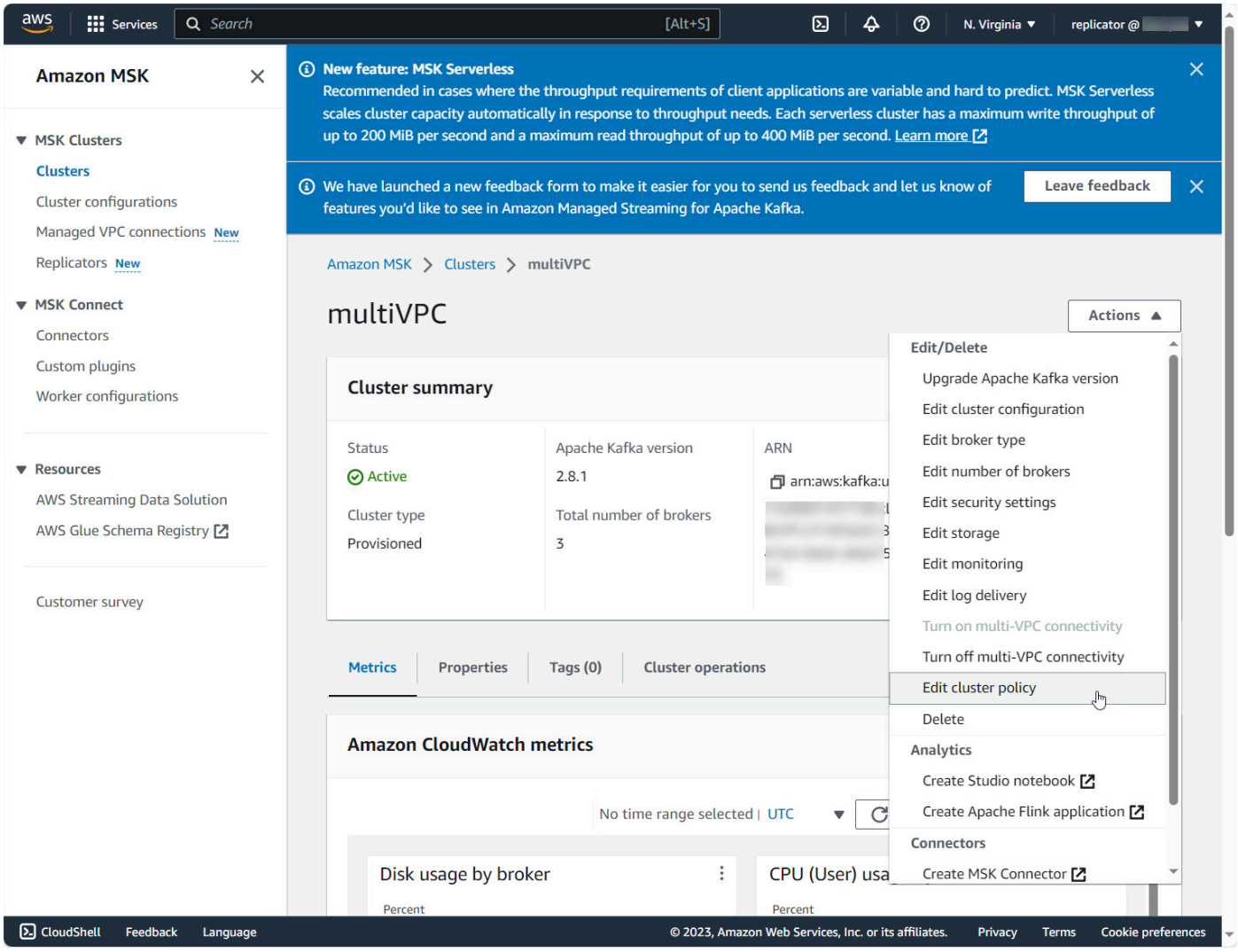
Console: create resource policy

Mettez à jour la politique du cluster source avec le code JSON suivant. Remplacez l'espace réservé par l'ARN de votre cluster source.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "Service": [
                "kafka.amazonaws.com"
            ]
        },
        "Action": [
            "kafka:CreateVpcConnection",
            "kafka:GetBootstrapBrokers",
            "kafka:DescribeClusterV2"
```

```
        ],
        "Resource": "<sourceClusterARN>"
    }
  ]
}
```

Utilisez l'option Modifier la politique du cluster dans le menu Actions de la page des détails du cluster.



CLI: create resource policy

Remarque : Si vous utilisez la AWS console pour créer un cluster source et que vous choisissez l'option permettant de créer un nouveau rôle IAM, vous AWS associez la politique de confiance requise au rôle. Si vous souhaitez que MSK utilise un rôle IAM existant ou si vous créez un rôle par vous-même, attachez les politiques d'approbation suivantes à ce rôle afin que le réplicateur

MSK puisse l'assumer. Pour de plus amples informations sur la modification de la relation d'approbation d'un rôle, veuillez consulter Modification d'un rôle.

1. Obtenez la version actuelle de la politique de cluster MSK à l'aide de cette commande. Remplacez les espaces réservés par l'ARN du cluster réel.

```
aws kafka get-cluster-policy –cluster-arn <Cluster ARN>
{
"CurrentVersion": "K1PA6795UKM GR7",
"Policy": "..."
}
```

2. Créez une politique basée sur les ressources pour autoriser le réplicateur MSK à accéder à votre cluster source. Utilisez la syntaxe suivante comme modèle, en remplaçant l'espace réservé par l'ARN du cluster source réel.

```
aws kafka put-cluster-policy --cluster-arn "<sourceClusterARN>" --policy '{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": [
"kafka.amazonaws.com"
]
},
"Action": [
"kafka:CreateVpcConnection",
"kafka:GetBootstrapBrokers",
"kafka:DescribeClusterV2"
],
"Resource": "<sourceClusterARN>"
}
]
```

Étape 2 : Préparer le cluster cible Amazon MSK

Créez un cluster cible MSK (provisionné ou sans serveur) avec le contrôle d'accès IAM activé. Le cluster cible ne nécessite pas l'activation de la connectivité privée multi-VPC. Le cluster cible peut se trouver dans la même AWS région ou dans une région différente de celle du cluster source. Les

clusters source et cible doivent se trouver dans le même AWS compte. Votre cluster cible doit avoir au moins trois agents.

Étape 3 : Créer un réplicateur Amazon MSK

Avant de créer le réplicateur Amazon MSK, assurez-vous que vous avez. Autorisations requises pour créer un réplicateur MSK

Rubriques

- Créez un réplicateur à l'aide de la console AWS dans la région du cluster cible
- Choisissez votre cluster source
- Choisissez votre cluster cible
- Configurez les paramètres et les autorisations du réplicateur

Créez un réplicateur à l'aide de la console AWS dans la région du cluster cible

1. Dans la AWS région où se trouve votre cluster MSK cible, ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Choisissez Réplicateurs pour afficher la liste des réplicateurs du compte.
3. Choisissez Créer un réplicateur.
4. Dans le volet Détails du réplicateur, attribuez un nom unique au nouveau réplicateur.

Choisissez votre cluster source

Le cluster source contient les données que vous souhaitez copier vers un cluster MSK cible.

1. Dans le volet Cluster source, choisissez la région AWS dans laquelle se trouve le cluster source.

   Vous pouvez rechercher la région d'un cluster en accédant à Clusters MSK et en consultant l'ARN des détails du cluster. Le nom de la région est intégré dans la chaîne ARN. Dans l'exemple d'ARN suivant, le cluster se trouve dans la région `ap-southeast-2`.

   ```
   arn:aws:kafka:ap-southeast-2:123456789012:cluster/cluster-11/
   eec93c7f-4e8b-4baf-89fb-95de01ee639c-s1
   ```

2. Entrez l'ARN de votre cluster source ou naviguez pour choisir votre cluster source.
3. Choisissez un ou plusieurs sous-réseaux pour votre cluster source.

La console affiche les sous-réseaux disponibles dans la région du cluster source que vous pouvez sélectionner. Vous devez sélectionner au moins deux sous-réseaux. Pour un réplicateur MSK de même région, les sous-réseaux que vous sélectionnez définis pour accéder au cluster source et les sous-réseaux pour accéder au cluster cible doivent se trouver dans la même zone de disponibilité.

4. Choisissez un ou plusieurs groupes de sécurité pour que le réplicateur MSK accède à votre cluster source.

   - Pour la réplication entre régions (CRR), il n'est pas nécessaire de fournir un ou plusieurs groupes de sécurité pour votre cluster source.
   - Pour la réplication dans la même région (SRR), accédez à la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/ et assurez-vous que les groupes de sécurité que vous fournirez au réplicateur disposent de règles de sortie autorisant le trafic vers les groupes de sécurité de votre cluster source. Assurez-vous également que les groupes de sécurité de votre cluster source disposent de règles entrantes qui autorisent le trafic provenant des groupes de sécurité Replicator fournis pour la source.

     Pour ajouter des règles de trafic entrant au groupe de sécurité de votre cluster source :

     1. Dans la AWS console, accédez aux détails de votre cluster source en sélectionnant le nom du cluster.
     2. Sélectionnez l'onglet Propriétés, puis faites défiler l'écran jusqu'au volet des paramètres réseau pour sélectionner le nom du groupe de sécurité appliqué.
     3. Accédez aux règles entrantes et sélectionnez Modifier les règles entrantes.
     4. Sélectionnez Ajouter une règle.
     5. Dans la colonne Type de la nouvelle règle, sélectionnez TCP personnalisé.
     6. Dans la colonne Plage de ports, tapez`9098`. MSK Replicator utilise le contrôle d'accès IAM pour se connecter à votre cluster qui utilise le port 9098.
     7. Dans la colonne Source, tapez le nom du groupe de sécurité que vous fournirez lors de la création du réplicateur pour le cluster source (il peut être identique au groupe de sécurité du cluster source MSK), puis sélectionnez Enregistrer les règles.

Pour ajouter des règles de sortie au groupe de sécurité de Replicator fourni pour la source :

1. Dans la AWS console pour Amazon EC2, accédez au groupe de sécurité que vous fournirez lors de la création du réplicateur pour la source.
2. Accédez aux règles sortantes et sélectionnez Modifier les règles sortantes.
3. Sélectionnez Ajouter une règle.
4. Dans la colonne Type de la nouvelle règle, sélectionnez TCP personnalisé.
5. Dans la colonne Plage de ports, tapez`9098`. MSK Replicator utilise le contrôle d'accès IAM pour se connecter à votre cluster qui utilise le port 9098.
6. Dans la colonne Source, tapez le nom du groupe de sécurité du cluster source MSK, puis sélectionnez Enregistrer les règles.

> **Note**
>
> Si vous ne souhaitez pas restreindre le trafic à l'aide de vos groupes de sécurité, vous pouvez également ajouter des règles entrantes et sortantes autorisant tout le trafic.
> 1. Sélectionnez Ajouter une règle.
> 2. Dans la colonne Type, choisissez Tout le trafic.
> 3. Dans la colonne Source, tapez `0.0.0.0/0`, puis sélectionnez Enregistrer les règles.

Choisissez votre cluster cible

Le cluster cible est le cluster approvisionné par MSK ou le cluster sans serveur vers lequel les données sources sont copiées.

> **Note**
>
> Le réplicateur MSK crée de nouvelles rubriques dans le cluster cible avec un préfixe généré automatiquement ajouté au nom de la rubrique. Par exemple, le réplicateur MSK réplique les données dans « `topic` » du cluster source vers une nouvelle rubrique du cluster cible appelée `<sourceKafkaClusterAlias>.topic`. Cela permet de distinguer les rubriques contenant des données répliquées à partir du cluster source des autres rubriques du cluster cible et d'éviter que les données ne soient répliquées de manière circulaire entre les clusters. Vous trouverez le préfixe qui sera ajouté aux noms des rubriques dans le cluster cible dans le champ sourceKafkaClusterAlias à l'aide de l'`DescribeReplicator`API ou dans la page de

détails du réplicateur sur la console MSK. Le préfixe du cluster cible est < sourceKafkaCluster Alias>.

1. Dans le volet Cluster cible, choisissez la AWS région dans laquelle se trouve le cluster cible.
2. Entrez l'ARN de votre cluster cible ou naviguez pour choisir votre cluster cible.
3. Choisissez un ou plusieurs sous-réseaux pour votre cluster cible.

   La console affiche les sous-réseaux disponibles dans la région du cluster cible que vous pouvez sélectionner. Sélectionnez au moins deux sous-réseaux.
4. Choisissez un ou plusieurs groupes de sécurité pour que le réplicateur MSK accède à votre cluster cible.

   Les groupes de sécurité disponibles dans la région du cluster cible sont affichés pour que vous puissiez les sélectionner. Le groupe de sécurité choisi est associé à chaque connexion. Pour plus d'informations sur l'utilisation des groupes de sécurité, consultez la section Contrôlez le trafic vers vos AWS ressources à l'aide de groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

   - Pour la réplication entre régions (CRR) et pour la réplication entre régions (SRR), accédez à la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/ et assurez-vous que les groupes de sécurité que vous fournirez au réplicateur disposent de règles de sortie autorisant le trafic vers les groupes de sécurité de votre cluster cible. Veillez également à ce que les groupes de sécurité de votre cluster cible disposent de règles entrantes qui autorisent le trafic vers les groupes de sécurité du réplicateur fournis pour la cible.

     Pour ajouter des règles de trafic entrant au groupe de sécurité de votre cluster cible :

     1. Dans la AWS console, accédez aux détails de votre cluster cible en sélectionnant le nom du cluster.
     2. Sélectionnez l'onglet Propriétés, puis faites défiler l'écran jusqu'au volet des paramètres réseau pour sélectionner le nom du groupe de sécurité appliqué.
     3. Accédez aux règles entrantes et sélectionnez Modifier les règles entrantes.
     4. Sélectionnez Ajouter une règle.
     5. Dans la colonne Type de la nouvelle règle, sélectionnez TCP personnalisé.

6. Dans la colonne Plage de ports, tapez`9098`. MSK Replicator utilise le contrôle d'accès IAM pour se connecter à votre cluster qui utilise le port 9098.
7. Dans la colonne Source, tapez le nom du groupe de sécurité que vous fournirez lors de la création du réplicateur pour le cluster cible (il peut être identique au groupe de sécurité du cluster cible MSK), puis sélectionnez Enregistrer les règles.

Pour ajouter des règles de sortie au groupe de sécurité de Replicator fourni à la cible :

1. Dans la AWS console, accédez au groupe de sécurité que vous allez fournir lors de la création du réplicateur pour la cible.
2. Sélectionnez l'onglet Propriétés, puis faites défiler l'écran jusqu'au volet des paramètres réseau pour sélectionner le nom du groupe de sécurité appliqué.
3. Accédez aux règles sortantes et sélectionnez Modifier les règles sortantes.
4. Sélectionnez Ajouter une règle.
5. Dans la colonne Type de la nouvelle règle, sélectionnez TCP personnalisé.
6. Dans la colonne Plage de ports, tapez`9098`. MSK Replicator utilise le contrôle d'accès IAM pour se connecter à votre cluster qui utilise le port 9098.
7. Dans la colonne Source, tapez le nom du groupe de sécurité du cluster cible MSK, puis sélectionnez Enregistrer les règles.

> **Note**
>
> Si vous ne souhaitez pas restreindre le trafic à l'aide de vos groupes de sécurité, vous pouvez également ajouter des règles entrantes et sortantes autorisant tout le trafic.
> 1. Sélectionnez Ajouter une règle.
> 2. Dans la colonne Type, choisissez Tout le trafic.
> 3. Dans la colonne Source, tapez `0.0.0.0/0`, puis sélectionnez Enregistrer les règles.

Configurez les paramètres et les autorisations du réplicateur

1. Dans le volet Paramètres du réplicateur, spécifiez les rubriques que vous souhaitez répliquer à l'aide d'expressions régulières dans les listes d'autorisation et de refus. Par défaut, toutes les rubriques sont répliquées.

> **Note**
>
> MSK Replicator ne réplique que 750 sujets par ordre trié. Si vous devez répliquer d'autres rubriques, nous vous recommandons de créer un réplicateur distinct. Accédez au centre de support de la AWS console et créez un dossier de support si vous avez besoin d'assistance pour plus de 750 sujets par réplicateur. Vous pouvez contrôler le nombre de sujets répliqués à l'aide de la métrique « TopicCount ». veuillez consulter Quota d'Amazon MSK.

2. Par défaut, MSK Replicator démarre la réplication à partir du dernier décalage (le plus récent) dans les rubriques sélectionnées. Vous pouvez également démarrer la réplication à partir du décalage le plus ancien (le plus ancien) des rubriques sélectionnées si vous souhaitez répliquer les données existantes sur vos rubriques. Une fois le réplicateur créé, vous ne pouvez pas modifier ce paramètre. Ce paramètre correspond au `startingPosition`champ des API de `CreateReplicator`demande et de `DescribeReplicator`réponse.

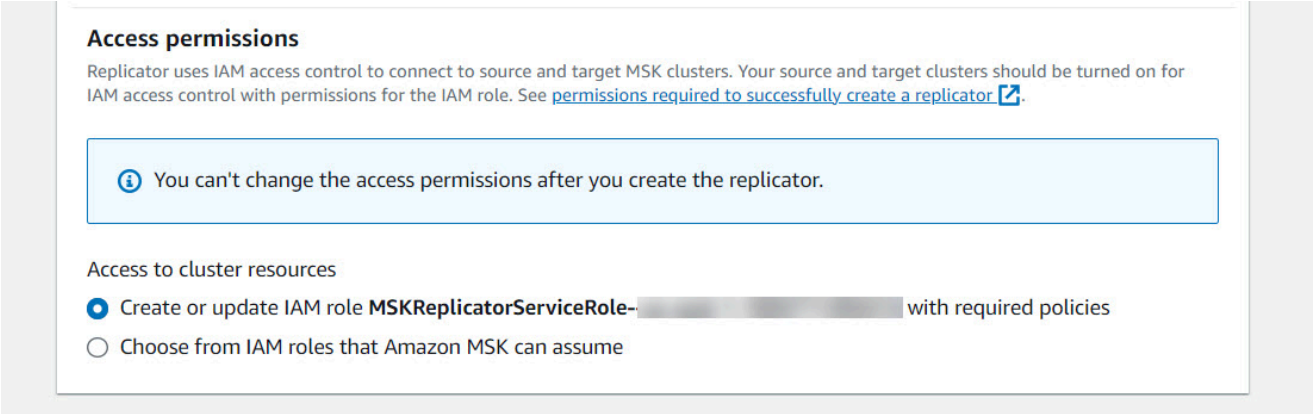
   > **Note**
   >
   > MSK Replicator agit comme un nouveau consommateur pour votre cluster source. En fonction de la quantité de données que vous répliquez et de la capacité de consommation de votre cluster source, cela peut entraîner une limitation des autres consommateurs de votre cluster source. Si vous créez un réplicateur réglé sur la position de départ la plus ancienne, MSK Replicator lira une rafale de données au début, susceptible de consommer toute la capacité de consommation de votre cluster source. Une fois que votre réplicateur aura rattrapé son retard, le taux de consommation devrait baisser pour correspondre au débit des rubriques de votre cluster source. Si vous répliquez depuis la première position, nous vous recommandons de gérer le débit du réplicateur à l'aide de quotas Kafka afin de vous assurer que les autres consommateurs ne sont pas limités.

3. Par défaut, le réplicateur MSK copie toutes les métadonnées, y compris les configurations des rubriques, les listes de contrôle d'accès (ACL) et les décalages des groupes de consommateurs pour un basculement fluide. Si vous ne créez pas le réplicateur pour le basculement, vous pouvez éventuellement choisir de désactiver un ou plusieurs de ces paramètres disponibles dans la section Paramètres supplémentaires.

> **Note**
>
> Le réplicateur MSK ne réplique pas les ACL d'écriture car vos producteurs ne doivent pas écrire directement sur la rubrique répliquée dans le cluster cible. Vos producteurs doivent écrire sur la rubrique locale du cluster cible après le basculement. Consultez Réalisation d'un basculement planifié vers la région secondaire AWS pour plus de détails.

4. Dans le volet Réplication de groupe de consommateurs, spécifiez les groupes de consommateurs que vous souhaitez répliquer à l'aide d'expressions régulières dans les listes d'autorisation et de refus. Par défaut, tous les groupes de consommateurs sont répliqués.
5. Dans le volet Compression, vous pouvez éventuellement choisir de compresser les données écrites sur le cluster cible. Si vous comptez utiliser la compression, nous vous recommandons d'utiliser la même méthode de compression que les données de votre cluster source.
6. Dans le volet Autorisations d'accès, effectuez l'une des opérations suivantes :

   a. Sélectionnez Créer ou mettre à jour le rôle IAM avec les politiques requises. La console MSK attachera automatiquement les autorisations et la politique d'approbation nécessaires au rôle d'exécution du service requis pour lire et écrire sur vos clusters MSK source et cible.



   b. Indiquez votre propre rôle IAM en sélectionnant Choisir parmi les rôles IAM qu'Amazon MSK peut assumer. Nous vous recommandons d'associer la stratégie IAM `AWSMSKReplicatorExecutionRole` gérée à votre rôle d'exécution de service, au lieu d'écrire votre propre stratégie IAM.

      - Créez le rôle IAM que le réplicateur utilisera pour lire et écrire sur vos clusters MSK source et cible avec le code JSON ci-dessous dans le cadre de la politique d'approbation et la `AWSMSKReplicatorExecutionRole` attachée au rôle. Dans la

politique d'approbation, remplacez l'espace réservé <yourAccountID> par votre ID de compte réel.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "kafka.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "<yourAccountID>"
                }
            }
        }
    ]
}
```

7. Dans le volet Balises du réplicateur, vous pouvez éventuellement attribuer des balises à la ressource du réplicateur MSK. Pour plus d'informations, consultez Balisage d'un cluster Amazon MSK. Pour un réplicateur MSK entre régions, les balises sont automatiquement synchronisées avec la région distante lors de la création du réplicateur. Si vous modifiez les balises après la création du réplicateur, la modification n'est pas automatiquement synchronisée avec la région distante. Vous devrez donc synchroniser manuellement les références du réplicateur local et du réplicateur distant.
8. Sélectionnez Créer.

Si vous souhaitez restreindre les `kafka-cluster:WriteData` autorisations, reportez-vous à la section Créer des politiques d'autorisation de Comment fonctionne le contrôle d'accès IAM pour Amazon MSK. Vous devez ajouter une `kafka-cluster:WriteDataIdempotently` autorisation au cluster source et au cluster cible.

Il faut environ 30 minutes pour que le réplicateur MSK soit créé et qu'il passe au statut RUNNING.

Si vous créez un nouveau réplicateur MSK pour remplacer un réplicateur que vous avez supprimé, le nouveau réplicateur démarre la réplication à partir du dernier décalage.

Si votre réplicateur MSK est passé au statut FAILED, reportez-vous à la section Dépannage du réplicateur MSK.

Modifier les paramètres du réplicateur MSK

Vous ne pouvez pas modifier le cluster source, le cluster cible ou la position de départ du réplicateur une fois que le réplicateur MSK a été créé. Vous pouvez toutefois modifier d'autres paramètres du Replicator, tels que les sujets et les groupes de consommateurs à répliquer.

1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Dans le volet de navigation de gauche, choisissez Réplicateurs pour afficher la liste des réplicateurs du compte et sélectionnez le réplicateur MSK que vous souhaitez modifier.
3. Choisissez l'onglet Propriétés.
4. Dans la section Paramètres du réplicateur, choisissez Modifier le réplicateur.
5. Vous pouvez modifier les paramètres du réplicateur MSK en modifiant n'importe lequel de ces paramètres.

    - Spécifiez les rubriques que vous souhaitez répliquer à l'aide d'expressions régulières dans les listes d'autorisation et de refus. Par défaut, le réplicateur MSK copie toutes les métadonnées, y compris les configurations des rubriques, les listes de contrôle d'accès (ACL) et les décalages des groupes de consommateurs pour un basculement fluide. Si vous ne créez pas le réplicateur pour le basculement, vous pouvez éventuellement choisir de désactiver un ou plusieurs de ces paramètres disponibles dans la section Paramètres supplémentaires.

        > **Note**
        >
        > Le réplicateur MSK ne réplique pas les ACL d'écriture car vos producteurs ne doivent pas écrire directement sur la rubrique répliquée dans le cluster cible. Vos producteurs doivent écrire sur la rubrique locale du cluster cible après le basculement. Consultez Réalisation d'un basculement planifié vers la région secondaire AWS pour plus de détails.

    - Pour la réplication de groupes de consommateurs, vous pouvez spécifier les groupes de consommateurs que vous souhaitez répliquer à l'aide d'expressions régulières dans les listes d'autorisation et de refus. Par défaut, tous les groupes de consommateurs sont répliqués. Si

les listes d'autorisation et de refus sont vides, la réplication des groupes de consommateurs est désactivée.

- Dans le volet Type de compression cible, vous pouvez éventuellement choisir de compresser les données écrites sur le cluster cible. Si vous comptez utiliser la compression, nous vous recommandons d'utiliser la même méthode de compression que les données de votre cluster source.

6. Enregistrez vos modifications.

   Il faut environ 30 minutes pour que le réplicateur MSK soit créé et qu'il passe au statut RUNNING. Si votre réplicateur MSK est passé au statut FAILED, reportez-vous à la section ???.

Supprimer un réplicateur MSK

Vous devrez peut-être supprimer un réplicateur MSK s'il ne parvient pas à être créé (statut FAILED). Les clusters source et cible assignés à un réplicateur MSK ne peuvent pas être modifiés une fois le réplicateur MSK créé. Vous pouvez supprimer un réplicateur MSK existant et en créer un nouveau. Si vous créez un nouveau réplicateur MSK pour remplacer celui que vous avez supprimé, le nouveau réplicateur démarre la réplication à partir du dernier décalage.

1. Dans la AWS région où se trouve votre cluster source, connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Dans le volet de navigation, sélectionnez Réplicateurs.
3. Dans la liste des réplicateurs MSK, sélectionnez celui que vous souhaitez supprimer, puis choisissez Supprimer.

Surveiller la réplication

Vous pouvez utiliser https://console.aws.amazon.com/cloudwatch/ dans la région du cluster cible pour afficher les métriques pour `ReplicationLatency`, `MessageLag` et `ReplicatorThroughput` au niveau de la rubrique et agréger le niveau pour chaque réplicateur Amazon MSK. Les métriques sont visibles ci-dessous ReplicatorNamedans l'espace de noms « AWS /Kafka ». Vous pouvez également voir les métriques `ReplicatorFailure`, `AuthError` et `ThrottleTime` pour vérifier les problèmes.

La console MSK affiche un sous-ensemble de CloudWatch métriques pour chaque réplicateur MSK. Dans la liste des réplicateurs de la console, sélectionnez le nom d'un réplicateur et sélectionnez l'onglet Surveillance.

Métriques du réplicateur MSK

Les métriques suivantes décrivent les mesures de performance ou de connexion du réplicateur MSK.

AuthError les métriques ne couvrent pas les erreurs d'authentification au niveau du sujet. Pour surveiller les erreurs d'authentification au niveau thématique de votre MSK Replicator, surveillez les métriques du Replicator et ReplicationLatency les métriques thématiques du cluster source,. MessagesInPerSec Si un sujet passe ReplicationLatency à 0 mais que des données y sont toujours produites, cela indique que le réplicateur a un problème d'authentification avec le sujet. Vérifiez que le rôle IAM d'exécution du service du réplicateur dispose des autorisations suffisantes pour accéder à la rubrique.

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes	
Performance	ReplicationLatency	Temps nécessaire aux enregistrements pour se répliquer du cluster source au cluster cible ; durée entre le moment de production de l'enregistrement à la source et celui de réplication vers la cible. En	ReplicatorName	Millisecondes	Partition	Maximum	
			ReplicatorName, Sujet	Millisecondes	Partition	Maximum	

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes	
		cas d' ReplicationLatency augmentation, vérifiez si les clusters disposent de suffisamment de partitions pour prendre en charge la réplication. Une latence de réplication élevée peut se produire lorsque le nombre de partitions est trop faible pour un débit élevé.					

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes
Performance	MessageLag	Surveille la synchronisation entre le MSK Replicator et le cluster source. MessageLag indique le décalage entre les messages produits vers le cluster source et les messages consommés par le réplicateur. Il ne s'agit pas du décalage entre le cluster source et le cluster cible. Même si le cluster source est indisponible/interrompu, le réplicateur terminera d'écrire le message qu'il a consommé au cluster	ReplicatorName	Nombre	Partition	Somme
			ReplicatorName, Sujet	Nombre	Partition	Somme

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes	
		cible. Après une panne, MessageLag indique une augmentation indiquant le nombre de messages que le réplicateur se trouve derrière le cluster source. Cela peut être surveillé jusqu'à ce que le nombre de messages soit égal à 0, ce qui indique que le réplicateur a rattrapé le cluster source.					

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes	
Performance	ReplicatorThroughput	Nombre moyen d'octets répliqués par seconde. En cas ReplicatorThroughput d'abandon pour un sujet, vérifiez KafkaClusterPingSuccessCount les AuthError mesures pour vous assurer que le réplicateur peut communiquer avec les clusters, puis vérifiez les métriques du cluster pour vous assurer que le cluster n'est pas en panne.	ReplicatorName	BytesPerSecond	Partition	Somme	
			ReplicatorName, Sujet	BytesPerSecond	Partition	Somme	

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes
Débogag	AuthError	Nombre de connexions dont l'authentification a échoué par seconde. Si cette métrique est supérieure à 0, vous pouvez vérifier si la politique de rôle d'exécution du service pour le réplicateur est valide et vous assurer qu'aucune autorisation de refus n'est définie pour les autorisations du cluster. Sur la base de la dimension clusterAlias, vous pouvez identifier si le cluster source ou cible rencontre	ReplicatorName, ClusterAlias	Nombre	Nœuds	Somme

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes	
		des erreurs d'authentification.					

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes
Débogag	ThrottleTime	La durée moyenne en ms d'une demande a été limitée par les agents sur le cluster. Définissez la limitation pour éviter que le réplicateur MSK ne submerge le cluster. Si cette métrique est égale à 0, que replicationLatency n'est pas élevée et que replicatorThroughput est conforme aux attentes, cela signifie que la limitation fonctionne comme prévu. Si cette métrique est supérieure à 0, vous	ReplicatorName, ClusterAlias	Millisecondes	Nœuds	Maximum

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes
		pouvez ajuster la limitation en conséquence.				
Débogag	ReplicatorFailure	Nombre de défaillances rencontrées par le réplicateur.	ReplicatorName	Nombre		Somme

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes
Débogage	KafkaClusterPingSuccessCount	Indique l'état de la connexion du réplicateur au cluster Kafka. Si cette valeur est égale à 1, la connexion est saine. Si la valeur est 0 ou aucun point de données, la connexion n'est pas saine. Si la valeur est 0, vous pouvez vérifier les paramètres d'autorisation réseau ou IAM pour le cluster Kafka. En fonction de ClusterAlias la dimension, vous pouvez déterminer si cette métrique concerne le	ReplicatorName, ClusterAlias	Nombre		Somme

Type de métrique	Métrique	Description	Dimensions	Unité	Granularité des métriques brutes	Statistiques d'agrégation des métriques brutes	
		cluster source ou cible.					

Utilisation de la réplication pour augmenter la résilience d'une application de streaming Kafka dans toutes les régions

Vous pouvez utiliser MSK Replicator pour configurer des topologies de cluster actif-actif ou actif-passif afin d'accroître la résilience de votre application Apache Kafka dans toutes les régions. AWS Dans une configuration active-active, les deux clusters MSK effectuent activement des opérations de lecture et d'écriture. Dans une configuration active-passive, un seul cluster MSK à la fois diffuse activement des données, tandis que l'autre cluster est en veille.

Considérations relatives à la création d'applications Apache Kafka multi-régions

Vos consommateurs doivent être en mesure de retraiter les messages dupliqués sans impact en aval. MSK Replicator réplique les données, at-least-once ce qui peut entraîner des doublons dans le cluster de secours. Lorsque vous passez à la AWS région secondaire, vos consommateurs peuvent traiter les mêmes données plusieurs fois. Le réplicateur MSK donne la priorité à la copie des données plutôt qu'aux décalages destinés aux consommateurs pour de meilleures performances. Après un basculement, le consommateur peut commencer à lire des décalages antérieurs, ce qui entraîne un double traitement.

Les producteurs et les consommateurs doivent également accepter de perdre un minimum de données. Comme MSK Replicator réplique les données de manière asynchrone, lorsque la AWS région principale commence à rencontrer des défaillances, il n'y a aucune garantie que toutes les données soient répliquées dans la région secondaire. Vous pouvez utiliser la latence de réplication pour déterminer le maximum de données qui n'ont pas été copiées dans la région secondaire.

Utilisation d'une topologie de cluster actif-actif ou actif-passif

Une topologie de cluster actif-actif offre un temps de restauration proche de zéro et permet à votre application de streaming de fonctionner simultanément dans plusieurs régions AWS . Lorsqu'un cluster d'une région est endommagé, les applications connectées au cluster de l'autre région continuent de traiter les données.

Les configurations actives-passives sont adaptées aux applications qui ne peuvent s'exécuter que dans une seule région AWS à la fois, ou lorsque vous avez besoin d'un contrôle accru sur l'ordre de traitement des données. Les configurations actives-passives nécessitent un temps de restauration plus long que les configurations actives-actives, car vous devez démarrer l'ensemble de votre configuration active-passive, y compris vos producteurs et consommateurs, dans la région secondaire pour reprendre le streaming des données après un basculement.

Création d'une configuration de cluster Kafka active-passive et dénomination des rubriques répliquées

Pour une configuration active-passive, nous vous recommandons d'utiliser une configuration similaire composée de producteurs, de clusters MSK et de consommateurs (portant le même nom de groupe de consommateurs) dans deux régions différentes. AWS Il est important que les deux clusters MSK aient une capacité de lecture et d'écriture identique pour garantir une réplication fiable des données. Vous devez créer un réplicateur MSK pour copier en continu les données du cluster principal vers le cluster de secours. Vous devez également configurer vos producteurs pour qu'ils écrivent des données dans les rubriques d'un cluster de la même AWS région.

Pour vous assurer que vos consommateurs peuvent redémarrer le traitement de manière fiable depuis le cluster de secours, vous devez les configurer pour qu'ils lisent les données des rubriques à l'aide d'un opérateur générique « .* ». Par exemple, MSK Replicator réplique « topic1 » du cluster principal vers un nouveau sujet du cluster de secours appelé « **<** Alias**>**.topic1 ». sourceKafkaCluster Par exemple, vous pouvez configurer vos producteurs pour qu'ils écrivent dans « topic1 » et vos consommateurs pour qu'ils consomment en utilisant « *topic1 » dans les deux régions. Cet exemple inclurait également une rubrique comme footopic1. Ajustez donc l'opérateur générique en fonction de vos besoins.

Quand basculer vers la région secondaire AWS

Nous vous recommandons de surveiller la latence de réplication dans la AWS région secondaire à l'aide de CloudWatch. Lors d'un événement de service dans la AWS région principale, la latence de réplication peut augmenter soudainement. Si la latence ne cesse d'augmenter, utilisez le AWS

Service Health Dashboard pour vérifier les événements de service dans la AWS région principale. En cas d'événement, vous pouvez basculer vers la AWS région secondaire.

Réalisation d'un basculement planifié vers la région secondaire AWS

Vous pouvez effectuer un basculement planifié pour tester la résilience de votre application face à un événement inattendu dans votre AWS région principale où se trouve votre cluster MSK source. Un basculement planifié ne doit pas entraîner de perte de données.

1. Arrêtez tous les producteurs et consommateurs qui se connectent à votre cluster source.
2. Créez un nouveau réplicateur MSK pour répliquer les données de votre cluster MSK de la région secondaire vers votre cluster MSK de la région principale. Cette opération est nécessaire pour copier les données que vous allez écrire dans la région secondaire vers la région principale afin d'effectuer un failback vers la région principale une fois que l'événement inattendu est terminé.
3. Démarrez les producteurs sur le cluster cible de la AWS région secondaire.
4. Selon les exigences d'ordre des messages de votre application, suivez les étapes décrites dans l'un des onglets suivants.

No message ordering

Si votre application ne nécessite pas de classement des messages, lancez les utilisateurs de la AWS région secondaire qui lisent à la fois des sujets locaux (par exemple`topic`) et des sujets répliqués (par exemple,`<sourceKafkaClusterAlias>.topic`) en utilisant un opérateur générique (par exemple,. *sujet).

Message ordering

Si votre application nécessite un ordre des messages, démarrez les consommateurs uniquement pour les rubriques répliquées sur le cluster cible (par exemple, `<sourceKafkaClusterAlias>.topic`), mais pas pour les rubriques locales (par exemple, `topic`).

1. Attendez que tous les consommateurs des rubriques répliquées sur le cluster MSK cible aient fini de traiter toutes les données, de sorte que le décalage des consommateurs soit égal à 0 et que le nombre d'enregistrements traités soit également égal à 0. Arrêtez ensuite les consommateurs pour les rubriques répliquées sur le cluster cible. À ce stade, tous les enregistrements répliqués du cluster MSK source vers le cluster MSK cible ont été consommés.

2. Démarrez les consommateurs pour les rubriques locales (par exemple, `topic`) sur le cluster MSK cible.

Effectuer un basculement imprévu vers la région secondaire AWS

Vous pouvez effectuer un basculement imprévu lorsqu'un événement de service se produit dans la AWS région principale dans laquelle se trouve votre cluster MSK source et que vous souhaitez rediriger temporairement votre trafic vers la AWS région secondaire dans laquelle se trouve votre cluster MSK cible. Un basculement non planifié peut entraîner une perte de données.

1. Essayez de fermer tous les producteurs et consommateurs se connectant au cluster MSK source dans la région principale. Cela risque d'échouer.
2. Démarrez les producteurs qui se connectent au cluster MSK cible de la région secondaire.
3. Selon les exigences d'ordre des messages de votre application, suivez les étapes décrites dans l'un des onglets suivants.

   No message ordering

   Si votre application ne nécessite pas de classement des messages, commencez par utiliser un opérateur générique (par exemple,`topic`) pour les consommateurs de la AWS région cible qui lisent à la fois des sujets locaux (par exemple`<sourceKafkaClusterAlias>.topic`) et des sujets répliqués (par exemple,`.*topic`).

   Message ordering

   1. Démarrez les consommateurs uniquement pour les rubriques répliquées sur le cluster cible (par exemple, `<sourceKafkaClusterAlias>.topic`), mais pas pour les rubriques locales (par exemple, `topic`).
   2. Attendez que tous les consommateurs des rubriques répliquées sur le cluster MSK cible aient fini de traiter toutes les données, de sorte que le décalage soit égal à 0 et que le nombre d'enregistrements traités soit également égal à 0. Arrêtez ensuite les consommateurs pour les rubriques répliquées sur le cluster cible. À ce stade, tous les enregistrements répliqués du cluster MSK source vers le cluster MSK cible ont été consommés.
   3. Démarrez les consommateurs pour les rubriques locales (par exemple, `topic`) sur le cluster MSK cible.

4. Une fois l'événement de service terminé dans la région principale, créez un nouveau réplicateur MSK pour répliquer les données de votre cluster MSK de la région secondaire vers votre cluster MSK de la région principale, la position de départ du réplicateur étant définie au plus tôt. Cette opération est nécessaire pour copier les données que vous allez écrire dans la région secondaire vers la région principale afin d'effectuer un failback vers la région principale une fois que l'événement est terminé. Si vous ne définissez pas la position de départ du réplicateur au plus tôt, les données que vous avez produites pour le cluster dans la région secondaire lors de l'événement de service dans la région principale ne seront pas copiées vers le cluster de la région principale.

Effectuer un retour en arrière vers la région principale AWS

Vous pouvez revenir à la AWS région principale une fois que l'événement de service dans cette région est terminé. Le réplicateur MSK ignore automatiquement les rubriques dont le préfixe est l'alias du cluster source lors de la réplication des données vers la région principale pendant le failback.

Si vous avez suivi les étapes de basculement imprévues, vous devez déjà avoir créé le réplicateur de secours dans le cadre de la dernière étape du basculement de la région principale vers la région secondaire.

Si vous n'avez pas suivi les étapes de basculement imprévues, une fois l'événement de service terminé dans la région principale, créez un nouveau réplicateur MSK pour répliquer les données de votre cluster MSK de la région secondaire vers votre cluster MSK de la région principale, la position de départ du réplicateur étant définie au plus tôt. Cette opération est nécessaire pour copier les données que vous allez écrire dans la région secondaire vers la région principale afin d'effectuer un failback vers la région principale une fois que l'événement est terminé. Si vous ne modifiez pas la position de départ du réplicateur de sa valeur par défaut de la plus récente à la plus ancienne, les données que vous avez produites pour le cluster de la région secondaire lors de l'événement de service dans la région principale ne seront pas copiées vers le cluster de la région principale.

Vous ne devez lancer les étapes de retour en arrière qu'une fois que la réplication du cluster de la région secondaire vers le cluster de la région principale a rattrapé son retard et que la MessageLag métrique CloudWatch est proche de 0. Un failback planifié ne doit pas entraîner de perte de données.

1. Fermez tous les producteurs et consommateurs se connectant au cluster MSK source dans la région secondaire.

2. Pour une topologie active-passive, supprimez le réplicateur qui réplique les données du cluster de la région secondaire vers la région principale. Il n'est pas nécessaire de supprimer le réplicateur pour une topologie active-active.
3. Démarrez les producteurs qui se connectent au cluster MSK cible de la région secondaire.
4. Selon les exigences d'ordre des messages de votre application, suivez les étapes décrites dans l'un des onglets suivants.

   No message ordering

   Si votre application ne nécessite pas de classement des messages, commencez par utiliser un opérateur générique (par exemple,`topic`) pour les clients de la AWS région principale qui lisent à la fois des sujets locaux (par exemple`<sourceKafkaClusterAlias>.topic`) et des sujets répliqués (par exemple,`.*topic`). Les consommateurs sur les rubriques locales (par exemple : topic) reprendront leur activité à partir du dernier décalage qu'ils ont consommé avant le basculement. S'il y avait des données non traitées avant le basculement, elles seront traitées maintenant. Dans le cas d'un basculement planifié, aucun enregistrement de ce type ne devrait exister.

   Message ordering

   1. Démarrez les consommateurs uniquement pour les rubriques répliquées sur la région principale (par exemple, `<sourceKafkaClusterAlias>.topic`), mais pas pour les rubriques locales (par exemple, `topic`).
   2. Attendez que tous les consommateurs des rubriques répliquées sur le cluster dans la région principale aient fini de traiter toutes les données, de sorte que le décalage soit égal à 0 et que le nombre d'enregistrements traités soit égal aussi à 0. Arrêtez ensuite les consommateurs pour les rubriques répliquées sur le cluster dans la région principale. À ce stade, tous les enregistrements produits dans la région secondaire après le basculement ont été consommés dans la région principale.
   3. Démarrez les consommateurs pour les rubriques locales (par exemple, `topic`) sur le cluster dans la région principale.
5. Vérifiez que le réplicateur existant, du cluster de la région principale au cluster de la région secondaire, est en cours d'exécution et fonctionne comme prévu à l'aide des métriques `ReplicatorThroughput` et de latence.

Création d'une configuration active-active à l'aide du réplicateur MSK.

Procédez comme suit pour configurer une topologie active-active entre le cluster MSK source A et le cluster MSK cible B.

1. Créez un réplicateur MSK avec le cluster MSK A comme source et le cluster MSK B comme cible.
2. Une fois que le réplicateur MSK ci-dessus a été créé avec succès, créez un réplicateur avec le cluster B comme source et le cluster A comme cible.
3. Créez deux ensembles de producteurs, chacun écrivant des données en même temps dans la rubrique locale (par exemple, « topic ») dans le cluster situé dans la même région que le producteur.
4. Créez deux groupes de consommateurs, chacun lisant des données à l'aide d'un abonnement générique (tel que »). *topic ») du cluster MSK situé dans la même AWS région que le consommateur. Ainsi, vos consommateurs liront automatiquement les données produites localement dans la région à partir de la rubrique locale (par exemple, `topic`), ainsi que les données répliquées depuis une autre région (dans la rubrique avec le préfixe `<sourceKafkaClusterAlias>.topic`). Ces deux ensembles de consommateurs doivent avoir des identifiants de groupe de consommateurs différents afin que les décalages de groupes de consommateurs ne soient pas remplacés lorsque le réplicateur MSK les copie sur l'autre cluster.

Dépannage du réplicateur MSK

Rubriques

- L'état du réplicateur MSK passe de CREATING à FAILED
- Le réplicateur MSK semble bloqué dans l'état CREATING
- Le réplicateur MSK ne réplique pas les données ou ne réplique que des données partielles
- Les décalages de messages dans le cluster cible sont différents de ceux du cluster source
- MSK Replicator ne synchronise pas les groupes de consommateurs, les offsets ou le groupe de consommateurs n'existe pas sur le cluster cible
- La latence de réplication est élevée ou continue d'augmenter

La documentation suivante peut vous aider à résoudre les problèmes que vous pouvez rencontrer avec le réplicateur MSK. Vous pouvez également publier votre problème sur AWS re:Post.

L'état du réplicateur MSK passe de CREATING à FAILED

Les raisons courantes suivantes expliquent l'échec de création du réplicateur MSK.

1. Vérifiez que les groupes de sécurité que vous avez fourni pour la création du réplicateur dans la section du cluster cible comportent des règles de sortie autorisant le trafic vers les groupes de sécurité de votre cluster cible. Vérifiez également que les groupes de sécurité de votre cluster cible comportent des règles entrantes qui autorisent le trafic des groupes de sécurité que vous avez fournis pour la création du réplicateur dans la section du cluster cible. veuillez consulter Choisissez votre cluster cible.
2. Si vous créez un réplicateur pour la réplication entre régions, vérifiez que la connectivité multi-VPC de votre cluster source est activée pour la méthode d'authentification du contrôle d'accès IAM. veuillez consulter Connectivité privée à plusieurs VPC Amazon MSK dans une seule région. Vérifiez également que la politique de cluster est configurée sur le cluster source afin que le réplicateur MSK puisse se connecter au cluster source. veuillez consulter Étape 1 : Préparer le cluster source Amazon MSK.
3. Vérifiez que le rôle IAM que vous avez fourni lors de la création du réplicateur MSK dispose des autorisations requises pour lire et écrire sur vos clusters source et cible. Vérifiez également que le rôle IAM dispose des autorisations nécessaires pour écrire dans les rubriques. Consultez Configurez les paramètres et les autorisations du réplicateur.
4. Vérifiez que les listes ACL réseau ne bloquent pas la connexion entre le réplicateur MSK et vos clusters source et cible.
5. Il est possible que les clusters source ou cible ne soient pas entièrement disponibles lorsque le réplicateur MSK a essayé de s'y connecter. Cela peut être dû à une charge excessive, à une utilisation du disque ou du processeur, ce qui empêche le réplicateur de se connecter aux agents. Corrigez le problème avec les agents et réessayez de créer un réplicateur.

Après avoir effectué les validations ci-dessus, créez à nouveau le réplicateur MSK.

Le réplicateur MSK semble bloqué dans l'état CREATING

Parfois, la création du réplicateur MSK peut prendre jusqu'à 30 minutes. Attendez 30 minutes et vérifiez à nouveau l'état du réplicateur.

Le réplicateur MSK ne réplique pas les données ou ne réplique que des données partielles

Suivez ces étapes pour résoudre les problèmes de réplication des données.

1. Vérifiez que votre réplicateur ne rencontre aucune erreur d'authentification à l'aide de la AuthError métrique fournie par MSK Replicator dans. CloudWatch Si cette métrique est supérieure à 0, vérifiez si la politique du rôle IAM fourni pour le réplicateur est valide et qu'aucune autorisation de refus n'est définie pour les autorisations du cluster. Sur la base de la dimension clusterAlias, vous pouvez identifier si le cluster source ou cible rencontre des erreurs d'authentification.
2. Vérifiez que vos clusters source et cible ne rencontrent aucun problème. Il est possible que le réplicateur ne soit pas en mesure de se connecter à votre cluster source ou cible. Cela peut être dû à un trop grand nombre de connexions, à une capacité maximale du disque ou à une utilisation élevée du processeur.
3. Vérifiez que vos clusters source et cible sont accessibles depuis MSK Replicator à l'aide de la KafkaClusterPingSuccessCount métrique entrée. CloudWatch Sur la base de la dimension clusterAlias, vous pouvez identifier si le cluster source ou cible rencontre des erreurs d'authentification. Si la valeur est égale à 0 ou aucun point de données, la connexion n'est pas saine. Vous devez vérifier les autorisations réseau et de rôle IAM utilisées par le réplicateur MSK pour se connecter à vos clusters.
4. Vérifiez que votre réplicateur ne rencontre pas de défaillances en raison de l'absence d'autorisations au niveau du sujet à l'aide de la ReplicatorFailure métrique saisie. CloudWatch Si cette métrique est supérieure à 0, vérifiez le rôle IAM que vous avez fourni pour les autorisations au niveau de la rubrique.
5. Vérifiez que l'expression régulière que vous avez fournie dans la liste d'autorisation lors de la création du réplicateur correspond aux noms des rubriques que vous souhaitez répliquer. Vérifiez également que les rubriques ne sont pas exclues de la réplication en raison d'une expression régulière présente dans la liste de refus.
6. Notez que le réplicateur peut prendre jusqu'à 30 secondes pour détecter et créer les nouveaux sujets ou partitions de sujets sur le cluster cible. Les messages envoyés au sujet source avant sa création sur le cluster cible ne seront pas répliqués si la position de départ du réplicateur est la plus récente (par défaut). Vous pouvez également démarrer la réplication à partir du premier décalage dans les partitions des rubriques du cluster source si vous souhaitez répliquer les messages existants relatifs à vos sujets sur le cluster cible. veuillez consulter Configurez les paramètres et les autorisations du réplicateur.

Les décalages de messages dans le cluster cible sont différents de ceux du cluster source

Dans le cadre de la réplication des données, MSK Replicator consomme les messages du cluster source et les transmet au cluster cible. Cela peut entraîner des messages présentant des décalages différents sur vos clusters source et cible. Toutefois, si vous avez activé la synchronisation des offsets des groupes de consommateurs lors de la création du réplicateur, MSK Replicator traduira automatiquement les décalages lors de la copie des métadonnées afin qu'après avoir basculé vers le cluster cible, vos clients puissent reprendre le traitement là où ils s'étaient arrêtés dans le cluster source.

MSK Replicator ne synchronise pas les groupes de consommateurs, les offsets ou le groupe de consommateurs n'existe pas sur le cluster cible

Suivez ces étapes pour résoudre les problèmes de réplication des métadonnées.

1. Vérifiez que la réplication de vos données fonctionne comme prévu. Si ce n’est pas le cas, voyez Le réplicateur MSK ne réplique pas les données ou ne réplique que des données partielles.
2. Vérifiez que l'expression régulière que vous avez fournie dans la liste d'autorisation lors de la création du réplicateur correspond aux noms des groupes de consommateurs que vous souhaitez répliquer. Vérifiez également que les groupes de consommateurs ne sont pas exclus de la réplication en raison d'une expression régulière dans la liste de refus.
3. Vérifiez que MSK Replicator a créé le sujet sur le cluster cible. Le réplicateur peut prendre jusqu'à 30 secondes pour détecter et créer les nouveaux sujets ou partitions de sujets sur le cluster cible. Les messages envoyés au sujet source avant sa création sur le cluster cible ne seront pas répliqués si la position de départ du réplicateur est la plus récente (par défaut). Si votre groupe de consommateurs du cluster source n'a consommé que les messages qui n'ont pas été répliqués par MSK Replicator, le groupe de consommateurs ne sera pas répliqué vers le cluster cible. Une fois le sujet créé avec succès sur le cluster cible, MSK Replicator commence à répliquer les messages récemment écrits sur le cluster source vers la cible. Une fois que votre groupe de consommateurs commence à lire ces messages depuis la source, MSK Replicator répliquera automatiquement le groupe de consommateurs sur le cluster cible. Vous pouvez également démarrer la réplication à partir du premier décalage dans les partitions des rubriques du cluster source si vous souhaitez répliquer les messages existants relatifs à vos sujets sur le cluster cible. veuillez consulter Configurez les paramètres et les autorisations du réplicateur.

> **Note**
>
> MSK Replicator optimise la synchronisation des décalages des groupes de consommateurs pour vos clients du cluster source qui lisent à une position plus proche de la fin de la partition thématique. Si vos groupes de consommateurs sont en retard sur le cluster source, vous constaterez peut-être un retard plus important pour ces groupes de consommateurs sur le cluster cible par rapport à la source. Cela signifie qu'après le basculement vers le cluster cible, vos clients retraiteront un plus grand nombre de messages dupliqués. Pour réduire ce décalage, vos clients du cluster source devraient rattraper leur retard et commencer à consommer dès le début du stream (fin de la partition thématique). Au fur et à mesure que vos clients rattrapent leur retard, MSK Replicator réduira automatiquement le décalage.

La latence de réplication est élevée ou continue d'augmenter

Les raisons courantes suivantes expliquent une latence de réplication élevée.

1. Vérifiez que vous disposez du bon nombre de partitions sur vos clusters MSK source et cible. Le fait d'avoir trop peu ou trop de partitions peut avoir un impact sur les performances. Pour obtenir des conseils sur le choix du nombre de partitions, reportez-vous à la section Bonnes pratiques pour l'utilisation du réplicateur MSK. Le tableau suivant indique le nombre minimum de partitions recommandé pour obtenir le débit souhaité avec le réplicateur MSK.

   Débit et nombre minimal de partitions recommandé

Débit (Mo/s)	Nombre minimal de partitions requis
50	167
100	334
250	833
500	1666
1 000	3333

2. Vérifiez que vous disposez d'une capacité de lecture et d'écriture suffisante dans vos clusters MSK source et cible pour prendre en charge le trafic de réplication. Le réplicateur MSK agit en tant que consommateur pour votre cluster source (sortie) et en tant que producteur pour votre cluster cible

(entrée). Par conséquent, vous devez prévoir une capacité de cluster pour prendre en charge le trafic de réplication en plus du reste du trafic sur vos clusters. Pour obtenir des conseils sur le dimensionnement correct de votre cluster, consultez ???.

3. La latence de réplication peut varier pour les clusters MSK dans différentes paires de AWS régions source et de destination, en fonction de la distance géographique entre les clusters. Par exemple, la latence de réplication est généralement inférieure lors de la réplication entre clusters des régions Europe (Irlande) et Europe (Londres) par rapport à la réplication entre clusters des régions Europe (Irlande) et Asie-Pacifique (Sydney).
4. Vérifiez que votre réplicateur n'est pas limité en raison de quotas trop agressifs définis sur vos clusters source ou cible. Vous pouvez utiliser la ThrottleTime métrique fournie par MSK Replicator CloudWatch pour voir le temps moyen en millisecondes pendant lequel une demande a été limitée par les courtiers de votre cluster source/cible. Si cette métrique est supérieure à 0, vous devez ajuster les quotas de Kafka pour réduire la limitation afin que le réplicateur puisse rattraper son retard. Consultez Gestion du débit du réplicateur MSK à l'aide des quotas de Kafka pour plus d'informations sur la gestion des quotas de Kafka pour le réplicateur.
5. ReplicationLatency et MessageLag peut augmenter lorsqu'une AWS région se dégrade. Utilisez le Tableau de bord de l'état des services AWS pour vérifier la présence d'un événement de service MSK dans la région où se trouve votre cluster MSK principal. En cas d'événement de service, vous pouvez rediriger temporairement les opérations de lecture et d'écriture de votre application dans l'autre région.

Bonnes pratiques pour l'utilisation du réplicateur MSK

Cette section décrit les bonnes pratiques et les stratégies de mise en œuvre courantes pour l'utilisation du réplicateur MSK.

Rubriques

- Gestion du débit du réplicateur MSK à l'aide des quotas de Kafka
- Définition de la période de conservation des données des clusters

Gestion du débit du réplicateur MSK à l'aide des quotas de Kafka

Comme le réplicateur MSK agit en tant que consommateur pour votre cluster source, la réplication peut entraîner une limitation des autres consommateurs sur votre cluster source. Le niveau de limitation dépend de la capacité de lecture dont dispose votre cluster source et du débit des données

que vous répliquez. Nous vous recommandons de fournir une capacité identique pour vos clusters source et cible, et de prendre en compte le débit de réplication lors du calcul de la capacité dont vous avez besoin.

Vous pouvez également définir des quotas Kafka pour le réplicateur sur vos clusters source et cible afin de contrôler la capacité que le réplicateur MSK peut utiliser. Un quota de bande passante du réseau est recommandé. Un quota de bande passante du réseau définit un seuil de débit, défini en octets par seconde, pour un ou plusieurs clients partageant un quota. Ce quota est défini sur une base par agent.

Suivez ces étapes pour appliquer un quota.

1. Récupérez la chaîne du serveur d'amorçage pour le cluster source. veuillez consulter Obtention des agents d'amorçage pour un cluster Amazon MSK.
2. Récupérez le rôle d'exécution de service (SER) utilisé par le réplicateur MSK. Il s'agit du SER que vous avez utilisé pour une demande `CreateReplicator`. Vous pouvez également extraire le SER de la DescribeReplicator réponse d'un réplicateur existant.
3. À l'aide des outils de l'interface de ligne de commande Kafka, exécutez la commande suivante sur le cluster source.

```
./kafka-configs.sh --bootstrap-server <source-cluster-bootstrap-server> --alter --
add-config 'consumer_byte_
rate=<quota_in_bytes_per_second>' --entity-type users --entity-name
 arn:aws:sts::<customer-account-id>:assumed-role/<ser-role-name>/<customer-account-
id> --command-config <client-properties-for-iam-auth></programlisting>
```

4. Après avoir exécuté la commande ci-dessus, vérifiez que la métrique `ReplicatorThroughput` ne dépasse pas le quota que vous avez défini.

Notez que si vous réutilisez un rôle d'exécution de service entre plusieurs réplicateurs MSK, ils seront tous soumis à ce quota. Si vous souhaitez conserver des quotas distincts par réplicateur, utilisez des rôles d'exécution de service distincts.

Pour plus d'informations sur l'utilisation de l'authentification IAM de MSK avec des quotas, consultez Clusters Apache Kafka multi-locataires dans Amazon MSK avec contrôle d'accès IAM et Quotas de Kafka — 1e partie.

> **Warning**
>
> Si vous définissez un consumer_byte_rate extrêmement bas, votre réplicateur MSK peut agir de manière inattendue.

Définition de la période de conservation des données des clusters

Vous pouvez définir la période de conservation des journaux pour les clusters provisionnés par MSK et les clusters sans serveur. La période de conservation par défaut est de 7 jours. Voir Modifications dans la configurations des clusters ou Configuration du cluster MSK sans serveur.

États du cluster

Le tableau ci-dessous montre les quatre états possibles d'un cluster et décrit leur signification. Il décrit également les actions que vous pouvez et ne pouvez pas effectuer lorsqu'un cluster se trouve à l'un de ces états. Pour connaître l'état d'un cluster, vous pouvez consulter la AWS Management Console. Vous pouvez également utiliser la commande describe-cluster-v2 ou l'opération DescribeClusterV2 pour décrire le cluster. La description d'un cluster inclut son état.

État du cluster	Signification et actions possibles
ACTIF	Vous pouvez produire et consommer des données. Vous pouvez également exécuter l'API Amazon MSK et effectuer AWS CLI des opérations sur le cluster.
CREAtioN	Amazon MSK est en train de configurer le cluster. Vous devez attendre que le cluster atteigne l'état ACTIF avant de pouvoir l'utiliser pour produire ou consommer des données ou pour exécuter l'API Amazon MSK ou AWS CLI des opérations sur celui-ci.
SUPPRESSION	Le cluster est en cours de suppression. Vous ne pouvez pas l'utiliser pour produire ou consommer des données. Vous ne pouvez pas non plus exécuter l'API Amazon MSK ou effectuer AWS CLI des opérations sur celle-ci.
ÉCHEC	Le processus de création ou de suppression du cluster a échoué. Vous ne pouvez pas utiliser le cluster pour produire ou consommer des données. Vous pouvez supprimer le cluster, mais vous ne pouvez pas effectuer d'opérations d'API Amazon MSK ou de AWS CLI mise à jour sur celui-ci.

État du cluster	Signification et actions possibles
RÉPARATION	Amazon MSK exécute une opération interne, comme le remplacement d'un agent non sain. Par exemple, il se peut que l'agent ne réponde pas. Vous pouvez encore utiliser le cluster pour produire ou consommer des données. Cependant, vous ne pouvez pas effectuer d'opérations d'API Amazon MSK ou de AWS CLI mise à jour sur le cluster tant qu'il ne revient pas à l'état ACTIF.
MAINTENANCE	Amazon MSK effectue des opérations de maintenance de routine sur le cluster. Ces opérations de maintenance incluent l'applica tion de correctifs de sécurité. Vous pouvez encore utiliser le cluster pour produire ou consommer des données. Cependant, vous ne pouvez pas effectuer d'opérations d'API Amazon MSK ou de AWS CLI mise à jour sur le cluster tant qu'il ne revient pas à l'état ACTIF.
REDÉMARRAGE_AGENT	Amazon MSK est en train de redémarrer un agent. Vous pouvez encore utiliser le cluster pour produire ou consommer des données. Cependant, vous ne pouvez pas effectuer d'opérations d'API Amazon MSK ou de AWS CLI mise à jour sur le cluster tant qu'il ne revient pas à l'état ACTIF.

État du cluster	Signification et actions possibles
MISE À JOUR	Une API ou une AWS CLI opération Amazon MSK initiée par l'utilisateur met à jour le cluster. Vous pouvez encore utiliser le cluster pour produire ou consommer des données. Cependant, vous ne pouvez pas effectuer d'autres opérations d'API Amazon MSK ou de AWS CLI mise à jour sur le cluster tant qu'il ne revient pas à l'état ACTIF.

Sécurité dans Amazon Managed Streaming for Apache Kafka

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 cela comme la sécurité du cloud et la 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 AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Managed Streaming for Apache Kafka, consultez Services Amazon Web Services concernés par le programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon MSK. Les rubriques suivantes vous montrent comment configurer Amazon MSK pour répondre à vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres services Amazon Web Services qui vous aident à contrôler et sécuriser vos ressources Amazon MSK.

Rubriques

- Résilience dans Amazon Managed Streaming for Apache Kafka
- Sécurité de l'infrastructure dans Amazon Managed Streaming for Apache Kafka

Protection des données dans Amazon Managed Streaming for Apache Kafka

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Amazon Managed Streaming for Apache Kafka. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

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

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

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

Rubriques

Chiffrement Amazon MSK

Amazon MSK fournit des options de chiffrement des données que vous pouvez utiliser pour répondre à des exigences strictes en matière de gestion des données. Les certificats utilisés par Amazon MSK pour le chiffrement doivent être renouvelés tous les 13 mois. Amazon MSK renouvelle automatiquement ces certificats pour tous les clusters. L'état du cluster est défini en tant que `MAINTENANCE` lorsque l'opération de mise à jour des certificats démarre. Puis, l'état sera remis sur `ACTIVE` à la fin de la mise à jour. Lorsque l'état d'un cluster est `MAINTENANCE`, vous pouvez continuer à produire et à consommer des données mais vous ne pouvez pas effectuer d'opérations de mise à jour sur celui-ci.

Chiffrement au repos

Amazon MSK s'intègre à AWS Key Management Service (KMS) pour permettre le chiffrement transparent côté serveur. Amazon MSK chiffre toujours vos données au repos. Lorsque vous créez un cluster MSK, vous pouvez spécifier la AWS KMS key que vous souhaitez qu'Amazon MSK utilise pour chiffrer vos données au repos. Si vous ne spécifiez pas de clé KMS, Amazon MSK crée une Clé gérée par AWS pour vous et l'utilise en votre nom. Pour plus d'informations sur les clés KMS, consultez AWS KMS keys dans le Guide du développeur AWS Key Management Service .

Chiffrement en transit

Amazon MSK utilise TLS 1.2. Par défaut, il chiffre les données en transit entre les agents de votre cluster MSK. Vous pouvez remplacer cette valeur par défaut au moment de la création du cluster.

Pour la communication entre clients et brokers, vous devez spécifier l'un des trois paramètres suivants :

- Autoriser uniquement les données chiffrées TLS. Il s'agit du paramètre par défaut.
- Autoriser à la fois le texte brut, ainsi que les données chiffrées TLS.
- Autoriser uniquement les données en texte brut.

Les courtiers Amazon MSK utilisent des AWS Certificate Manager certificats publics. Par conséquent, tout magasin fiable qui fait confiance à Amazon Trust Services approuve également les certificats des agents Amazon MSK.

Bien que nous vous recommandions d'activer le chiffrement en transit, celui-ci peut entraîner des charges supplémentaires d'UC et quelques millisecondes de latence. La plupart des cas d'utilisation ne sont toutefois pas sensibles à ces différences, cependant l'ampleur de l'impact dépend de la configuration du cluster, des clients et du profil d'utilisation.

Comment démarrer avec le chiffrement ?

Lors de la création d'un cluster MSK, vous pouvez spécifier les paramètres de chiffrement au format JSON. Voici un exemple.

```
{
   "EncryptionAtRest": {
       "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcdabcd-1234-
abcd-1234-abcd123e8e8e"
    },
   "EncryptionInTransit": {
        "InCluster": true,
        "ClientBroker": "TLS"
    }
}
```

Pour `DataVolumeKMSKeyId`, vous pouvez spécifier une clé gérée par le client ou la Clé gérée par AWS pour MSK dans votre compte (`alias/aws/kafka`). Si vous ne le spécifiez pas`EncryptionAtRest`, Amazon MSK chiffre toujours vos données au repos sous le. Clé gérée par AWS Pour déterminer la clé utilisée par votre cluster, envoyez une requête `GET` ou invoquez l'opération d'API `DescribeCluster`.

Pour `EncryptionInTransit`, la valeur par défaut de `InCluster` est true, mais vous pouvez la définir sur false si vous ne voulez pas qu'Amazon MSK chiffre vos données au fur et à mesure qu'elles passent entre les agents.

Pour spécifier le mode de chiffrement des données en transit entre les clients et les brokers, définissez `ClientBroker` sur l'une des trois valeurs suivantes : `TLS`, `TLS_PLAINTEXT` ou `PLAINTEXT`.

Pour spécifier des paramètres de chiffrement lors de la création d'un cluster

1. Enregistrez le contenu de l'exemple précédent dans un fichier et donnez au fichier le nom souhaité. Par exemple, appelez-le `encryption-settings.json`.
2. Exécutez la commande `create-cluster` et utilisez l'option `encryption-info` pour pointer vers le fichier dans lequel vous avez enregistré votre JSON de configuration. Voici un exemple. Remplacez *`{VOTRE VERSION MSK}`* par une version qui correspond à la version du client Apache Kafka. Pour de plus amples informations sur la recherche de la version de votre cluster MSK, consultez To find the version of your MSK cluster. Sachez que l'utilisation d'une version du client Apache Kafka différente de la version de votre cluster MSK peut entraîner la corruption, la perte et l'arrêt des données d'Apache Kafka.

   ```
   aws kafka create-cluster --cluster-name "ExampleClusterName" --broker-node-group-
   info file://brokernodegroupinfo.json --encryption-info file://encryptioninfo.json
    --kafka-version "{YOUR MSK VERSION}" --number-of-broker-nodes 3
   ```

   Voici un exemple de réponse réussie après l'exécution de cette commande.

   ```
   {
       "ClusterArn": "arn:aws:kafka:us-east-1:123456789012:cluster/SecondTLSTest/
   abcdabcd-1234-abcd-1234-abcd123e8e8e",
       "ClusterName": "ExampleClusterName",
       "State": "CREATING"
   }
   ```

Pour tester le chiffrement TLS

1. Créez une machine client en suivant les instructions de the section called “Étape 3 : créer un ordinateur client”.
2. Installez Apache Kafka sur l'ordinateur client.

3. Dans cet exemple, nous utilisons le magasin fiable JVM pour parler au cluster MSK. Pour ce faire, créez d'abord un dossier nommé `/tmp` sur l'ordinateur client. Ensuite, accédez au dossier `bin` de l'installation d'Apache Kafka et exécutez la commande suivante. (Votre chemin JVM peut être différent.)

```
cp /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.201.b09-0.amzn2.x86_64/jre/lib/security/
cacerts /tmp/kafka.client.truststore.jks
```

4. Dans le dossier `bin` de l'installation d'Apache Kafka sur l'ordinateur client, créez un fichier texte nommé `client.properties` avec le contenu suivant.

```
security.protocol=SSL
ssl.truststore.location=/tmp/kafka.client.truststore.jks
```

5. Exécutez la commande suivante sur une machine sur laquelle le *`ClusterArn est AWS CLI installé, en remplaçant ClusterArn`* par l'ARN de votre cluster.

```
aws kafka get-bootstrap-brokers --cluster-arn clusterARN
```

Un résultat réussi ressemble à ce qui suit. Enregistrez ce résultat car vous en avez besoin pour l'étape suivante.

```
{
    "BootstrapBrokerStringTls": "a-1.example.g7oein.c2.kafka.us-
east-1.amazonaws.com:0123,a-3.example.g7oein.c2.kafka.us-
east-1.amazonaws.com:0123,a-2.example.g7oein.c2.kafka.us-east-1.amazonaws.com:0123"
}
```

6. Exécutez la commande suivante, en la *`BootstrapBrokerStringTls`*remplaçant par l'un des points de terminaison du broker que vous avez obtenus à l'étape précédente.

```
<path-to-your-kafka-installation>/bin/kafka-console-producer.sh --broker-
list BootstrapBrokerStringTls --producer.config client.properties --topic
 TLSTestTopic
```

7. Ouvrez une nouvelle fenêtre de commande et connectez-vous au même ordinateur client. Exécutez ensuite la commande suivante pour créer un consommateur de console.

```
<path-to-your-kafka-installation>/bin/kafka-console-consumer.sh --bootstrap-
server BootstrapBrokerStringTls --consumer.config client.properties --topic
 TLSTestTopic
```

8. Dans la fenêtre du producteur, tapez un message texte suivi d'un retour et recherchez le même message dans la fenêtre du consommateur. Amazon MSK a chiffré ce message en transit.

Pour de plus amples informations sur la configuration des clients Apache Kafka pour qu'ils fonctionnent avec des données chiffrées, veuillez consulter Configuration des clients Kafka.

Authentification et autorisation pour les API Amazon MSK

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. Des administrateurs IAM contrôlent les personnes qui peuvent être authentifiées (connectées) et autorisées (disposant d'autorisations) à utiliser des ressources Amazon MSK. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Cette page décrit comment vous pouvez utiliser IAM pour contrôler qui peut effectuer des opérations Amazon MSK sur votre cluster. Pour plus d'informations sur le contrôle des personnes autorisées à effectuer des opérations Apache Kafka sur votre cluster, consultez the section called “Authentification et autorisation pour les API Apache Kafka”.

Rubriques

- Fonctionnement d'Amazon MSK avec IAM
- Exemples de politiques basées sur l'identité d'Amazon MSK
- Utilisation des rôles liés à un service pour Amazon MSK
- AWS politiques gérées pour Amazon MSK
- Résolution de problèmes pour identité et accès Amazon MSK

Fonctionnement d'Amazon MSK avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon MSK, vous devez comprendre quelles sont les fonctionnalités IAM pouvant être utilisées dans cette situation. Pour obtenir une vue d'ensemble de la

manière dont Amazon MSK et les autres AWS services fonctionnent avec IAM, consultez la section AWS Services That Work with IAM dans le guide de l'utilisateur IAM.

Rubriques

Politiques basées sur l'identité Amazon MSK

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. Amazon MSK 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, consultez 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 dans Amazon MSK utilisent le préfixe suivant avant l'action : `kafka:`. Par exemple, pour accorder à une personne l'autorisation de décrire un cluster MSK avec l'opération d'API Amazon MSK `DescribeCluster`, vous incluez l'action `kafka:DescribeCluster` dans

sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Amazon MSK définit son propre ensemble d'actions qui décrivent 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": ["kafka:action1", "kafka: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 `Describe`, incluez l'action suivante :

```
"Action": "kafka:Describe*"
```

Pour afficher la liste des actions Amazon MSK, consultez Actions, ressources et clés de condition pour Amazon Managed Streaming for Apache Kafka 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 auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne 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": "*"
```

La ressource d'instance Amazon MSK possède l'ARN suivant :

```
arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${UUID}
```

Pour plus d'informations sur le format des ARN, consultez les sections Amazon Resource Names (ARN) et AWS Service Namespaces.

Par exemple, pour spécifier l'instance `CustomerMessages` dans votre instruction, utilisez l'ARN suivant :

```
"Resource": "arn:aws:kafka:us-east-1:123456789012:cluster/CustomerMessages/abcd1234-abcd-dcba-4321-a1b2abcd9f9f-2"
```

Pour spécifier toutes les instances qui appartiennent à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:kafka:us-east-1:123456789012:cluster/*"
```

Certaines actions Amazon MSK, telles que celles destinées à la création de ressources, ne peuvent pas être exécutées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

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

Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": ["resource1", "resource2"]
```

Pour afficher une liste des types de ressources Amazon MSK et de leurs ARN, consultez Ressources définies par Amazon Managed Streaming for Apache Kafka dans le Guide de l'utilisateur IAM. Pour savoir les actions avec lesquelles vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon Managed Streaming for Apache Kafka.

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.

Amazon MSK définit son propre ensemble de clés de condition et est également compatible avec l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, consultez la section Clés contextuelles de condition AWS globale dans le guide de l'utilisateur IAM.

Pour afficher une liste des clés de condition Amazon MSK, consultez Clés de condition pour Amazon Managed Streaming for Apache Kafka dans le Guide de l'utilisateur IAM. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon Managed Streaming for Apache Kafka.

Exemples

Pour voir des exemples de politiques Amazon MSK basées sur l'identité, consultez Exemples de politiques basées sur l'identité d'Amazon MSK.

Politiques basées sur des ressources Amazon MSK

Amazon MSK prend en charge une politique de cluster (également appelée politique basée sur des ressources) à utiliser avec les clusters Amazon MSK. Vous pouvez utiliser une politique de cluster pour définir quels principaux IAM disposent d'autorisations intercompte pour configurer une

connectivité privée avec votre cluster Amazon MSK. Lorsqu'elle est utilisée avec l'authentification du client IAM, vous pouvez également utiliser la politique de cluster pour définir de manière granulaire les autorisations de plan de données Kafka pour les clients qui se connectent.

Pour voir un exemple de configuration d'une politique de cluster, reportez-vous à Étape 2 : attacher une politique de cluster au cluster MSK.

AWS politiques gérées

Autorisation basée sur les balises Amazon MSK

Vous pouvez attacher des balises aux clusters Amazon MSK. Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `kafka:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Pour plus d'informations sur le balisage des ressources Amazon MSK, consultez the section called "Balisage d'un cluster".

Pour visualiser un exemple de stratégie basée sur l'identité permettant de limiter l'accès à un cluster en fonction des balises de ce cluster, consultez Accès aux clusters Amazon MSK à l'aide de balises.

Rôles IAM Amazon MSK

Un rôle IAM est une entité au sein de votre compte Amazon Web Services qui dispose d'autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec Amazon MSK

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.

Amazon MSK prend en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

Les rôles liés à un service permettent aux services Amazon Web Services d'accéder à des ressources dans 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 peut consulter, mais ne peut pas modifier les autorisations concernant les rôles liés à un service.

Amazon MSK prend en charge les rôles liés à un service. Pour plus d'informations sur la création ou la gestion de rôles liés à un service dans Amazon MSK, consultez the section called “Rôles liés à un service”.

Exemples de politiques basées sur l'identité d'Amazon MSK

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à effectuer des actions d'API Amazon MSK. Un administrateur 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.

Rubriques

- Bonnes pratiques en matière de politiques
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Accès à un cluster Amazon MSK
- Accès aux clusters Amazon MSK à l'aide de balises

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Amazon MSK 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 plus d’informations, consultez politiques gérées par AWS ou politiques gérées par 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 plus d'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 plus d'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.

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": "*"
        }
    ]
}
```

Accès à un cluster Amazon MSK

Dans cet exemple, vous souhaitez accorder à un utilisateur IAM de votre compte Amazon Web Services l'accès à l'un de vos clusters, `purchaseQueriesCluster`. Cette stratégie permet à l'utilisateur de décrire le cluster, d'obtenir ses brokers d'amorçage, de répertorier ses nœuds de broker et de le mettre à jour.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"UpdateCluster",
         "Effect":"Allow",
```

```
         "Action":[
            "kafka:Describe*",
            "kafka:Get*",
            "kafka:List*",
            "kafka:Update*"
         ],
         "Resource":"arn:aws:kafka:us-east-1:012345678012:cluster/
purchaseQueriesCluster/abcdefab-1234-abcd-5678-cdef0123ab01-2"
      }
   ]
}
```

Accès aux clusters Amazon MSK à l'aide de balises

Vous pouvez utiliser des conditions dans votre politique basée sur l'identité pour contrôler l'accès aux ressources Amazon MSK en fonction des balises. Cet exemple montre comment créer une stratégie qui permet à l'utilisateur de décrire le cluster, d'obtenir ses brokers d'amorçage, de répertorier ses nœuds de broker, de le mettre à jour et de le supprimer. Toutefois, l'autorisation est accordée uniquement si la balise de cluster `Owner` a la valeur du nom d'utilisateur de cet utilisateur.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AccessClusterIfOwner",
      "Effect": "Allow",
      "Action": [
        "kafka:Describe*",
        "kafka:Get*",
        "kafka:List*",
        "kafka:Update*",
        "kafka:Delete*"
      ],
      "Resource": "arn:aws:kafka:us-east-1:012345678012:cluster/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Owner": "${aws:username}"
        }
      }
    }
  ]
}
```

Vous pouvez rattacher cette politique aux utilisateurs IAM de votre compte. Si un utilisateur nommé `richard-roe` tente de mettre à jour un cluster MSK, le cluster doit être balisé `0wner=richard-roe` ou `owner=richard-roe`. Dans le cas contraire, l'utilisateur se voit refuser l'accès. La clé de condition d'étiquette `0wner` correspond à la fois à `0wner` et à `owner`, car les noms de clé de condition ne sont pas sensibles à la casse. Pour plus d'informations, veuillez consulter la rubrique Éléments de stratégie JSON IAM : Condition dans le Guide de l'utilisateur IAM.

Utilisation des rôles liés à un service pour Amazon MSK

Amazon MSK utilise des rôles liés à un service AWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM qui est lié directement à Amazon MSK. Les rôles liés à un service sont prédéfinis par Amazon MSK et incluent toutes les autorisations requises par le service pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service simplifie la configuration d'Amazon MSK, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Amazon MSK définit les autorisations de ses rôles liés à un service. Sauf indication contraire, seul Amazon MSK peut assumer 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.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services Amazon Web Services qui fonctionnent avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Rubriques

- Autorisations du rôle lié à un service pour Amazon MSK
- Création d'un rôle lié à un service pour Amazon MSK
- Modification d'un rôle lié à un service pour Amazon MSK
- Régions prises en charge pour les rôles liés à un service Amazon MSK

Autorisations du rôle lié à un service pour Amazon MSK

Amazon MSK utilise le rôle lié à un service nommé AWSServiceRoleForKafka. Amazon MSK utilise ce rôle pour accéder à vos ressources et effectuer des opérations telles que :

- `*NetworkInterface` - créer et gérer des interfaces réseau dans le compte client qui rendent les agents de cluster accessibles aux clients dans le VPC du client.

- `*VpcEndpoints`— gérez les points de terminaison VPC dans le compte client afin de rendre les courtiers de clusters accessibles aux clients utilisant le VPC du client. AWS PrivateLink Amazon MSK utilise des autorisations pour `DescribeVpcEndpoints`, `ModifyVpcEndpoint` et `DeleteVpcEndpoints`.
- `secretsmanager`— gérez les informations d'identification des clients avec AWS Secrets Manager.
- `GetCertificateAuthorityCertificate` - récupérer le certificat pour votre autorité de certification privée.

Ce rôle lié à un service est attaché à la politique gérée suivante : `KafkaServiceRolePolicy`. Pour les mises à jour de cette politique, consultez KafkaServiceRolePolicy.

Le rôle lié à un service AWSServiceRoleForKafka approuve les services suivants pour endosser le rôle :

- `kafka.amazonaws.com`

La politique d'autorisations liée au rôle permet à Amazon MSK de réaliser les actions suivantes au niveau des ressources.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:CreateNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:AttachNetworkInterface",
    "ec2:DeleteNetworkInterface",
    "ec2:DetachNetworkInterface",
    "ec2:DescribeVpcEndpoints",
    "acm-pca:GetCertificateAuthorityCertificate",
    "secretsmanager:ListSecrets"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
```

```
    "Action": [
     "ec2:ModifyVpcEndpoint"
    ],
    "Resource": "arn:*:ec2:*:*:subnet/*"
   },
   {
    "Effect": "Allow",
    "Action": [
     "ec2:DeleteVpcEndpoints",
     "ec2:ModifyVpcEndpoint"
    ],
    "Resource": "arn:*:ec2:*:*:vpc-endpoint/*",
    "Condition": {
     "StringEquals": {
      "ec2:ResourceTag/AWSMSKManaged": "true"
     },
     "StringLike": {
      "ec2:ResourceTag/ClusterArn": "*"
     }
    }
   },
   {
    "Effect": "Allow",
    "Action": [
     "secretsmanager:GetResourcePolicy",
     "secretsmanager:PutResourcePolicy",
     "secretsmanager:DeleteResourcePolicy",
     "secretsmanager:DescribeSecret"
    ],
    "Resource": "*",
    "Condition": {
     "ArnLike": {
      "secretsmanager:SecretId": "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
     }
    }
   }
  ]
}
```

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 Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à un service pour Amazon MSK

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un cluster Amazon MSK dans l'API AWS Management Console, dans le AWS CLI ou dans l' AWS API, Amazon MSK crée le rôle lié au service pour vous.

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 un cluster Amazon MSK, Amazon MSK crée à nouveau automatiquement le rôle lié au service.

Modification d'un rôle lié à un service pour Amazon MSK

Amazon MSK ne vous autorise pas à modifier le rôle lié à un service AWSServiceRoleForKafka. 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 plus d'informations, consultez Modification 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 Amazon MSK

Amazon MSK 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 AWS Régions et points de terminaison.

AWS politiques gérées pour Amazon MSK

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les 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.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service

AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonMSK FullAccess

Cette politique accorde des autorisations administratives qui permettent à un principal d'accéder pleinement à toutes les actions Amazon MSK. Les autorisations définies dans cette politique sont regroupées comme suit :

- Les autorisations Amazon MSK autorisent toutes les actions Amazon MSK.
- **`Amazon EC2`**autorisations : dans cette politique, elles sont requises pour valider les ressources transmises dans une demande d'API. Cela permet de s'assurer qu'Amazon MSK est en mesure d'utiliser correctement les ressources avec un cluster. Les autres autorisations Amazon EC2 de cette politique permettent à Amazon MSK de créer les AWS ressources nécessaires pour vous permettre de vous connecter à vos clusters.
- **`AWS KMS`**autorisations — sont utilisées lors des appels d'API pour valider les ressources transmises dans une demande. Elles sont nécessaires pour qu'Amazon MSK puisse utiliser la clé transmise avec le cluster Amazon MSK.
- **`CloudWatch Logs, Amazon S3, and Amazon Data Firehose`**autorisations : elles sont nécessaires pour qu'Amazon MSK puisse s'assurer que les destinations de livraison des journaux sont accessibles et qu'elles sont valides pour l'utilisation des journaux des courtiers.
- **`IAM`**autorisations : elles sont nécessaires pour qu'Amazon MSK puisse créer un rôle lié à un service dans votre compte et pour vous permettre de transmettre un rôle d'exécution de service à Amazon MSK.

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": [
    "kafka:*",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "S3:GetBucketPolicy",
        "firehose:TagDeliveryStream"
       ],
       "Resource": "*"
      },
      {
       "Effect": "Allow",
       "Action": [
        "ec2:CreateVpcEndpoint"
       ],
       "Resource": [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
       ]
      },
      {
       "Effect": "Allow",
       "Action": [
        "ec2:CreateVpcEndpoint"
       ],
       "Resource": [
        "arn:*:ec2:*:*:vpc-endpoint/*"
       ],
       "Condition": {
        "StringEquals": {
         "aws:RequestTag/AWSMSKManaged": "true"
        },
        "StringLike": {
         "aws:RequestTag/ClusterArn": "*"
        }
       }
```

```
      },
      {
       "Effect": "Allow",
       "Action": [
        "ec2:CreateTags"
       ],
       "Resource": "arn:*:ec2:*:*:vpc-endpoint/*",
       "Condition": {
        "StringEquals": {
         "ec2:CreateAction": "CreateVpcEndpoint"
        }
       }
      },
      {
       "Effect": "Allow",
       "Action": [
        "ec2:DeleteVpcEndpoints"
       ],
       "Resource": "arn:*:ec2:*:*:vpc-endpoint/*",
       "Condition": {
        "StringEquals": {
         "ec2:ResourceTag/AWSMSKManaged": "true"
        },
        "StringLike": {
         "ec2:ResourceTag/ClusterArn": "*"
        }
       }
      },
      {
       "Effect": "Allow",
       "Action": "iam:PassRole",
       "Resource": "*",
       "Condition": {
        "StringEquals": {
         "iam:PassedToService": "kafka.amazonaws.com"
        }
       }
      },
      {
       "Effect": "Allow",
       "Action": "iam:CreateServiceLinkedRole",
       "Resource": "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*",
       "Condition": {
```

```
        "StringLike": {
         "iam:AWSServiceName": "kafka.amazonaws.com"
        }
       }
      },
      {
       "Effect": "Allow",
       "Action": [
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
       ],
       "Resource": "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*"
      },
      {
       "Effect": "Allow",
       "Action": "iam:CreateServiceLinkedRole",
       "Resource": "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery*",
       "Condition": {
        "StringLike": {
         "iam:AWSServiceName": "delivery.logs.amazonaws.com"
        }
       }
      }

     ]
    }
```

AWS politique gérée : AmazonMSK Access ReadOnly

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de consulter des informations dans Amazon MSK. Les principaux auxquels cette politique est attachée ne peuvent effectuer aucune mise à jour ou supprimer des ressources existantes, ni créer de nouvelles ressources Amazon MSK. Par exemple, les principaux disposant de ces autorisations peuvent consulter la liste des clusters et des configurations associés à leur compte, mais ne peuvent pas modifier la configuration ou les paramètres des clusters. Les autorisations définies dans cette politique sont regroupées comme suit :

- **`Amazon MSK`**autorisations : vous permettent de répertorier les ressources Amazon MSK, de les décrire et d'obtenir des informations à leur sujet.

- **`Amazon EC2`**autorisations : sont utilisées pour décrire le VPC Amazon, les sous-réseaux, les groupes de sécurité et les ENI associés à un cluster.
- **`AWS KMS`**permission — est utilisée pour décrire la clé associée au cluster.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "kafka:Describe*",
                "kafka:List*",
                "kafka:Get*",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS politique gérée : KafkaServiceRolePolicy

Vous ne pouvez pas vous associer KafkaServiceRolePolicy à vos entités IAM. Cette politique est attachée à un rôle lié à un service qui permet à Amazon MSK d'effectuer des actions telles que la gestion des points de terminaison de VPC (connecteurs) sur les clusters MSK, la gestion des interfaces réseau et la gestion des informations d'identification du cluster avec AWS Secrets Manager. Pour plus d’informations, consultez the section called “Rôles liés à un service”.

AWS politique gérée : AWSMSKReplicatorExecutionRole

La `AWSMSKReplicatorExecutionRole` politique accorde des autorisations au réplicateur Amazon MSK pour répliquer les données entre les clusters MSK. Les autorisations définies dans cette politique sont regroupées comme suit :

- **`cluster`**— Accorde à Amazon MSK Replicator l'autorisation de se connecter au cluster à l'aide de l'authentification IAM. Accorde également les autorisations nécessaires pour décrire et modifier le cluster.
- **`topic`**— Accorde à Amazon MSK Replicator les autorisations nécessaires pour décrire, créer et modifier un sujet, ainsi que pour modifier la configuration dynamique du sujet.
- **`consumer group`**— Accorde à Amazon MSK Replicator l'autorisation de décrire et de modifier les groupes de consommateurs, de lire et d'écrire la date d'un cluster MSK et de supprimer les sujets internes créés par le réplicateur.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ClusterPermissions",
   "Effect": "Allow",
   "Action": [
    "kafka-cluster:Connect",
    "kafka-cluster:DescribeCluster",
    "kafka-cluster:AlterCluster",
    "kafka-cluster:DescribeTopic",
    "kafka-cluster:CreateTopic",
    "kafka-cluster:AlterTopic",
    "kafka-cluster:WriteData",
    "kafka-cluster:ReadData",
    "kafka-cluster:AlterGroup",
    "kafka-cluster:DescribeGroup",
    "kafka-cluster:DescribeTopicDynamicConfiguration",
    "kafka-cluster:AlterTopicDynamicConfiguration",
    "kafka-cluster:WriteDataIdempotently"
   ],
   "Resource": [
    "arn:aws:kafka:*:*:cluster/*"
   ]
  },
  {
   "Sid": "TopicPermissions",
   "Effect": "Allow",
   "Action": [
    "kafka-cluster:DescribeTopic",
    "kafka-cluster:CreateTopic",
    "kafka-cluster:AlterTopic",
```

```
    "kafka-cluster:WriteData",
    "kafka-cluster:ReadData",
    "kafka-cluster:DescribeTopicDynamicConfiguration",
    "kafka-cluster:AlterTopicDynamicConfiguration",
    "kafka-cluster:AlterCluster"
   ],
   "Resource": [
    "arn:aws:kafka:*:*:topic/*/*"
   ]
  },
  {
   "Sid": "GroupPermissions",
   "Effect": "Allow",
   "Action": [
    "kafka-cluster:AlterGroup",
    "kafka-cluster:DescribeGroup"
   ],
   "Resource": [
    "arn:aws:kafka:*:*:group/*/*"
   ]
  }
 ]
}
```

Amazon MSK met à jour les politiques AWS gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon MSK depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
WriteDataIdempotently autorisation ajoutée à AWSMSKReplicatorExecutionRole — Mise à jour d'une politique existante	Amazon MSK a ajouté WriteDataIdempotently l'autorisation à la AWSMSKReplicatorExecutionRole politique pour prendre en charge la réplication des données entre les clusters MSK.	12 mars 2024

Modification	Description	Date
AWSMSKReplicatorExecutionRole : nouvelle politique	Amazon MSK a ajouté une AWSMSKReplicatorExecutionRole politique pour prendre en charge Amazon MSK Replicator.	4 décembre 2023
AmazonMSK FullAccess — Mise à jour d'une politique existante	Amazon MSK a ajouté des autorisations pour prendre en charge le réplicateur Amazon MSK.	28 septembre 2023
KafkaServiceRolePolicy – Mise à jour d'une politique existante	Amazon MSK a ajouté des autorisations pour prendre en charge la connectivité privée à plusieurs VPC.	8 mars 2023
AmazonMSK FullAccess — Mise à jour d'une politique existante	Amazon MSK a ajouté de nouvelles autorisations Amazon EC2 pour permettre la connexion à un cluster.	30 novembre 2021
AmazonMSK FullAccess — Mise à jour d'une politique existante	Amazon MSK a ajouté une nouvelle autorisation lui permettant de décrire les tables de routage Amazon EC2.	19 novembre 2021
Amazon MSK a commencé à assurer le suivi des modifications	Amazon MSK a commencé à suivre les modifications apportées à ses politiques AWS gérées.	19 novembre 2021

Résolution de problèmes pour identité et accès Amazon MSK

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous utilisez Amazon MSK et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Amazon MSK

Je ne suis pas autorisé à effectuer une action dans Amazon MSK

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 vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur IAM `mateojackson` tente d'utiliser la console pour supprimer un cluster, mais ne dispose pas des autorisations `kafka:DeleteCluster`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 kafka:DeleteCluster on resource: purchaseQueriesCluster
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource `purchaseQueriesCluster` à l'aide de l'action `kafka:DeleteCluster`.

Authentification et autorisation pour les API Apache Kafka

Vous pouvez utiliser IAM pour authentifier les clients et autoriser ou refuser des actions Apache Kafka. Vous pouvez également utiliser TLS ou SASL/SCRAM pour authentifier les clients et les listes de contrôle d'accès (ACL) Apache Kafka pour autoriser ou refuser des actions.

Pour plus d'informations sur le contrôle des personnes autorisées à effectuer des opérations Amazon MSK sur votre cluster, consultez the section called "Authentification et autorisation pour les API Amazon MSK".

Rubriques

- Contrôle d'accès IAM
- Authentification TLS mutuelle
- Authentification des identifiants de connexion avec AWS Secrets Manager

- Listes de contrôle d'accès (ACL) Apache Kafka

Contrôle d'accès IAM

Le contrôle d'accès IAM pour Amazon MSK vous permet de gérer à la fois l'authentification et l'autorisation pour votre cluster MSK. Cela élimine la nécessité d'utiliser un mécanisme unique pour l'authentification et un autre pour l'autorisation. Par exemple, lorsqu'un client tente d'écrire sur votre cluster, Amazon MSK utilise IAM pour vérifier si ce client est une identité authentifiée et s'il est autorisé à produire sur votre cluster. Le contrôle d'accès IAM fonctionne pour les clients Java et non-Java, y compris les clients Kafka écrits en Python JavaScript, Go et .NET.

Amazon MSK journalise les événements d'accès afin que vous puissiez les contrôler. Pour plus d'informations, consultez the section called “CloudTrail événements”.

Pour rendre le contrôle d'accès IAM possible, Amazon MSK apporte des modifications mineures au code source d'Apache Kafka. Ces modifications n'entraîneront pas de différence notable dans votre expérience avec Apache Kafka.

Important

Le contrôle d'accès IAM ne s'applique pas aux ZooKeeper nœuds Apache. Pour plus d'informations sur la manière de contrôler l'accès à ces nœuds, consultez the section called “Contrôle de l'accès à Apache ZooKeeper”.

Important

Le paramètre Apache Kafka `allow.everyone.if.no.acl.found` n'a aucun effet si votre cluster utilise le contrôle d'accès IAM.

Important

Vous pouvez invoquer les API ACL Apache Kafka pour un cluster MSK qui utilise le contrôle d'accès IAM. Cependant, les ACL Apache Kafka n'ont aucun effet sur l'autorisation pour les rôles IAM. Vous devez utiliser des politiques IAM pour le contrôle d'accès des rôles IAM.

Fonctionnement du contrôle d'accès IAM pour Amazon MSK

Pour utiliser le contrôle d'accès IAM pour Amazon MSK, effectuez les étapes suivantes, décrites en détail dans le reste de cette section.

- the section called “Créer un cluster qui utilise le contrôle d'accès IAM”
- the section called “Configurer les clients pour le contrôle d'accès IAM”
- the section called “Créer des politiques d'autorisation”
- the section called “Obtenez les agents d'amorçage pour le contrôle d'accès IAM”

Créer un cluster qui utilise le contrôle d'accès IAM

Cette section explique comment vous pouvez utiliser l' AWS Management Console API ou le AWS CLI pour créer un cluster qui utilise le contrôle d'accès IAM. Pour plus d'informations sur l'activation du contrôle d'accès IAM pour un cluster existant, consultez the section called “Mise à jour de sécurité”.

Utilisez le AWS Management Console pour créer un cluster qui utilise le contrôle d'accès IAM

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez Créer un cluster.
3. Choisissez Créer un cluster avec des paramètres personnalisés.
4. Dans la section Authentification, choisissez Contrôle d'accès IAM.
5. Suivez le reste du flux de travail pour créer un cluster.

Utilisez l'API ou le AWS CLI pour créer un cluster qui utilise le contrôle d'accès IAM

- Pour créer un cluster avec le contrôle d'accès IAM activé, utilisez l'CreateClusterAPI ou la commande create-cluster CLI et transmettez le JSON suivant pour `ClientAuthentication` le paramètre :. `"ClientAuthentication": { "Sasl": { "Iam": { "Enabled": true } }`

Configurer les clients pour le contrôle d'accès IAM

Pour permettre aux clients de communiquer avec un cluster MSK qui utilise le contrôle d’accès IAM, vous pouvez utiliser l’un des mécanismes suivants :

- Configuration du client non Java à l'aide du mécanisme SASL_OAUTHBEARER
- Configuration du client Java à l'aide du mécanisme SASL_OAUTHBEARER ou AWS_MSK_IAM

Utilisation du mécanisme SASL_OAUTHBEARER pour configurer IAM

1. Modifiez votre fichier de configuration client.properties en utilisant la syntaxe surlignée dans l'exemple de client Python Kafka ci-dessous à titre de guide. Les modifications de configuration sont similaires dans les autres langages.

```
#!/usr/bin/python3from kafka import KafkaProducer
from kafka.errors import KafkaError
import socket
import time
from aws_msk_iam_sasl_signer import MSKAuthTokenProvider

class MSKTokenProvider():
    def token(self):
        token, _ = MSKAuthTokenProvider.generate_auth_token('<my aws region>')
        return token

tp = MSKTokenProvider()

producer = KafkaProducer(
    bootstrap_servers='<my bootstrap string>',
    security_protocol='SASL_SSL',
    sasl_mechanism='OAUTHBEARER',
    sasl_oauth_token_provider=tp,
    client_id=socket.gethostname(),
)

topic = "<my-topic>"
while True:
    try:
        inp=input(">")
        producer.send(topic, inp.encode())
        producer.flush()
        print("Produced!")
    except Exception:
        print("Failed to send message:", e)

producer.close()
```

2. Téléchargez la bibliothèque d'assistance correspondant à la langue de configuration que vous avez choisie et suivez les instructions de la section Démarrage de la page d'accueil de cette bibliothèque de langages.
   - JavaScript: https://github.com/aws/aws-msk-iam-sasl-signer-js#getting-started
   - Python : https://github.com/aws/aws-msk-iam-sasl-signer-python#get-started
   - Go : https://github.com/aws/aws-msk-iam-sasl-signer-go#getting-started
   - .NET : https://github.com/aws/aws-msk-iam-sasl-signer-net#getting-started
   - JAVA : la prise en charge de SASL_OAUTHBEARER pour Java est disponible via le fichier jar `aws-msk-iam-auth`

Utilisation du mécanisme personnalisé AWS_MSK_IAM de MSK pour configurer IAM

1. Ajoutez ce qui suit dans le fichier `client.properties`. Remplacez *<PATH_TO_TRUST_STORE_FILE>* par le chemin d'accès qualifié complet vers le fichier de magasin d'approbations sur le client.

   > **Note**
   >
   > Si vous ne souhaitez pas utiliser un certificat spécifique, vous pouvez supprimer `ssl.truststore.location=`*<PATH_TO_TRUST_STORE_FILE>* de votre fichier `client.properties`. Si vous ne spécifiez aucune valeur pour `ssl.truststore.location`, le processus Java utilise le certificat par défaut.

   ```
   ssl.truststore.location=<PATH_TO_TRUST_STORE_FILE>
   security.protocol=SASL_SSL
   sasl.mechanism=AWS_MSK_IAM
   sasl.jaas.config=software.amazon.msk.auth.iam.IAMLoginModule required;
   sasl.client.callback.handler.class=software.amazon.msk.auth.iam.IAMClientCallbackHandler
   ```

   Pour utiliser un profil nommé que vous avez créé pour les AWS informations d'identification, `awsProfileName="`*your profile name*`";` incluez-le dans votre fichier de configuration client. Pour plus d'informations sur les profils nommés, consultez la section Profils nommés dans la AWS CLI documentation.

2. Téléchargez le dernier fichier JAR stable aws-msk-iam-auth et placez-le dans le chemin de classe. Si vous utilisez Maven, ajoutez la dépendance suivante, en ajustant le numéro de version selon les besoins :

```
<dependency>
    <groupId>software.amazon.msk</groupId>
    <artifactId>aws-msk-iam-auth</artifactId>
    <version>1.0.0</version>
</dependency>
```

Le plug-in client Amazon MSK est open source sous la licence Apache 2.0.

Créer des politiques d'autorisation

Attachez une politique d'autorisation au rôle IAM qui correspond au client. Dans une politique d'autorisation, vous spécifiez les actions à autoriser ou à refuser pour le rôle. Si votre client utilise une instance Amazon EC2, associez la politique d'autorisation au rôle IAM pour cette instance Amazon EC2. Vous pouvez également configurer votre client pour qu'il utilise un profil nommé, puis associer la politique d'autorisation au rôle de ce profil nommé. the section called “Configurer les clients pour le contrôle d'accès IAM” décrit comment configurer un client pour utiliser un profil nommé.

Pour plus d'informations sur la création d'une politique IAM, consultez Création de politiques IAM.

Voici un exemple de politique d'autorisation pour un cluster nommé MyTestCluster. Pour comprendre la sémantique des éléments `Action` et `Resource`, consultez the section called “Sémantique des actions et des ressources”.

> **Important**
>
> Les modifications que vous apportez à une politique IAM sont immédiatement reflétées dans les API IAM et l' AWS CLI . Cependant, la modification de la politique peut prendre un certain temps avant d'être effective. Dans la plupart des cas, les modifications de politique prennent effet en moins d'une minute. Les conditions du réseau peuvent parfois augmenter le délai.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:AlterCluster",
                "kafka-cluster:DescribeCluster"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:0123456789012:cluster/MyTestCluster/
abcd1234-0123-abcd-5678-1234abcd-1"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:*Topic*",
                "kafka-cluster:WriteData",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:0123456789012:topic/MyTestCluster/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeGroup"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:0123456789012:group/MyTestCluster/*"
            ]
        }
    ]
}
```

Pour savoir comment créer une politique avec des éléments d'action correspondant aux cas d'utilisation courants d'Apache Kafka, tels que la production et la consommation de données, consultez the section called “Cas d’utilisation courants”.

Pour les versions 2.8.0 et supérieures de Kafka, l'autorisation WriteDataIdempotently est obsolète (KIP-679). Par défaut, `enable.idempotence = true` est défini. Par conséquent, pour les versions 2.8.0 et supérieures de Kafka, IAM n'offre pas les mêmes fonctionnalités que les listes de contrôle

d'accès (ACL) Kafka. Il n'est pas possible de définir `WriteDataIdempotently` à une rubrique en fournissant uniquement un accès `WriteData` à cette rubrique. Cela n'affecte pas le cas lorsque `WriteData` est fourni à TOUTES les rubriques. Dans ce cas, `WriteDataIdempotently` est autorisé. Cela est dû à des différences dans l'implémentation de la logique IAM par rapport à la manière dont les listes de contrôle d'accès (ACL) Kafka sont implémentées.

Pour contourner ce problème, nous vous recommandons d'utiliser une politique similaire à l'exemple ci-dessous :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:AlterCluster",
                "kafka-cluster:DescribeCluster",
                "kafka-cluster:WriteDataIdempotently"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:0123456789012:cluster/MyTestCluster/
abcd1234-0123-abcd-5678-1234abcd-1"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:*Topic*",
                "kafka-cluster:WriteData",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:0123456789012:topic/MyTestCluster/
abcd1234-0123-abcd-5678-1234abcd-1/TestTopic"
            ]
        }
    ]
}
```

Dans ce cas, `WriteData` autorise les écritures vers la `TestTopic`, pendant que `WriteDataIdempotently` autorise les écritures idempotentes sur le cluster. Il est important de

noter que `WriteDataIdempotently` est une autorisation au niveau du cluster. Il ne peut pas être utilisé au niveau de la rubrique. Si `WriteDataIdempotently` est limité au niveau de la rubrique, cette politique ne fonctionnera pas.

Obtenez les agents d'amorçage pour le contrôle d'accès IAM

veuillez consulter the section called “Obtention des agents d'amorçage”.

Sémantique des actions et des ressources

Cette section explique la sémantique des éléments d'action et de ressource que vous pouvez utiliser dans une politique d'autorisation IAM. Pour un exemple de politique, consultez the section called “Créer des politiques d'autorisation”.

Actions

Le tableau suivant répertorie les actions que vous pouvez inclure dans une politique d'autorisation lorsque vous utilisez le contrôle d'accès IAM pour Amazon MSK. Lorsque vous incluez dans votre politique d'autorisation une action de la colonne Action du tableau, vous devez également inclure les actions correspondantes de la colonne Actions requises.

Action	Description	Actions requises	Ressources requises	Applicable aux clusters sans serveur
`kafka-cluster:Connect`	Octroie l'autorisation de se connecter et de s'authentifier à un cluster.	Aucun	cluster	Oui
`kafka-cluster:DescribeCluster`	Octroie l'autorisation de décrire divers aspects du cluster, équivalent à l'ACL DESCRIBE	`kafka-cluster:Connect`	cluster	Oui

Action	Description	Actions requises	Ressources requises	Applicable aux clusters sans serveur
	CLUSTER d'Apache Kafka.			
`kafka-cluster:AlterCluster`	Octroi l'autorisation de modifier divers aspects du cluster, équivalent à l'ACL ALTER CLUSTER d'Apache Kafka.	`kafka-cluster:Connect` `kafka-cluster:DescribeCluster`	cluster	Non
`kafka-cluster:DescribeClusterDynamicConfiguration`	Octroie l'autorisation de décrire la configuration dynamique d'un cluster, équivalent à l'ACL DESCRIBE_CONFIGS CLUSTER d'Apache Kafka.	`kafka-cluster:Connect`	cluster	Non

Action	Description	Actions requises	Ressources requises	Applicable aux clusters sans serveur
`kafka-cluster:AlterClusterDynamicConfiguration`	Octroie l'autorisation de modifier la configuration dynamique d'un cluster, équivalente à l'ACL ALTER_CONFIGS CLUSTER d'Apache Kafka.	`kafka-cluster:Connect` `kafka-cluster:DescribeClusterDynamicConfiguration`	cluster	Non
`kafka-cluster:WriteDataIdempotently`	Octroie l'autorisation d'écrire des données de manière idempotente dans un cluster, équivalent à l'ACL IDEMPOTENT_WRITE CLUSTER d'Apache Kafka.	`kafka-cluster:Connect` `kafka-cluster:WriteData`	cluster	Oui
`kafka-cluster:CreateTopic`	Octroie l'autorisation de créer des rubriques dans un cluster, équivalent à l'ACL CREATE CLUSTER/TOPIC d'Apache Kafka.	`kafka-cluster:Connect`	topic	Oui

Action	Description	Actions requises	Ressources requises	Applicable aux clusters sans serveur
`kafka-cluster:DescribeTopic`	Octroie l'autorisation de décrire des rubriques dans un cluster, équivalent à l'ACL DESCRIBE TOPIC d'Apache Kafka.	`kafka-cluster:Connect`	topic	Oui
`kafka-cluster:AlterTopic`	Octroie l'autorisation de modifier des rubriques dans un cluster, équivalent à l'ACL ALTER TOPIC d'Apache Kafka.	`kafka-cluster:Connect` `kafka-cluster:DescribeTopic`	topic	Oui
`kafka-cluster:DeleteTopic`	Octroie l'autorisation de supprimer des rubriques dans un cluster, équivalent à l'ACL DELETE TOPIC d'Apache Kafka.	`kafka-cluster:Connect` `kafka-cluster:DescribeTopic`	topic	Oui

Action	Description	Actions requises	Ressources requises	Applicable aux clusters sans serveur
`kafka-cluster:DescribeTopicDynamicConfiguration`	Octroie l'autorisation de décrire la configuration dynamique des rubriques dans un cluster, équivalent à l'ACL DESCRIBE_CONFIGS TOPIC d'Apache Kafka.	`kafka-cluster:Connect`	topic	Oui

`kafka-cluster:AlterTopicDynamicConfiguration`	Octroie l'autorisation de modifier la configuration dynamique des rubriques dans un cluster, équivalent à l'ACL ALTER_CONFIGS TOPIC d'Apache Kafka.	`kafka-cluster:Connect`
		
		`kafka-cluster:DescribeTopicDynamicConfiguration`
			topic	Oui

Action	Description	Actions requises	Ressources requises	Applicable aux clusters sans serveur

`kafka-cluster:ReadData`	Octroie l'autorisation de lire des données provenant de rubriques dans un cluster, équivalent à l'ACL READ TOPIC d'Apache Kafka.	`kafka-cluster:Connect`
		`kafka-cluster:DescribeTopic`
		`kafka-cluster:AlterGroup`
			topic	Oui

`kafka-cluster:WriteData`	Autorise l'écriture des données dans les rubriques d'un cluster, équivalent à l'ACL WRITE TOPIC d'Apache Kafka.	`kafka-cluster:Connect` `kafka-cluster:DescribeTopic`	topic	Oui
`kafka-cluster:DescribeGroup`	Octroie l'autorisation de décrire des groupes dans un cluster, équivalent à l'ACL DESCRIBE GROUP d'Apache Kafka.	`kafka-cluster:Connect`	groupe	Oui

Action	Description	Actions requises	Ressources requises	Applicable aux clusters sans serveur
`kafka-cluster:AlterGroup`	Octroie l'autorisation de rejoindre des groupes dans un cluster, équivalent à l'ACL READ GROUP d'Apache Kafka.	`kafka-cluster:Connect` `kafka-cluster:DescribeGroup`	groupe	Oui
`kafka-cluster:DeleteGroup`	Octroie l'autorisation de supprimer des groupes d'un cluster, équivalent à l'ACL DELETE GROUP d'Apache Kafka.	`kafka-cluster:Connect` `kafka-cluster:DescribeGroup`	groupe	Oui
`kafka-cluster:DescribeTransactionalId`	Octroie l'autorisation de décrire des ID transactionnels dans un cluster, équivalent à l'ACL DESCRIBE TRANSACTIONAL_ID d'Apache Kafka.	`kafka-cluster:Connect`	transactional-id	Oui

Action	Description	Actions requises	Ressources requises	Applicable aux clusters sans serveur

`kafka-cluster:AlterTransactionalId`	Octroie l'autorisation de modifier des ID transactionnels dans un cluster, équivalent à l'ACL WRITE TRANSACTIONAL_ID d'Apache Kafka.	`kafka-cluster:Connect`
		
		`kafka-cluster:DescribeTransactionalId`
		
		`kafka-cluster:WriteData`
			transactional-id	Oui

Vous pouvez utiliser le caractère générique astérisque (*) autant de fois que vous le souhaitez dans une action après deux points. Voici quelques exemples.

- `kafka-cluster:*Topic` représente `kafka-cluster:CreateTopic`, `kafka-cluster:DescribeTopic`, `kafka-cluster:AlterTopic` et `kafka-cluster:DeleteTopic`. Cela n'inclut pas `kafka-cluster:DescribeTopicDynamicConfiguration` ou `kafka-cluster:AlterTopicDynamicConfiguration`.
- `kafka-cluster:*` représente toutes les autorisations.

Ressources

Le tableau suivant montre les quatre types de ressources que vous pouvez utiliser dans une politique d'autorisation lorsque vous utilisez le contrôle d'accès IAM pour Amazon MSK. Vous pouvez obtenir le nom de ressource Amazon (ARN) du cluster à partir du AWS Management Console ou en utilisant l'DescribeClusterAPI ou la commande describe-cluster AWS CLI . Vous pouvez ensuite utiliser l'ARN du cluster pour construire des ARN de rubrique, de groupe et d'ID transactionnel. Pour spécifier une ressource dans une politique d'autorisation, utilisez l'ARN de cette ressource.

Ressource	Format ARN
Cluster	arn:aws:kafka:*region*:*account-id* :cluster/*cluster-name* /*cluster-uuid*
Rubrique	arn:aws:kafka:*region*:*account-id* :topic/*cluster-name* /*cluster-uuid* /*topic-name*
Groupe	arn:aws:kafka:*region*:*account-id* :group/*cluster-name* /*cluster-uuid* /*group-name*
ID transactionnel	arn:aws:kafka:*region*:*account-id* :transactional-id/*cluster-name* /*cluster-uuid* /*transactional-id*

Vous pouvez utiliser le caractère générique astérisque (*) autant de fois que vous le souhaitez dans la partie de l'ARN située après `:cluster/`, `:topic/`, `:group/` et `:transactional-id/`. Les exemples suivants illustrent la manière dont vous pouvez utiliser le caractère générique astérisque (*) pour faire référence à plusieurs ressources :

- `arn:aws:kafka:us-east-1:0123456789012:topic/MyTestCluster/*`: tous les sujets de n'importe quel cluster nommé MyTestCluster, quel que soit l'UUID du cluster.
- `arn:aws:kafka:us-east-1:0123456789012:topic/MyTestCluster/abcd1234-0123-abcd-5678-1234abcd-1/*_test`: toutes les rubriques dont le nom se termine par « _test » dans le cluster dont le nom est MyTestCluster et dont l'UUID est abcd1234-0123-abcd-5678-1234abcd-1.
- `arn:aws:kafka:us-east-1:0123456789012:transactional-id/MyTestCluster/*/5555abcd-1111-abcd-1234-abcd1234-1`: toutes les transactions dont l'ID transactionnel est 5555abcd-1111-abcd-1234-abcd1234-1, dans toutes les incarnations d'un cluster nommé dans votre compte. MyTestCluster Cela signifie que si vous créez un cluster nommé MyTestCluster, que vous le supprimez, puis que vous créez un autre cluster portant le même nom, vous pouvez utiliser cet ARN de ressource pour représenter le même identifiant de transaction sur les deux clusters. Cependant, le cluster supprimé n'est pas accessible.

Cas d’utilisation courants

La première colonne du tableau suivant présente certains cas d'utilisation courants. Pour autoriser un client à exécuter un cas d'utilisation donné, incluez les actions requises pour ce cas d'utilisation dans la politique d'autorisation du client et définissez `Effect` sur `Allow`.

Pour plus d'informations sur toutes les actions faisant partie du contrôle d'accès IAM pour Amazon MSK, consultez the section called “Sémantique des actions et des ressources”.

> **Note**
>
> Les actions sont refusées par défaut. Vous devez autoriser explicitement chaque action que vous souhaitez autoriser le client à effectuer.

Cas d’utilisation	Actions requises
Administrateur	`kafka-cluster:*`
Créer une rubrique	`kafka-cluster:Connect` `kafka-cluster:CreateTopic`

Produire des données	`kafka-cluster:Connect`
	`kafka-cluster:DescribeTopic`
	`kafka-cluster:WriteData`

Consommer des données	`kafka-cluster:Connect`
	`kafka-cluster:DescribeTopic`
	`kafka-cluster:DescribeGroup`
	`kafka-cluster:AlterGroup`
	`kafka-cluster:ReadData`

Produire des données de manière idempotente	`kafka-cluster:Connect`

Cas d’utilisation	Actions requises

	`kafka-cluster:DescribeTopic`
	
	`kafka-cluster:WriteData`
	
	`kafka-cluster:WriteDataIdempotently`

Produire des données de manière transactionnelle	`kafka-cluster:Connect`
	
	`kafka-cluster:DescribeTopic`
	
	`kafka-cluster:WriteData`
	
	`kafka-cluster:DescribeTransactionalId`
	
	`kafka-cluster:AlterTransactionalId`

Décrire la configuration d'un cluster	`kafka-cluster:Connect`
	
	`kafka-cluster:DescribeClusterDynamicConfiguration`

Mettre à jour la configuration d'un cluster	`kafka-cluster:Connect`
	
	`kafka-cluster:DescribeClusterDynamicConfiguration`
	
	`kafka-cluster:AlterClusterDynamicConfiguration`

Décrire la configuration d'une rubrique	`kafka-cluster:Connect`
	
	`kafka-cluster:DescribeTopicDynamicConfiguration`

Cas d'utilisation	Actions requises

Mettre à jour la configuration d'une rubrique	`kafka-cluster:Connect`
	
	`kafka-cluster:DescribeTopicDynamicConfiguration`
	
	`kafka-cluster:AlterTopicDynamicConfiguration`

Modifier une rubrique	`kafka-cluster:Connect`
	
	`kafka-cluster:DescribeTopic`
	
	`kafka-cluster:AlterTopic`

Authentification TLS mutuelle

Vous pouvez activer l'authentification client avec TLS pour les connexions entre vos applications et vos courtiers Amazon MSK. Pour utiliser l'authentification client, vous avez besoin d'une Autorité de certification privée AWS. Ils Autorité de certification privée AWS peuvent se trouver dans le même compte Compte AWS que celui de votre cluster ou dans un autre compte. Pour plus d'informations sur Autorité de certification privée AWS s, voir Création et gestion d'un Autorité de certification privée AWS.

> **Note**
>
> L'authentification TLS n'est pas disponible pour l'instant dans les régions Pékin et Ningxia.

Amazon MSK ne prend pas en charge les listes de révocation des certificats (CRL). Pour contrôler l'accès aux rubriques de votre cluster ou bloquer les certificats compromis, utilisez les ACL et les groupes de AWS sécurité Apache Kafka. Pour en savoir plus sur l'utilisation des listes de contrôle d'accès (ACL) Apache Kafka, consultez the section called “Listes de contrôle d'accès (ACL) Apache Kafka”.

Cette rubrique contient les sections suivantes :

- Pour créer un cluster prenant en charge l'authentification client

- Pour configurer un client pour utiliser l'authentification
- Pour produire et consommer des messages à l'aide de l'authentification

Pour créer un cluster prenant en charge l'authentification client

Cette procédure explique comment activer l'authentification du client à l'aide d'un Autorité de certification privée AWS.

> **Note**
>
> Nous vous recommandons vivement d'utiliser le protocole indépendant Autorité de certification privée AWS pour chaque cluster MSK lorsque vous utilisez le protocole TLS mutuel pour contrôler l'accès. Cela garantira que les certificats TLS signés par les PCA ne s'authentifient qu'auprès d'un seul cluster MSK.

1. Créez un fichier nommé `clientauthinfo.json` avec les contenus suivants. Remplacez *`Private-CA-ARN`* par l'ARN de votre PCA.

   ```
   {
      "Tls": {
          "CertificateAuthorityArnList": ["Private-CA-ARN"]
       }
   }
   ```

2. Créez un fichier nommé `brokernodegroupinfo.json` comme décrit à la section the section called “Création d'un cluster à l'aide du AWS CLI”.
3. L'authentification du client nécessite également l'activation du chiffrement lors du transit entre les clients et les brokers. Créez un fichier nommé `encryptioninfo.json` avec les contenus suivants. Remplacez *`KMS-KEY-ARN`* par l'ARN de votre clé KMS. Vous pouvez définir `ClientBroker` sur `TLS` ou `TLS_PLAINTEXT`.

   ```
   {
      "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "KMS-Key-ARN"
       },
      "EncryptionInTransit": {
           "InCluster": true,
           "ClientBroker": "TLS"
   ```

```
    }
}
```

iPour de plus amples informations sur le chiffrement, veuillez consulter the section called “Chiffrement”.

4. Sur une machine sur laquelle vous l'avez AWS CLI installé, exécutez la commande suivante pour créer un cluster sur lequel l'authentification et le chiffrement en transit sont activés. Enregistrez l'ARN de cluster fourni dans la réponse.

```
aws kafka create-cluster --cluster-name "AuthenticationTest" --broker-node-group-
info file://brokernodegroupinfo.json --encryption-info file://encryptioninfo.json
 --client-authentication file://clientauthinfo.json --kafka-version "{YOUR KAFKA
 VERSION}" --number-of-broker-nodes 3
```

Pour configurer un client pour utiliser l'authentification

1. Créez une instance Amazon EC2 à utiliser en tant qu'ordinateur client. Pour plus de simplicité, créez cette instance dans le même VPC que celui utilisé pour le cluster. Consultez the section called “Étape 3 : créer un ordinateur client” pour un exemple de création d'une machine client.
2. Créer une rubrique. Pour obtenir un exemple, consultez les instructions dans the section called “Étape 4 : créer une rubrique”.
3. Sur une machine sur laquelle vous l'avez AWS CLI installé, exécutez la commande suivante pour obtenir les courtiers bootstrap du cluster. Remplacez *Cluster-ARN* par l'ARN de votre cluster.

```
aws kafka get-bootstrap-brokers --cluster-arn Cluster-ARN
```

Enregistrez la chaîne associée à `BootstrapBrokerStringTls` dans la réponse.

4. Sur votre ordinateur client, exécutez la commande suivante pour utiliser le magasin de confiance JVM pour créer votre magasin de confiance client. Si votre chemin JVM est différent, ajustez la commande en conséquence.

```
cp /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.201.b09-0.amzn2.x86_64/jre/lib/security/
cacerts kafka.client.truststore.jks
```

5. Sur votre ordinateur client, exécutez la commande suivante pour créer une clé privée pour votre client. Remplacez *Distinguished-Name*, *Example-Alias*, *Your-Store-Pass*, et *Your-Key-Pass* par des chaînes de votre choix.

```
keytool -genkey -keystore kafka.client.keystore.jks -validity 300 -storepass Your-Store-Pass -keypass Your-Key-Pass -dname "CN=Distinguished-Name" -alias Example-Alias -storetype pkcs12
```

6. Sur votre ordinateur client, exécutez la commande suivante pour créer une demande de certificat avec la clé privée que vous avez créée à l'étape précédente.

```
keytool -keystore kafka.client.keystore.jks -certreq -file client-cert-sign-request
 -alias Example-Alias -storepass Your-Store-Pass -keypass Your-Key-Pass
```

7. Ouvrez le fichier `client-cert-sign-request` et assurez-vous qu'il commence par `-----BEGIN CERTIFICATE REQUEST-----` et se termine par `-----END CERTIFICATE REQUEST-----`. Si elle commence par `-----BEGIN NEW CERTIFICATE REQUEST-----`, supprimez le mot `NEW` (et l'espace unique qui le suit) du début et de la fin du fichier.

8. Sur une machine sur laquelle vous l'avez AWS CLI installé, exécutez la commande suivante pour signer votre demande de certificat. Remplacez *Private-CA-ARN* par l'ARN de votre PCA. Vous pouvez modifier la valeur de validité si vous le souhaitez. Ici, nous utilisons 300 comme exemple.

```
aws acm-pca issue-certificate --certificate-authority-arn Private-CA-ARN --csr
 fileb://client-cert-sign-request --signing-algorithm "SHA256WITHRSA" --validity
 Value=300,Type="DAYS"
```

   Enregistrez l'ARN de certificat fourni dans la réponse.

> **Note**
>
> Pour récupérer votre certificat client, utilisez la commande `acm-pca get-certificate` et spécifiez l'ARN de votre certificat. Pour plus d'informations, consultez get-certificate dans la Référence des commandes AWS CLI .

9. Exécutez la commande suivante pour obtenir le certificat Autorité de certification privée AWS signé pour vous. Remplacez *Certificate-ARN* par l'ARN obtenu à partir de la réponse à la commande précédente.

```
aws acm-pca get-certificate --certificate-authority-arn Private-CA-ARN --
certificate-arn Certificate-ARN
```

10. À partir du résultat JSON de l'exécution de la commande précédente, copiez les chaînes associées à `Certificate` et `CertificateChain`. Collez ces deux chaînes dans un nouveau fichier nommé signed-certificate-from-acm. Collez la chaîne associée à `Certificate` en premier, suivie de la chaîne associée à `CertificateChain`. Remplacez les caractères `\n` par de nouvelles lignes. Voici la structure du fichier après avoir collé le certificat et la chaîne de certificats.

```
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

11. Exécutez la commande suivante sur l'ordinateur client pour ajouter ce certificat à votre magasin de clés afin que vous puissiez le présenter lorsque vous parlez aux agents MSK.

```
keytool -keystore kafka.client.keystore.jks -import -file signed-certificate-from-
acm -alias Example-Alias -storepass Your-Store-Pass -keypass Your-Key-Pass
```

12. Créez un fichier nommé `client.properties` avec les contenus suivants. Ajustez les emplacements du magasin de confiance et du magasin de clés aux chemins d'accès où vous avez enregistré `kafka.client.truststore.jks`. Remplacez la version de votre client Kafka par les espaces réservés *{VOTRE VERSION KAFKA}*.

```
security.protocol=SSL
ssl.truststore.location=/tmp/kafka_2.12-{YOUR KAFKA VERSION}/
kafka.client.truststore.jks
ssl.keystore.location=/tmp/kafka_2.12-{YOUR KAFKA VERSION}/
kafka.client.keystore.jks
ssl.keystore.password=Your-Store-Pass
ssl.key.password=Your-Key-Pass
```

Pour produire et consommer des messages à l'aide de l'authentification

1. Exécutez la commande suivante pour créer une rubrique. Le fichier nommé `client.properties` est celui que vous avez créé lors de la procédure précédente.

```
<path-to-your-kafka-installation>/bin/kafka-topics.sh --create --bootstrap-
server BootstrapBroker-String --replication-factor 3 --partitions 1 --topic
 ExampleTopic --command-config client.properties
```

2. Exécutez la commande suivante pour démarrer un producteur de console. Le fichier nommé `client.properties` est celui que vous avez créé lors de la procédure précédente.

```
<path-to-your-kafka-installation>/bin/kafka-console-producer.sh --bootstrap-
server BootstrapBroker-String --topic ExampleTopic --producer.config
 client.properties
```

3. Dans une nouvelle fenêtre de commande sur votre ordinateur client, exécutez la commande suivante pour démarrer un consommateur de console.

```
<path-to-your-kafka-installation>/bin/kafka-console-consumer.sh --bootstrap-
server BootstrapBroker-String --topic ExampleTopic --consumer.config
 client.properties
```

4. Tapez des messages dans la fenêtre du producteur et regardez-les apparaître dans la fenêtre du consommateur.

Authentification des identifiants de connexion avec AWS Secrets Manager

Vous pouvez contrôler l'accès à vos clusters Amazon MSK à l'aide d'informations de connexion stockées et sécurisées à l'aide de AWS Secrets Manager. Le stockage des informations d'identification des utilisateurs dans Secrets Manager réduit les coûts liés à l'authentification du cluster, comme l'audit, la mise à jour et la rotation des informations d'identification. Secrets Manager vous permet également de partager les informations d'identification des utilisateurs entre les clusters.

Cette rubrique contient les sections suivantes :

- Limites

Comment ça marche

L'authentification des informations d'identification pour Amazon MSK utilise l'authentification SASL/SCRAM (Simple Authentication and Security Layer/Salted Challenge Response Authentication Mechanism). Pour configurer l'authentification des informations d'identification de connexion pour un cluster, vous devez créer une ressource secrète dans AWS Secrets Manager et associer les informations d'identification de connexion à ce secret.

L'authentification SASL/SCRAM est définie dans RFC 5802. SCRAM utilise des algorithmes de hachage sécurisés et ne transmet pas d'informations d'identification de connexion en texte brut entre le client et le serveur.

> **Note**
>
> Lorsque vous configurez l'authentification SASL/SCRAM pour votre cluster, Amazon MSK active le chiffrement TLS pour tout le trafic entre les clients et les agents.

Configuration de l'authentification SASL/SCRAM pour un cluster Amazon MSK

Pour configurer un secret dans AWS Secrets Manager, suivez le didacticiel de création et de récupération d'un secret figurant dans le guide de l'utilisateur de AWS Secrets Manager.

Tenez compte des exigences suivantes lors de la création d'un secret pour un cluster Amazon MSK :

- Choisissez Autre type de secrets (p. ex. clé d'API) pour le type de secret.
- Votre nom secret doit commencer par le préfixe AmazonMSK_.
- Vous devez soit utiliser une AWS KMS clé personnalisée existante, soit créer une nouvelle AWS KMS clé personnalisée pour votre secret. Secrets Manager utilise la AWS KMS clé par défaut pour un secret.

> **Important**
>
> Un secret créé avec la AWS KMS clé par défaut ne peut pas être utilisé avec un cluster Amazon MSK.

- Vos informations d'identification de connexion doivent être au format suivant pour saisir des paires clé-valeur à l'aide de l'option Texte brut.

```
{
  "username": "alice",
  "password": "alice-secret"
}
```

- Enregistrez la valeur ARN (Amazon Resource Name) de votre secret.
-

> **Important**
>
> Vous ne pouvez pas associer un secret de Secrets Manager à un cluster qui dépasse les limites décrites dans the section called “ Dimensionnez correctement votre cluster : nombre de partitions par agent”.

- Si vous utilisez le AWS CLI pour créer le secret, spécifiez un ID de clé ou un ARN pour le `kms-key-id` paramètre. Ne spécifiez pas d'alias.
- Pour associer le secret à votre cluster, utilisez soit la console Amazon MSK, soit l' BatchAssociateScramSecretopération.

> **Important**
>
> Lorsque vous associez un secret à un cluster, Amazon MSK associe une politique de ressource au secret qui permet à votre cluster d'accéder aux valeurs secrètes que vous avez définies et de les lire. Vous ne devez pas modifier cette politique de ressource. Cela peut empêcher votre cluster d'accéder à votre secret.

L'exemple d'entrée JSON suivant pour l'opération `BatchAssociateScramSecret` associe un secret à un cluster :

```
{
  "clusterArn" : "arn:aws:kafka:us-west-2:0123456789019:cluster/SalesCluster/
abcd1234-abcd-cafe-abab-9876543210ab-4",
  "secretArnList": [
    "arn:aws:secretsmanager:us-west-2:0123456789019:secret:AmazonMSK_MyClusterSecret"
  ]
}
```

Connexion à votre cluster à l'aide des informations d'identification de connexion

Après avoir créé un secret et l'avoir associé à votre cluster, vous pouvez connecter votre client au cluster. Les exemples d'étapes suivants montrent comment connecter un client à un cluster qui utilise l'authentification SASL/SCRAM, et comment produire vers et consommer à partir d'un exemple de rubrique.

1. Exécutez la commande suivante sur une machine sur laquelle la AWS CLI est installée, en remplaçant *ClusterArn* par l'ARN de votre cluster.

```
aws kafka get-bootstrap-brokers --cluster-arn clusterARN
```

2. Pour créer un exemple de rubrique, exécutez la commande suivante en remplaçant *BootstrapServerString* par l'un des points de terminaison du broker que vous avez obtenus à l'étape précédente.

```
<path-to-your-kafka-installation>/bin/kafka-topics.sh --create --bootstrap-
server BootstrapServerString --replication-factor 3 --partitions 1 --topic
 ExampleTopicName
```

3. Sur votre ordinateur client, créez un fichier de configuration JAAS contenant les informations d'identification d'utilisateur stockées dans votre secret. Par exemple, pour l'utilisateur alice, créez un fichier appelé `users_jaas.conf` avec le contenu suivant.

```
KafkaClient {
   org.apache.kafka.common.security.scram.ScramLoginModule required
   username="alice"
   password="alice-secret";
};
```

4. Utilisez la commande suivante pour exporter votre fichier de configuration JAAS en tant que paramètre d'environnement `KAFKA_OPTS`.

```
export KAFKA_OPTS=-Djava.security.auth.login.config=<path-to-jaas-file>/
users_jaas.conf
```

5. Créez un fichier nommé `kafka.client.truststore.jks` dans un répertoire `./tmp`.
6. Utilisez la commande suivante pour copier le fichier de stockage de clés JDK de votre dossier `cacerts` JVM dans le fichier `kafka.client.truststore.jks` que vous avez créé à l'étape précédente. Remplacez *JDKFolder* par le nom du dossier JDK

de votre instance. Par exemple, votre dossier JDK peut être nommé `java-1.8.0-openjdk-1.8.0.201.b09-0.amzn2.x86_64`.

```
cp /usr/lib/jvm/JDKFolder/jre/lib/security/cacerts /tmp/kafka.client.truststore.jks
```

7. Dans le répertoire `bin` de votre installation d'Apache Kafka, créez un fichier de propriétés client appelé `client_sasl.properties` avec le contenu suivant. Ce fichier définit le mécanisme et le protocole SASL.

```
security.protocol=SASL_SSL
sasl.mechanism=SCRAM-SHA-512
ssl.truststore.location=<path-to-keystore-file>/kafka.client.truststore.jks
```

8. Récupérez la chaîne de votre agent d'amorçage à l'aide de la commande suivante. *ClusterArn*Remplacez-le par le Amazon Resource Name (ARN) de votre cluster :

```
aws kafka get-bootstrap-brokers --cluster-arn ClusterArn
```

   À partir du résultat JSON de la commande, enregistrez la valeur associée à la chaîne nommée `BootstrapBrokerStringSaslScram`.

9. Pour produire un exemple de rubrique que vous avez créé, exécutez la commande suivante sur votre ordinateur client. Remplacez *BootstrapBrokerStringSaslScram* par la valeur que vous avez récupérée à l'étape précédente.

```
<path-to-your-kafka-installation>/bin/kafka-console-producer.sh --broker-
list BootstrapBrokerStringSaslScram --topic ExampleTopicName --producer.config
 client_sasl.properties
```

10. Pour consommer à partir de la rubrique que vous avez créée, exécutez la commande suivante sur votre ordinateur client. Remplacez *BootstrapBrokerStringSaslScram* par la valeur que vous avez obtenue précédemment.

```
<path-to-your-kafka-installation>/bin/kafka-console-consumer.sh --bootstrap-
server BootstrapBrokerStringSaslScram --topic ExampleTopicName --from-beginning --
consumer.config client_sasl.properties
```

Utilisation des utilisateurs

Création d'utilisateurs : vous créez des utilisateurs dans votre secret sous forme de paires valeur-clé. Lorsque vous utilisez l'option Texte brut dans la console Secrets Manager, vous devez spécifier les informations d'identification de connexion au format suivant.

```
{
  "username": "alice",
  "password": "alice-secret"
}
```

Révocation de l'accès utilisateur : pour révoquer les informations d'identification d'un utilisateur lui permettant d'accéder à un cluster, nous vous recommandons de supprimer ou d'appliquer une liste de contrôle d'accès (ACL) sur le cluster, puis de dissocier le secret. Ceci pour les raisons suivantes :

- La suppression d'un utilisateur ne ferme pas les connexions existantes.
- Les modifications de votre secret prennent jusqu'à 10 minutes pour se propager.

Pour en savoir plus sur l'utilisation d'une liste de contrôle d'accès (ACL) avec Amazon MSK, consultez Listes de contrôle d'accès (ACL) Apache Kafka.

Pour les clusters utilisant ZooKeeper le mode, nous vous recommandons de restreindre l'accès à vos ZooKeeper nœuds afin d'empêcher les utilisateurs de modifier les ACL. Pour de plus amples informations, consultez Contrôle de l'accès à Apache ZooKeeper.

Limites

Notez les limitations suivantes lorsque vous utilisez des secrets SCRAM :

- Amazon MSK prend uniquement en charge l'authentification SCRAM-SHA-512.
- Un cluster Amazon MSK peut avoir jusqu'à 1 000 utilisateurs.
- Vous devez utiliser un AWS KMS key avec votre secret. Vous ne pouvez pas utiliser un secret qui utilise la clé de chiffrement par défaut de Secrets Manager avec Amazon MSK. Pour plus d'informations sur la création d'une clé KMS, consultez Création de clés de chiffrements symétriques.
- Vous ne pouvez pas utiliser une clé KMS asymétrique avec Secrets Manager.
- Vous pouvez associer jusqu'à 10 secrets à un cluster à la fois à l'aide de cette BatchAssociateScramSecretopération.

- Le nom des secrets associés à un cluster Amazon MSK doit comporter le préfixe AmazonMSK_.
- Les secrets associés à un cluster Amazon MSK doivent se trouver dans le même compte Amazon Web Services et dans la même AWS région que le cluster.

Listes de contrôle d'accès (ACL) Apache Kafka

Apache Kafka possède un autorisateur enfichable et est livré avec une implémentation d'autorisateur. out-of-box Amazon MSK active ce mécanisme d'autorisation dans le fichier `server.properties` sur les brokers.

Les ACL Apache Kafka ont le format « Le P principal est [autorisé/refusé] Opération O depuis l'hôte H sur toute ressource R correspondant au RP ». ResourcePattern Si RP ne correspond pas à une ressource spécifique R, alors R n'a aucune ACL associée et, par conséquent, seul un super-utilisateur est autorisé à accéder à R. Pour modifier ce comportement d'Apache Kafka, vous devez définir la propriété `allow.everyone.if.no.acl.found` en tant que vrai. Amazon MSK la définit par défaut en tant que vrai. Cela signifie qu'avec les clusters Amazon MSK, si vous ne définissez pas explicitement les ACL sur une ressource, tous les serveurs mandataires peuvent accéder à cette ressource. Si vous définissez les ACL sur une ressource, seuls les serveurs mandataires autorisés peuvent y accéder. Si vous souhaitez restreindre l'accès à une rubrique et autoriser un client à l'aide de l'authentification mutuelle TLS, ajoutez des ACL en vous servant de l'interface de ligne de commande du mécanisme d'autorisation d'Apache Kafka. Pour de plus amples informations sur l'ajout, la suppression et la liste des ACL, veuillez consulter Interface de ligne de commande d'autorisation Kafka.

En plus de l'autorisation pour le client, vous devez également donner l'accès à vos rubriques à tous vos brokers afin qu'ils puissent répliquer des messages à partir de la partition principale. Si les brokers n'ont pas accès à une rubrique, la réplication de cette dernière échoue.

Pour ajouter ou supprimer l'accès en lecture et en écriture à une rubrique

1. Ajoutez vos brokers au tableau ACL pour leur permettre de lire toutes les rubriques qui ont des ACL en place. Pour donner l'accès à vos agents à la lecture d'une rubrique, exécutez la commande suivante sur un ordinateur client qui peut communiquer avec le cluster MSK.

   Remplacez le *`Nom unique`* par le serveur DNS de l'un des brokers d'amorçage de votre cluster, puis remplacez la chaîne avant le premier point de ce nom unique par un astérisque (*). Par exemple, si l'un des brokers d'amorçage de votre cluster possède le serveur DNS `b-6.mytestcluster.67281x.c4.kafka.us-`

`east-1.amazonaws.com`, remplacez le *`Distinguished-Name`* dans la commande suivante par `*.mytestcluster.67281x.c4.kafka.us-east-1.amazonaws.com`. Pour de plus amples informations sur la façon d'obtenir les brokers d'amorçage, veuillez consulter the section called “Obtention des agents d'amorçage”.

```
<path-to-your-kafka-installation>/bin/kafka-acls.sh --authorizer-properties
 --bootstrap-server BootstrapServerString --add --allow-principal
 "User:CN=Distinguished-Name" --operation Read --group=* --topic Topic-Name
```

2. Pour accorder l'accès en lecture à une rubrique, exécutez la commande suivante sur votre ordinateur client. Si vous utilisez l'authentification TLS mutuelle, utilisez le même *`Distinguised-Name`* que celui utilisé lors de la création de la clé privée.

   ```
   <path-to-your-kafka-installation>/bin/kafka-acls.sh --authorizer-properties
    --bootstrap-server BootstrapServerString --add --allow-principal
    "User:CN=Distinguished-Name" --operation Read --group=* --topic Topic-Name
   ```

   Pour supprimer l'accès en lecture, vous pouvez exécuter la même commande, en remplaçant `--add` par `--remove`.

3. Pour accorder un accès en écriture à une rubrique, exécutez la commande suivante sur votre ordinateur client. Si vous utilisez l'authentification TLS mutuelle, utilisez le même *`Distinguised-Name`* que celui utilisé lors de la création de la clé privée.

   ```
   <path-to-your-kafka-installation>/bin/kafka-acls.sh --authorizer-properties
    --bootstrap-server BootstrapServerString --add --allow-principal
    "User:CN=Distinguished-Name" --operation Write --topic Topic-Name
   ```

   Pour supprimer l'accès en écriture, vous pouvez exécuter la même commande, en remplaçant `--add` par `--remove`.

Modification du groupe de sécurité d'un cluster Amazon MSK

Cette page explique comment modifier le groupe de sécurité d'un cluster MSK existant. Vous devrez peut-être modifier le groupe de sécurité d'un cluster afin de fournir l'accès à un certain ensemble d'utilisateurs ou de limiter l'accès au cluster. Pour plus d'informations sur les groupes de sécurité, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC.

1. Utilisez l'ListNodesAPI ou la commande list-nodes du AWS CLI pour obtenir la liste des courtiers de votre cluster. Les résultats de cette opération incluent les ID des interfaces réseau Elastic (ENI) associées aux agents.
2. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
3. À l'aide de la liste déroulante située dans le coin supérieur droit de l'écran, sélectionnez la région dans laquelle le cluster est déployé.
4. Dans le volet de navigation, sous Réseau et sécurité, choisissez Interfaces réseau.
5. Sélectionnez la première ENI que vous avez obtenue lors de la première étape. Choisissez le menu Actions en haut de l'écran, puis choisissez Modifier les groupes de sécurité. Assignez le nouveau groupe de sécurité à cette ENI. Répétez cette étape pour chacune des ENI que vous avez obtenues à la première étape.

   > **Note**
   >
   > Les modifications que vous apportez au groupe de sécurité d'un cluster à l'aide de la console Amazon EC2 ne sont pas reflétées dans la console MSK sous Paramètres réseau.

6. Configurez les règles du nouveau groupe de sécurité pour garantir que vos clients ont accès aux agents. Pour de plus amples informations sur la définition de règles de groupe de sécurité, consultez Ajout, Suppression et Mise à jour de règles dans le Guide de l'utilisateur Amazon VPC.

> **Important**
>
> Si vous modifiez le groupe de sécurité associé aux agents d'un cluster, puis que vous ajoutez de nouveaux agents à ce cluster, Amazon MSK associe les nouveaux agents au groupe de sécurité d'origine associé au cluster lors de sa création. Toutefois, pour qu'un cluster fonctionne correctement, tous ses agents doivent être associés au même groupe de sécurité. Par conséquent, si vous ajoutez de nouveaux agents après avoir modifié le groupe de sécurité, vous devez suivre à nouveau la procédure précédente et mettre à jour les ENI des nouveaux agents.

Contrôle de l'accès à Apache ZooKeeper

Pour des raisons de sécurité, vous pouvez limiter l'accès aux ZooKeeper nœuds Apache qui font partie de votre cluster Amazon MSK. Pour limiter l'accès aux nœuds, vous pouvez leur attribuer un groupe de sécurité distinct. Vous pouvez ensuite décider qui a accès à ce groupe de sécurité.

> **Important**
>
> Cette section ne s'applique pas aux clusters exécutés en mode KraFT. veuillez consulter the section called “Mode Kraft ”.

Cette rubrique contient les sections suivantes :

- Pour placer vos ZooKeeper nœuds Apache dans un groupe de sécurité distinct
- Utilisation de la sécurité TLS avec Apache ZooKeeper

Pour placer vos ZooKeeper nœuds Apache dans un groupe de sécurité distinct

1. Obtenez la chaîne de ZooKeeper connexion Apache pour votre cluster. Pour savoir comment procéder, veuillez consulter la section the section called “ZooKeeper mode”. La chaîne de connexion contient les noms DNS de vos ZooKeeper nœuds Apache.
2. Utilisez un outil comme `host` ou `ping` pour convertir les noms DNS que vous avez obtenus à l'étape précédente en adresses IP. Enregistrez ces adresses IP car vous en aurez besoin plus tard dans cette procédure.
3. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
4. Dans le panneau de navigation, sous Network & Security (Réseau et sécurité), choisissez Network Interfaces (Interfaces réseau).
5. Dans le champ de recherche au-dessus de la table des interfaces réseau, tapez le nom de votre cluster, puis appuyer sur retour. Cela limite le nombre d'interfaces réseau qui apparaissent dans la table aux interfaces associées à votre cluster.
6. Activez la case à cocher au début de la ligne qui correspond à la première interface réseau de la liste.

7. Dans le volet d'informations en bas de la page, recherchez l'IP IPv4 privée principale. Si cette adresse IP correspond à l'une des adresses IP que vous avez obtenues lors de la première étape de cette procédure, cela signifie que cette interface réseau est attribuée à un ZooKeeper nœud Apache qui fait partie de votre cluster. Sinon, désactivez la case à cocher en regard de cette interface réseau et sélectionnez l'interface réseau suivante dans la liste. L'ordre dans lequel vous sélectionnez les interfaces réseau n'a pas d'importance. Dans les étapes suivantes, vous allez effectuer les mêmes opérations sur toutes les interfaces réseau assignées aux ZooKeeper nœuds Apache, une par une.
8. Lorsque vous sélectionnez une interface réseau correspondant à un ZooKeeper nœud Apache, choisissez le menu Actions en haut de la page, puis choisissez Modifier les groupes de sécurité. Attribuez un nouveau groupe de sécurité à cette interface réseau. Pour de plus amples informations sur la création des groupes de sécurité, consultez Création d'un groupe de sécurité dans la documentation Amazon VPC.
9. Répétez l'étape précédente pour attribuer le même nouveau groupe de sécurité à toutes les interfaces réseau associées aux ZooKeeper nœuds Apache de votre cluster.
10. Vous pouvez désormais choisir qui a accès à ce nouveau groupe de sécurité. Pour de plus amples informations sur la définition de règles de groupe de sécurité, consultez Ajout, Suppression et Mise à jour de règles dans la documentation Amazon VPC.

Utilisation de la sécurité TLS avec Apache ZooKeeper

Vous pouvez utiliser la sécurité TLS pour le chiffrement en transit entre vos clients et vos ZooKeeper nœuds Apache. Pour implémenter la sécurité TLS avec vos ZooKeeper nœuds Apache, procédez comme suit :

- Les clusters doivent utiliser Apache Kafka version 2.5.1 ou ultérieure pour utiliser la sécurité TLS avec Apache. ZooKeeper
- Activez la sécurité TLS lorsque vous créez ou configurez votre cluster. Les clusters créés avec Apache Kafka version 2.5.1 ou ultérieure avec TLS activé utilisent automatiquement la sécurité TLS avec les points de terminaison Apache. ZooKeeper Pour plus d'informations sur la configuration de la sécurité TLS, consultez Comment démarrer avec le chiffrement ?.
- Récupérez les ZooKeeper points de terminaison TLS Apache à l'aide de l'opération DescribeCluster .

- Créez un fichier ZooKeeper de configuration Apache à utiliser avec les kafka-acls.shoutils `kafka-configs.sh` et ou avec le ZooKeeper shell. Avec chaque outil, vous utilisez le `--zk-tls-config-file` paramètre pour spécifier votre ZooKeeper configuration Apache.

  L'exemple suivant montre un fichier de ZooKeeper configuration Apache typique :

  ```
  zookeeper.ssl.client.enable=true
  zookeeper.clientCnxnSocket=org.apache.zookeeper.ClientCnxnSocketNetty
  zookeeper.ssl.keystore.location=kafka.jks
  zookeeper.ssl.keystore.password=test1234
  zookeeper.ssl.truststore.location=truststore.jks
  zookeeper.ssl.truststore.password=test1234
  ```

- Pour les autres commandes (telles quekafka-topics), vous devez utiliser la variable d'KAFKA_OPTSenvironnement pour configurer les ZooKeeper paramètres Apache. L'exemple suivant montre comment configurer la variable d'KAFKA_OPTSenvironnement pour transmettre les ZooKeeper paramètres Apache à d'autres commandes :

  ```
  export KAFKA_OPTS="
  -Dzookeeper.clientCnxnSocket=org.apache.zookeeper.ClientCnxnSocketNetty
  -Dzookeeper.client.secure=true
  -Dzookeeper.ssl.trustStore.location=/home/ec2-user/kafka.client.truststore.jks
  -Dzookeeper.ssl.trustStore.password=changeit"
  ```

  Après avoir configuré la variable d'environnement KAFKA_OPTS, vous pouvez utiliser les commandes de l'interface de ligne de commande normalement. L'exemple suivant crée un sujet Apache Kafka en utilisant la ZooKeeper configuration Apache à partir de la variable d'KAFKA_OPTSenvironnement :

  ```
  <path-to-your-kafka-installation>/bin/kafka-topics.sh --create --
  zookeeper ZooKeeperTLSConnectString --replication-factor 3 --partitions 1 --topic
   AWSKafkaTutorialTopic
  ```

> **Note**
>
> Les noms des paramètres que vous utilisez dans votre fichier de ZooKeeper configuration Apache et ceux que vous utilisez dans votre variable d'KAFKA_OPTSenvironnement ne sont

pas cohérents. Faites attention aux noms que vous utilisez et aux paramètres de votre fichier de configuration et de votre variable d'environnement `KAFKA_OPTS`.

Pour plus d'informations sur l'accès à vos ZooKeeper nœuds Apache avec TLS, voir KIP-515 : Permettre au client ZK d'utiliser la nouvelle authentification prise en charge par TLS.

Journalisation

Vous pouvez envoyer les journaux des courtiers Apache Kafka vers un ou plusieurs des types de destination suivants : Amazon CloudWatch Logs, Amazon S3, Amazon Data Firehose. Vous pouvez également enregistrer les appels d'API Amazon MSK avec AWS CloudTrail.

Journaux d'agent

Les journaux d'agent vous permettent de dépanner vos applications Apache Kafka et d'analyser leurs communications avec votre cluster MSK. Vous pouvez configurer votre cluster MSK nouveau ou existant pour fournir des journaux de broker de niveau Info à un ou plusieurs des types de ressources de destination suivants : un groupe de CloudWatch journaux, un compartiment S3, un flux de diffusion Firehose. Grâce à Firehose, vous pouvez ensuite transmettre les données du journal de votre flux de diffusion au OpenSearch Service. Vous devez créer une ressource de destination avant de configurer votre cluster pour qu'il y envoie les journaux d'agent. Amazon MSK ne crée pas ces ressources de destination pour vous si elles n'existent pas déjà. Pour plus d'informations sur ces trois types de ressources de destination et sur la façon de les créer, consultez la documentation suivante :

- Amazon CloudWatch Logs
- Amazon S3
- Amazon Data Firehose

Autorisations nécessaires

Pour configurer une destination pour les journaux d'agent Amazon MSK, l'identité IAM que vous utilisez pour les actions Amazon MSK doit disposer des autorisations décrites dans la politique AWS politique gérée : AmazonMSK FullAccess.

Pour diffuser des journaux d'agent vers un compartiment S3, vous avez également besoin de l'autorisation `s3:PutBucketPolicy`. Pour plus d'informations sur les politiques de compartiment

S3, consultez Comment ajouter une politique de compartiment S3 ? dans le Guide de l'utilisateur Amazon S3. Pour plus d'informations sur les politiques IAM en général, consultez Gestion des accès dans le Guide de l'utilisateur IAM.

Stratégie de clé KMS obligatoire à utiliser avec les compartiments SSE-KMS

Si vous avez activé le chiffrement côté serveur pour votre compartiment S3 à l'aide de clés AWS KMS gérées (SSE-KMS) avec une clé gérée par le client, ajoutez ce qui suit à la politique de clé pour votre clé KMS afin qu'Amazon MSK puisse écrire des fichiers de broker dans le compartiment.

```
{
  "Sid": "Allow Amazon MSK to use the key.",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "delivery.logs.amazonaws.com"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Configuration des journaux des courtiers à l'aide du AWS Management Console

Si vous créez un cluster, recherchez l'en-tête de Broker log delivery (Transmission du journal d’agent) dans la section Monitoring (Surveillance) . Vous pouvez spécifier les destinations vers lesquelles vous souhaitez qu'Amazon MSK diffuse vos journaux d'agent.

Pour un cluster existant, choisissez ce dernier dans votre liste de clusters, puis sélectionnez l'onglet Propriétés. Faites défiler jusqu'à la section Diffusion de journaux, puis choisissez son bouton Modifier. Vous pouvez spécifier les destinations vers lesquelles vous souhaitez qu'Amazon MSK diffuse vos journaux d'agent.

Configuration des journaux des courtiers à l'aide du AWS CLI

Lorsque vous utilisez les commande `update-monitoring` ou `create-cluster`, vous pouvez éventuellement spécifier le paramètre `logging-info` et lui transmettre une structure JSON comme dans l'exemple suivant. Dans ce JSON, les trois types de destination sont facultatifs.

```
{
  "BrokerLogs": {
    "S3": {
      "Bucket": "ExampleBucketName",
      "Prefix": "ExamplePrefix",
      "Enabled": true
    },
    "Firehose": {
      "DeliveryStream": "ExampleDeliveryStreamName",
      "Enabled": true
    },
    "CloudWatchLogs": {
      "Enabled": true,
      "LogGroup": "ExampleLogGroupName"
    }
  }
}
```

Configuration des journaux d'agent à l'aide de l'API

Vous pouvez spécifier la `loggingInfo` structure facultative dans le JSON que vous transmettez aux UpdateMonitoringopérations CreateClusteror.

> **Note**
>
> Par défaut, lorsque la journalisation des agents est activée, Amazon MSK journalise les journaux de niveau `INFO` vers les destinations spécifiées. Toutefois, les utilisateurs de la version 2.4.X et ultérieure d'Apache Kafka peuvent définir dynamiquement le niveau de journalisation de l'agent sur n'importe quel niveau de journalisation log4j. Pour plus d'informations sur la définition dynamique du niveau de journalisation de l'agent, consultez KIP-412 : Extension de l'API Admin pour prendre en charge les niveaux de journalisation dynamiques des applications. Si vous définissez dynamiquement le niveau de journalisation sur `DEBUG` ou`TRACE`, nous vous recommandons d'utiliser Amazon S3 ou Firehose comme destination du journal. Si vous utilisez CloudWatch les journaux comme destination

des journaux et que vous activez `DEBUG` ou `TRACE` nivelez la journalisation de manière dynamique, Amazon MSK peut fournir en permanence un échantillon de journaux. Cela peut avoir un impact significatif sur les performances de l'agent et ne doit être utilisé que lorsque le niveau de journalisation `INFO` n'est pas suffisamment détaillé pour déterminer la cause première d'un problème.

Journalisation des appels d'API AWS CloudTrail avec

> **Note**
>
> AWS CloudTrail les journaux ne sont disponibles pour Amazon MSK que lorsque vous les utilisezContrôle d'accès IAM.

Amazon MSK est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Amazon MSK. CloudTrail capture les appels d'API sous forme d'événements. Ces captures incluent les appels de la console Amazon MSK et les appels de code vers les opérations d'API Amazon MSK. Il capture également les actions Apache Kafka telles que la création et la modification de rubriques et de groupes.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon MSK. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Amazon MSK ou l'action Apache Kafka, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour en savoir plus CloudTrail, notamment comment le configurer et l'activer, consultez le guide de AWS CloudTrail l'utilisateur.

Informations Amazon MSK dans CloudTrail

CloudTrail est activé sur votre compte Amazon Web Services lorsque vous créez le compte. Lorsqu'une activité événementielle prise en charge se produit dans un cluster MSK, 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 Amazon Web Services. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements dans votre compte Amazon Web Services, y compris les événements pour Amazon MSK, créez un journal d'activité. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions . Le journal de suivi consigne les événements de toutes les régions dans la partition AWS , et il livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services Amazon pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Amazon MSK enregistre toutes les opérations Amazon MSK sous forme d'événements dans des fichiers CloudTrail journaux. En outre, il journalise les actions Apache Kafka suivantes.

- cluster Kafka : DescribeClusterDynamicConfiguration
- cluster Kafka : AlterClusterDynamicConfiguration
- cluster Kafka : CreateTopic
- cluster Kafka : DescribeTopicDynamicConfiguration
- cluster Kafka : AlterTopic
- cluster Kafka : AlterTopicDynamicConfiguration
- cluster Kafka : DeleteTopic

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

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou de l'utilisateur 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 demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Exemple : entrées du fichier journal Amazon MSK

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

L'exemple suivant montre des entrées de CloudTrail journal illustrant les actions `DescribeCluster` et `DeleteCluster` Amazon MSK.


```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEF0123456789ABCDE",
        "arn": "arn:aws:iam::012345678901:user/Joe",
        "accountId": "012345678901",
        "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "Joe"
      },
      "eventTime": "2018-12-12T02:29:24Z",
      "eventSource": "kafka.amazonaws.com",
      "eventName": "DescribeCluster",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.14.67 Python/3.6.0 Windows/10 botocore/1.9.20",
      "requestParameters": {
        "clusterArn": "arn%3Aaws%3Akafka%3Aus-east-1%3A012345678901%3Acluster
%2Fexamplecluster%2F01234567-abcd-0123-abcd-abcd0123efa-2"
      },
```

```
      "responseElements": null,
      "requestID": "bd83f636-fdb5-abcd-0123-157e2fbf2bde",
      "eventID": "60052aba-0123-4511-bcde-3e18dbd42aa4",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "recipientAccountId": "012345678901"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEF0123456789ABCDE",
        "arn": "arn:aws:iam::012345678901:user/Joe",
        "accountId": "012345678901",
        "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "Joe"
      },
      "eventTime": "2018-12-12T02:29:40Z",
      "eventSource": "kafka.amazonaws.com",
      "eventName": "DeleteCluster",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.14.67 Python/3.6.0 Windows/10 botocore/1.9.20",
      "requestParameters": {
        "clusterArn": "arn%3Aaws%3Akafka%3Aus-east-1%3A012345678901%3Acluster
%2Fexamplecluster%2F01234567-abcd-0123-abcd-abcd0123efa-2"
      },
      "responseElements": {
        "clusterArn": "arn:aws:kafka:us-east-1:012345678901:cluster/
examplecluster/01234567-abcd-0123-abcd-abcd0123efa-2",
        "state": "DELETING"
      },
      "requestID": "c6bfb3f7-abcd-0123-afa5-293519897703",
      "eventID": "8a7f1fcf-0123-abcd-9bdb-1ebf0663a75c",
      "readOnly": false,
      "eventType": "AwsApiCall",
      "recipientAccountId": "012345678901"
    }
  ]
}
```


L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`kafka-cluster:CreateTopic`action.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "ABCDEFGH1IJKLMN2P34Q5",
    "arn": "arn:aws:iam::111122223333:user/Admin",
    "accountId": "111122223333",
    "accessKeyId": "CDEFAB1C2UUUUU3AB4TT",
    "userName": "Admin"
  },
  "eventTime": "2021-03-01T12:51:19Z",
  "eventSource": "kafka-cluster.amazonaws.com",
  "eventName": "CreateTopic",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "198.51.100.0/24",
  "userAgent": "aws-msk-iam-auth/unknown-version/aws-internal/3 aws-sdk-java/1.11.970
 Linux/4.14.214-160.339.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.272-b10 java/1.8.0_272
 scala/2.12.8 vendor/Red_Hat,_Inc.",
  "requestParameters": {
    "kafkaAPI": "CreateTopics",
    "resourceARN": "arn:aws:kafka:us-east-1:111122223333:topic/IamAuthCluster/3ebafd8e-
dae9-440d-85db-4ef52679674d-1/Topic9"
  },
  "responseElements": null,
  "requestID": "e7c5e49f-6aac-4c9a-a1d1-c2c46599f5e4",
  "eventID": "be1f93fd-4f14-4634-ab02-b5a79cb833d2",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


Validation de conformité pour Amazon Managed Streaming for Apache Kafka

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon Managed Streaming for Apache Kafka dans le cadre de programmes de conformité AWS . Ceux-ci comprennent PCI et HIPAA BAA.

Pour obtenir la liste des AWS services concernés par des programmes de conformité spécifiques, consultez Amazon Services inclus dans le champ d'application par programme de conformité . 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 .

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

- Guides démarrage rapide de la sécurité et de la conformité. Ces guides de déploiement traitent des considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS.
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA — Ce livre blanc décrit comment les entreprises peuvent créer des applications conformes à la loi HIPAA. AWS
- 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.
- 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— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans Amazon Managed Streaming for Apache Kafka

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

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

Sécurité de l'infrastructure dans Amazon Managed Streaming for Apache Kafka

En tant que service géré, Amazon Managed Streaming for Apache Kafka est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc Amazon Web Services : Overview of Security Processes.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon MSK via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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.

Connexion à un cluster Amazon MSK

Par défaut, les clients peuvent accéder à un cluster MSK uniquement s'ils se trouvent dans le même VPC que le cluster. Toutes les communications entre vos clients Kafka et votre cluster MSK sont privées par défaut et vos données de streaming ne transitent jamais par Internet. Pour vous connecter à votre cluster MSK à partir d'un client situé dans le même VPC que le cluster, veillez à ce que le groupe de sécurité du cluster dispose d'une règle entrante qui accepte le trafic provenant du groupe de sécurité du client. Pour plus d'informations sur la configuration de ces règles, consultez Règles des groupes de sécurité. Pour obtenir un exemple de la façon d'accéder à un cluster à partir d'une instance Amazon EC2 située dans le même VPC que le cluster, consultez Premiers pas.

Pour vous connecter à votre cluster MSK depuis un client situé en dehors du VPC du cluster, voir Accès depuis le VPC du cluster mais depuis AWS l'extérieur.

Rubriques

Accès public

Amazon MSK vous donne la possibilité d'activer l'accès public aux agents des clusters MSK exécutant Apache Kafka 2.6.0 ou des versions ultérieures. Pour des raisons de sécurité, vous ne pouvez pas activer l'accès public lors de la création d'un cluster MSK. Toutefois, vous pouvez mettre à jour un cluster existant pour le rendre accessible au public. Vous pouvez également créer un cluster, puis le mettre à jour pour le rendre accessible au public.

Vous pouvez activer l'accès public à un cluster MSK sans frais supplémentaires, mais les coûts de transfert de AWS données standard s'appliquent pour le transfert de données vers et depuis le cluster. Pour plus d'informations sur la tarification, consultez Tarification à la demande Amazon EC2.

Pour activer l'accès public à un cluster, assurez-vous d'abord que le cluster répond à toutes les conditions suivantes :

- Les sous-réseaux associés au cluster doivent être publics. Cela signifie que les sous-réseaux doivent avoir une table de routage associée à une passerelle Internet. Pour plus d'informations sur la manière de créer et d'attacher une passerelle Internet, consultez Passerelles Internet dans le Guide de l'utilisateur Amazon VPC.

- Le contrôle d'accès non authentifié doit être désactivé et au moins l'une des méthodes de contrôle d'accès suivantes doit être activée : SASL/IAM, SASL/SCRAM, mTLS. Pour de plus amples informations sur la manière de mettre à jour la méthode de contrôle d'accès d'un cluster, consultez the section called “Mise à jour de sécurité”.
- Le chiffrement au sein du cluster doit être activé. Le paramètre Activé est la valeur par défaut lors de la création d'un cluster. Il n'est pas possible d'activer le chiffrement au sein du cluster pour un cluster créé alors qu'il était désactivé. Il n'est dès lors pas possible d'activer l'accès public pour un cluster créé alors que le chiffrement était désactivé.
- Le trafic en texte brut entre les agents et les clients doit être désactivé. Pour plus d'informations sur la manière de le désactiver s'il est activé, consultez the section called “Mise à jour de sécurité”.
- Si vous utilisez les méthodes de contrôle d'accès SASL/SCRAM ou mTLS, vous devez définir des listes de contrôle d'accès (ACL) Apache Kafka pour votre cluster. Après avoir défini les listes de contrôle d'accès (ACL) Apache Kafka pour votre cluster, mettez à jour la configuration du cluster pour que la propriété `allow.everyone.if.no.acl.found` soit définie sur false pour le cluster. Pour de plus amples informations sur la manière de mettre à jour la configuration d'un cluster, consultez the section called “Opérations de configuration”. Si vous utilisez le contrôle d'accès IAM et que vous souhaitez appliquer des politiques d'autorisation ou mettre à jour vos politiques d'autorisation, consultez the section called “Contrôle d'accès IAM”. Pour en savoir plus sur les listes de contrôle d'accès (ACL) Apache Kafka, consultez the section called “Listes de contrôle d'accès (ACL) Apache Kafka”.

Une fois que vous vous êtes assuré qu'un cluster MSK répond aux conditions répertoriées ci-dessus, vous pouvez utiliser l' AWS Management Console API Amazon MSK ou l'API Amazon MSK pour activer l'accès public. AWS CLI Après avoir activé l'accès public à un cluster, vous pouvez obtenir une chaîne bootstrap-brokers publique pour celui-ci. Pour de plus amples informations sur l'obtention des agents d'amorçage pour un cluster, consultez the section called “Obtention des agents d'amorçage”.

> **Important**
>
> Outre l'activation de l'accès public, assurez-vous que les groupes de sécurité du cluster disposent de règles TCP entrantes qui autorisent l'accès public à partir de votre adresse IP. Nous vous recommandons de rendre ces règles aussi restrictives que possible. Pour plus d'informations sur les groupes de sécurité et les règles entrantes, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC. Pour les numéros de port, consultez the section called “Informations sur le port”. Pour obtenir des instructions

sur la manière de modifier le groupe de sécurité d'un cluster, consultez the section called “Modification des groupes de sécurité”.

> **Note**
>
> Si vous utilisez les instructions suivantes pour activer l'accès public et que vous ne parvenez toujours pas à accéder au cluster, consultez the section called “Impossible d'accéder au cluster dont l'accès public est activé”.

Activation de l'accès public à l'aide de la console

1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Dans la liste des clusters, choisissez le cluster pour lequel vous souhaitez activer l'accès public.
3. Choisissez l'onglet Propriétés, puis recherchez la section Paramètres réseau.
4. Choisissez Modifier l'accès public.

Activation de l'accès public à l'aide du AWS CLI

1. Exécutez la AWS CLI commande suivante en remplaçant *ClusterArn* *Current-Cluster-Version* par l'ARN et la version actuelle du cluster. Pour trouver la version actuelle du cluster, utilisez l'DescribeClusteropération ou la commande describe-cluster AWS CLI . Voici un exemple de version : `KTVPDKIKX0DER`.

   ```
   aws kafka update-connectivity --cluster-arn ClusterArn --current-
   version Current-Cluster-Version --connectivity-info '{"PublicAccess": {"Type":
    "SERVICE_PROVIDED_EIPS"}}'
   ```

   La sortie de cette commande `update-connectivity` ressemble à l'exemple JSON suivant.

   ```
   {
       "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/exampleClusterName/
   abcdefab-1234-abcd-5678-cdef0123ab01-2",
       "ClusterOperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
   operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
   abcd-4f7f-1234-9876543210ef"
   ```

```
}
```

> **Note**
>
> Pour désactiver l'accès public, utilisez une AWS CLI commande similaire, mais avec les informations de connectivité suivantes à la place :
>
> ```
> '{"PublicAccess": {"Type": "DISABLED"}}'
> ```

2. Pour obtenir le résultat de l'`update-connectivity`opération, exécutez la commande suivante en remplaçant *`ClusterOperationArn`* par l'ARN que vous avez obtenu dans le résultat de la `update-connectivity` commande.

```
aws kafka describe-cluster-operation --cluster-operation-arn ClusterOperationArn
```

La sortie de cette commande `describe-cluster-operation` ressemble à l'exemple JSON suivant.

```
{
    "ClusterOperationInfo": {
        "ClientRequestId": "982168a3-939f-11e9-8a62-538df00285db",
        "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/
exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2",
        "CreationTime": "2019-06-20T21:08:57.735Z",
        "OperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef",
        "OperationState": "UPDATE_COMPLETE",
        "OperationType": "UPDATE_CONNECTIVITY",
        "SourceClusterInfo": {
            "ConnectivityInfo": {
                "PublicAccess": {
                    "Type": "DISABLED"
                }
            }
        },
        "TargetClusterInfo": {
            "ConnectivityInfo": {
                "PublicAccess": {
                    "Type": "SERVICE_PROVIDED_EIPS"
```

```
                }
            }
        }
    }
}
```

Si `OperationState` a la valeur `UPDATE_IN_PROGRESS`, attendez un moment, puis exécutez à nouveau la commande `describe-cluster-operation`.

Activation de l'accès public à l'aide de l'API Amazon MSK

- Pour utiliser l'API afin d'activer ou de désactiver l'accès public à un cluster, consultez UpdateConnectivity.

> **Note**
>
> Pour des raisons de sécurité, Amazon MSK n'autorise pas l'accès public aux nœuds de contrôleur Apache ZooKeeper ou Kraft.

Accès depuis le VPC du cluster AWS mais depuis l'extérieur

Pour vous connecter à un cluster MSK depuis l'intérieur AWS mais en dehors de l'Amazon VPC du cluster, les options suivantes existent.

Appairage de VPC Amazon

Pour vous connecter à votre cluster MSK à partir d'un VPC autre que celui du cluster, vous pouvez créer une connexion d'appairage entre les deux VPC. Pour plus d'informations sur l'appairage de VPC, consultez le Manuel d’appairage de VPC Amazon.

AWS Direct Connect

AWS Direct Connect relie votre réseau sur site à AWS un câble à fibre optique Ethernet standard de 1 ou 10 gigabits. Une extrémité du câble est connectée à votre routeur, l'autre à un AWS Direct Connect routeur. Une fois cette connexion établie, vous pouvez créer des interfaces virtuelles directement vers le AWS cloud et Amazon VPC, en contournant les fournisseurs de services Internet sur votre chemin réseau. Pour plus d’informations, consultez AWS Direct Connect.

AWS Transit Gateway

AWS Transit Gateway est un service qui vous permet de connecter vos VPC et vos réseaux locaux à une passerelle unique. Pour plus d'informations sur la façon d'utiliser AWS Transit Gateway, consultez AWS Transit Gateway.

Connexions VPN

Vous pouvez connecter le VPC de votre cluster MSK à des réseaux distants et à des utilisateurs à l'aide des options de connectivité VPN décrites dans la rubrique suivante : Connexions VPN.

Proxies REST

Vous pouvez installer un proxy REST sur une instance qui s'exécute dans le VPC Amazon de votre cluster. Les proxies REST permettent à vos producteurs et consommateurs de communiquer avec le cluster via des requêtes API HTTP.

Connectivité à plusieurs VPC dans plusieurs régions

Le document suivant décrit les options de connectivité pour plusieurs VPC résidant dans différentes régions : Connectivité à plusieurs VPC dans plusieurs régions.

Connectivité privée à plusieurs VPC dans une seule région

La connectivité privée multi-VPC (optimisée par AWS PrivateLink) pour les clusters Amazon Managed Streaming for Apache Kafka (Amazon MSK) est une fonctionnalité qui vous permet de connecter plus rapidement des clients Kafka hébergés dans différents comptes AWS et clouds privés virtuels (VPC) à un cluster Amazon MSK.

Consultez Connectivité à plusieurs VPC dans une seule région pour les clients intercompte.

Le réseau EC2-Classic est retiré

Amazon MSK ne prend plus en charge les instances Amazon EC2 exécutées avec le réseau Amazon EC2-Classic.

Voir EC2-Classic Networking est en train de prendre sa retraite. Voici comment vous y préparer.

Connectivité privée à plusieurs VPC Amazon MSK dans une seule région

La connectivité privée multi-VPC (optimisée par AWS PrivateLink) pour les clusters Amazon Managed Streaming for Apache Kafka (Amazon MSK) est une fonctionnalité qui vous permet de connecter plus rapidement des clients Kafka hébergés dans différents comptes AWS et clouds privés virtuels (VPC) à un cluster Amazon MSK.

La connectivité privée à plusieurs VPC est une solution gérée qui simplifie l'infrastructure réseau pour la connectivité à plusieurs VPC et intercompte. Les clients peuvent se connecter au cluster Amazon MSK PrivateLink tout en conservant tout le trafic sur le AWS réseau. La connectivité privée multi-VPC pour les clusters Amazon MSK est disponible dans toutes les régions AWS où Amazon MSK est disponible.

Rubriques

Qu'est-ce que la connectivité privée à plusieurs VPC ?

La connectivité privée multi-VPC pour Amazon MSK est une option de connectivité qui vous permet de connecter des clients Apache Kafka hébergés dans différents AWS comptes et clouds privés virtuels (VPC) à un cluster MSK.

Amazon MSK simplifie l'accès intercompte grâce à des politiques de cluster. Ces politiques permettent au propriétaire du cluster d'accorder des autorisations à d'autres AWS comptes afin d'établir une connectivité privée avec le cluster MSK.

Avantages de la connectivité privée à plusieurs VPC

La connectivité privée à plusieurs VPC présente plusieurs avantages par rapport aux autres solutions de connectivité :

- Il automatise la gestion opérationnelle de la solution de AWS PrivateLink connectivité.
- Elle permet le chevauchement des adresses IP entre les VPC connectés, éliminant ainsi le besoin de conserver des adresses IP qui ne se chevauchent pas, l'appairage complexe et les tables de routage associées à d'autres solutions de connectivité VPC.

Vous utilisez une politique de cluster pour votre cluster MSK afin de définir les AWS comptes autorisés à configurer une connectivité privée entre comptes avec votre cluster MSK. L'administrateur intercompte peut déléguer des autorisations aux rôles ou aux utilisateurs appropriés. Lorsqu'elle est utilisée avec l'authentification du client IAM, vous pouvez également utiliser la politique de cluster pour définir sur une base granulaire les autorisations de plan de données Kafka pour les clients qui se connectent.

Exigences et limites relatives à la connectivité privée à plusieurs VPC

Notez ces exigences de cluster MSK lors de l'exécution d'une connectivité privée à plusieurs VPC :

- La connectivité privée à plusieurs VPC n'est prise en charge que sur la version 2.7.1 ou ultérieure d'Apache Kafka. Assurez-vous que tous les clients que vous utilisez avec le cluster MSK exécutent des versions d'Apache Kafka compatibles avec le cluster.
- La connectivité privée à plusieurs VPC prend en charge les types d'authentification IAM, TLS et SASL/SCRAM. Les clusters non authentifiés ne peuvent pas utiliser la connectivité privée à plusieurs VPC.
- Si vous utilisez les méthodes de contrôle d'accès SASL/SCRAM ou mTLS, vous devez définir des listes de contrôle d'accès (ACL) Apache Kafka pour votre cluster. Définissez d'abord les listes de contrôle d'accès (ACL) Apache Kafka pour votre cluster. Mettez ensuite à jour la configuration du cluster pour que la propriété `allow.everyone.if.no.acl.found` soit définie sur false pour le cluster. Pour de plus amples informations sur la manière de mettre à jour la configuration d'un cluster, consultez the section called “Opérations de configuration”. Si vous utilisez le contrôle d'accès IAM et que vous souhaitez appliquer des politiques d'autorisation ou mettre à jour vos politiques d'autorisation, consultez the section called “Contrôle d'accès IAM”. Pour en savoir plus sur les listes de contrôle d'accès (ACL) Apache Kafka, consultez the section called “Listes de contrôle d'accès (ACL) Apache Kafka”.
- La connectivité privée à plusieurs VPC ne prend pas en charge le type d'instance t3.small.
- La connectivité privée multi-VPC n'est pas prise en charge dans toutes AWS les régions, uniquement sur les AWS comptes d'une même région.

- Amazon MSK ne prend pas en charge la connectivité privée à plusieurs VPC aux nœuds ZooKeeper.

Mise en route avec la connectivité privée à plusieurs VPC

Rubriques

- Étape 1 : sur le cluster MSK du compte A, activez la connectivité à plusieurs VPC pour le schéma d'authentification IAM sur le cluster
- Étape 2 : attacher une politique de cluster au cluster MSK
- Étape 3 : actions des utilisateurs intercompte pour configurer les connexions VPC gérées par le client

Ce didacticiel utilise un cas d'utilisation courant comme exemple de la manière dont vous pouvez utiliser la connectivité multi-VPC pour connecter en privé un client Apache Kafka à un cluster MSK depuis l'intérieur du VPC du cluster AWS, mais depuis l'extérieur. Ce processus nécessite que l'utilisateur intercompte crée une connexion VPC gérée par MSK et une configuration pour chaque client, y compris les autorisations client requises. Le processus nécessite également que le propriétaire du cluster MSK active la PrivateLink connectivité sur le cluster MSK et sélectionne des schémas d'authentification pour contrôler l'accès au cluster.

Dans différentes parties de ce didacticiel, nous choisissons les options qui s'appliquent à cet exemple. Cela ne signifie pas qu'il s'agit des seules options qui fonctionnent pour configurer un cluster MSK ou des instances clients.

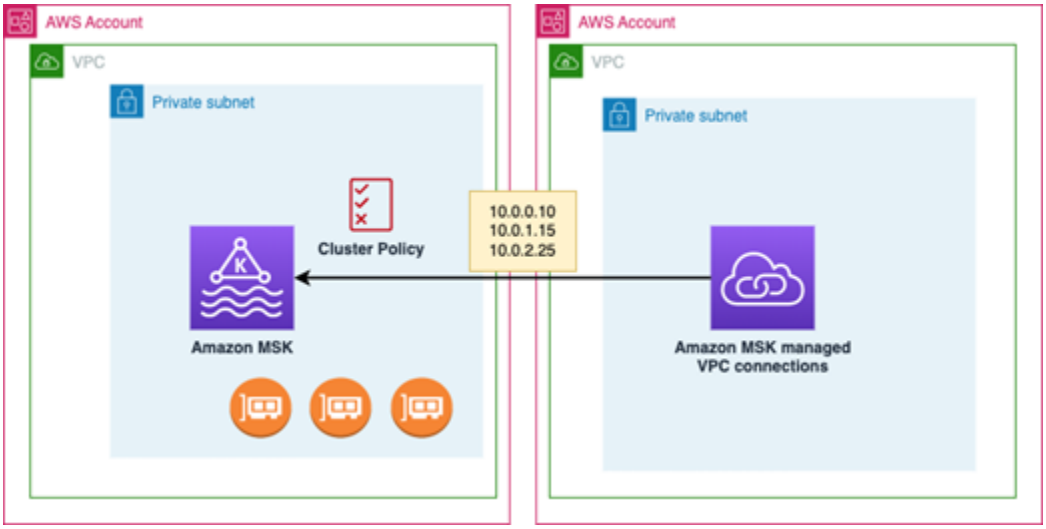
La configuration réseau pour ce cas d'utilisation est la suivante :

- Un utilisateur intercompte (client Kafka) et un cluster MSK se trouvent dans le(la) même réseau/région AWS , mais dans des comptes différents :
  - Cluster MSK dans le compte A
  - Client Kafka dans le compte B
- L'utilisateur intercompte se connectera en privé au cluster MSK à l'aide du schéma d'authentification IAM.

Ce didacticiel part du principe qu'un cluster MSK alloué a été créé avec la version 2.7.1 ou supérieure d'Apache Kafka. Le cluster MSK doit être à l'état ACTIF avant de commencer le processus de configuration. Pour éviter d'éventuelles pertes de données ou interruptions de service, les clients qui

utiliseront une connexion privée à plusieurs VPC pour se connecter au cluster doivent utiliser des versions d'Apache Kafka compatibles avec le cluster.

Le schéma suivant illustre l'architecture de la connectivité multi-VPC Amazon MSK connectée à un client dans un autre compte. AWS



Étape 1 : sur le cluster MSK du compte A, activez la connectivité à plusieurs VPC pour le schéma d'authentification IAM sur le cluster

Le propriétaire du cluster MSK doit définir les paramètres de configuration du cluster MSK une fois que celui-ci a été créé et qu'il est à l'état ACTIF.

Le propriétaire du cluster active la connectivité privée à plusieurs VPC sur le cluster ACTIF pour tous les schémas d'authentification qui seront actifs sur le cluster. Cela peut être fait à l'aide de l'UpdateSecurity API ou de la console MSK. Les schémas d'authentification IAM, SASL/SCRAM et TLS prennent en charge la connectivité privée à plusieurs VPC. La connectivité privée à plusieurs VPC ne peut pas être activée pour les clusters non authentifiés.

Dans ce cas d'utilisation, vous allez configurer le cluster pour qu'il utilise le schéma d'authentification IAM.

> **Note**
>
> Si vous configurez votre cluster MSK pour utiliser le schéma d'authentification SASL/SCRAM, la propriété « `allow.everyone.if.no.acl.found=false` » des listes de contrôle d'accès (ACL) Apache Kafka est obligatoire. Consultez Listes de contrôle d'accès (ACL) Apache Kafka.

Lorsque vous mettez à jour les paramètres de connectivité privée à plusieurs VPC, Amazon MSK lance un redémarrage progressif des nœuds d'agent qui met à jour les configurations des agents. Cela peut prendre jusqu'à 30 minutes ou plus. Vous ne pouvez pas apporter d'autres mises à jour au cluster pendant que la connectivité est en cours de mise à jour.

Activez la connectivité à plusieurs VPC pour les schémas d'authentification sélectionnés sur le cluster dans le compte A à l'aide de la console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/ pour le compte sur lequel se trouve le cluster.
2. Dans le volet de navigation, sous Clusters MSK, choisissez Clusters pour afficher la liste des clusters du compte.
3. Sélectionnez le cluster à configurer pour la connectivité privée à plusieurs VPC. Le cluster doit être à l'état ACTIF.
4. Sélectionnez l'onglet Propriétés du cluster, puis accédez aux paramètres Réseau.
5. Sélectionnez le menu déroulant Modifier, puis sélectionnez Activer la connectivité à plusieurs VPC.
6. Sélectionnez un ou plusieurs types d'authentification que vous souhaitez activer pour ce cluster. Pour ce cas d'utilisation, sélectionnez Authentification basée sur les rôles IAM.
7. Sélectionnez Enregistrer les modifications.

Example - UpdateConnectivity API qui active les schémas d'authentification de connectivité privée multi-VPC sur un cluster

Comme alternative à la console MSK, vous pouvez utiliser l'UpdateConnectivity API pour activer la connectivité privée multi-VPC et configurer des schémas d'authentification sur un cluster ACTIVE. L'exemple suivant illustre le schéma d'authentification IAM activé pour le cluster.

```
{
  "currentVersion": "K3T4TT2Z381HKD",
  "connectivityInfo": {
    "vpcConnectivity": {
      "clientAuthentication": {
        "sasl": {
          "iam": {
            "enabled": TRUE
            }
        }
```

```
      }
    }
  }
}
```

Amazon MSK crée l'infrastructure réseau requise pour la connectivité privée. Amazon MSK crée également un nouvel ensemble de points de terminaison d'agent d'amorçage pour chaque type d'authentification nécessitant une connectivité privée. Notez que le schéma d'authentification en texte brut ne prend pas en charge la connectivité privée à plusieurs VPC.

Étape 2 : attacher une politique de cluster au cluster MSK

Le propriétaire du cluster peut attacher une politique de cluster (également appelée politique basée sur des ressources) au cluster MSK pour lequel vous activerez la connectivité privée à plusieurs VPC. La politique de cluster autorise les clients à accéder au cluster à partir d'un autre compte. Avant de pouvoir modifier la politique de cluster, vous avez besoin du ou des ID des comptes qui doivent être autorisés à accéder au cluster MSK. Consultez Fonctionnement d'Amazon MSK avec IAM.

Le propriétaire du cluster doit attacher une politique de cluster au cluster MSK qui autorise l'utilisateur intercompte du compte B à obtenir des agents d'amorçage pour le cluster et à autoriser les actions suivantes sur le cluster MSK dans le compte A :

- CreateVpcRaccordement
- GetBootstrapCourtiers
- DescribeCluster
- DescribeClusterV2

Example

À titre de référence, voici un exemple du JSON pour une politique de cluster de base, similaire à la politique par défaut affichée dans l'éditeur de politiques IAM de la console MSK.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012"
```

```
                ]
            },
            "Action": [
                "kafka:CreateVpcConnection",
                "kafka:GetBootstrapBrokers",
                "kafka:DescribeCluster",
                "kafka:DescribeClusterV2"
            ],
            "Resource": "arn:aws:kafka:us-east-1:123456789012:cluster/testing/
de8982fa-8222-4e87-8b20-9bf3cdfa1521-2"
        }
    ]
}
```

Attacher une politique de cluster au cluster MSK

1. Dans la console Amazon MSK, sous Clusters MSK, sélectionnez Clusters.
2. Faites défiler la page jusqu'à Paramètres de sécurité et sélectionnez Modifier la politique de cluster.
3. Dans la console, sur l'écran Modifier la politique de cluster, sélectionnez Politique de base pour la connectivité à plusieurs VPC.
4. Dans le champ ID de compte, entrez l'ID de compte pour chaque compte qui doit être autorisé à accéder à ce cluster. Lorsque vous tapez l'ID, il est automatiquement copié dans la syntaxe JSON de politique affichée. Dans notre exemple de politique de cluster, l'ID de compte est `123456789012`.
5. Sélectionnez Enregistrer les modifications.

Pour plus d'informations sur les API de politique de cluster, consultez Politiques basées sur des ressources Amazon MSK.

Étape 3 : actions des utilisateurs intercompte pour configurer les connexions VPC gérées par le client

Pour configurer une connectivité privée à plusieurs VPC entre un client d'un compte différent de celui du cluster MSK, l'utilisateur intercompte crée une connexion VPC gérée pour le client. Plusieurs clients peuvent être connectés au cluster MSK en répétant cette procédure. Dans le cadre de ce cas d'utilisation, vous ne configurerez qu'un seul client.

Les clients peuvent utiliser les schémas d'authentification pris en charge (IAM, SASL/SCRAM ou TLS). Chaque connexion VPC gérée ne peut être associée qu'à un seul schéma d'authentification.

Le schéma d'authentification du client doit être configuré sur le cluster MSK auquel le client va se connecter.

Dans ce cas d'utilisation, configurez le schéma d'authentification du client de sorte que le client du compte B utilise le schéma d'authentification IAM.

Prérequis

Ce processus nécessite les éléments suivants :

- Politique de cluster créée précédemment qui accorde au client du compte B l'autorisation d'effectuer des actions sur le cluster MSK du compte A.
- Politique d'identité attachée au client dans le compte B qui accorde des `kafka:CreateVpcConnection` autorisations `ec2:CreateVPCEndpoint` et `ec2:CreateTags` des `ec2:DescribeVpcAttribute` actions.

Example

À titre de référence, voici un exemple du JSON pour une politique d'identité client de base.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kafka:CreateVpcConnection",
        "ec2:CreateTags",
        "ec2:CreateVPCEndpoint",
        "ec2:DescribeVpcAttribute"
      ],
      "Resource": "*"
    }
  ]
}
```

Pour créer une connexion VPC gérée pour un client dans le compte B

1. Obtenez auprès de l'administrateur du cluster l'ARN de cluster du cluster MSK du compte A auquel vous souhaitez que le client du compte B se connecte. Notez l'ARN du cluster à utiliser ultérieurement.

2. Dans la console MSK du compte client B, choisissez Connexions VPC gérées, puis sélectionnez Créer une connexion.
3. Dans le volet Paramètres de connexion, collez l'ARN du cluster dans le champ de texte ARN du cluster, puis choisissez Vérifier.
4. Sélectionnez le type d'authentification pour le client dans le compte B. Pour ce cas d'utilisation, choisissez IAM lors de la création de la connexion VPC du client.
5. Choisissez le VPC pour le client.
6. Choisissez au moins deux zones de disponibilité et les sous-réseaux associés. Vous pouvez obtenir les ID de zone de disponibilité dans les détails du cluster de la console de AWS gestion ou à l'aide de l'DescribeClusterAPI ou de la commande describe-cluster AWS CLI. Les ID de zone que vous spécifiez pour le sous-réseau client doivent correspondre à ceux du sous-réseau du cluster. Si les valeurs d'un sous-réseau sont manquantes, créez d'abord un sous-réseau avec le même ID de zone que votre cluster MSK.
7. Choisissez un groupe de sécurité pour cette connexion VPC. Vous pouvez utiliser le groupe de sécurité par défaut. Pour plus d'informations sur la configuration d'un groupe de sécurité, consultez Contrôler le trafic vers vos ressources à l'aide de groupes de sécurité.
8. Sélectionnez Créer une connexion.
9. Pour obtenir la liste des nouvelles chaînes d'agent d'amorçage à partir de la console MSK de l'utilisateur intercompte (Détails du cluster > Connexion VPC gérée), consultez les chaînes d'agent d'amorçage affichées sous « Chaîne de connexion au cluster ». À partir du compte client B, la liste des courtiers bootstrap peut être consultée en appelant l'API GetBootstrapBrokers ou en consultant la liste des courtiers bootstrap dans les détails du cluster de console.
10. Mettez à jour les groupes de sécurité associés aux connexions VPC comme suit :

    a. Définissez des règles entrantes pour le PrivateLink VPC afin d'autoriser tout le trafic de la plage d'adresses IP en provenance du réseau du compte B.

    b. [Facultatif] Définissez des règles sortantes pour la connectivité au cluster MSK. Choisissez le groupe de sécurité dans la console VPC, modifiez les règles sortantes et ajoutez une règle pour le trafic TCP personnalisé pour les plages de ports 14001 à 14100. L'équilibreur de charge Network Load Balancer à plusieurs VPC écoute les plages de ports 14001 à 14100. Consultez Équilibreurs de charge réseau.
11. Configurez le client du compte B pour utiliser les nouveaux agents d'amorçage pour la connectivité privée à plusieurs VPC afin de se connecter au cluster MSK du compte A. Consultez Produire et consommer des données.

Une fois l'autorisation terminée, Amazon MSK crée une connexion VPC gérée pour chaque VPC et schéma d'authentification spécifiés. Le groupe de sécurité choisi est associé à chaque connexion. Cette connexion VPC gérée est configurée par Amazon MSK pour se connecter en privé aux agents. Vous pouvez utiliser le nouvel ensemble d'agents d'amorçage pour vous connecter en privé au cluster Amazon MSK.

Mettre à jour les schémas d'autorisation sur un cluster

La connectivité privée à plusieurs VPC prend en charge les schémas d'authentification SASL/SCRAM, IAM et TLS. Le propriétaire du cluster peut activer/désactiver la connectivité privée pour un ou plusieurs schémas d'authentification. Le cluster doit être à l'état ACTIF pour effectuer cette action.

Pour activer un schéma d'authentification à l'aide de la console Amazon MSK

1. Ouvrez la console Amazon MSK dans la AWS Management Console du cluster que vous souhaitez modifier.
2. Dans le volet de navigation, sous Clusters MSK, choisissez Clusters pour afficher la liste des clusters du compte.
3. Sélectionnez le cluster que vous souhaitez modifier. Le cluster doit être à l'état ACTIF.
4. Sélectionnez l'onglet Propriétés du cluster, puis accédez aux paramètres réseau.
5. Sélectionnez le menu déroulant Modifier, puis sélectionnez Activer la connectivité à plusieurs VPC pour activer un nouveau schéma d'authentification.
6. Sélectionnez un ou plusieurs types d'authentification que vous souhaitez activer pour ce cluster.
7. Sélectionnez Activer la sélection.

Lorsque vous activez un nouveau schéma d'authentification, vous devez également créer de nouvelles connexions VPC gérées pour le nouveau schéma d'authentification et mettre à jour vos clients afin qu'ils utilisent les agents d'amorçage spécifiques au nouveau schéma d'authentification.

Pour désactiver un schéma d'authentification à l'aide de la console Amazon MSK

> **Note**
>
> Lorsque vous désactivez la connectivité privée à plusieurs VPC pour les schémas d'authentification, toutes les infrastructures liées à la connectivité, y compris les connexions VPC gérées, sont supprimées.

Lorsque vous désactivez la connectivité privée à plusieurs VPC pour les schémas d'authentification, les connexions VPC existantes côté client deviennent INACTIVES, et l'infrastructure Privatelink côté cluster, y compris les connexions VPC gérées, est supprimée. L'utilisateur intercompte peut uniquement supprimer la connexion VPC inactive. Si la connectivité privée est réactivée sur le cluster, l'utilisateur intercompte doit créer une nouvelle connexion au cluster.

1. Ouvrez la console Amazon MSK dans la AWS Management Console.
2. Dans le volet de navigation, sous Clusters MSK, choisissez Clusters pour afficher la liste des clusters du compte.
3. Sélectionnez le cluster que vous souhaitez modifier. Le cluster doit être à l'état ACTIF.
4. Sélectionnez l'onglet Propriétés du cluster, puis accédez aux paramètres réseau.
5. Sélectionnez le menu déroulant Modifier, puis sélectionnez Désactiver la connectivité à plusieurs VPC (pour désactiver un schéma d'authentification).
6. Sélectionnez un ou plusieurs types d'authentification que vous souhaitez désactiver pour ce cluster.
7. Sélectionnez Désactiver la sélection.

Example Pour activer/désactiver un schéma d'authentification avec l'API

Comme alternative à la console MSK, vous pouvez utiliser l'UpdateConnectivity API pour activer la connectivité privée multi-VPC et configurer des schémas d'authentification sur un cluster ACTIVE. L'exemple suivant illustre les schémas d'authentification SASL/SCRAM et IAM activé pour le cluster.

Lorsque vous activez un nouveau schéma d'authentification, vous devez également créer de nouvelles connexions VPC gérées pour le nouveau schéma d'authentification et mettre à jour vos clients afin qu'ils utilisent les agents d'amorçage spécifiques au nouveau schéma d'authentification.

Lorsque vous désactivez la connectivité privée à plusieurs VPC pour les schémas d'authentification, les connexions VPC existantes côté client deviennent INACTIVES, et l'infrastructure Privatelink côté cluster, y compris les connexions VPC gérées, est supprimée. L'utilisateur intercompte peut uniquement supprimer la connexion VPC inactive. Si la connectivité privée est réactivée sur le cluster, l'utilisateur intercompte doit créer une nouvelle connexion au cluster.

```
Request:
{
  "currentVersion": "string",
  "connnectivityInfo": {
```

```
    "publicAccess": {
      "type": "string"
    },
    "vpcConnectivity": {
      "clientAuthentication": {
        "sasl": {
          "scram": {
            "enabled": TRUE
          },
          "iam": {
            "enabled": TRUE
          }
        },
        "tls": {
          "enabled": FALSE
        }
      }
    }
  }
}

Response:
{
  "clusterArn": "string",
  "clusterOperationArn": "string"
}
```

Refuser une connexion VPC gérée à un cluster Amazon MSK

Dans la console Amazon MSK du compte administrateur du cluster, vous pouvez refuser une connexion VPC du client. La connexion VPC du client doit être à l'état DISPONIBLE pour être refusée. Vous souhaiterez peut-être refuser une connexion VPC gérée provenant d'un client qui n'est plus autorisé à se connecter à votre cluster. Pour empêcher les nouvelles connexions VPC gérées de se connecter à un client, refusez l'accès au client dans la politique de cluster. Une connexion refusée entraîne toujours des frais jusqu'à ce qu'elle soit supprimée par le propriétaire de la connexion. Consultez Supprimer une connexion VPC gérée à un cluster Amazon MSK.

Pour refuser une connexion VPC du client à l'aide de la console MSK

1. Ouvrez la console Amazon MSK dans la AWS Management Console.
2. Dans le volet de navigation, sélectionnez Clusters et accédez à la liste Paramètres réseau > Connexions VPC du client.

3. Sélectionnez la connexion que vous souhaitez refuser, puis sélectionnez Refuser la connexion VPC du client.
4. Confirmez que vous souhaitez refuser la connexion VPC du client sélectionnée.

Pour refuser une connexion VPC gérée à l'aide de l'API, utilisez l'API `RejectClientVpcConnection`.

Supprimer une connexion VPC gérée à un cluster Amazon MSK

L'utilisateur intercompte peut supprimer une connexion VPC gérée pour un cluster MSK dans la console du compte client. Étant donné que l'utilisateur propriétaire du cluster ne possède pas la connexion VPC gérée, celle-ci ne peut pas être supprimée du compte administrateur du cluster. Une fois qu'une connexion VPC est supprimée, elle n'entraîne plus de frais.

Pour supprimer une connexion VPC gérée à l'aide de la console MSK

1. Dans le compte client, ouvrez la console Amazon MSK dans la AWS Management Console.
2. Dans le volet de navigation, sélectionnez Connexions VPC gérées.
3. Dans la liste des connexions, sélectionnez la connexion que vous souhaitez supprimer.
4. Confirmez que vous voulez supprimer la connexion VPC.

Pour supprimer une connexion VPC gérée à l'aide de l'API, utilisez l'API `DeleteVpcConnection`.

Autorisations pour la connectivité privée à plusieurs VPC

Cette section résume les autorisations requises pour les clients et les clusters à l'aide de la fonctionnalité de connectivité privée à plusieurs VPC. La connectivité privée à plusieurs VPC nécessite que l'administrateur du client crée des autorisations pour chaque client qui disposera d'une connexion VPC gérée au cluster MSK. L'administrateur du cluster MSK doit également activer la PrivateLink connectivité sur le cluster MSK et sélectionner des schémas d'authentification pour contrôler l'accès au cluster.

Type d'authentification du cluster et autorisations d'accès aux rubriques

Activez la fonctionnalité de connectivité privée à plusieurs VPC pour les schémas d'authentification activés pour votre cluster MSK. veuillez consulter Exigences et limites relatives à la connectivité privée à plusieurs VPC. Si vous configurez votre cluster MSK pour utiliser le schéma d'authentification SASL/SCRAM, la propriété `allow.everyone.if.no.acl.found=false` des

listes de contrôle d'accès (ACL) Apache Kafka est obligatoire. Après avoir défini les Listes de contrôle d'accès (ACL) Apache Kafka pour votre cluster, mettez à jour la configuration du cluster pour que la propriété `allow.everyone.if.no.acl.found` soit définie sur false pour le cluster. Pour de plus amples informations sur la manière de mettre à jour la configuration d'un cluster, consultez Opérations de configuration d'Amazon MSK.

Autorisations de politique de cluster intercompte

Si le AWS compte d'un client Kafka est différent de celui du cluster MSK, associez au cluster MSK une politique basée sur le cluster qui autorise l'utilisateur root du client à établir une connectivité entre comptes. Vous pouvez modifier la politique de cluster à plusieurs VPC à l'aide de l'éditeur de politiques IAM de la console MSK (paramètres de sécurité du cluster > Modifier la politique de cluster) ou utiliser les API suivantes pour gérer la politique de cluster :

PutClusterPolitique

Attache une politique de cluster au cluster. Vous pouvez utiliser cette API pour créer ou mettre à jour la politique de cluster MSK spécifiée. Si vous mettez à jour la politique, le champ CurrentVersion est obligatoire dans la charge utile de la demande.

GetClusterPolitique

Récupère le texte JSON du document de politique de cluster attaché au cluster.

DeleteClusterPolitique

Supprime la politique de cluster.

Voici un exemple du JSON pour une politique de cluster de base, similaire à celle affichée dans l'éditeur de politiques IAM de la console MSK.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            },
            "Action": [
```

```
                "kafka:CreateVpcConnection",
                "kafka:GetBootstrapBrokers",
                "kafka:DescribeCluster",
                "kafka:DescribeClusterV2"
            ],
            "Resource": "arn:aws:kafka:us-east-1:123456789012:cluster/testing/
de8982fa-8222-4e87-8b20-9bf3cdfa1521-2"
        }
    ]
}
```

Autorisations client pour la connectivité privée à plusieurs VPC à un cluster MSK

Pour configurer une connectivité privée à plusieurs VPC entre un client Kafka et un cluster MSK, le client a besoin d'une politique d'identité attachée qui accorde des autorisations pour des actions `kafka:CreateVpcConnection`, `ec2:CreateTags` et `ec2:CreateVPCEndpoint` sur le client. À titre de référence, voici un exemple du JSON pour une politique d'identité client de base.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kafka:CreateVpcConnection",
        "ec2:CreateTags",
        "ec2:CreateVPCEndpoint"
      ],
      "Resource": "*"
    }
  ]
}
```

Informations sur le port

Utilisez les numéros de port suivants pour qu'Amazon MSK puisse communiquer avec les ordinateurs clients :

- Pour communiquer avec les agents en texte brut, utilisez le port 9092.
- Pour communiquer avec les courtiers à l'aide du chiffrement TLS, utilisez le port 9094 pour l'accès depuis l'intérieur AWS et le port 9194 pour l'accès public.

- Pour communiquer avec les courtiers via SASL/SCRAM, utilisez le port 9096 pour l'accès depuis l'intérieur AWS et le port 9196 pour l'accès public.
- Pour communiquer avec les courtiers d'un cluster configuré pour être utiliséthe section called “Contrôle d'accès IAM”, utilisez le port 9098 pour l'accès depuis l'intérieur AWS et le port 9198 pour l'accès public.
- Pour communiquer avec Apache à ZooKeeper l'aide du chiffrement TLS, utilisez le port 2182. ZooKeeper Les nœuds Apache utilisent le port 2181 par défaut.

Migration vers un cluster Amazon MSK

Le réplicateur Amazon MSK peut être utilisé pour la migration de clusters MSK. veuillez consulter Qu'est-ce que le réplicateur Amazon MSK ?. Vous pouvez également utiliser Apache MirrorMaker 2.0 pour migrer d'un cluster non MSK vers un cluster Amazon MSK. Pour un exemple de la procédure à suivre, consultez Migrer un cluster Apache Kafka sur site vers Amazon MSK à l'aide de. MirrorMaker Pour plus d'informations sur son utilisation MirrorMaker, consultez la section Mise en miroir des données entre clusters dans la documentation d'Apache Kafka. Nous vous recommandons de l'installer MirrorMaker dans une configuration à haute disponibilité.

Aperçu des étapes à suivre lors de l'utilisation MirrorMaker pour migrer vers un cluster MSK

1. Créez le cluster MSK de destination
2. Commencez MirrorMaker à partir d'une instance Amazon EC2 au sein du même Amazon VPC que le cluster de destination.
3. Inspectez le MirrorMaker décalage.
4. Après le MirrorMaker rattrapage, redirigez les producteurs et les consommateurs vers le nouveau cluster à l'aide des courtiers bootstrap du cluster MSK.
5. Arrêtez MirrorMaker.

Migration de votre cluster Apache Kafka vers Amazon MSK

Supposons que vous ayez un cluster Apache Kafka nommé `CLUSTER_ONPREM`. Ce cluster est rempli de rubriques et de données. Si vous souhaitez migrer ce cluster vers un cluster Amazon MSK nouvellement créé nommé `CLUSTER_AWSMSK`, cette procédure fournit une vision globale des étapes à suivre.

Pour migrer votre cluster Apache Kafka existant vers Amazon MSK

1. Dans `CLUSTER_AWSMSK`, créez toutes les rubriques que vous souhaitez migrer.

   Vous ne pouvez pas utiliser MirrorMaker cette étape car elle ne recrée pas automatiquement les sujets que vous souhaitez migrer avec le niveau de réplication approprié. Vous pouvez créer les rubriques dans Amazon MSK avec les mêmes facteurs de réplication et le même nombre de partitions qu'elles avaient dans `CLUSTER_ONPREM`. Vous pouvez également créer les rubriques avec différents facteurs de réplication et nombres de partitions.

2. Commencez MirrorMaker par une instance disposant d'un accès en lecture `CLUSTER_ONPREM` et en écritureCLUSTER_AWSMSK.
3. Exécutez la commande suivante pour mettre en miroir toutes les rubriques :

```
<path-to-your-kafka-installation>/bin/kafka-mirror-maker.sh --consumer.config
 config/mirrormaker-consumer.properties --producer.config config/mirrormaker-
producer.properties --whitelist '.*'
```

   Dans cette commande, `config/mirrormaker-consumer.properties` pointe vers un broker d'amorçage dans `CLUSTER_ONPREM` ; par exemple, `bootstrap.servers=localhost:9092`. Et `config/mirrormaker-producer.properties` pointe vers un broker bootstrap dans CLUSTER_ AWSMSK ; par exemple,. `bootstrap.servers=10.0.0.237:9092,10.0.2.196:9092,10.0.1.233:9092`
4. Continuez à MirrorMaker exécuter en arrière-plan et continuez à utiliserCLUSTER_ONPREM. MirrorMaker reflète toutes les nouvelles données.
5. Vérifiez la progression de la mise en miroir en inspectant le décalage entre le dernier décalage de chaque sujet et le décalage actuel par rapport auquel il MirrorMaker est consommé.

   N'oubliez pas qu' MirrorMaker il s'agit simplement de faire appel à un consommateur et à un producteur. Ainsi, vous pouvez vérifier le lag en utilisant l'outil `kafka-consumer-groups.sh`. Pour trouver le nom du groupe de consommateurs, recherchez la `group.id` dans le fichier `mirrormaker-consumer.properties` et utilisez sa valeur. S'il n'y a pas de clé de ce type dans le fichier, vous pouvez la créer. Par exemple, définissez `group.id=mirrormaker-consumer-group`.
6. Une fois que vous aurez MirrorMaker fini de refléter tous les sujets, arrêtez tous les producteurs et consommateurs, puis arrêtez MirrorMaker. Ensuite, redirigez les producteurs et les consommateurs vers le cluster `CLUSTER_AWSMSK` en changeant leurs valeurs de brokers d'amorçage pour les producteurs et les consommateurs. Redémarrez tous les producteurs et consommateurs sur `CLUSTER_AWSMSK`.

Migration d'un cluster Amazon MSK vers un autre

Vous pouvez utiliser Apache MirrorMaker 2.0 pour migrer d'un cluster non MSK vers un cluster MSK. Par exemple, vous pouvez migrer d'une version d'Apache Kafka vers une autre. Pour un exemple de la procédure à suivre, consultez Migrer un cluster Apache Kafka sur site vers Amazon MSK à l'aide

de. MirrorMaker Le réplicateur Amazon MSK peut être également utilisé pour la migration de clusters MSK. Pour de plus amples informations sur le réplicateur Amazon MSK, consultez Réplicateur MSK.

MirrorMaker 1.0 meilleures pratiques

Cette liste de bonnes pratiques s'applique à la MirrorMaker version 1.0.

- Exécutez MirrorMaker sur le cluster de destination. De cette façon, si un problème de réseau se produit, les messages sont toujours disponibles dans le cluster source. Si vous exécutez MirrorMaker sur le cluster source et que les événements sont mis en mémoire tampon dans le producteur et qu'il y a un problème réseau, les événements risquent d'être perdus.
- Si le chiffrement est requis en transit, exécutez-le dans le cluster source.
- Pour les consommateurs, définissez auto.commit.enabled=false
- Pour les producteurs, définissez
  - max.in.flight.requests.per.connection=1
  - nouvelles tentatives=int.max_value
  - acks=all
  - max.block.ms = Long.Max_Value
- Pour un rendement élevé du producteur :
  - Les messages de tampon et les lots de messages de remplissage - ajustent buffer.memory, batch.size, linger.ms
  - Ajustez les tampons de socket - receive.buffer.bytes, send.buffer.bytes
- Pour éviter toute perte de données, désactivez la validation automatique à la source, afin de contrôler les validations, ce qu'elle fait généralement après avoir reçu le pack du cluster de destination. MirrorMaker Si le producteur a acks=all et que le cluster de destination a min.insync.replicas défini sur plus de 1, les messages sont conservés sur plusieurs courtiers à la destination avant que le consommateur ne valide le décalage à la source. MirrorMaker
- Si l'ordre est important, vous pouvez définir les nouvelles tentatives sur 0. Sinon, pour un environnement de production, définissez la valeur 1 maximum de connexions en transit pour vous assurer que les lots envoyés ne sont pas validés hors service si un lot échoue au milieu. De cette façon, chaque lot envoyé est réessayé jusqu'à ce que le lot suivant soit envoyé. Si max.block.ms n'est pas défini sur la valeur maximale et si le tampon du producteur est plein, il peut y avoir une perte de données (selon certains des autres paramètres). Cela peut bloquer le consommateur et lui envoyer une contre-pression.

- Pour un débit élevé
  - Augmentez buffer.memory.
  - Augmentez la taille du lot.
  - Ajustez linger.ms de façon à permettre aux lots de se remplir. Cela permet également une meilleure compression, moins d'utilisation de la bande passante réseau et moins de stockage sur le cluster. Cela se traduit par une rétention accrue.
  - Surveillez l'utilisation du processeur et de la mémoire.
- Pour un débit élevé pour les consommateurs
  - Augmentez le nombre de threads/consommateurs par MirrorMaker processus — num.streams.
  - Augmentez d'abord le nombre de MirrorMaker processus sur les machines avant d'augmenter le nombre de threads pour garantir une haute disponibilité.
  - Augmentez le nombre de MirrorMaker processus d'abord sur la même machine, puis sur différentes machines (avec le même identifiant de groupe).
  - Isolez les sujets à très haut débit et utilisez des MirrorMaker instances distinctes.
- Pour la gestion et la configuration
  - Outils de gestion de l'utilisation AWS CloudFormation et de la configuration tels que Chef et Ansible.
  - Utilisez des montages Amazon EFS pour garder tous les fichiers de configuration accessibles à partir de toutes les instances Amazon EC2.
  - Utilisez des conteneurs pour faciliter le dimensionnement et la gestion des MirrorMaker instances.
- En général, il faut plus d'un consommateur pour saturer un producteur. MirrorMaker Par conséquent, veillez à mettre en place plusieurs consommateurs. Tout d'abord, configurez-les sur différents ordinateurs pour fournir une haute disponibilité. Ensuite, mettez à l'échelle des ordinateurs individuels jusqu'à avoir un consommateur pour chaque partition, les consommateurs étant répartis également entre les ordinateurs.
- Pour l'ingestion et la livraison à haut débit, ajustez les tampons de réception et d'envoi car leurs valeurs par défaut peuvent être trop faibles. Pour des performances optimales, assurez-vous que le nombre total de flux (num.streams) correspond à toutes les partitions de rubrique qui MirrorMaker tentent de copier vers le cluster de destination.

MirrorMaker 2.* avantages

- Utilise le framework et l’écosystème d’Apache Kafka Connect.
- Détecte les nouvelles rubriques et partitions.
- Synchronise automatiquement la configuration des rubriques entre les clusters.
- Prend en charge les paires de clusters « actifs/actifs », ainsi que n'importe quel nombre de clusters actifs.
- Fournit de nouvelles mesures, notamment end-to-end la latence de réplication entre plusieurs centres de données et clusters.
- Émet les décalages nécessaires pour migrer les consommateurs entre les clusters et fournit des outils pour la translation de décalage.
- Prend en charge un fichier de configuration de haut niveau pour spécifier plusieurs clusters et flux de réplication en un seul endroit, par rapport aux propriétés producteur/consommateur de bas niveau pour chaque MirrorMaker processus 1.*.

Surveillance d'un cluster Amazon MSK

Amazon MSK peut vous aider à surveiller l'état de votre cluster Amazon MSK de plusieurs manières.

- Amazon MSK vous aide à surveiller votre capacité de stockage sur disque en vous envoyant automatiquement des alertes de capacité de stockage lorsqu'un cluster est sur le point d'atteindre sa limite de capacité de stockage. Les alertes fournissent également des recommandations sur les mesures à prendre pour résoudre les problèmes détectés. Vous pouvez ainsi identifier et résoudre rapidement les problèmes de capacité du disque avant qu'ils ne deviennent critiques. Amazon MSK envoie automatiquement ces alertes à la console Amazon MSK, à AWS Health Dashboard Amazon EventBridge et aux contacts e-mail associés à votre AWS compte. Pour plus d'informations sur les alertes relatives à la capacité de stockage, consultez Alertes relatives à la capacité de stockage d'Amazon MSK.
- Amazon MSK collecte les métriques d'Apache Kafka et les envoie à Amazon CloudWatch où vous pouvez les consulter. Pour de plus amples informations sur les métriques Apache Kafka, y compris celles qu'Amazon MSK révèle, consultez Surveillance dans la documentation Apache Kafka.
- Vous pouvez également surveiller votre cluster MSK avec Prometheus, une application de surveillance open-source. Pour plus d'informations sur Prometheus, consultez Présentation dans la documentation Prometheus. Pour savoir comment surveiller votre cluster avec Prometheus, consultez the section called "Surveillance ouverte avec Prometheus".

Rubriques

Métriques Amazon MSK à surveiller avec CloudWatch

Amazon MSK s'intègre à Amazon CloudWatch afin que vous puissiez collecter, consulter et analyser les CloudWatch métriques de votre cluster Amazon MSK. Les métriques que vous configurez pour votre cluster MSK sont automatiquement collectées et transmises CloudWatch. Vous pouvez définir le niveau de surveillance d'un cluster MSK sur l'un des niveaux suivants :`DEFAULT`, `PER_BROKER`,

PER_TOPIC_PER_BROKER ou PER_TOPIC_PER_PARTITION. Les tableaux des sections suivantes présentent toutes les métriques disponibles à partir de chaque niveau de surveillance.

> **Note**
>
> Les noms de certaines métriques Amazon MSK destinées à la CloudWatch surveillance ont changé dans les versions 3.6.0 et supérieures. Utilisez les nouveaux noms pour surveiller ces métriques. Pour les métriques dont le nom a changé, le tableau ci-dessous indique le nom utilisé dans les versions 3.6.0 et supérieures, suivi du nom dans la version 2.8.2.tiered.

Les métriques de niveau DEFAULT sont gratuites. La tarification des autres statistiques est décrite sur la page de CloudWatch tarification d'Amazon.

Surveillance de niveau **DEFAULT**

Les métriques décrites dans le tableau suivant sont disponibles au niveau de la surveillance DEFAULT. Elles sont libres.

Métriques disponibles au niveau de la surveillance **DEFAULT**

Nom	Lorsqu'il est visible	Dimensions	Description
ActiveControllerCount	Une fois que le cluster a atteint l'état Actif.	Nom du cluster	Un seul contrôleur par cluster doit être actif à un moment donné.
BurstBalance	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID de l'agent	Solde restant des crédits en rafale d'entrées-sorties pour les volumes EBS du cluster. Utilisez-le pour étudier la latence ou la diminution du débit. BurstBalance n'est pas signalé pour les volumes EBS lorsque les performances de base d'un volume sont supérieures aux performances en rafale maximales. Pour de

Nom	Lorsqu'il est visible	Dimensions	Description
			plus amples informations, consultez Crédits d'E/S et performances en rafale.
BytesInPerSec	Après avoir créé une rubrique.	Nom du cluster, ID de broker, rubrique	Nombre d'octets par seconde reçus des clients. Cette métrique est disponible par agent et également par rubrique.
BytesOutPerSec	Après avoir créé une rubrique.	Nom du cluster, ID de broker, rubrique	Nombre d'octets par seconde envoyés aux clients. Cette métrique est disponible par agent et également par rubrique.
ClientConnectionCount	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID de l'agent, authentification client	Nombre de connexions client authentifiées actives.
ConnectionCount	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre de connexions actives authentifiées, non authentifiées et entre agents.

Nom	Lorsqu'il est visible	Dimensions	Description
`CPUCreditBalance`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre de crédits UC gagnés qu'un agent a accumulés depuis son lancement. Les crédits sont accumulés dans le solde de crédits quand ils sont gagnés et supprimés du solde de crédits lorsqu'ils sont dépensés. Si vous avez épuisé le solde de crédits UC, cela peut avoir un impact négatif sur les performances de votre cluster. Vous pouvez prendre des mesures pour réduire la charge de l'UC. Par exemple, vous pouvez réduire le nombre de demandes des clients ou remplacer le type d'agent par un type d'agent M5.
`CpuIdle`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pourcentage de temps d'inactivité du processeur.
`CpuIoWait`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pourcentage de temps d'inactivité de l'UC pendant une opération sur disque en attente.
`CpuSystem`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pourcentage de CPU dans l'espace du noyau.

Nom	Lorsqu'il est visible	Dimensions	Description
`CpuUser`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pourcentage de CPU dans l'espace utilisateur.
`GlobalPartitionCount`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster	Nombre de partitions parmi toutes les rubriques du cluster, à l'exception des réplicas. Comme il `GlobalPartitionCount` n'inclut pas les répliques, la somme des `PartitionCount` valeurs peut être plus élevée que GlobalPartitionCount si le facteur de réplication d'un sujet est supérieur à 1.
`GlobalTopicCount`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster	Nombre total de rubriques parmi tous les brokers du cluster.
`EstimatedMaxTimeLag`	Après que le groupe de consommateurs a consommé à partir d'une rubrique.	Groupe de consommateurs, rubrique	Estimation du temps (en secondes) de purge de `MaxOffsetLag` .
`KafkaAppLogsDiskUsed`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pourcentage d'espace disque utilisé pour les journaux d'application.

Nom	Lorsqu'il est visible	Dimensions	Description
`KafkaDataLogsDiskUsed` (dimension `ClusterName, Broker ID`)	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pourcentage d'espace disque utilisé pour les journaux de données.
`KafkaDataLogsDiskUsed` (dimension `ClusterName`)	Une fois que le cluster a atteint l'état Actif.	Nom du cluster	Pourcentage d'espace disque utilisé pour les journaux de données.
`LeaderCount`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre total de leaders de partitions par agent, sans inclure les réplicas.
`MaxOffsetLag`	Après que le groupe de consommateurs a consommé à partir d'une rubrique.	Groupe de consommateurs, rubrique	Retard de décalage maximal entre toutes les partitions d'une rubrique.
`MemoryBuffered`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Taille en octets de mémoire tampon pour le broker.
`MemoryCached`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Taille en octets de mémoire cache pour le broker.

Nom	Lorsqu'il est visible	Dimensions	Description
`MemoryFree`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	La taille en octets de mémoire qui est libre et disponible pour le broker.
`HeapMemoryAfterGC`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pourcentage de mémoire de tas totale utilisée après le récupérateur de mémoire.
`MemoryUsed`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Taille en octets de mémoire utilisée pour le broker.
`MessagesInPerSec`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre de messages entrants par seconde pour le broker.
`NetworkRxDropped`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre de paquets de réception supprimés.
`NetworkRxErrors`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre d'erreurs de réception réseau pour le broker.

Nom	Lorsqu'il est visible	Dimensions	Description
`NetworkRxPackets`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre de paquets reçus par le broker.
`NetworkTxDropped`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre de paquets de transmission abandonnés.
`NetworkTxErrors`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre d'erreurs de transmission réseau pour le broker.
`NetworkTxPackets`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre de paquets transmis par le broker.
`OfflinePartitionsCount`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster	Nombre total de partitions hors connexion dans le cluster.
`PartitionCount`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre total de partitions de rubrique par agent, y compris les réplicas.

Nom	Lorsqu'il est visible	Dimensions	Description
`ProduceTotalTimeMsMean`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Temps moyen de production en millisecondes.
`RequestBytesMean`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre moyen d'octets de demandes pour le broker.
`RequestTime`	Après l'application de la limitation de demande.	Nom du cluster, ID du broker	Temps moyen en millisecondes passé dans le réseau de courtage et les threads d'E/S pour traiter les demandes.
`RootDiskUsed`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pourcentage du disque racine utilisé par le broker.
`SumOffsetLag`	Après que le groupe de consommateurs a consommé à partir d'une rubrique.	Groupe de consommateurs, rubrique	Retard de décalage agrégé pour toutes les partitions d'une rubrique.
`SwapFree`	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Taille en octets de mémoire d'échange disponible pour le broker.

Nom	Lorsqu'il est visible	Dimensions	Description
SwapUsed	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Taille en octets de mémoire d'échange utilisée pour le broker.
TrafficShaping	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Métriques de haut niveau indiquant le nombre de paquets formés (abandonnés ou mis en file d'attente) en raison du dépassement des allocations réseau. Des détails plus fins sont disponibles avec les métriques PER_BROKER.
UnderMinIsrPartitionCount	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre de partitions sous minIsr pour le broker.
UnderReplicatedPartitions	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Nombre de partitions sous-répliquées pour le broker.
ZooKeeperRequestLatencyMsMean	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pour ZooKeeper un cluster basé. Latence moyenne en millisecondes pour les ZooKeeper requêtes Apache provenant du broker.

Nom	Lorsqu'il est visible	Dimensions	Description
ZooKeeperSessionState	Une fois que le cluster a atteint l'état Actif.	Nom du cluster, ID du broker	Pour ZooKeeper un cluster basé. État de connexion de la ZooKeeper session du courtier, qui peut être l'un des suivants : NOT_CONNECTED : '0.0', ASSOCIATING : '0.1', CONNECTING : '0.5', CONNECTEDREADONLY : '0.8', CONNECTED : '1.0', CLOSED : '5.0', AUTH_FAILED : '10.0'.

Surveillance de niveau **PER_BROKER**

Lorsque vous définissez le niveau de surveillance sur PER_BROKER, vous obtenez les métriques décrites dans le tableau suivant en plus de toutes les métriques de niveau DEFAULT. Vous payez les métriques dans le tableau suivant, alors que les métriques de niveau DEFAULT restent libres. Les métriques que contient ce tableau présentent les dimensions suivantes : Nom du cluster, ID d'agent.

Métriques supplémentaires disponibles à partir du niveau de surveillance **PER_BROKER**

Nom	Lorsqu'il est visible	Description
BwInAllowanceExceeded	Une fois que le cluster a atteint l'état Actif.	Nombre de paquets formés parce que la bande passante agrégée entrante a dépassé le maximum de l'agent.
BwOutAllowanceExceeded	Une fois que le cluster a atteint l'état Actif.	Nombre de paquets formés parce que la bande passante agrégée sortante a dépassé le maximum de l'agent.
ConnTrackAllowanceExceeded	Une fois que le cluster a atteint l'état Actif.	Nombre de paquets formés parce que le suivi des connexions a dépassé le maximum de l'agent. Le suivi des connexions est lié aux groupes de sécurité qui assurent le suivi de chaque connexion établie pour que les

Nom	Lorsqu'il est visible	Description
		paquets de retour soient livrés comme prévu.
`ConnectionCloseRate`	Une fois que le cluster a atteint l'état Actif.	Nombre de connexions fermées par seconde et par écouteur. Ce nombre est agrégé par écouteur et filtré pour les écouteurs clients.
`ConnectionCreationRate`	Une fois que le cluster a atteint l'état Actif.	Nombre de nouvelles connexions établies par seconde et par écouteur. Ce nombre est agrégé par écouteur et filtré pour les écouteurs clients.
`CpuCreditUsage`	Une fois que le cluster a atteint l'état Actif.	Nombre de crédits UC dépensés par l'agent. Si vous avez épuisé le solde de crédits UC, cela peut avoir un impact négatif sur les performances de votre cluster. Vous pouvez prendre des mesures pour réduire la charge de l'UC. Par exemple, vous pouvez réduire le nombre de demandes des clients ou remplacer le type d'agent par un type d'agent M5.
`FetchConsumerLocalTimeMsMean`	Une fois qu'il y a un producteur/consommateur.	Temps moyen, en millisecondes, pendant lequel la demande du consommateur est traitée au niveau du leader.
`FetchConsumerRequestQueueTimeMsMean`	Une fois qu'il y a un producteur/consommateur.	Temps moyen, en millisecondes, pendant lequel la demande du consommateur attend dans la file d'attente des demandes.

Nom	Lorsqu'il est visible	Description
FetchConsumerResponseQueueTimeMsMean	Une fois qu'il y a un producteur/consommateur.	Temps moyen, en millisecondes, pendant lequel la demande du consommateur attend dans la file d'attente de réponses.
FetchConsumerResponseSendTimeMsMean	Une fois qu'il y a un producteur/consommateur.	Temps moyen, en millisecondes, pour envoyer une réponse au consommateur.
FetchConsumerTotalTimeMsMean	Une fois qu'il y a un producteur/consommateur.	Temps total moyen, en millisecondes, que les consommateurs consacrent à l'extraction des données du broker.
FetchFollowerLocalTimeMsMean	Une fois qu'il y a un producteur/consommateur.	Temps moyen, en millisecondes, pendant lequel la demande de suivi est traitée au niveau du leader.
FetchFollowerRequestQueueTimeMsMean	Une fois qu'il y a un producteur/consommateur.	Temps moyen, en millisecondes, pendant lequel la demande de suivi attend dans la file d'attente des demandes.
FetchFollowerResponseQueueTimeMsMean	Une fois qu'il y a un producteur/consommateur.	Temps moyen, en millisecondes, pendant lequel la demande de suivi attend dans la file d'attente des réponses.
FetchFollowerResponseSendTimeMsMean	Une fois qu'il y a un producteur/consommateur.	Temps moyen, en millisecondes, d'envoi d'une réponse par le suiveur.
FetchFollowerTotalTimeMsMean	Une fois qu'il y a un producteur/consommateur.	Temps total moyen, en millisecondes, consacré par les abonnés à la récupération des données du broker.

Nom	Lorsqu'il est visible	Description
FetchMessageConversionsPerSec	Après avoir créé une rubrique.	Nombre de conversions de messages d'extraction par seconde pour le broker.
FetchThrottleByteRate	Une fois la limitation de la bande passante appliquée.	Nombre d'octets limités par seconde.
FetchThrottleQueueSize	Une fois la limitation de la bande passante appliquée.	Nombre de messages dans la file d'attente des limites.
FetchThrottleTime	Une fois la limitation de la bande passante appliquée.	Temps moyen de récupération des limites en millisecondes.
IAMNumberOfConnectionRequests	Une fois que le cluster a atteint l'état Actif.	Le nombre de demandes d'authentification IAM par seconde.
IAMTooManyConnections	Une fois que le cluster a atteint l'état Actif.	Le nombre de connexions tentées au-delà de 100. 0 signifie que le nombre de connexions est dans les limites. Si >0, la limite d'accélération est dépassée et vous devez réduire le nombre de connexions.
NetworkProcessorAvgIdlePercent	Une fois que le cluster a atteint l'état Actif.	Pourcentage moyen de temps pendant lequel les processeurs réseau sont inactifs.
PpsAllowanceExceeded	Une fois que le cluster a atteint l'état Actif.	Nombre de paquets formés parce que le PPS bidirectionnel a dépassé le maximum de l'agent.

Nom	Lorsqu'il est visible	Description
`ProduceLocalTimeMsMean`	Une fois que le cluster a atteint l'état Actif.	Temps moyen, en millisecondes, pendant lequel la demande est traitée au niveau du leader.
`ProduceMessageConversionsPerSec`	Après avoir créé une rubrique.	Nombre de conversions de messages de production par seconde pour le broker.
`ProduceMessageConversionsTimeMsMean`	Une fois que le cluster a atteint l'état Actif.	Temps moyen, en millisecondes, consacré aux conversions de format de message.
`ProduceRequestQueueTimeMsMean`	Une fois que le cluster a atteint l'état Actif.	Temps moyen, en millisecondes, que les messages de demande passent dans la file d'attente.
`ProduceResponseQueueTimeMsMean`	Une fois que le cluster a atteint l'état Actif.	Temps moyen, en millisecondes, que les messages de réponse passent dans la file d'attente.
`ProduceResponseSendTimeMsMean`	Une fois que le cluster a atteint l'état Actif.	Temps moyen, en millisecondes, consacré à l'envoi de messages de réponse.
`ProduceThrottleByteRate`	Une fois la limitation de la bande passante appliquée.	Nombre d'octets limités par seconde.
`ProduceThrottleQueueSize`	Une fois la limitation de la bande passante appliquée.	Nombre de messages dans la file d'attente des limites.
`ProduceThrottleTime`	Une fois la limitation de la bande passante appliquée.	Temps moyen de production de limites en millisecondes.

Nom	Lorsqu'il est visible	Description
`ProduceTotalTimeMs Mean`	Une fois que le cluster a atteint l'état Actif.	Temps moyen de production en millisecondes.
`RemoteFetchBytesPe rSec (RemoteBy tesInPerSec in v2.8.2.tiered)`	Une fois qu'il y a un producteur/consomm ateur.	Nombre total d'octets transférés depuis le stockage hiérarchisé en réponse aux extractions du consommateur. Cette métrique inclut toutes les partitions de rubrique qui contribuent au trafic de transfert de données en aval. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.
`RemoteCopyBytesPerSec (RemoteBytesOutPerSec in v2.8.2.tiered)`	Une fois qu'il y a un producteur/consomm ateur.	Nombre total d'octets transférés vers le stockage hiérarchisé, y compris les données provenant de segments de journal, d'index et d'autres fichiers auxiliaires. Cette métrique inclut toutes les partitions de rubrique qui contribuent au trafic de transfert de données en amont. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.
`RemoteLogManagerTa sksAvgIdlePercent`	Une fois que le cluster a atteint l'état Actif.	Pourcentage de temps moyen pendant lequel le gestionnaire de journaux distant est resté inactif. Le gestionna ire de journaux distant transfère les données de l'agent vers le stockage hiérarchisé. Catégorie : Activité interne. Il s'agit d'une métrique KIP-405.

Nom	Lorsqu'il est visible	Description
`RemoteLogReaderAvgIdlePercent`	Une fois que le cluster a atteint l'état Actif.	Pourcentage de temps moyen pendant lequel le lecteur de journaux distant est resté inactif. Le lecteur de journaux distant transfère les données du stockage distant à l'agent en réponse aux extractions du consommateur. Catégorie : Activité interne. Il s'agit d'une métrique KIP-405.
`RemoteLogReaderTaskQueueSize`	Une fois que le cluster a atteint l'état Actif.	Nombre de tâches responsables des lectures depuis le stockage hiérarchisé qui attendent d'être planifiées. Catégorie : Activité interne. Il s'agit d'une métrique KIP-405.
`RemoteFetchErrorsPerSec (RemoteReadErrorPerSec in v2.8.2.tiered)`	Une fois que le cluster a atteint l'état Actif.	Taux total d'erreurs en réponse aux demandes de lecture que l'agent spécifié a envoyées au stockage hiérarchisé pour récupérer des données en réponse aux extractions du consommateur. Cette métrique inclut toutes les partitions de rubrique qui contribuent au trafic de transfert de données en aval. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.

Nom	Lorsqu'il est visible	Description
`RemoteFetchRequestsPerSec (RemoteReadRequestsPerSec in v2.8.2.tiered)`	Une fois que le cluster a atteint l'état Actif.	Nombre total de demandes de lecture que l'agent spécifié a envoyées au stockage hiérarchisé pour récupérer des données en réponse aux extractions du consommateur. Cette métrique inclut toutes les partitions de rubrique qui contribuent au trafic de transfert de données en aval. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.
`RemoteCopyErrorsPerSec (RemoteWriteErrorPerSec in v2.8.2.tiered)`	Une fois que le cluster a atteint l'état Actif.	Taux total d'erreurs en réponse aux demandes d'écriture que l'agent spécifié a envoyées au stockage hiérarchisé pour transférer des données en amont. Cette métrique inclut toutes les partitions de rubrique qui contribuent au trafic de transfert de données en amont. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.
`ReplicationBytesInPerSec`	Après avoir créé une rubrique.	Nombre d'octets par seconde reçus des autres agents.
`ReplicationBytesOutPerSec`	Après avoir créé une rubrique.	Nombre d'octets envoyés par seconde aux autres agents.
`RequestExemptFromThrottleTime`	Après l'application de la limitation de demande.	Temps moyen en millisecondes passé dans le réseau de courtage et les threads d'E/S pour traiter les demandes exemptées de la limitation.
`RequestHandlerAvgIdlePercent`	Une fois que le cluster a atteint l'état Actif.	Pourcentage moyen de temps pendant lequel les threads du gestionnaire de demandes sont inactifs.

Nom	Lorsqu'il est visible	Description
`RequestThrottleQueueSize`	Après l'application de la limitation de demande.	Nombre de messages dans la file d'attente des limites.
`RequestThrottleTime`	Après l'application de la limitation de demande.	Temps moyen de limitation de demande en millisecondes.
`TcpConnections`	Une fois que le cluster a atteint l'état Actif.	Affiche le nombre de segments TCP entrants et sortants avec l'indicateur SYN défini.
`RemoteCopyLagBytes (TotalTierBytesLag in v2.8.2.tiered)`	Après avoir créé une rubrique.	Nombre total d'octets de données éligibles à la hiérarchisation sur l'agent mais qui n'ont pas encore été transférés vers le stockage hiérarchisé. Ces métriques montrent l'efficacité du transfert de données en amont. À mesure que le retard augmente, la quantité de données qui ne sont pas conservées dans le stockage hiérarchisé augmente. Catégorie : Retard d'archivage. Il ne s'agit pas d'une métrique KIP-405.
`TrafficBytes`	Une fois que le cluster a atteint l'état Actif.	Affiche le trafic réseau en nombre total d'octets entre les clients (producteurs et consommateurs) et les agents. Le trafic entre les agents n'est pas signalé.
`VolumeQueueLength`	Une fois que le cluster a atteint l'état Actif.	Nombre de demandes d'opérations de lecture et d'écriture en attente de réalisation au cours d'une période donnée.

Nom	Lorsqu'il est visible	Description
VolumeReadBytes	Une fois que le cluster a atteint l'état Actif.	Nombre d'octets lus au cours d'une période donnée.
VolumeReadOps	Une fois que le cluster a atteint l'état Actif.	Nombre total d'opérations de lecture au cours d'une période donnée.
VolumeTotalReadTime	Une fois que le cluster a atteint l'état Actif.	Nombre total de secondes passées par toutes les opérations de lecture terminées, au cours d'une période donnée.
VolumeTotalWriteTime	Une fois que le cluster a atteint l'état Actif.	Nombre total de secondes passées par toutes les opérations d'écriture terminées, au cours d'une période donnée.
VolumeWriteBytes	Une fois que le cluster a atteint l'état Actif.	Nombre d'octets écrits au cours d'une période donnée.
VolumeWriteOps	Une fois que le cluster a atteint l'état Actif.	Nombre total d'opérations d'écriture au cours d'une période donnée.

Surveillance de niveau **PER_TOPIC_PER_BROKER**

Lorsque vous définissez le niveau de surveillance sur PER_TOPIC_PER_BROKER, vous obtenez les métriques décrites dans le tableau suivant, en plus de toutes les métriques des niveaux PER_BROKER et par défaut. Seules les métriques de niveau DEFAULT sont gratuites. Les métriques que contient ce tableau présentent les dimensions suivantes : Nom du cluster, ID d’agent, Rubrique.

> **Important**
>
> Pour un cluster Amazon MSK qui utilise Apache Kafka 2.4.1 ou une version plus récente, les métriques du tableau suivant apparaissent uniquement après que leurs valeurs sont devenues non nulles pour la première fois. Par exemple, pour voir `BytesInPerSec`, un ou plusieurs producteurs doivent d'abord envoyer des données au cluster.

Métriques supplémentaires disponibles à partir du niveau de surveillance **`PER_TOPIC_PER_BROKER`**

Nom	Lorsqu'il est visible	Description
`FetchMessageConversionsPerSec`	Après avoir créé une rubrique.	Nombre de messages récupérés convertis par seconde.
`MessagesInPerSec`	Après avoir créé une rubrique.	Nombre de messages reçus par seconde.
`ProduceMessageConversionsPerSec`	Après avoir créé une rubrique.	Nombre de conversions par seconde pour les messages produits.
`RemoteFetchBytesPerSec (RemoteBytesInPerSec in v2.8.2.tiered)`	Lorsque vous créez une rubrique et que la rubrique est en train de produire/consommer.	Nombre d'octets transférés depuis le stockage hiérarchisé en réponse aux extractions du consommateur pour la rubrique et l'agent spécifiés. Cette métrique inclut toutes les partitions de la rubrique qui contribuent au trafic de transfert de données en aval sur l'agent spécifié. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.
`RemoteCopyBytesPerSec (RemoteBytesOutPerSec in v2.8.2.tiered)`	Lorsque vous créez une rubrique et que la rubrique est en train de produire/consommer.	Nombre d'octets transférés vers le stockage hiérarchisé, pour la rubrique et l'agent spécifiés . Cette métrique inclut toutes les partitions de la rubrique qui contribuent au trafic de transfert de données en amont sur l'agent spécifié. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.

Nom	Lorsqu'il est visible	Description
`RemoteFetchErrorsPerSec (RemoteReadErrorPerSec in v2.8.2.tiered)`	Lorsque vous créez une rubrique et que la rubrique est en train de produire/consommer.	Taux d'erreurs en réponse aux demandes de lecture que l'agent spécifié envoie au stockage hiérarchisé pour récupérer des données en réponse aux extractions du consommateur sur la rubrique spécifiée. Cette métrique inclut toutes les partitions de la rubrique qui contribuent au trafic de transfert de données en aval sur l'agent spécifié. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.
`RemoteFetchRequestsPerSec (RemoteReadRequestsPerSec in v2.8.2.tiered)`	Lorsque vous créez une rubrique et que la rubrique est en train de produire/consommer.	Nombre de demandes de lecture que l'agent spécifié envoie au stockage hiérarchisé pour récupérer des données en réponse aux extractions du consommateur sur la rubrique spécifiée. Cette métrique inclut toutes les partitions de la rubrique qui contribuent au trafic de transfert de données en aval sur l'agent spécifié. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.
`RemoteCopyErrorsPerSec (RemoteWriteErrorPerSec in v2.8.2.tiered)`	Lorsque vous créez une rubrique et que la rubrique est en train de produire/consommer.	Taux d'erreurs en réponse aux demandes d'écriture que l'agent spécifié envoie au stockage hiérarchisé pour transférer des données en amont. Cette métrique inclut toutes les partitions de la rubrique qui contribuent au trafic de transfert de données en amont sur l'agent spécifié. Catégorie : Trafic et taux d'erreur. Il s'agit d'une métrique KIP-405.

Surveillance de niveau **PER_TOPIC_PER_PARTITION**

Lorsque vous définissez le niveau de surveillance sur `PER_TOPIC_PER_PARTITION`, vous obtenez les métriques décrites dans le tableau suivant, en plus de toutes les métriques des niveaux

PER_TOPIC_PER_BROKER, PER_BROKER et PAR DÉFAUT. Seules les métriques de niveau DEFAULT sont gratuites. Les métriques de ce tableau ont les dimensions suivantes : Groupe de consommateurs, Rubrique, Partition.

Métriques supplémentaires disponibles à partir du niveau de surveillance **PER_TOPIC_PER_PARTITION**

Nom	Lorsqu'il est visible	Description
EstimatedTimeLag	Après que le groupe de consommateurs a consommé à partir d'une rubrique.	Estimation du temps (en secondes) nécessaire pour éliminer le retard de décalage de la partition.
OffsetLag	Après que le groupe de consommateurs a consommé à partir d'une rubrique.	Retard des consommateurs au niveau de la partition en nombre de décalages.

Afficher les métriques Amazon MSK à l'aide de CloudWatch

Vous pouvez surveiller les métriques pour Amazon MSK à l'aide de la CloudWatch console, de la ligne de commande ou de l' CloudWatch API. Les procédures suivantes vous montrent comment accéder aux métriques à l'aide de ces différentes méthodes.

Pour accéder aux métriques à l'aide de la CloudWatch console

Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.

1. Dans le panneau de navigation, sélectionnez Métriques.
2. Choisissez l'onglet Toutes les métriques, puis AWS/Kafka.

3. Pour afficher les métriques au niveau de la rubrique, choisissez Rubrique, ID de broker, Nom du cluster ; pour les métriques au niveau du broker, choisissez ID de broker, Nom du cluster ; et pour les métriques au niveau du cluster, choisissez Nom du cluster.
4. (Facultatif) Dans le volet graphique, sélectionnez une statistique et une période, puis créez une CloudWatch alarme à l'aide de ces paramètres.

Pour accéder aux métriques à l'aide du AWS CLI

Utilisez les commandes list-metrics et get-metric-statistics.

Pour accéder aux métriques à l'aide de la CloudWatch CLI

Utilisez les commandes mon-list-metrics et mon-get-stats.

Pour accéder aux métriques à l'aide de l' CloudWatch API

Utilisez les opérations ListMetricset GetMetricstatistiques.

Surveillance du retard des consommateurs

La surveillance du retard des consommateurs vous permet d'identifier les consommateurs lents ou bloqués qui ne suivent pas les dernières données disponibles dans une rubrique. Si nécessaire, vous pouvez ensuite prendre des mesures correctives, telles que la mise à l'échelle ou le redémarrage de ces consommateurs. Pour surveiller le retard des consommateurs, vous pouvez utiliser Amazon CloudWatch ou ouvrir la surveillance avec Prometheus.

Les métriques de retard des consommateurs quantifient la différence entre les dernières données écrites dans vos rubriques et les données lues par vos applications. Amazon MSK fournit les indicateurs de retard de consommation suivants, que vous pouvez obtenir via Amazon CloudWatch ou via une surveillance ouverte avec Prometheus :,,, et. `EstimatedMaxTimeLag` `EstimatedTimeLag` `MaxOffsetLag` `OffsetLag` `SumOffsetLag` Pour en savoir plus sur ces métriques, consultez the section called “Métriques Amazon MSK à surveiller avec CloudWatch”.

> **Note**
>
> Les indicateurs de retard de consommation ne sont visibles que pour les groupes de consommateurs dont l'état est STABLE. Un groupe de consommateurs est STABLE une fois le rééquilibrage terminé avec succès, ce qui garantit que les partitions sont réparties uniformément entre les consommateurs.

Amazon MSK prend en charge les métriques de retard des consommateurs pour les clusters utilisant la version 2.2.1 ou ultérieure d'Apache Kafka.

Surveillance ouverte avec Prometheus

Vous pouvez surveiller votre cluster MSK avec Prometheus, un système de surveillance open-source pour les données de métriques chronologiques. Vous pouvez publier ces données sur Amazon Managed Service for Prometheus à l'aide de la fonctionnalité d'écriture à distance de Prometheus. Vous pouvez également utiliser des outils compatibles avec les métriques au format Prometheus ou des outils qui s'intègrent avec Amazon MSK Open Monitoring, notamment Datadog, Lenses, New Relic et Sumo logic. La surveillance ouverte est disponible gratuitement, mais des frais s'appliquent pour le transfert de données entre les zones de disponibilité. Pour plus d'informations sur Prometheus, consultez la documentation Prometheus.

Création d'un cluster Amazon MSK avec surveillance ouverte activée

En utilisant le AWS Management Console

1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Dans la section Monitoring (Surveillance), cochez la case en regard de Enable open monitoring with Prometheus (Activer la surveillance ouverte avec Prometheus).
3. Fournissez les informations requises dans toutes les sections de la page et examinez toutes les options disponibles.
4. Choisissez Créer un cluster.

En utilisant le AWS CLI

- Invoquez la commande create-cluster et spécifiez son option `open-monitoring`. Activez le `JmxExporter`, le `NodeExporter`, ou les deux. Si vous spécifiez `open-monitoring`, les deux exportateurs ne peuvent pas être désactivés en même temps.

Utilisation de l’API

- Invoquez l'CreateClusteropération et spécifiez`OpenMonitoring`. Activez le `jmxExporter`, le `nodeExporter`, ou les deux. Si vous spécifiez `OpenMonitoring`, les deux exportateurs ne peuvent pas être désactivés en même temps.

Activation de la surveillance ouverte pour un cluster Amazon MSK existant

Pour activer la surveillance ouverte, assurez-vous que l'état du cluster est `ACTIVE`.

En utilisant le AWS Management Console

1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à l'adresse https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. Choisissez le nom du cluster que vous voulez mettre à jour. Vous accédez alors à une page contenant les détails du cluster.
3. Dans l'onglet Propriétés, faites défiler vers le bas pour accéder à la section Surveillance.
4. Choisissez Modifier.
5. Cochez la case en regard de Enable open monitoring with Prometheus (Activer la surveillance ouverte avec Prometheus).
6. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

- Invoquez la commande update-monitoring et spécifiez son option `open-monitoring`. Activez le `JmxExporter`, le `NodeExporter`, ou les deux. Si vous spécifiez `open-monitoring`, les deux exportateurs ne peuvent pas être désactivés en même temps.

Utilisation de l'API

- Invoquez l'UpdateMonitoringopération et spécifiez`OpenMonitoring`. Activez le `jmxExporter`, le `nodeExporter`, ou les deux. Si vous spécifiez `OpenMonitoring`, les deux exportateurs ne peuvent pas être désactivés en même temps.

Configuration d'un hôte Prometheus sur une instance Amazon EC2

1. Téléchargez le serveur Prometheus à partir de https://prometheus.io/download/#prometheus vers votre instance Amazon EC2.
2. Extrayez le fichier téléchargé dans un répertoire et allez dans ce dernier.
3. Créez un fichier avec le contenu suivant et appelez-le `prometheus.yml`.

```
# file: prometheus.yml
```

```
# my global config
global:
  scrape_interval:     60s

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  # The job name is added as a label `job=<job_name>` to any timeseries scraped
 from this config.
  - job_name: 'prometheus'
    static_configs:
    # 9090 is the prometheus server port
    - targets: ['localhost:9090']
  - job_name: 'broker'
    file_sd_configs:
    - files:
      - 'targets.json'
```

4. Utilisez l'ListNodesopération pour obtenir la liste des courtiers de votre cluster.
5. Créez un fichier appelé `targets.json` avec le JSON suivant. Remplacez *broker_dns_1*, *broker_dns_2*, et le reste des noms DNS de l'agent par les noms DNS que vous avez obtenus pour vos agents à l'étape précédente. Incluez tous les agents que vous avez obtenus à l'étape précédente. Amazon MSK utilise le port 11001 pour JMX Exporter et le port 11002 pour Node Exporter.

   ZooKeeper mode targets.json

```
[
  {
    "labels": {
      "job": "jmx"
    },
    "targets": [
      "broker_dns_1:11001",
      "broker_dns_2:11001",
      .
      .
      .
      "broker_dns_N:11001"
    ]
  },
  {
```

```
    "labels": {
      "job": "node"
    },
    "targets": [
      "broker_dns_1:11002",
      "broker_dns_2:11002",
      .
      .
      .
      "broker_dns_N:11002"
    ]
  }
]
```

KRaft mode targets.json

```
[
  {
    "labels": {
      "job": "jmx"
    },
    "targets": [
      "broker_dns_1:11001",
      "broker_dns_2:11001",
      .
      .
      .
      "broker_dns_N:11001",
      "controller_dns_1:11001",
      "controller_dns_2:11001",
      "controller_dns_3:11001"
    ]
  },
  {
    "labels": {
      "job": "node"
    },
    "targets": [
      "broker_dns_1:11002",
      "broker_dns_2:11002",
      .
      .
      .
```

```
      "broker_dns_N:11002"
    ]
  }
]
```

> **Note**
>
> Pour extraire les métriques JMX des contrôleurs KraFT, ajoutez les noms DNS des contrôleurs en tant que cibles dans le fichier JSON. Par exemple : `controller_dns_1:11001` en `controller_dns_1` remplaçant par le nom DNS réel du contrôleur.

6. Pour démarrer le serveur Prometheus sur votre instance Amazon EC2, exécutez la commande suivante dans le répertoire où vous avez extrait les fichiers Prometheus et enregistré `prometheus.yml` et `targets.json`.

```
./prometheus
```

7. Recherchez l'adresse IP publique IPv4 de l'instance Amazon EC2 sur laquelle vous avez exécuté Prometheus à l'étape précédente. Vous aurez besoin de cette adresse IP publique lors de l'étape suivante.
8. Pour accéder à l'interface utilisateur Web de Prometheus, ouvrez un navigateur qui peut accéder à votre instance Amazon EC2 et accédez à *`Prometheus-Instance-Public-IP`*`:9090`, où *`Prometheus-instance-public-IP`* est l'adresse IP publique que vous avez obtenue à l'étape précédente.

Métriques Prometheus

Toutes les métriques émises par Apache Kafka vers JMX sont accessibles en utilisant une surveillance ouverte avec Prometheus. Pour plus d'informations sur les métriques d'Apache Kafka, consultez Surveillance dans la documentation Apache Kafka. Outre les métriques Apache Kafka, les métriques du retard des consommateurs sont également disponibles sur le port 11001 sous le nom JMX MBean `kafka.consumer.group:type=ConsumerLagMetrics`. Vous pouvez également utiliser Prometheus Node Exporter pour obtenir des métriques de l'UC et du disque pour vos agents sur le port 11002.

Stockage de vos métriques Prometheus dans Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus est un service de surveillance et d'alerte compatible avec Prometheus que vous pouvez utiliser pour surveiller les clusters Amazon MSK. Il s'agit d'un service entièrement géré qui met automatiquement à l'échelle l'ingestion, le stockage, l'interrogation et l'alerte de vos métriques. Il s'intègre également aux services AWS de sécurité pour vous donner un accès rapide et sécurisé à vos données. Vous pouvez utiliser le langage de requête open source PromQL pour interroger vos métriques et émettre des alertes à leur sujet.

Pour plus d'informations, consultez Démarrage avec Amazon Managed Service for Prometheus.

Alertes relatives à la capacité de stockage d’Amazon MSK

Sur les clusters provisionnés par Amazon MSK, vous choisissez la capacité de stockage principale du cluster. Si vous épuisez la capacité de stockage d’un agent dans votre cluster provisionné, cela peut affecter sa capacité à produire et à consommer des données, entraînant des temps d’arrêt coûteux. Amazon MSK propose des CloudWatch métriques pour vous aider à surveiller la capacité de stockage de votre cluster. Toutefois, pour vous permettre de détecter et de résoudre plus facilement les problèmes de capacité de stockage, Amazon MSK vous envoie automatiquement des alertes dynamiques relatives à la capacité de stockage du cluster. Les alertes relatives à la capacité de stockage incluent des recommandations concernant les étapes à court et à long terme pour gérer la capacité de stockage de votre cluster. Depuis la console Amazon MSK, vous pouvez utiliser les liens rapides contenus dans les alertes pour prendre immédiatement les mesures recommandées.

Il existe deux types d’alertes relatives à la capacité de stockage MSK : les alertes proactives et les alertes correctives.

- Les alertes de capacité de stockage proactives (« Action requise ») vous avertissent des problèmes de stockage potentiels liés à votre cluster. Lorsqu’un agent d’un cluster MSK a utilisé plus de 60 % ou 80 % de sa capacité de stockage sur disque, vous recevez des alertes proactives pour l’agent concerné.
- Les alertes de capacité de stockage correctives (« Action critique requise ») vous obligent à prendre des mesures correctives pour résoudre un problème critique de cluster lorsque l’un des agents de votre cluster MSK n’a plus de capacité de stockage sur disque.

Amazon MSK envoie automatiquement ces alertes à la console Amazon MSK, au AWS Health Dashboard EventBridge, à Amazon et aux contacts e-mail associés à votre AWS compte. Vous pouvez également configurer Amazon EventBridge pour envoyer ces alertes à Slack ou à des outils tels que New Relic et Datadog.

Les alertes de capacité de stockage sont activées par défaut pour tous les clusters provisionnés de MSK et ne peuvent pas être désactivées. Cette fonctionnalité est disponible dans toutes les régions où MSK est disponible.

Surveillance des alertes relatives à la capacité de stockage d'Amazon MSK

Vous pouvez rechercher les alertes relatives à la capacité de stockage de plusieurs manières :

- Accédez à la console Amazon MSK. Les alertes relatives à la capacité de stockage sont affichées dans le volet des alertes du cluster pendant 90 jours. Elles contiennent des recommandations et des actions de liaison en un seul clic pour résoudre les problèmes de capacité de stockage sur disque.
- Utilisez ListClustersles API ListClustersDescribeClusterV2 ou V2 pour afficher toutes `CustomerActionStatus` les alertes d'un cluster. DescribeCluster
- Accédez au AWS Health Dashboard pour consulter les alertes de MSK et d'autres AWS services.
- Configurez AWS Health API et Amazon EventBridge pour acheminer les notifications d'alerte vers des plateformes tierces telles que Datadog et NewRelic Slack.

Utilisation LinkedIn du régulateur de vitesse pour Apache Kafka avec Amazon MSK

Vous pouvez utiliser LinkedIn le régulateur de vitesse pour rééquilibrer votre cluster Amazon MSK, détecter et corriger les anomalies, et surveiller l'état et l'état de santé du cluster.

Pour télécharger et créer Cruise Control

1. Créez une instance Amazon EC2 dans le même Amazon VPC que le cluster Amazon MSK.
2. Installez Prometheus sur l'instance Amazon EC2 que vous avez créée à l'étape précédente. Notez l'adresse IP privée et le port. Le numéro de port par défaut est 9090. Pour de plus amples informations sur la configuration de Prometheus pour agréger les métriques de votre cluster, consultez the section called “Surveillance ouverte avec Prometheus”.
3. Téléchargez Cruise Control sur l'instance Amazon EC2. (Vous pouvez également utiliser une instance Amazon EC2 distincte pour Cruise Control si vous préférez.) Pour un cluster doté de la version 2.4.* d'Apache Kafka, utilisez la dernière version 2.4.* de Cruise Control. Si votre cluster possède une version d'Apache Kafka antérieure à la version 2.4.*, utilisez la dernière version 2.0.* de Cruise Control.
4. Décompressez le fichier Cruise Control, puis accédez au dossier décompressé.
5. Exécutez la commande suivante pour installer git.

```
sudo yum -y install git
```

6. Exécutez la commande suivante pour initialiser le référentiel local. Remplacez *Your-Cruise-Control-Folder* par le nom de votre dossier actuel (le dossier que vous avez obtenu lorsque vous avez décompressé le téléchargement de Cruise Control).

```
git init && git add . && git commit -m "Init local repo." && git tag -a Your-Cruise-Control-Folder -m "Init local version."
```

7. Exécutez la commande suivante pour créer le code source.

```
./gradlew jar copyDependantLibs
```

Pour configurer et exécuter Cruise Control

1. Effectuez les mises à jour suivantes du fichier `config/cruisecontrol.properties`. Remplacez les exemples de serveurs bootstrap et de chaîne bootstrap-brokers par les valeurs de votre cluster. Pour obtenir ces chaînes pour votre cluster, vous pouvez consulter les détails du cluster dans la console. Vous pouvez également utiliser les opérations GetBootstrapBrokersetDescribeClusterAPI ou leurs équivalents CLI.

```
# If using TLS encryption, use 9094; use 9092 if using plaintext
bootstrap.servers=b-1.test-cluster.2skv42.c1.kafka.us-
east-1.amazonaws.com:9094,b-2.test-cluster.2skv42.c1.kafka.us-
east-1.amazonaws.com:9094,b-3.test-cluster.2skv42.c1.kafka.us-
east-1.amazonaws.com:9094

# SSL properties, needed if cluster is using TLS encryption
security.protocol=SSL
ssl.truststore.location=/home/ec2-user/kafka.client.truststore.jks

# Use the Prometheus Metric Sampler
metric.sampler.class=com.linkedin.kafka.cruisecontrol.monitor.sampling.prometheus.Prometheu

# Prometheus Metric Sampler specific configuration
prometheus.server.endpoint=1.2.3.4:9090 # Replace with your Prometheus IP and port

# Change the capacity config file and specify its path; details below
capacity.config.file=config/capacityCores.json
```

2. Modifiez le fichier `config/capacityCores.json` pour spécifier la taille de disque, le nombre de cœurs d'UC et les limites d'entrée/sortie réseau appropriés. Vous pouvez utiliser l'opération DescribeClusterAPI (ou son équivalent en CLI) pour obtenir la taille du disque. Pour connaître les cœurs d'UC et les limites d'entrée/sortie du réseau, consultez Types d'instances Amazon EC2.

```
{
  "brokerCapacities": [
    {
      "brokerId": "-1",
      "capacity": {
        "DISK": "10000",
        "CPU": {
          "num.cores": "2"
        },
        "NW_IN": "5000000",
```

```
        "NW_OUT": "5000000"
      },
      "doc": "This is the default capacity. Capacity unit used for disk is in MB,
 cpu is in number of cores, network throughput is in KB."
    }
  ]
}
```

3. Vous pouvez éventuellement installer l'interface utilisateur de Cruise Control. Pour le télécharger, rendez-vous sur Configuration du frontend de Cruise Control.
4. Exécutez la commande suivante pour démarrer Cruise Control. Envisagez d'utiliser un outil tel que `screen` ou `tmux` pour maintenir une session de longue durée ouverte.

```
<path-to-your-kafka-installation>/bin/kafka-cruise-control-start.sh config/
cruisecontrol.properties 9091
```

5. Utilisez les API de Cruise Control ou l'interface utilisateur pour vous assurer que Cruise Control dispose des données de charge du cluster et qu'il propose des suggestions de rééquilibrage. L'obtention d'une fenêtre de métriques valide peut durer plusieurs minutes.

Modèle de déploiement automatisé du régulateur de vitesse pour Amazon MSK

Vous pouvez également utiliser ce CloudFormation modèle pour déployer facilement Cruise Control et Prometheus afin de mieux comprendre les performances de votre cluster Amazon MSK et d'optimiser l'utilisation des ressources.

Fonctions principales :

- Provisionnement automatisé d'une instance Amazon EC2 avec Cruise Control et Prometheus préconfigurés.
- Support pour le cluster provisionné Amazon MSK.
- Authentification flexible avec PlainText et IAM.
- Aucune dépendance à Zookeeper pour le régulateur de vitesse.
- Personnalisez facilement les cibles Prometheus, les paramètres de capacité du régulateur de vitesse et les autres configurations en fournissant vos propres fichiers de configuration stockés dans un compartiment Amazon S3.

Quota d'Amazon MSK

Votre AWS compte dispose de quotas par défaut pour Amazon MSK. Sauf indication contraire, chaque quota par compte est spécifique à la région de votre compte. AWS

Quota d'Amazon MSK

- Jusqu'à 90 courtiers par compte. 30 courtiers par cluster de ZooKeeper modes. 60 courtiers par cluster de mode KraFT. Pour demander un quota plus élevé, rendez-vous dans le Centre de support de la AWS console et créez un dossier de support.
- Un minimum de 1 Gio de stockage par agent.
- Un maximum de 16 384 Gio de stockage par agent.
- Un cluster qui utilise le the section called “Contrôle d'accès IAM” peut avoir à un moment donné jusqu'à 3 000 connexions TCP par agent. Pour augmenter cette limite, vous pouvez ajuster la propriété `listener.name.client_iam.max.connections` ou la `listener.name.client_iam_public.max.connections` configuration à l'aide de l' AlterConfig API Kafka ou de l'`kafka-configs.sh`outil. Il est important de noter que l'augmentation de la valeur de l'une ou l'autre propriété peut entraîner une indisponibilité.
- Limites relatives aux connexions TCP. Lorsque les rafales de débit de connexion sont activées, MSK autorise 100 connexions par seconde. L'exception est le type d'instance kafka.t3.small, qui est autorisé à 4 connexions par seconde avec les rafales de débit activées. Les clusters plus anciens pour lesquels les rafales de débit de connexion ne sont pas activées verront cette fonctionnalité automatiquement activée lorsque le cluster sera patché.

  Pour gérer les tentatives en cas d'échec des connexions, vous pouvez définir le paramètre de configuration `reconnect.backoff.ms` côté client. Par exemple, si vous souhaitez qu'un client tente à nouveau de se connecter au bout d'une seconde, définissez la valeur `reconnect.backoff.ms` sur 1000. Pour plus d'informations, consultez reconnect.backoff.ms dans la documentation Apache Kafka.
- Jusqu'à 100 configurations par compte. Pour demander un ajustement de quota, rendez-vous dans la console AWS Centre de support et créez une demande de support.
- Un maximum de 50 révisions par configuration.
- Pour mettre à jour la configuration ou la version Apache Kafka d'un cluster MSK, assurez-vous d'abord que le nombre de partitions par agent est inférieur aux limites décrites dans the section called “ Dimensionnez correctement votre cluster : nombre de partitions par agent”.

Quotas du réplicateur MSK

- Un maximum de 15 réplicateurs MSK par compte.
- MSK Replicator ne réplique que 750 sujets par ordre trié. Si vous devez répliquer d'autres rubriques, nous vous recommandons de créer un réplicateur distinct. Accédez au centre de support de la AWS console et créez un dossier de support si vous avez besoin d'assistance pour plus de 750 sujets par réplicateur. Vous pouvez contrôler le nombre de sujets répliqués à l'aide de la métrique « TopicCount ».
- Un débit d'entrée maximal de 1 Go par seconde par réplicateur MSK. Pour demander un quota plus élevé, rendez-vous dans le Centre de support de la AWS console et créez un dossier de support.
- Taille d'enregistrement du réplicateur MSK : taille d'enregistrement maximale de 10 Mo (message.max.bytes). Pour demander un quota plus élevé, rendez-vous dans le Centre de support de la AWS console et créez un dossier de support.

Quota de MSK sans serveur

> **Note**
>
> Si vous rencontrez des problèmes avec les limites de quotas, contactez le AWS Support en créant un dossier d'assistance.

Les limites s'appliquent par cluster, sauf indication contraire.

Dimension	Quota	Résultat de violation de quota
Débit d'entrée maximal	200 Mbit/s	Ralentissement avec durée de limitation en réponse
Débit de sortie maximal	400 Mbit/s	Ralentissement avec durée de limitation en réponse
Durée de conservation maximale	Illimité	N/A

Dimension	Quota	Résultat de violation de quota
Nombre maximal de connexions client	3000	Fermeture de connexion
Nombre maximal de tentatives de connexion	100 par seconde	Fermeture de connexion
Taille maximale du message	8 Mo	La requête échoue avec ErrorCode : INVALID_REQUEST
Taux maximal de demandes	15 000 par seconde	Ralentissement avec durée de limitation en réponse
Taux maximal de demandes d'API de gestion de rubriques	2 par seconde	Ralentissement avec durée de limitation en réponse
Nombre maximal d'octets à récupérer par demande	55 Mo	La requête échoue avec ErrorCode : INVALID_REQUEST
Nombre maximal de groupes de consommateurs	500	JoinGroup la demande échoue
Nombre maximum de partitions (leaders)	2 400 pour les rubriques non compactées. 120 pour les rubriques compactées. Pour demander un ajustement de quota, rendez-vous dans le Centre de support de la AWS console et créez un dossier de support.	La requête échoue avec ErrorCode : INVALID_REQUEST
Taux maximal de création et de suppression de partitions	250 en 5 minutes	La requête échoue avec ErrorCode : THROUGHPUT_QUOTA_EXCEDED

Dimension	Quota	Résultat de violation de quota
Débit d'entrée maximal par partition	5 Mbit/s	Ralentissement avec durée de limitation en réponse
Débit de sortie maximal par partition	10 Mbit/s	Ralentissement avec durée de limitation en réponse
Taille maximale de partition (pour les rubriques compactées)	250 Go	La requête échoue avec ErrorCode : THROUGHPUT_QUOTA_EXCEDED
Nombre maximal de VPC client par cluster sans serveur	5	
Nombre maximal de clusters sans serveur par compte	10. Pour demander un ajustement de quota, rendez-vous dans le Centre de support de la AWS console et créez un dossier de support.	

Quota de MSK Connect

- Jusqu'à 100 plug-ins personnalisés.
- Jusqu'à 100 configurations de worker.
- Jusqu'à 60 workers de Connect. Si un connecteur est configuré pour avoir une capacité automatiquement mise à l'échelle, le nombre maximum de workers pour lequel le connecteur est configuré est le nombre utilisé par MSK Connect pour calculer le quota du compte.
- Jusqu'à 10 workers par connecteur.

Pour demander un quota plus élevé pour MSK Connect, rendez-vous dans le Centre de support de la AWS console et créez un dossier d'assistance.

Ressources Amazon MSK

Le terme ressources a deux significations dans Amazon MSK, selon le contexte. Dans le contexte des API, une ressource est une structure sur laquelle vous pouvez invoquer une opération. Pour obtenir la liste de ces ressources et des opérations que vous pouvez invoquer, consultez la section Ressources du manuel de référence de l'API Amazon MSK. Dans le contexte du the section called “Contrôle d'accès IAM”, une ressource est une entité à laquelle vous pouvez autoriser ou refuser l'accès, comme défini dans la section the section called “Ressources”.

Intégrations MSK

Cette section fournit des références aux AWS fonctionnalités intégrées à Amazon MSK.

Rubriques

Connecteur Amazon Athena pour Amazon MSK

Le connecteur Amazon Athena pour Amazon MSK permet à Amazon Athena d'exécuter des requêtes SQL sur des rubriques Apache Kafka. Utilisez ce connecteur pour afficher les rubriques Apache Kafka sous forme de tableaux et les messages sous forme de lignes dans Athena.

Pour de plus amples informations, consultez Connecteur Amazon Athena pour MSK dans le Guide de l'utilisateur Amazon Athena.

Ingestion de données de streaming Amazon Redshift

Amazon Redshift prend en charge l'ingestion en streaming provenant d'Amazon MSK. La fonctionnalité d'ingestion en streaming Amazon Redshift garantit une ingestion à faible latence et à haute vitesse des données de streaming provenant d'Amazon MSK dans une vue matérialisée Amazon Redshift. Comme il n'a pas besoin d'organiser les données dans Amazon S3, Amazon Redshift peut ingérer des données de streaming avec une latence plus faible et un coût de stockage réduit. Vous pouvez configurer l'ingestion en streaming Amazon Redshift sur un cluster Amazon Redshift à l'aide d'instructions SQL pour vous authentifier et vous connecter à une rubrique Amazon MSK.

Pour en savoir plus, consultez Ingestion en streaming dans le Guide du développeur de base de données Amazon Redshift.

Firehose

Amazon MSK s'intègre à Firehose pour fournir une solution sans serveur et sans code permettant de diffuser des flux depuis des clusters Apache Kafka vers des lacs de données Amazon S3. Firehose est un service d'extraction, de transformation et de chargement (ETL) en streaming qui lit les données de vos rubriques Amazon MSK Kafka, effectue des transformations telles que la conversion vers Parquet, puis agrège et écrit les données sur Amazon S3. En quelques clics depuis la console, vous pouvez configurer un stream Firehose pour lire un sujet de Kafka et le diffuser vers un emplacement S3. Il n'y a aucun code à écrire, aucune application de connecteur et aucune ressource à allouer. Firehose évolue automatiquement en fonction de la quantité de données publiées sur le sujet Kafka, et vous ne payez que pour les octets ingérés par Kafka.

Pour en savoir plus sur cette fonctionnalité, consultez :

- Écrire sur Kinesis Data Firehose à l'aide d'Amazon MSK - Amazon Kinesis Data Firehose dans le manuel du développeur Amazon Data Firehose
- Blog : Amazon MSK introduit la diffusion de données gérée depuis Apache Kafka vers votre lac de données
- Atelier : Livraison vers Amazon S3 à l'aide de Firehose

Accès à Amazon EventBridge Pipes via la console Amazon MSK

Amazon EventBridge Pipes connecte les sources aux cibles. Les tubes sont destinés aux point-to-point intégrations entre les sources et les cibles prises en charge, avec la prise en charge des transformations avancées et de l'enrichissement. EventBridge Les pipes constituent un moyen hautement évolutif de connecter votre cluster Amazon MSK à des AWS services tels que Step Functions, Amazon SQS et API Gateway, ainsi qu'à des applications logicielles en tant que service (SaaS) tierces telles que Salesforce.

Pour configurer un canal, vous devez choisir la source, ajouter un filtrage facultatif, définir un enrichissement facultatif et choisir la cible pour les données d'événement.

Sur la page de détails d'un cluster Amazon MSK, vous pouvez voir les canaux qui utilisent ce cluster comme source. À partir de là, vous pouvez également :

- Lancez la EventBridge console pour afficher les détails du canal.
- Lancez la EventBridge console pour créer un nouveau canal avec le cluster comme source.

Pour plus d'informations sur la configuration d'un cluster Amazon MSK en tant que source de canal, consultez le cluster Amazon Managed Streaming for Apache Kafka en tant que source dans le guide de l'utilisateur EventBridge Amazon. Pour plus d'informations sur EventBridge les tuyaux en général, voir EventBridge Tuyaux.

Pour accéder aux EventBridge canaux d'un cluster Amazon MSK donné

1. Ouvrez la console Amazon MSK et sélectionnez Clusters.
2. Sélectionnez un cluster.
3. Sur la page Détails du cluster, choisissez l'onglet Intégration.

   L'onglet Intégration inclut une liste de tous les canaux actuellement configurés pour utiliser le cluster sélectionné comme source, notamment :

   - nom du canal
   - état actuel
   - cible du canal
   - date à laquelle le canal a été modifié pour la dernière fois
4. Gérez les canaux de votre cluster Amazon MSK comme vous le souhaitez :

   Pour accéder à plus de détails sur un canal

   - Choisissez le canal.

     Cela ouvre la page de détails de Pipe de la EventBridge console.

   Pour créer un nouveau canal

   - Choisissez Connecter un cluster Amazon MSK à un canal.

     Cela lance la page Create pipe de la EventBridge console, avec le cluster Amazon MSK spécifié comme source de canal. Pour plus d'informations, consultez la section Création d'un EventBridge canal dans le guide de EventBridge l'utilisateur Amazon.

   - Vous pouvez également créer un canal pour un cluster à partir de la page Clusters. Sélectionnez le cluster, puis dans le menu Actions, sélectionnez Create EventBridge Pipe.

Versions Apache Kafka

Lorsque vous créez un cluster Amazon MSK, vous spécifiez la version Apache Kafka que vous souhaitez avoir sur lui. Vous pouvez également mettre à jour la version Apache Kafka d'un cluster existant. Les rubriques de ce chapitre vous aident à comprendre les délais de prise en charge des versions de Kafka et à vous suggérer des bonnes pratiques.

Rubriques

Versions Apache Kafka prises en charge

Amazon Managed Streaming for Apache Kafka (Amazon MSK) prend en charge les versions Apache Kafka et Amazon MSK suivantes. La communauté Apache Kafka fournit environ 12 mois de support pour une version après sa date de sortie. Pour plus de détails, consultez la politique EOL (fin de vie) d'Apache Kafka.

Versions Apache Kafka prises en charge

Version d'Apache Kafka	Date de sortie de MSK	Date de fin du support
1.1.1	--	05/06/2022
2.1.0	--	05/06/2022
2.2.1	2019-07-31	2024-06-08
2.3.1	2019-12-19	2024-06-08
2.4.1	2020-04-02	2024-06-08
2.4.1.1	2020-09-09	2024-06-08
2.5.1	2020-09-30	2024-06-08
2.6.0	21/10/2020	11/09/2024
2.6.1	19/01/2021	11/09/2024

Version d'Apache Kafka	Date de sortie de MSK	Date de fin du support
2.6.2	29/04/2021	11/09/2024
2.6.3	2021-12-21	11/09/2024
2.7.0	29/12/2020	11/09/2024
2.7.1	25/05/2021	11/09/2024
2.7.2	2021-12-21	11/09/2024
2.8.0	--	11/09/2024
2.8.1	28/10	11/09/2024
2.8.2 à plusieurs niveaux	28/10	À annoncer
3.1.1	22/06/2018	11/09/2024
3.2.0	22/06/2018	11/09/2024
3.3.1	26/10	11/09/2024
3.3.2	03 avril	11/09/2024
3.4.0	04/05/2023	17/06/2025
3.5.1 (recommandé)	26/09/2023	--
3.6.0	16/11/2023	--
3,7. x	29/05/2024	--

Pour plus d'informations sur la politique de support des versions d'Amazon MSK, consultezPolitique de support des versions d'Amazon MSK.

Apache Kafka version 3.7.x (avec stockage hiérarchisé prêt pour la production)

La version 3.7.x d'Apache Kafka sur MSK inclut le support de la version 3.7.0 d'Apache Kafka. Vous pouvez créer des clusters ou mettre à niveau des clusters existants pour utiliser la nouvelle version 3.7.x. Avec ce changement de dénomination des versions, vous n'avez plus à adopter les nouvelles versions de correctifs telles que 3.7.1 lorsqu'elles sont publiées par la communauté Apache Kafka. Amazon MSK mettra automatiquement à jour la version 3.7.x pour prendre en charge les futures versions de correctifs une fois qu'elles seront disponibles. Cela vous permet de bénéficier de la sécurité et des corrections de bogues disponibles via les versions corrigées sans déclencher de mise à niveau de version. Ces versions de correctifs publiées par Apache Kafka n'interrompent pas la compatibilité des versions et vous pouvez bénéficier des nouvelles versions de correctifs sans vous soucier des erreurs de lecture ou d'écriture pour vos applications clientes. Assurez-vous que les outils d'automatisation de votre infrastructure, tels que CloudFormation, sont mis à jour pour tenir compte de ce changement de dénomination de version.

Amazon MSK prend désormais en charge le mode KraFT (Apache Kafka Raft) dans la version 3.7.x d'Apache Kafka. Sur Amazon MSK, comme pour les ZooKeeper nœuds, les contrôleurs Kraft sont inclus sans frais supplémentaires pour vous et ne nécessitent aucune configuration ou gestion supplémentaire de votre part. Vous pouvez désormais créer des clusters en mode KraFT ou ZooKeeper en mode Apache Kafka version 3.7.x. En mode Kraft, vous pouvez ajouter jusqu'à 60 courtiers pour héberger davantage de partitions par cluster, sans demander d'augmentation de limite, par rapport au quota de 30 courtiers sur les clusters basés sur ZooKeeper. Pour en savoir plus sur KraFT sur MSK, consultez le mode KraFT.

La version 3.7.x d'Apache Kafka inclut également plusieurs corrections de bogues et de nouvelles fonctionnalités qui améliorent les performances. Les principales améliorations incluent l'optimisation de la découverte des leaders pour les clients et les options d'optimisation du vidage des segments de journal. Pour une liste complète des améliorations et des corrections de bogues, consultez les notes de mise à jour d'Apache Kafka pour la version 3.7.0.

Apache Kafka version 3.6.0 (avec stockage hiérarchisé prêt pour la production)

Pour plus d'informations sur Apache Kafka version 3.6.0 (avec stockage hiérarchisé prêt pour production), consultez les notes de mise à jour correspondantes sur le site de téléchargement d'Apache Kafka.

Amazon MSK continuera d'utiliser et de gérer ZooKeeper pour la gestion du quorum dans cette version à des fins de stabilité.

Amazon MSK version 3.5.1

Amazon Managed Streaming for Apache Kafka (Amazon MSK) prend désormais en charge la version 3.5.1 d'Apache Kafka pour les clusters nouveaux et existants. Apache Kafka 3.5.1 inclut plusieurs corrections de bogues et de nouvelles fonctionnalités qui améliorent les performances. Les principales fonctionnalités incluent l'introduction d'une nouvelle attribution de partitions adaptée aux racks pour les consommateurs. Amazon MSK continuera d'utiliser et de gérer Zookeeper pour la gestion du quorum dans cette version. Pour une liste complète des améliorations et des corrections de bogues, consultez les notes de mise à jour d'Apache Kafka pour la version 3.5.1.

Pour plus d'informations sur Apache Kafka, version 3.5.1, consultez ses notes de mise à jour sur le site de téléchargement Apache Kafka.

Amazon MSK version 3.4.0

Amazon Managed Streaming for Apache Kafka (Amazon MSK) prend désormais en charge la version 3.4.0 d'Apache Kafka pour les clusters nouveaux et existants. Apache Kafka 3.4.0 inclut plusieurs corrections de bogues et de nouvelles fonctionnalités qui améliorent les performances. Les principales fonctionnalités incluent un correctif pour améliorer la stabilité lors de l'extraction depuis la réplique la plus proche. Amazon MSK continuera d'utiliser et de gérer Zookeeper pour la gestion du quorum dans cette version. Pour une liste complète des améliorations et des corrections de bogues, consultez les notes de mise à jour d'Apache Kafka pour la version 3.4.0.

Pour plus d'informations sur Apache Kafka, version 3.4.0, consultez ses notes de mise à jour sur le site de téléchargement Apache Kafka.

Amazon MSK version 3.3.2

Amazon Managed Streaming for Apache Kafka (Amazon MSK) prend désormais en charge la version 3.3.2 d'Apache Kafka pour les clusters nouveaux et existants. Apache Kafka 3.3.2 inclut plusieurs corrections de bogues et de nouvelles fonctionnalités qui améliorent les performances. Les principales fonctionnalités incluent un correctif pour améliorer la stabilité lors de l'extraction depuis la réplique la plus proche. Amazon MSK continuera d'utiliser et de gérer Zookeeper pour la gestion du quorum dans cette version. Pour une liste complète des améliorations et des corrections de bogues, consultez les notes de publication d'Apache Kafka pour la version 3.3.2.

Pour plus d'informations sur Apache Kafka, version 3.3.2, consultez ses notes de mise à jour sur le site de téléchargement Apache Kafka.

Amazon MSK version 3.3.1

Amazon Managed Streaming for Apache Kafka (Amazon MSK) prend désormais en charge la version 3.3.1 d'Apache Kafka pour les clusters nouveaux et existants. Apache Kafka 3.3.1 inclut plusieurs corrections de bogues et de nouvelles fonctionnalités qui améliorent les performances. Parmi les principales fonctionnalités, citons les améliorations apportées aux métriques et au partitionneur. Amazon MSK continuera d'utiliser et de gérer ZooKeeper pour la gestion du quorum dans cette version à des fins de stabilité. Pour une liste complète des améliorations et des corrections de bogues, consultez les notes de publication d'Apache Kafka pour la version 3.3.1.

Pour plus d'informations sur Apache Kafka, version 3.3.1, consultez ses notes de mise à jour sur le site de téléchargement Apache Kafka.

Amazon MSK version 3.1.1

Amazon Managed Streaming for Apache Kafka (Amazon MSK) prend désormais en charge les versions 3.1.1 et 3.2.0 d'Apache Kafka pour les clusters nouveaux et existants. Apache Kafka 3.1.1 et Apache Kafka 3.2.0 incluent plusieurs corrections de bogues et de nouvelles fonctionnalités qui améliorent les performances. Parmi les principales fonctionnalités, citons l'amélioration des métriques et l'utilisation des identifiants de sujets. MSK continuera d'utiliser et de gérer Zookeeper pour la gestion du quorum dans cette version à des fins de stabilité. Pour une liste complète des améliorations et des corrections de bogues, consultez les notes de mise à jour d'Apache Kafka pour les versions 3.1.1 et 3.2.0.

Pour plus d'informations sur les versions 3.1.1 et 3.2.0 d'Apache Kafka, consultez ses notes de mise à jour 3.2.0 et 3.1.1 sur le site de téléchargement d'Apache Kafka.

Stockage hiérarchisé Amazon MSK version 2.8.2.tiered

Cette version est une version uniquement Amazon MSK de la version 2.8.2 d'Apache Kafka et est compatible avec les clients Apache Kafka open source.

La version 2.8.2.tiered contient une fonctionnalité de stockage hiérarchisé compatible avec les API introduites dans KIP-405 pour Apache Kafka. Pour de plus amples informations sur la fonctionnalité de stockage hiérarchisé Amazon MSK, consultez Stockage hiérarchisé.

Apache Kafka, version 2.5.1

La version 2.5.1 d'Apache Kafka inclut plusieurs corrections de bogues et de nouvelles fonctionnalités, notamment le chiffrement en transit pour Apache ZooKeeper et les clients d'administration. Amazon MSK fournit des ZooKeeper points de terminaison TLS, que vous pouvez interroger lors de l'opération. DescribeCluster

Le résultat de l' DescribeClusteropération inclut le `ZookeeperConnectStringTls` nœud, qui répertorie les points de terminaison TLS Zookeeper.

L'exemple suivant montre le nœud `ZookeeperConnectStringTls` de la réponse à l'opération `DescribeCluster` :

```
"ZookeeperConnectStringTls": "z-3.awskafkatutorialc.abcd123.c3.kafka.us-
east-1.amazonaws.com:2182,z-2.awskafkatutorialc.abcd123.c3.kafka.us-
east-1.amazonaws.com:2182,z-1.awskafkatutorialc.abcd123.c3.kafka.us-
east-1.amazonaws.com:2182"
```

Pour obtenir des informations sur l'utilisation du chiffrement TLS avec ZooKeeper, consultez Utilisation de la sécurité TLS avec Apache ZooKeeper.

Pour plus d'informations sur Apache Kafka, version 2.5.1, consultez ses notes de mise à jour sur le site de téléchargement Apache Kafka.

Version de correction de bogues Amazon MSK 2.4.1.1

Cette version est une version de correction de bogues uniquement pour Amazon MSK de la version 2.4.1 d'Apache Kafka. Cette version de correction de bogues contient un correctif pour KAFKA-9752, un problème rare qui oblige les groupes de consommateurs à se rééquilibrer continuellement et à rester à l'état `PreparingRebalance`. Ce problème concerne les clusters exécutant les versions 2.3.1 et 2.4.1 d'Apache Kafka. Cette version contient un correctif produit par la communauté qui est disponible dans la version 2.5.0 d'Apache Kafka.

> **Note**
>
> Les clusters Amazon MSK exécutant la version 2.4.1.1 sont compatibles avec tous les clients Apache Kafka compatibles avec la version 2.4.1 d'Apache Kafka.

Nous vous recommandons d'utiliser la version de correction de bogues MSK 2.4.1.1 pour les nouveaux clusters Amazon MSK si vous préférez utiliser la version 2.4.1 d'Apache Kafka. Vous pouvez mettre à jour les clusters existants exécutant la version 2.4.1 d'Apache Kafka vers cette version afin d'intégrer ce correctif. Pour de plus amples informations sur la mise à niveau d'un cluster existant, consultez Mise à jour de la version Apache Kafka.

Pour contourner ce problème sans mettre à niveau le cluster vers la version 2.4.1.1, consultez la section Groupe de consommateurs bloqué à l'état `PreparingRebalance` du guide Résolution des problèmes de votre cluster Amazon MSK.

Apache Kafka version 2.4.1 (utilisez plutôt 2.4.1.1)

> **Note**
>
> Vous ne pouvez plus créer de cluster MSK avec la version 2.4.1 d'Apache Kafka. Vous pouvez plutôt utiliser Version de correction de bogues Amazon MSK 2.4.1.1 avec des clients compatibles avec la version 2.4.1 d'Apache Kafka. De même, si vous possédez déjà un cluster MSK avec la version 2.4.1 d'Apache Kafka, nous vous recommandons de le mettre à jour pour utiliser la version 2.4.1.1 d'Apache Kafka à la place.

KIP-392 est l'une des principales propositions d'amélioration de Kafka qui sont incluses dans la version 2.4.1 d'Apache Kafka. Cette amélioration permet aux consommateurs de récupérer le réplica le plus proche. Pour utiliser cette fonctionnalité, définissez `client.rack` dans les propriétés du consommateur pour l'ID de la zone de disponibilité du consommateur. Un exemple d'ID de zone de disponibilité est `use1-az1`. Amazon MSK définit `broker.rack` pour les ID des zones de disponibilité des agents. Vous devez également définir la propriété de configuration `replica.selector.class` sur `org.apache.kafka.common.replica.RackAwareReplicaSelector`, qui est une implémentation de la prise en compte du rack fournie par Apache Kafka.

Lorsque vous utilisez cette version d'Apache Kafka, les mesures du niveau de surveillance `PER_TOPIC_PER_BROKER` s'affichent seulement lorsque leurs valeurs sont devenues non nulles pour la première fois. Pour de plus amples informations à ce sujet, veuillez consulter the section called “Surveillance de niveau `PER_TOPIC_PER_BROKER`”.

Pour plus d'informations sur la façon de trouver les ID de zone de disponibilité, consultez la section Identifiants AZ pour votre ressource dans le guide de AWS Resource Access Manager l'utilisateur.

Pour plus d'informations sur la définition des propriétés de configuration, consultez Configuration.

Pour plus d'informations sur KIP-392, consultez Autoriser les consommateurs à extraire du réplica le plus proche dans les pages Confluence.

Pour plus d'informations sur Apache Kafka, version 2.4.1, consultez ses notes de mise à jour sur le site de téléchargement Apache Kafka.

Prise en charge des versions d'Amazon MSK

Cette rubrique décrit la procédure Politique de support des versions d'Amazon MSK et la procédure à suivre pourMise à jour de la version Apache Kafka. Si vous mettez à niveau votre version de Kafka, suivez les meilleures pratiques décrites dansBonnes pratiques pour les mises à niveau de version.

Politique de support des versions d'Amazon MSK

Cette section décrit la politique de support pour les versions de Kafka prises en charge par Amazon MSK.

- Toutes les versions de Kafka sont prises en charge jusqu'à leur date de fin de support. Pour plus de détails sur les dates de fin de support, consultezVersions Apache Kafka prises en charge. Mettez à niveau votre cluster MSK vers la version recommandée de Kafka ou une version supérieure avant la date de fin du support. Pour plus de détails sur la mise à jour de votre version d'Apache Kafka, consultezMise à jour de la version Apache Kafka. Un cluster utilisant une version de Kafka après sa date de fin de support est automatiquement mis à niveau vers la version recommandée de Kafka.
- MSK supprimera progressivement le support pour les clusters nouvellement créés qui utilisent des versions de Kafka avec des dates de fin de support publiées.

Mise à jour de la version Apache Kafka

Vous pouvez mettre à jour un cluster MSK existant vers une version plus récente d'Apache Kafka. Vous ne pouvez pas la mettre à jour vers une version plus ancienne. Lorsque vous mettez à jour la version Apache Kafka d'un cluster MSK, vérifiez également votre logiciel côté client pour vous assurer que sa version vous permet d'utiliser les fonctionnalités de la nouvelle version Apache Kafka du cluster. Amazon MSK ne met à jour que le logiciel du serveur. Il ne met pas à jour vos clients.

Pour plus d'informations sur la manière de rendre un cluster hautement disponible lors d'une mise à jour, reportez-vous à la section the section called “Créer des clusters hautement disponibles”.

> **Important**
>
> Vous ne pouvez pas mettre à jour la version d'Apache Kafka pour un cluster MSK qui dépasse les limites décrites dans the section called “ Dimensionnez correctement votre cluster : nombre de partitions par agent”.

Mettre à jour la version d'Apache Kafka à l'aide du AWS Management Console

1. Ouvrez la console Amazon MSK à l'adresse https://console.aws.amazon.com/msk/.
2. Choisissez le cluster MSK sur lequel vous souhaitez mettre à jour la version Apache Kafka.
3. Dans l'onglet Propriétés, choisissez Mettre à niveau dans la section Version Apache Kafka.

Mettre à jour la version d'Apache Kafka à l'aide du AWS CLI

1. Exécutez la commande suivante, en la *ClusterArn*remplaçant par le Amazon Resource Name (ARN) que vous avez obtenu lors de la création de votre cluster. Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d’informations, consultez the section called “Liste des clusters”.

   ```
   aws kafka get-compatible-kafka-versions --cluster-arn ClusterArn
   ```

   La sortie de cette commande inclut une liste des versions d'Apache Kafka vers lesquelles vous pouvez mettre à jour le cluster. Elle ressemble à l'exemple suivant :

   ```
   {
       "CompatibleKafkaVersions": [
           {
               "SourceVersion": "2.2.1",
               "TargetVersions": [
                   "2.3.1",
                   "2.4.1",
                   "2.4.1.1",
                   "2.5.1"
               ]
           }
       ]
   }
   ```

2. Exécutez la commande suivante, en la *ClusterArn*remplaçant par le Amazon Resource Name (ARN) que vous avez obtenu lors de la création de votre cluster. Si vous n'avez pas l'ARN pour votre cluster, vous pouvez le trouver en listant tous les clusters. Pour plus d'informations, consultez the section called "Liste des clusters".

   Remplacez *Current-Cluster-Version* par la version actuelle du cluster. Car *TargetVersion*vous pouvez spécifier n'importe quelle version cible à partir de la sortie de la commande précédente.

   > **Important**
   >
   > Les versions de cluster ne sont pas des entiers simples. Pour trouver la version actuelle du cluster, utilisez l'DescribeClusteropération ou la commande describe-cluster AWS CLI . Voici un exemple de version : `KTVPDKIKX0DER`.

   ```
   aws kafka update-cluster-kafka-version --cluster-arn ClusterArn --current-
   version Current-Cluster-Version --target-kafka-version TargetVersion
   ```

   La sortie de la commande précédente ressemble au JSON suivant.

   ```
   {

       "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/exampleClusterName/
   abcdefab-1234-abcd-5678-cdef0123ab01-2",
       "ClusterOperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
   operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
   abcd-4f7f-1234-9876543210ef"
   }
   ```

3. Pour obtenir le résultat de l'`update-cluster-kafka-version`opération, exécutez la commande suivante en remplaçant *ClusterOperationArn* par l'ARN que vous avez obtenu dans le résultat de la `update-cluster-kafka-version` commande.

   ```
   aws kafka describe-cluster-operation --cluster-operation-arn ClusterOperationArn
   ```

   La sortie de cette commande `describe-cluster-operation` ressemble à l'exemple JSON suivant.

```
{
    "ClusterOperationInfo": {
        "ClientRequestId": "62cd41d2-1206-4ebf-85a8-dbb2ba0fe259",
        "ClusterArn": "arn:aws:kafka:us-east-1:012345678012:cluster/
exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2",
        "CreationTime": "2021-03-11T20:34:59.648000+00:00",
        "OperationArn": "arn:aws:kafka:us-east-1:012345678012:cluster-
operation/exampleClusterName/abcdefab-1234-abcd-5678-cdef0123ab01-2/0123abcd-
abcd-4f7f-1234-9876543210ef",
        "OperationState": "UPDATE_IN_PROGRESS",
        "OperationSteps": [
            {
                "StepInfo": {
                    "StepStatus": "IN_PROGRESS"
                },
                "StepName": "INITIALIZE_UPDATE"
            },
            {
                "StepInfo": {
                    "StepStatus": "PENDING"
                },
                "StepName": "UPDATE_APACHE_KAFKA_BINARIES"
            },
            {
                "StepInfo": {
                    "StepStatus": "PENDING"
                },
                "StepName": "FINALIZE_UPDATE"
            }
        ],
        "OperationType": "UPDATE_CLUSTER_KAFKA_VERSION",
        "SourceClusterInfo": {
            "KafkaVersion": "2.4.1"
        },
        "TargetClusterInfo": {
            "KafkaVersion": "2.6.1"
        }
    }
}
```


Si `OperationState` a la valeur `UPDATE_IN_PROGRESS`, attendez un moment, puis exécutez à nouveau la commande `describe-cluster-operation`. Lorsque l'opération est terminée, la

valeur de `OperationState` devient `UPDATE_COMPLETE`. Étant donné que le temps nécessaire à Amazon MSK pour effectuer l'opération varie, vous devrez peut-être vérifier à plusieurs reprises jusqu'à ce que l'opération soit terminée.

Mise à jour de la version Apache Kafka à l'aide de l'API

1. Appelez l'GetCompatibleKafkaVersionsopération pour obtenir une liste des versions d'Apache Kafka vers lesquelles vous pouvez mettre à jour le cluster.
2. Appelez l'UpdateClusterKafkaVersionopération pour mettre à jour le cluster vers l'une des versions compatibles d'Apache Kafka.

Bonnes pratiques pour les mises à niveau de version

Pour garantir la continuité du client pendant la mise à jour continue effectuée dans le cadre du processus de mise à niveau de la version de Kafka, passez en revue la configuration de vos clients et vos rubriques Apache Kafka comme suit :

- Définissez le facteur de réplication (RF) du sujet sur une valeur minimale de 2 pour les clusters à deux AZ et une valeur minimale de 3 pour les clusters à trois AZ. Une valeur RF de 2 peut entraîner la création de partitions hors ligne lors de l'application de correctifs.
- Définissez le nombre minimal de répliques synchronisées (MinISR) sur une valeur maximale de pour garantir que l'ensemble de répliques `RF - 1` de partitions puisse tolérer qu'une réplique soit hors ligne ou sous-répliquée.
- Configurez les clients pour qu'ils utilisent plusieurs chaînes de connexion Broker. La présence de plusieurs courtiers dans la chaîne de connexion d'un client permet un basculement si un courtier spécifique prenant en charge les E/S du client commence à être corrigé. Pour plus d'informations sur la façon d'obtenir une chaîne de connexion avec plusieurs courtiers, consultez Obtenir les courtiers bootstrap pour un cluster Amazon MSK.
- Nous vous recommandons de mettre à niveau les clients de connexion vers la version recommandée ou une version supérieure pour bénéficier des fonctionnalités disponibles dans la nouvelle version. Les mises à niveau des clients ne sont pas soumises aux dates de fin de vie (EOL) de la version Kafka de votre cluster MSK et ne doivent pas nécessairement être terminées avant la date de fin de vie. Apache Kafka fournit une politique de compatibilité client bidirectionnelle qui permet aux anciens clients de travailler avec des clusters plus récents et vice versa.
- Les clients Kafka utilisant les versions 3.x.x sont susceptibles de présenter les valeurs par défaut suivantes : et. `acks=all` `enable.idempotence=true` `acks=all`est différent de

la valeur par défaut précédente de `acks=1` et offre une durabilité accrue en garantissant que toutes les répliques synchronisées accusent réception de la demande de production. De même, la valeur par défaut pour `enable.idempotence` était précédemment`false`. Le passage à `enable.idempotence=true` la valeur par défaut réduit le risque de doublons de messages. Ces modifications sont considérées comme des paramètres conformes aux meilleures pratiques et peuvent introduire une petite latence supplémentaire conforme aux paramètres de performance normaux.

- Utilisez la version recommandée de Kafka lors de la création de nouveaux clusters MSK. L'utilisation de la version recommandée de Kafka vous permet de bénéficier des dernières fonctionnalités de Kafka et MSK.

Résolution des problèmes de votre cluster Amazon MSK

La documentation suivante peut vous aider à résoudre les problèmes que vous pouvez rencontrer avec votre cluster Amazon MSK. Vous pouvez également publier votre problème sur AWS re:Post.

Rubriques

Le remplacement du volume entraîne une saturation du disque en raison d'une surcharge de réplication

En cas de panne matérielle imprévue d'un volume, Amazon MSK peut remplacer le volume par une nouvelle instance. Kafka reremplit le nouveau volume en répliquant les partitions provenant d'autres courtiers du cluster. Une fois les partitions répliquées et rattrapées, elles peuvent devenir membres de Leadership and In-Sync Replica (ISR).

Problème

Dans un courtier qui se remet d'un remplacement de volume, certaines partitions de tailles différentes peuvent être remises en ligne avant d'autres. Cela peut être problématique car ces partitions peuvent servir du trafic provenant du même courtier qui continue de rattraper (répliquer) d'autres partitions. Ce trafic de réplication peut parfois saturer les limites de débit du volume sous-jacentes, qui sont de 250 MiB par seconde dans le cas par défaut. Lorsque cette saturation se produit, toutes les partitions déjà rattrapées seront affectées, ce qui se traduira par une latence au sein du cluster pour tous les courtiers partageant l'ISR avec les partitions rattrapées (et pas seulement les partitions principales en raison de prises distantes`acks=all`). Ce problème est plus fréquent dans le cas de grands clusters comportant un plus grand nombre de partitions dont la taille varie.

Recommandation

- Pour améliorer la posture des E/S de réplication, assurez-vous que les paramètres de thread conformes aux meilleures pratiques sont en place.
- Pour réduire le risque de saturation des volumes sous-jacents, activez le stockage provisionné avec un débit plus élevé. Une valeur de débit minimum de 500 Mbits/s est recommandée pour les cas de réplication à haut débit, mais la valeur réelle requise varie en fonction du débit et du cas d'utilisation. Provisionnement du débit de stockage.
- Pour minimiser la pression de réplication, abaissez `num.replica.fetchers` la valeur par défaut de2.

Groupe de consommateurs bloqué à l'état **`PreparingRebalance`**

Si un ou plusieurs de vos groupes de consommateurs sont bloqués dans un état de rééquilibrage perpétuel, cela peut être dû au problème KAFKA-9752 d'Apache Kafka, qui affecte les versions 2.3.1 et 2.4.1 d'Apache Kafka.

Pour résoudre ce problème, nous vous recommandons de mettre à niveau votre cluster vers la version Version de correction de bogues Amazon MSK 2.4.1.1, qui contient un correctif pour ce problème. Pour plus d'informations sur la mise à jour d'un cluster existant vers la version de correction de bogues Amazon MSK 2.4.1.1, consultez Mise à jour de la version Apache Kafka.

Les solutions pour résoudre ce problème sans mettre à niveau le cluster vers la version de correction des bogues Amazon MSK 2.4.1.1 consistent soit à configurer les clients Kafka pour qu'ils utilisent Protocole d'appartenance statique, soit à les placer sur le nœud d'agent de coordination Identifier et redémarrer du groupe de consommateurs bloqué.

Mise en œuvre d'un protocole d'appartenance statique

Pour mettre en œuvre le protocole d'appartenance statique dans vos clients, procédez comme suit :

1. Définissez la propriété `group.instance.id` de la configuration de vos consommateurs Kafka sur une chaîne statique identifiant le consommateur dans le groupe.
2. Assurez-vous que les autres instances de la configuration sont mises à jour pour qu'elles utilisent la chaîne statique.
3. Déployez les modifications dans vos consommateurs Kafka.

L'utilisation du protocole d'appartenance statique est plus efficace si le délai d'expiration de la session dans la configuration client est défini sur une durée qui permet au consommateur de récupérer sans déclencher prématurément un rééquilibrage du groupe de consommateurs. Par exemple, si votre application consommateur peut tolérer 5 minutes d'indisponibilité, une valeur raisonnable pour le délai d'expiration de la session serait de 4 minutes au lieu de la valeur par défaut de 10 secondes.

> **Note**
>
> L'utilisation du protocole d'appartenance statique ne fait que réduire la probabilité de rencontrer ce problème. Vous pouvez toujours le rencontrer même lorsque vous utilisez le protocole d'appartenance statique.

Redémarrage du nœud d'agent de coordination

Pour redémarrer le nœud d'agent de coordination, procédez comme suit :

1. Identifiez le coordinateur du groupe à l'aide de la commande `kafka-consumer-groups.sh`.

2. Redémarrez le coordinateur du groupe de consommateurs bloqué à l'aide de l'action RebootBrokerAPI.

Erreur lors de la transmission des journaux du courtier à Amazon CloudWatch Logs

Lorsque vous essayez de configurer votre cluster pour envoyer les journaux des courtiers à Amazon CloudWatch Logs, il se peut que vous obteniez l'une des deux exceptions suivantes.

Si vous obtenez une exception `InvalidInput.LengthOfCloudWatchResourcePolicyLimitExceeded`, réessayez mais utilisez les groupes de journaux qui commencent par `/aws/vendedlogs/`. Pour de plus amples informations, consultez Activation de la journalisation à partir de certains services Amazon Web Services.

En cas d'`InvalidInput.NumberOfCloudWatchResourcePoliciesLimitExceeded`exception, choisissez une politique Amazon CloudWatch Logs existante dans votre compte et ajoutez-y le code JSON suivant.

```
{"Sid":"AWSLogDeliveryWrite","Effect":"Allow","Principal":
{"Service":"delivery.logs.amazonaws.com"},"Action":
["logs:CreateLogStream","logs:PutLogEvents"],"Resource":["*"]}
```

Si vous essayez d'ajouter le JSON ci-dessus à une politique existante mais que vous recevez un message d'erreur indiquant que vous avez atteint la longueur maximale pour la politique que vous avez sélectionnée, essayez d'ajouter le JSON à une autre de vos politiques Amazon CloudWatch Logs. Après avoir ajouté le JSON à une politique existante, essayez à nouveau de configurer la livraison des journaux de courtage à Amazon Logs. CloudWatch

Aucun groupe de sécurité par défaut

Si vous essayez de créer un cluster et que vous obtenez une erreur indiquant qu'il n'y a pas de groupe de sécurité par défaut, cela peut être dû au fait que vous utilisez un VPC partagé avec vous. Demandez à votre administrateur de vous accorder l'autorisation de décrire les groupes de sécurité sur ce VPC et réessayez. Pour obtenir un exemple de stratégie autorisant cette action, consultez Amazon EC2 : Autorise la gestion des groupes de sécurité EC2 associés à un VPC spécifique, par programme et dans la console.

Le cluster apparaît bloqué à l'état En cours de création.

Parfois, la création de cluster peut prendre jusqu'à 30 minutes. Attendez 30 minutes et vérifiez à nouveau l'état du cluster.

L'état du cluster passe de En cours de création à En échec.

Réessayez de créer le cluster.

L'état du cluster est Actif mais les producteurs ne peuvent pas envoyer de données ou les consommateurs ne peuvent pas en recevoir.

- Si la création du cluster réussit (l'état du cluster est `ACTIVE`), mais que vous ne pouvez pas envoyer ou recevoir de données, assurez-vous que vos applications producteur et grand public ont accès au cluster. Pour de plus amples informations, veuillez consulter the section called “Étape 3 : créer un ordinateur client”.

- Si vos producteurs et consommateurs ont accès au cluster, mais rencontrent toujours des problèmes de production et de consommation de données, la cause peut être KAFKA-7697, qui affecte Apache Kafka version 2.1.0 et peut entraîner un blocage dans un ou plusieurs brokers. Envisagez de migrer vers Apache Kafka 2.2.1, qui n'est pas affecté par ce bogue. Pour de plus amples informations sur l'intégration, veuillez consulter Migration.

AWS CLI ne reconnaît pas Amazon MSK

Si vous avez AWS CLI installé les commandes Amazon MSK, mais qu'elles ne les reconnaissent pas, passez AWS CLI à la dernière version. Pour obtenir des instructions détaillées sur la mise à niveau du AWS CLI, consultez la section Installation du AWS Command Line Interface. Pour plus d'informations sur l'utilisation des commandes AWS CLI pour exécuter Amazon MSK, consultezComment ça marche.

Les partitions se déconnectent ou les réplicas sont désynchronisés

Ceux-ci peuvent être des symptômes de faible espace disque. veuillez consulter the section called “L'espace disque est faible”.

L'espace disque est faible

Consultez les bonnes pratiques suivantes pour gérer l'espace disque : the section called “Surveiller l'espace disque” et the section called “Ajuster les paramètres de rétention des données”.

Mémoire faible

Si vous voyez que la métrique `MemoryUsed` est élevée ou que la métrique `MemoryFree` est faible, cela ne signifie pas qu'il y a un problème. Apache Kafka est conçu pour utiliser autant de mémoire que possible, et il le gère de manière optimale.

Le producteur obtient NotLeaderForPartitionException

Il s'agit souvent d'une erreur transitoire. Définissez le paramètre de configuration `retries` du producteur sur une valeur supérieure à sa valeur actuelle.

Partitions sous-répliquées (URP) supérieures à zéro

La métrique `UnderReplicatedPartitions` est importante à surveiller. Dans un cluster MSK sain, cette métrique a la valeur 0. Si elle est supérieure à zéro, cela peut être pour l'une des raisons suivantes.

- Si `UnderReplicatedPartitions` est irrégulier, le problème peut être que le cluster n'est pas provisionné à la bonne taille pour gérer le trafic entrant et sortant. veuillez consulter Bonnes pratiques.
- Si la valeur `UnderReplicatedPartitions` est toujours supérieure à 0, y compris pendant les périodes de faible trafic, le problème peut être que vous avez défini des listes de contrôle d'accès (ACL) restrictives qui n'autorisent pas les agents à accéder aux rubriques. Pour répliquer les partitions, les brokers doivent être autorisés à lire et à décrire les rubriques. DESCRIBE est accordé par défaut avec l'autorisation READ. Pour de plus amples informations sur la définition des ACL, veuillez consulter Autorisation et ACL dans la documentation Apache Kafka.

Le cluster contient des rubriques appelées __amazon_msk_canary et __amazon_msk_canary_state

Il se peut que votre cluster MSK possède une rubrique portant le nom `__amazon_msk_canary` et une autre portant le nom `__amazon_msk_canary_state`. Il s'agit de rubriques internes créées et utilisées par Amazon MSK pour les métriques d'intégrité et de diagnostic du cluster. Ces rubriques sont d'une taille négligeable et ne peuvent pas être supprimées.

Échec de la réplication des partitions

Assurez-vous que vous n'avez pas défini d'ACL sur CLUSTER_ACTIONS.

Impossible d'accéder au cluster dont l'accès public est activé

Si l'accès public est activé sur votre cluster, mais que vous ne pouvez toujours pas y accéder depuis Internet, procédez comme suit :

1. Assurez-vous que les règles entrantes du groupe de sécurité du cluster autorisent votre adresse IP et le port du cluster. Pour obtenir la liste des numéros de port du cluster, consultez the section called “Informations sur le port”. Assurez-vous également que les règles sortantes du groupe de sécurité autorisent les communications sortantes. Pour plus d'informations sur les groupes de sécurité et leurs règles entrantes et sortantes, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC.
2. Assurez-vous que votre adresse IP et le port du cluster sont autorisés dans les règles entrantes de l'ACL du réseau VPC du cluster. Contrairement aux groupes de sécurité, les listes de contrôle d'accès (ACL) réseau sont sans état. Cela signifie que vous devez configurer à la fois des règles entrantes et sortantes. Dans les règles sortantes, autorisez tout le trafic (plage de ports : 0 à 65535) vers votre adresse IP. Pour plus d'informations, consultez Ajouter et supprimer des règles dans le Guide de l'utilisateur Amazon VPC.
3. Assurez-vous que vous utilisez la chaîne bootstrap-brokers à accès public pour accéder au cluster. Un cluster MSK dont l'accès public est activé possède deux chaînes bootstrap-brokers différentes, l'une pour l'accès public et l'autre pour l'accès depuis AWS. Pour plus d’informations, consultez the section called “Faire en sorte que les courtiers Bootstrap utilisent le AWS Management Console”.

Impossible d'accéder au cluster depuis l'intérieur AWS : problèmes de réseau

Si vous disposez d'une application Apache Kafka qui ne parvient pas à communiquer avec un cluster MSK, commencez par effectuer le test de connectivité suivant.

1. Utilisez l'une des méthodes décrites dans the section called “Obtention des agents d'amorçage” pour obtenir les adresses des brokers d’amorçage.
2. Dans la commande suivante, remplacez le *broker d’amorçage* par l'une des adresses de broker que vous avez obtenues à l'étape précédente. Remplacez *port-number* par 9094 si le cluster est configuré pour utiliser l'authentification TLS. Si le cluster n'utilise pas l'authentification TLS, remplacez le *port-number* par 9092. Exécutez la commande à partir de l'ordinateur du client.

   ```
   telnet bootstrap-broker port-number
   ```

   Où le numéro de port est :

   - 9094 si le cluster est configuré pour utiliser l'authentification TLS.
   - 9092 Si le cluster n'utilise pas l'authentification TLS.
   - Un numéro de port différent est requis si l'accès public est activé.

   Exécutez la commande à partir de l'ordinateur du client.
3. Répétez la commande précédente pour tous les brokers d’amorçage.

Si la machine cliente est en mesure d'accéder aux courtiers, cela signifie qu'il n'y a aucun problème de connectivité. Dans ce cas, exécutez la commande suivante pour vérifier si votre client Apache Kafka dispose de la configuration adéquate. Pour obtenir des *brokers d’amorçage*, utilisez l'une des méthodes décrites dans the section called “Obtention des agents d'amorçage”. Mettez le nom de votre rubrique dans *rubrique*.

```
<path-to-your-kafka-installation>/bin/kafka-console-producer.sh --broker-
list bootstrap-brokers --producer.config client.properties --topic topic
```

Si la commande précédente réussit, cela signifie que votre client possède la bonne configuration. Si vous ne parvenez toujours pas à produire et à consommer à partir d'une application, déboguez le problème au niveau de cette dernière.

Si la machine cliente n'est pas en mesure d'accéder aux courtiers, consultez les sous-sections suivantes pour obtenir des instructions basées sur votre configuration client-machine.

Client Amazon EC2 et cluster MSK dans le même VPC

Si l'ordinateur client se trouve dans le même VPC que le cluster MSK, assurez-vous que le groupe de sécurité du cluster dispose d'une règle entrante qui accepte le trafic provenant du groupe de sécurité de l'ordinateur client. Pour plus d'informations sur la configuration de ces règles, consultez Règles des groupes de sécurité. Pour obtenir un exemple de la façon d'accéder à un cluster à partir d'une instance Amazon EC2 située dans le même VPC que le cluster, consultez Premiers pas.

Client Amazon EC2 et cluster MSK dans différents VPC

Si l'ordinateur du client et le cluster se trouvent dans deux VPC différents, veillez à ce que :

- Les deux VPC soient appairés.
- L'état de la connexion d'appairage soit actif.
- Les tables de routage des deux VPC soient configurées correctement.

Pour de plus amples informations sur l'appairage de VPC, veuillez consulter Utilisation des connexions d'appairage de VPC.

Client sur site

Dans le cas d'un client sur site configuré pour se connecter au cluster MSK à l'aide de AWS VPN, assurez-vous de ce qui suit :

- Le statut de la connexion VPN est UP. Pour de plus amples informations sur la façon de vérifier le statut de la connexion VPN, veuillez consulter Comment vérifier le statut actuel d'un tunnel VPN ?
- La table de routage du VPC du cluster contient la route d'un CIDR sur site dont la cible a le format `Virtual private gateway(vgw-xxxxxxxx)`.
- Le groupe de sécurité du cluster MSK autorise le trafic sur les ports 2181, 9092 (si votre cluster accepte le trafic en texte brut) et 9094 (si votre cluster accepte le trafic chiffré TLS).

Pour plus d'informations sur la AWS VPN résolution des problèmes, consultez la section Résolution des problèmes liés au VPN du Client.

AWS Direct Connect

Si le client l'utilise AWS Direct Connect, consultez la section Résolution des problèmes AWS Direct Connect.

Si les instructions données dans la résolution de problèmes ne suffisent pas, vérifiez si un pare-feu ne bloque pas le trafic. Pour un débogage plus poussé, utilisez des outils comme `tcpdump` et `Wireshark` pour analyser le trafic et pour vous assurer qu'il atteint le cluster MSK.

Échec de l'authentification : trop de connexions

L'erreur `Failed authentication ... Too many connects` indique qu'un agent se protège parce qu'un ou plusieurs clients IAM tentent de s'y connecter à un rythme effréné. Pour aider les agents à accepter un taux plus élevé de nouvelles connexions IAM, vous pouvez augmenter le paramètre de configuration `reconnect.backoff.ms`.

Pour en savoir plus sur les limites de taux applicables aux nouvelles connexions par agent, consultez la page Quota d'Amazon MSK.

MSK sans serveur : échec de la création du cluster

Si vous essayez de créer un cluster MSK sans serveur et que le flux de travail échoue, vous n'êtes peut-être pas autorisé à créer un point de terminaison de VPC. Vérifiez que votre administrateur vous a autorisé à créer un point de terminaison de VPC en autorisant l'action `ec2:CreateVpcEndpoint`.

Pour obtenir la liste complète des autorisations requises pour effectuer toutes les actions Amazon MSK, consultez AWS politique gérée : AmazonMSK FullAccess.

Bonnes pratiques

Cette rubrique décrit les bonnes pratiques à suivre lors de l'utilisation d'Amazon MSK.

Dimensionnez correctement votre cluster : nombre de partitions par agent

Le tableau suivant indique le nombre recommandé de partitions (y compris les réplicas de leader et de suiveur) par agent.

Taille du courtier	Nombre recommandé de partitions (y compris les réplicas de leader et de suiveur) par agent
`kafka.t3.small`	300
`kafka.m5.large` ou `kafka.m5.xlarge`	1 000
`kafka.m5.2xlarge`	2000
`kafka.m5.4xlarge` , `kafka.m5.8xlarge` , `kafka.m5.12xlarge` , `kafka.m5.16xlarge` ou `kafka.m5.24xlarge`	4000
`kafka.m7g.large` ou `kafka.m7g.xlarge`	1 000
`kafka.m7g.2xlarge`	2000
`kafka.m7g.4xlarge` ,`kafka.m7g.8xlarge` ,`kafka.m7g.12xlarge` , ou `kafka.m7g.16xlarge`	4000

Si le nombre de partitions par agent dépasse la valeur recommandée et que votre cluster est surchargé, il se peut que vous ne puissiez pas effectuer les opérations suivantes :

- Mettre à jour la configuration du cluster

- Mettre à jour le cluster vers une taille de courtier plus petite
- Associer un AWS Secrets Manager secret à un cluster doté d'une authentification SASL/SCRAM

Un nombre élevé de partitions peut également entraîner l'absence de métriques Kafka sur CloudWatch et sur le scraping de Prometheus.

Pour obtenir des conseils sur le choix du nombre de partitions, veuillez consulter Apache Kafka prend en charge les 200k partitions par cluster. Nous vous recommandons également d'effectuer vos propres tests afin de déterminer la bonne taille pour vos courtiers. Pour plus d'informations sur les différentes tailles de courtier, consultezthe section called “Tailles des courtiers”.

Dimensionnez correctement votre cluster : nombre d'agents par cluster

Afin de déterminer le nombre approprié d'agents pour votre cluster MSK et comprendre les coûts, consultez la feuille de calcul Tailles et tarification MSK. Cette feuille de calcul fournit une estimation du dimensionnement d'un cluster MSK et des coûts associés d'Amazon MSK par rapport à un cluster Apache Kafka basé sur EC2 similaire, auto-géré. Pour de plus amples informations sur les paramètres d'entrée dans la feuille de calcul, pointez la souris sur les descriptions des paramètres. Les estimations fournies par cette feuille sont prudentes et fournissent un point de départ pour un nouveau cluster. Les performances, la taille et les coûts du cluster dépendent de votre cas d'utilisation et nous vous recommandons de les vérifier à l'aide de tests réels.

Pour comprendre comment l'infrastructure sous-jacente affecte les performances d'Apache Kafka, consultez la section Meilleures pratiques pour dimensionner correctement vos clusters Apache Kafka afin d'optimiser les performances et les coûts dans le AWS blog Big Data. Le billet de blog fournit des informations sur la manière de dimensionner vos clusters pour répondre à vos exigences en matière de débit, de disponibilité et de latence. Il fournit également des réponses à des questions telles que le moment où vous devez augmenter ou monter en puissance, et des conseils sur la manière de vérifier en permanence la taille de vos clusters de production.

Optimisation du débit du cluster pour les instances m5.4xl, m7g.4xl ou supérieures

Lorsque vous utilisez des instances m5.4xl, m7g.4xl ou supérieures, vous pouvez optimiser le débit du cluster en ajustant les configurations num.io.threads et num.network.threads.

Num.io.threads est le nombre de threads qu'un agent utilise pour traiter les demandes. L'ajout de threads supplémentaires, dans la limite du nombre de cœurs de processeur pris en charge par la taille de l'instance, peut contribuer à améliorer le débit du cluster.

Num.network.threads est le nombre de threads que l'agent utilise pour recevoir toutes les demandes entrantes et renvoyer les réponses. Les threads réseau placent les demandes entrantes dans une file d'attente de demandes pour être traitées par io.threads. La définition de num.network.threads sur la moitié du nombre de cœurs de processeur pris en charge pour la taille de l'instance permet d'utiliser pleinement la nouvelle taille d'instance.

> **Important**
>
> N'augmentez pas num.network.threads sans d'abord augmenter num.io.threads, car cela peut entraîner une congestion liée à la saturation de la file d'attente.

Paramètres recommandés

Taille d’instance	Valeur recommandée pour num.io.threads	Valeur recommandée pour num.network.threads
m5.4xl	16	8
m5.8xl	32	16
m5.12xl	48	24
m5.16xl	64	32
m5.24xl	96	48
m7g.4xlarge	16	8
m7g.8xlarge	32	16
m7g.12xlarge	48	24
m7g.16xlarge	64	32

Utilisez la dernière version de Kafka AdminClient pour éviter le problème de non-concordance entre les identifiants des sujets

L'identifiant d'un sujet est perdu (erreur : ne correspond pas à l'identifiant du sujet de la partition) lorsque vous utilisez une AdminClient version de Kafka inférieure `--zookeeper` à 2.8.0 avec l'indicateur pour augmenter ou réaffecter les partitions de sujet pour un cluster utilisant la version 2.8.0 ou supérieure de Kafka. Notez que l'indicateur `--zookeeper` est obsolète dans Kafka 2.5 et qu'il est supprimé à partir de Kafka 3.0. Consultez Mise à niveau vers la version 2.5.0 à partir de n'importe quelle version 0.8.x à 2.4.x.

Pour éviter toute non-correspondance entre les ID de rubrique, utilisez une version 2.8.0 ou supérieure de client Kafka pour les opérations d'administration de Kafka. Les clients de version 2.5 ou supérieure peuvent également utiliser l'indicateur `--bootstrap-servers` au lieu de l'indicateur `--zookeeper`.

Créer des clusters hautement disponibles

Suivez les recommandations suivantes afin que votre cluster MSK soit hautement disponible lors d'une mise à jour (par exemple lorsque vous modifiez la taille du broker ou la version d'Apache Kafka) ou lorsqu'Amazon MSK remplace un broker.

- Configurez un cluster à trois AZ.
- Assurez-vous que le facteur de réplication (RF) est d'au moins 3. Notez qu'un RF de 1 peut entraîner des partitions hors ligne pendant une mise à jour propagée ; et un RF de 2 peut entraîner une perte de données.
- Définissez les réplicas en synchronisation minimum (minISR) sur au moins RF - 1. Un minISR égal au RF peut empêcher la production vers le cluster pendant une mise à jour propagée. Un minISR de 2 permet de disposer de rubriques répliquées à trois voies lorsqu'un réplica est hors ligne.
- Assurez-vous que les chaînes de connexion client incluent au moins un agent de chaque zone de disponibilité. La présence de plusieurs agents dans la chaîne de connexion d'un client permet le basculement lorsqu'un agent spécifique est hors ligne pour une mise à jour. Pour plus d'informations sur la façon d'obtenir une chaîne de connexion avec plusieurs agents, reportez-vous à la section the section called “Obtention des agents d'amorçage”.

Surveiller l'utilisation de l'UC

Amazon MSK vous recommande vivement de maintenir l'utilisation totale de l'UC (définie comme `CPU User + CPU System`) inférieure à 60 % pour vos agents. Lorsque vous disposez d'au moins 40 % de l'UC totale de votre cluster, Apache Kafka peut redistribuer la charge de l'UC entre les agents du cluster si nécessaire. Cela est par exemple nécessaire lorsqu'Amazon MSK détecte et rétablit une erreur de l'agent ; dans ce cas, Amazon MSK effectue une maintenance automatique, telle que l'application de correctifs. Autre exemple : lorsqu'un utilisateur demande une modification de la taille du courtier ou une mise à niveau de version ; dans ces deux cas, Amazon MSK déploie des flux de travail progressifs qui mettent un courtier hors ligne à la fois. Lorsque des agents dotés de partitions principales se déconnectent, Apache Kafka réaffecte la direction des partitions afin de redistribuer le travail aux autres agents du cluster. En suivant cette bonne pratique, vous pouvez vous assurer que votre cluster dispose d'une marge d'UC suffisante pour tolérer de tels événements opérationnels.

Vous pouvez utiliser Amazon CloudWatch Metric Math pour créer une métrique composite qui est`CPU User + CPU System`. Définissez une alarme qui se déclenche lorsque la métrique composite atteint une utilisation moyenne de l'UC de 60 %. Lorsque cette alarme est déclenchée, mettez le cluster à l'échelle à l'aide de l'une des options suivantes :

- Option 1 (recommandée) : mettez à jour la taille de votre courtier à la taille supérieure suivante. Par exemple, si la taille actuelle est la suivante`kafka.m5.large`, mettez à jour le cluster à utiliser`kafka.m5.xlarge`. N'oubliez pas que lorsque vous mettez à jour la taille des courtiers dans le cluster, Amazon MSK met les courtiers hors ligne de manière continue et réaffecte temporairement la direction de la partition à d'autres courtiers. Une mise à jour de taille prend généralement 10 à 15 minutes par agent.
- Option 2 : Si certaines rubriques contiennent tous les messages ingérés à partir de producteurs utilisant des écritures circulaires (en d'autres termes, les messages ne sont pas saisis et les commandes ne sont pas importantes pour les consommateurs), étendez votre cluster en ajoutant des agents. Ajoutez également des partitions aux rubriques existantes avec le débit le plus élevé. Ensuite, utilisez `kafka-topics.sh --describe` pour vous assurer que les partitions nouvellement ajoutées sont attribuées aux nouveaux agents. Le principal avantage de cette option par rapport à la précédente réside dans le fait que vous pouvez gérer les ressources et les coûts de manière plus précise. En outre, vous pouvez utiliser cette option si la charge de l'UC dépasse de manière significative 60 %, car cette forme de mise à l'échelle n'entraîne généralement pas d'augmentation de la charge sur les agents existants.
- Option 3 : étendez votre cluster en ajoutant des agents, puis réattribuez les partitions existantes à l'aide de l'outil de réattribution de partitions nommé `kafka-reassign-partitions.sh`.

Toutefois, si vous utilisez cette option, le cluster devra dépenser des ressources pour répliquer les données d'un agent à l'autre après la réaffectation des partitions. Par rapport aux deux options précédentes, cela peut augmenter considérablement la charge sur le cluster dans un premier temps. Par conséquent, Amazon MSK ne recommande pas d'utiliser cette option lorsque l'utilisation de l'UC est supérieure à 70 %, car la réplication entraîne une charge de l'UC et un trafic réseau supplémentaires. Amazon MSK recommande d'utiliser cette option uniquement si les deux options précédentes ne sont pas réalisables.

Autres recommandations :

- Surveillez l'utilisation totale de l'UC par agent en tant que proxy pour la répartition de la charge. Si les agents utilisent régulièrement l'UC de manière inégale, cela peut être le signe que la charge n'est pas répartie uniformément au sein du cluster. Amazon MSK recommande d'utiliser Cruise Control pour gérer en permanence la répartition de la charge via l'attribution des partitions.
- Surveiller la latence de production et de consommation. La latence de production et de consommation peut augmenter de façon linéaire en fonction de l'utilisation de l'UC.
- JMX Scrape Interval : si vous activez la surveillance ouverte avec la fonctionnalité Prometheus, il est recommandé d'utiliser un Scrape Interval de 60 secondes ou plus (scrape_interval : 60s) pour la configuration de votre hôte Prometheus (prometheus.yml). La réduction du Scrape Interval peut entraîner une utilisation élevée de l'UC sur votre cluster.

Surveiller l'espace disque

Pour éviter de manquer d'espace disque pour les messages, créez une CloudWatch alarme qui surveille la `KafkaDataLogsDiskUsed` métrique. Lorsque la valeur de cette mesure atteint ou dépasse 85 %, effectuez une ou plusieurs des actions suivantes :

- Utilisez the section called “Dimensionnement automatique”. Vous pouvez également augmenter manuellement le stockage des agents, comme décrit dans the section called “Mise à l'échelle manuelle”.
- Réduisez la période de rétention des messages ou la taille du journal. Pour de plus amples informations sur la procédure à utiliser, veuillez consulter the section called “Ajuster les paramètres de rétention des données”.
- Supprimer les rubriques inutilisées.

Pour plus d'informations sur la configuration et l'utilisation des alarmes, consultez la section Utilisation d'Amazon CloudWatch Alarms. Pour obtenir la liste complète de toutes les métriques Amazon MSK, consultez Surveillance d'un cluster.

Ajuster les paramètres de rétention des données

La consommation de messages ne les supprime pas du journal. Pour libérer régulièrement de l'espace disque, vous pouvez spécifier explicitement une période de rétention, c'est-à-dire la durée de conservation des messages dans le journal. Vous pouvez également spécifier une taille de journal de rétention. Lorsque la période de rétention ou la taille du journal de rétention sont atteintes, Apache Kafka commence à supprimer les segments inactifs du journal.

Pour spécifier une stratégie de rétention au niveau du cluster, définissez un ou plusieurs des paramètres suivants : `log.retention.hours`, `log.retention.minutes`, `log.retention.ms`, ou `log.retention.bytes`. Pour plus d'informations, consultez the section called “Configurations personnalisées”.

Vous pouvez également spécifier des paramètres de rétention au niveau de la rubrique :

- Pour spécifier une période de rétention par rubrique, utilisez la commande suivante.

```
kafka-configs.sh --bootstrap-server $bs --alter --entity-type topics --entity-
name TopicName --add-config retention.ms=DesiredRetentionTimePeriod
```

- Pour spécifier une taille de journal de rétention par rubrique, utilisez la commande suivante.

```
kafka-configs.sh --bootstrap-server $bs --alter --entity-type topics --entity-
name TopicName --add-config retention.bytes=DesiredRetentionLogSize
```

Les paramètres de rétention que vous spécifiez au niveau de la rubrique ont priorité sur les paramètres de niveau cluster.

Accélération de la récupération du journal après un arrêt incorrect

Après un arrêt incorrect, le redémarrage d'un agent peut prendre un certain temps, car il procède à la récupération du journal. Par défaut, Kafka n'utilise qu'un seul thread par répertoire de journal pour effectuer cette récupération. Par exemple, si vous avez des milliers de partitions, la récupération du journal peut prendre des heures. Pour accélérer la récupération du journal,

il est recommandé d'augmenter le nombre de threads à l'aide de la propriété de configuration `num.recovery.threads.per.data.dir`. Vous pouvez la définir sur le nombre de cœurs d'UC.

Surveiller la mémoire Apache Kafka

Nous vous recommandons de surveiller la mémoire utilisée par Apache Kafka. Dans le cas contraire, le cluster risque de devenir indisponible.

Pour déterminer la quantité de mémoire utilisée par Apache Kafka, vous pouvez surveiller la métrique `HeapMemoryAfterGC`. `HeapMemoryAfterGC` est le pourcentage de mémoire de tas totale qui est utilisée après le récupérateur de mémoire. Nous vous recommandons de créer une CloudWatch alarme qui agit lorsque les `HeapMemoryAfterGC` augmentations sont supérieures à 60 %.

Les étapes que vous pouvez suivre pour réduire l'utilisation de la mémoire varient. Elles dépendent de la façon dont vous configurez Apache Kafka. Par exemple, si vous utilisez la diffusion de messages transactionnels, vous pouvez réduire la valeur `transactional.id.expiration.ms` de votre configuration Apache Kafka de `604800000` ms à `86400000` ms (de 7 jours à 1 jour). Cela permet de réduire l'empreinte mémoire de chaque transaction.

Ne pas ajouter d'agents non-MSK

Pour les clusters ZooKeeper basés, si vous utilisez ZooKeeper les commandes Apache pour ajouter des courtiers, ces courtiers ne sont pas ajoutés à votre cluster MSK et votre Apache ZooKeeper contiendra des informations incorrectes sur le cluster. Cela peut entraîner une perte de données. Pour les opérations de cluster prises en charge, reportez-vous à la section Comment ça marche.

Utilisation du chiffrement en transit

Pour de plus amples informations sur le chiffrement en transit et sur la façon de l'activer, veuillez consulter the section called “Chiffrement en transit”.

Réaffecter les partitions

Pour déplacer des partitions vers différents brokers sur le même cluster, vous pouvez utiliser l'outil de réaffectation de partition nommé `kafka-reassign-partitions.sh`. Par exemple, après avoir ajouté de nouveaux courtiers pour étendre un cluster ou pour déplacer des partitions afin de supprimer des courtiers, vous pouvez rééquilibrer ce cluster en réattribuant des partitions aux

nouveaux courtiers. Pour de plus amples informations sur l'ajout de brokers à un cluster, veuillez consulter the section called “Expansion d'un cluster”. Pour plus d'informations sur la manière de supprimer des courtiers d'un cluster, consultezthe section called “Supprimer un courtier”. Pour de plus amples informations sur l'outil de réaffectation de partition, veuillez consulter Expansion de votre cluster dans la documentation Apache Kafka.

Historique du document pour le Guide du développeur Amazon MSK

Le tableau suivant décrit les modifications importantes apportées au Guide du développeur Amazon MSK.

Dernière mise à jour de la documentation : 25 juin 2024

Modification	Description	Date
Ajout de la fonctionnalité de mise à niveau de Graviton sur place.	Vous pouvez mettre à jour la taille de votre courtier de cluster de M5 ou T3 à M7g, ou de M7g à M5.	25/06/2024
3.4.0 Date de fin de support annoncée.	La date de fin du support pour la version 3.4.0 d'Apache Kafka est le 17 juin 2025.	24/06/2024
Ajout de la fonctionnalité de suppression du courtier.	Vous pouvez réduire la capacité de stockage et de calcul de votre cluster provisionné en supprimant des ensembles de courtiers , sans impact sur la disponibi lité, sans risque de durabilité des données ni interruption de vos applications de streaming de données.	16/05/2024
`WriteDataIdempoten tly` ajouté à AWSMSKRep licatorExecutionRole	WriteDataIdempotently une autorisation est ajoutée à la AWSMSKReplicatorEx ecutionRole politique pour prendre en charge la réplicati	16/05/2024

Modification	Description	Date
	on des données entre les clusters MSK.	
Lancement de courtiers Graviton M7g au Brésil et à Bahreïn.	Amazon MSK prend désormais en charge la disponibilité des courtiers m7G en Amérique du Sud (sa-east-1, São Paulo) et au Moyen-Orient (me-south-1, Bahreïn) à l'aide de processeurs Graviton (AWS processeurs ARM personnalisés conçus par Amazon Web Services).	2024-2-07
Libérez les courtiers Graviton M7g dans la région chinoise	Amazon MSK prend désormais en charge la disponibilité des courtiers m7G dans la région chinoise à l'aide de processeurs AWS Graviton (processeurs ARM personnalisés conçus par Amazon Web Services).	11/01/2022
Politique de support des versions d'Amazon MSK Kafka	Ajout d'une explication de la politique de support des versions de Kafka prises en charge par Amazon MSK. Pour plus d'informations, consultez les versions d'Apache Kafka.	08/12/2023

Modification	Description	Date
Nouvelle politique relative aux rôles d'exécution des services pour prendre en charge Amazon MSK Replicator.	Amazon MSK a ajouté une nouvelle `AWSMSKReplicatorExecutionRole` politique pour prendre en charge Amazon MSK Replicator. Pour plus d'informations, consultez Politique gérée par AWS : `AWSMSKReplicatorExecutionRole`.	06/12/2023
Support M7g Graviton	Amazon MSK prend désormais en charge les courtiers m7G utilisant des processeurs AWS Graviton (processeurs ARM personnalisés conçus par Amazon Web Services).	27/11/2023
Réplicateur Amazon MSK	Le réplicateur Amazon MSK est une nouvelle fonctionnalité que vous pouvez utiliser pour répliquer des données entre des clusters Amazon MSK. Amazon MSK Replicator inclut une mise à jour de la politique d'Amazon FullAccess MSK. Pour plus d'informations, consultez Politique gérée par AWS : `AmazonMSKFullAccess`.	28/09/2023

Modification	Description	Date
Mise à jour des bonnes pratiques IAM.	Mise à jour du guide s'aligner sur les bonnes pratiques IAM. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.	2023-03-08
Mises à jour du rôle lié à un service pour prendre en charge la connectivité privée à plusieurs VPC	Amazon MSK inclut désormais des mises à jour des rôles AWSServiceRoleForKafka liés aux services pour gérer les interfaces réseau et les points de terminaison VPC de votre compte, afin de rendre les courtiers de clusters accessibles aux clients de votre VPC. Amazon MSK utilise des autorisations pour `DescribeVpcEndpoints` , `ModifyVpcEndpoint` et `DeleteVpcEndpoints` . Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon MSK.	2023-03-08
Prise en charge d'Apache Kafka 2.7.2	Amazon MSK prend désormais en charge la version 2.7.2 d'Apache Kafka. Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	2021-12-21

Modification	Description	Date
Prise en charge d'Apache Kafka 2.6.3	Amazon MSK prend désormais en charge la version 2.6.3 d'Apache Kafka. Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	2021-12-21
Version préliminaire de MSK sans serveur	MSK sans serveur est une nouvelle fonctionnalité que vous pouvez utiliser pour créer des clusters sans serveur. Pour plus d'informations, consultez MSK sans serveur.	2021-11-29
Prise en charge d'Apache Kafka 2.8.1	Amazon MSK prend désormais en charge la version 2.8.1 d'Apache Kafka. Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	2021-09-30
MSK Connect	MSK Connect est une nouvelle fonctionnalité que vous pouvez utiliser pour créer et gérer des connecteurs Apache Kafka. Pour plus d'informations, consultez MSK Connect.	16/09/2021
Prise en charge d'Apache Kafka 2.7.1	Amazon MSK prend désormais en charge la version 2.7.1 d'Apache Kafka. Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	25/05/2021

Modification	Description	Date
Prise en charge d'Apache Kafka 2.8.0	Amazon MSK prend désormais en charge la version 2.8.0 d'Apache Kafka. Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	28/04/2021
Prise en charge d'Apache Kafka 2.6.2	Amazon MSK prend désormais en charge la version 2.6.2 d'Apache Kafka. Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	28/04/2021
Prise en charge de la mise à jour du type d'agent	Vous pouvez maintenant modifier le type d'agent pour un cluster existant. Pour plus d'informations, consultez Mise à jour de la taille du courtier.	21/01/2021
Prise en charge d'Apache Kafka 2.6.1	Amazon MSK prend désormais en charge la version 2.6.1 d'Apache Kafka. Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	19/01/2021
Prise en charge d'Apache Kafka 2.7.0	Amazon MSK prend désormais en charge la version 2.7.0 d'Apache Kafka. Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	29/12/2020

Modification	Description	Date
Aucun nouveau cluster avec la version 1.1.1 d'Apache Kafka	Vous ne pouvez plus créer de nouveau cluster Amazon MSK avec la version 1.1.1 d'Apache Kafka. Toutefois, si vous avez des clusters MSK existants qui exécutent la version 1.1.1 d'Apache Kafka, vous pouvez continuer à utiliser toutes les fonctionnalités actuellem ent prises en charge sur ces clusters existants. Pour plus d'informations, consultez Versions Apache Kafka.	24/11/2020
Métriques de retard des consommateurs	Amazon MSK fournit désormais des métriques vous permettant de surveille r le retard des consommat eurs. Pour plus d'informations, consultez Surveillance d'un cluster Amazon MSK.	23/11/2020
Prise en charge de Cruise Control	Amazon MSK prend désormais en charge LinkedIn le régulateur de vitesse. Pour plus d'informations, consultez Utilisation LinkedIn du régulateur de vitesse pour Apache Kafka avec Amazon MSK.	17/11/2020

Modification	Description	Date
Prise en charge d'Apache Kafka 2.6.0	Amazon MSK prend désormais en charge la version 2.6.0 d'Apache Kafka. Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	21/10/2020
Prise en charge d'Apache Kafka 2.5.1	Amazon MSK prend désormais en charge la version 2.5.1 d'Apache Kafka. Avec Apache Kafka version 2.5.1, Amazon MSK prend en charge le chiffrement lors du transit entre les clients et les points de terminaison. ZooKeeper Pour plus d'informations, consultez Versions Apache Kafka prises en charge.	2020-09-30
Extension automatique de l'application	Vous pouvez configurer Amazon Managed Streaming for Apache Kafka afin d'étendre automatiquement le stockage de votre cluster en réponse à une utilisation accrue. Pour plus d'informations, consultez Dimensionnement automatique.	2020-09-30

Modification	Description	Date
Prise en charge de la sécurité par nom d'utilisateur et mot de passe	Amazon MSK prend désormais en charge la connexion aux clusters à l'aide d'un nom d'utilisateur et d'un mot de passe. Amazon MSK stocke les informations d'identification dans AWS Secrets Manager. Pour plus d'informations, consultez Authentification SASL/SCRAM.	17/09/2020
Prise en charge de la mise à niveau de la version Apache Kafka d'un cluster Amazon MSK	Vous pouvez désormais mettre à niveau la version Apache Kafka d'un cluster MSK existant.	2020-05-28
Support pour nœuds de broker type T3.small	Amazon MSK prend désormais en charge la création de clusters pour des agents de type Amazon EC2 T3.small.	08/04/2020
Prise en charge d'Apache Kafka 2.4.1	Amazon MSK prend désormais en charge la version 2.4.1 d'Apache Kafka.	2020-04-02

Modification	Description	Date
Prise en charge de la diffusion des journaux d’agents	Amazon MSK peut désormais diffuser les journaux des courtiers vers CloudWatch Logs, Amazon S3 et Amazon Data Firehose. Firehose peut, à son tour, envoyer ces journaux aux destinations qu'il prend en charge, telles que OpenSearch Service.	2020-02-25
Prise en charge d'Apache Kafka 2.3.1	Amazon MSK prend désormais en charge la version 2.3.1 d'Apache Kafka.	2019-12-19
Surveillance ouverte	Amazon MSK prend désormais en charge la surveillance ouverte avec Prometheus.	2019-12-04
Prise en charge d'Apache Kafka 2.2.1	Amazon MSK prend désormais en charge la version 2.2.1 d'Apache Kafka.	2019-07-31
Disponibilité générale	Les nouvelles fonctionnalités incluent la prise en charge du balisage, l'authentification, le chiffrement TLS, les configurations et la possibilité de mettre à jour le stockage du broker.	2019-05-30
Prise en charge d'Apache Kafka 2.1.0	Amazon MSK prend désormais en charge la version 2.1.0 d'Apache Kafka.	2019-02-05

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.