aws

Guide de l’utilisateur

Amazon ECR

Version de l'API 2015-09-21

Amazon ECR: Guide de l’utilisateur

Table of Contents

Registre de conteneur Amazon Elastic

Amazon Elastic Container Registry (Amazon ECR) est AWS un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable. Amazon ECR prend en charge les référentiels privés dotés d'autorisations basées sur les ressources à l'aide d'IAM. AWS Cela permet aux utilisateurs spécifiés ou aux instances Amazon EC2 de pouvoir accéder à vos référentiels et à vos images de conteneurs. Vous pouvez utiliser votre CLI préférée pour pousser, extraire et gérer des images Docker, des images OCI (Open Container Initiative) et des artefacts compatibles OCI.

> **Note**
>
> Amazon ECR prend également en charge les référentiels d'images de conteneurs publics. Pour en savoir plus, consultez Qu'est-ce qu'Amazon ECR public dans le guide de l'utilisateur Amazon ECR Public.

L'équipe des services de AWS conteneurs tient à jour une feuille de route publique sur GitHub. Il contient des informations sur le travail des équipes et permet à tous les AWS clients de donner leur avis directement. Pour en savoir plus, consultez Feuille de route des conteneurs AWS.

Composants d'Amazon ECR

Amazon ECR se compose des éléments suivants :

Registre

Un registre privé Amazon ECR est fourni à chaque AWS compte ; vous pouvez créer un ou plusieurs référentiels dans votre registre et y stocker des images Docker, des images Open Container Initiative (OCI) et des artefacts compatibles OCI. Pour plus d'informations, consultez Registre privé Amazon ECR.

Jeton d'autorisation

Votre client doit s'authentifier auprès d'un registre privé Amazon ECR en tant qu'utilisateur AWS avant de pouvoir transmettre et extraire des images. Pour plus d'informations, consultez Authentification du registre privé dans Amazon ECR.

Référentiel.

Un référentiel Amazon ECR contient vos images Docker, des images Open Container Initiative (OCI) et des artefacts compatibles OCI. Pour plus d'informations, consultez Référentiels privés Amazon ECR.

Politique du référentiel

Vous pouvez contrôler l'accès à vos référentiels et à leur contenu grâce aux politiques de référentiel. Pour plus d'informations, consultez Politiques relatives aux référentiels privés dans Amazon ECR.

Image

Vous pouvez transmettre et extraire des images de conteneur à vos référentiels. Vous pouvez utiliser ces images localement sur votre système de développement ou les utiliser dans des définitions de tâche Amazon ECS et des spécifications de pod d'Amazon EKS. Pour en savoir plus, consultez Utiliser des images Amazon ECR avec Amazon ECS et Utiliser des images Amazon ECR avec Amazon EKS.

Fonctions d'Amazon ECR

Amazon ECR offre les fonctions suivantes :

- Les politiques de cycle de vie aident à gérer le cycle de vie des images dans vos référentiels. Vous définissez des règles qui entraînent le nettoyage des images inutilisées. Vous pouvez tester les règles avant de les appliquer à votre référentiel. Pour plus d'informations, consultez Automatisez le nettoyage des images en utilisant les politiques de cycle de vie d'Amazon ECR.
- La numérisation des images permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. Chaque référentiel peut être configuré pour numérisation sur poussée. Cela garantit que chaque nouvelle image poussée vers le référentiel est numérisée. Vous pouvez ensuite récupérer les résultats de la numérisation d'image. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités logicielles dans Amazon ECR.
- La réplication inter-régions et inter-comptes vous permet d'avoir plus facilement vos images là où vous en avez besoin. Elle est configurée en tant que paramètre de registre et en fonction de la région. Pour plus d'informations, consultez Paramètres du registre privé dans Amazon ECR.
- Les règles de mise en cache par extraction permettent de mettre en cache les référentiels dans un registre en amont de votre registre privé Amazon ECR. En utilisant une règle de mise en cache par extraction, Amazon ECR contactera périodiquement le registre en amont pour s'assurer que

l'image mise en cache dans votre registre privé Amazon ECR est à jour. Pour plus d'informations, consultez Synchroniser un registre en amont avec un registre privé Amazon ECR.

Comment démarrer avec Amazon ECR

Si vous utilisez Amazon Elastic Container Service (Amazon ECS) ou Amazon Elastic Kubernetes Service (Amazon EKS), notez que la configuration de ces deux services est similaire à celle d'Amazon ECR, car Amazon ECR est une extension des deux services.

Lorsque vous utilisez le AWS Command Line Interface avec Amazon ECR, utilisez une version du AWS CLI qui prend en charge les dernières fonctionnalités d'Amazon ECR. Si aucune fonctionnalité Amazon ECR n'est prise en charge dans le AWS CLI, passez à la dernière version du AWS CLI. Pour plus d'informations sur l'installation de la dernière version du AWS CLI, voir Installer ou mettre à jour vers la dernière version du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour savoir comment transférer une image de conteneur vers un référentiel Amazon ECR privé à l'aide de Docker AWS CLI et, consultez. Déplacement d'une image tout au long de son cycle de vie dans Amazon ECR

Tarification pour Amazon ECR

Avec Amazon ECR, vous payez uniquement pour la quantité de données que vous stockez dans vos référentiels et pour le transfert de données à partir de vos images poussées et tirées. Pour en savoir plus, consultez Tarification Amazon ECR.

Déplacement d'une image tout au long de son cycle de vie dans Amazon ECR

Si vous utilisez Amazon ECR pour la première fois, suivez les étapes suivantes avec la CLI Docker et AWS CLI pour créer un exemple d'image, vous authentifier auprès du registre par défaut et créer un référentiel privé. Transférez ensuite une image vers le dépôt privé et extrayez-la de celui-ci. Lorsque vous avez terminé avec l'exemple d'image, supprimez-le et le référentiel.

Pour utiliser le AWS Management Console au lieu du AWS CLI, voirthe section called "Création d'un référentiel pour stocker des images".

Pour plus d'informations sur les autres outils disponibles pour gérer vos AWS ressources, notamment les différents AWS SDK, boîtes à outils IDE et outils de ligne de PowerShell commande Windows, consultez http://aws.amazon.com/tools/.

Prérequis

Si la dernière version AWS CLI de Docker n'est pas installée et prête à être utilisée, procédez comme suit pour installer ces deux outils.

Installez le AWS CLI

Pour l'utiliser AWS CLI avec Amazon ECR, installez la dernière AWS CLI version. Pour plus d'informations, consultez Installation de la AWS Command Line Interface dans le Guide de l'utilisateur de la AWS Command Line Interface .

Installer Docker

Docker est disponible sur plusieurs systèmes d'exploitation, notamment les distributions Linux les plus modernes, comme Ubuntu et même MacOS et Windows. Pour en savoir plus sur la façon d'installer Docker sur votre système d'exploitation, consultez le guide d'installation Docker.

Vous n'avez pas besoin d'un système de développement local pour utiliser Docker. Si vous utilisez déjà Amazon EC2, vous pouvez lancer une instance Amazon Linux 2023 et installer Docker pour démarrer.

Si vous avez déjà installé Docker, passez à Étape 1 : Créer une image Docker.

Pour installer Docker sur une instance Amazon EC2 à l'aide d'une AMI Amazon Linux 2023

1. Lancez une instance avec la dernière AMI Amazon Linux 2023. Pour plus d'informations, consultez la section Lancement d'une instance dans le guide de l'utilisateur Amazon EC2.
2. Connectez-vous à votre instance. Pour plus d'informations, consultez Connect to your Linux instance dans le guide de l'utilisateur Amazon EC2.
3. Mettez à jour les packages installés et le cache du package sur votre instance.

```
sudo yum update -y
```

4. Installez le package de Docker Community Edition le plus récent.

```
sudo yum install docker
```

5. Lancez le service Docker.

```
sudo service docker start
```

6. Ajoutez le `ec2-user` au groupe `docker` afin de pouvoir exécuter les commandes Docker sans utiliser le `sudo`.

```
sudo usermod -a -G docker ec2-user
```

7. Déconnectez-vous et reconnectez-vous pour récupérer les nouvelles autorisations de groupe `docker`. Vous pouvez effectuer ces opérations en fermant votre fenêtre de terminal SSH actuelle et en vous reconnectant à votre instance dans une nouvelle fenêtre. Votre nouvelle session SSH disposera des autorisations de groupe `docker` appropriées.
8. Vérifiez que `ec2-user` peut exécuter les commandes Docker sans `sudo`.

```
docker info
```

> **Note**
>
> Dans certains cas, vous devrez peut-être redémarrer votre instance pour autoriser `ec2-user` à accéder au démon Docker. Essayez de redémarrer l'instance si vous voyez l'erreur suivante :

```
Cannot connect to the Docker daemon. Is the docker daemon running on this
 host?
```

Étape 1 : Créer une image Docker

Au cours de cette étape, vous créez une image Docker pour une application web simple et vous la testez sur votre système local ou l'instance Amazon EC2.

Créer une image Docker d'une application web simple

1. Créez un fichier, appelé `Dockerfile`. Un fichier Dockerfile est un manifeste qui décrit l'image de base à utiliser pour votre image Docker et ce que vous voulez installer et exécuter dessus. Pour en savoir plus sur les fichiers Dockerfile, consultez la référence Dockerfile.

   ```
   touch Dockerfile
   ```

2. Modifiez le `Dockerfile` que vous venez de créer et ajoutez le contenu qui suit.

   ```
   FROM public.ecr.aws/amazonlinux/amazonlinux:latest

   # Install dependencies
   RUN yum update -y && \
    yum install -y httpd

   # Install apache and write hello world message
   RUN echo 'Hello World!' > /var/www/html/index.html

   # Configure apache
   RUN echo 'mkdir -p /var/run/httpd' >> /root/run_apache.sh && \
    echo 'mkdir -p /var/lock/httpd' >> /root/run_apache.sh && \
    echo '/usr/sbin/httpd -D FOREGROUND' >> /root/run_apache.sh && \
    chmod 755 /root/run_apache.sh

   EXPOSE 80

   CMD /root/run_apache.sh
   ```

Ce fichier Dockerfile utilise l'image publique Amazon Linux 2 hébergée sur Amazon ECR Public. Les instructions RUN mettent à jour les caches du package, installent certains packages logiciels pour le serveur web et écrivent ensuite le message « Hello World! » contenu à la racine du document des serveurs Web. L'instruction EXPOSE expose le port 80 sur le conteneur et l'instruction CMD démarre le serveur Web.

3. Créez l'image Docker à partir de votre fichier Dockerfile.

> **Note**
>
> Certaines versions de Docker exigent le chemin d'accès complet à votre Dockerfile dans la commande suivante au lieu du chemin d'accès relatif indiqué ci-après.

```
docker build -t hello-world .
```

4. Répertoriez l'image de votre conteneur.

```
docker images --filter reference=hello-world
```

Sortie :

```
REPOSITORY          TAG                 IMAGE ID            CREATED
 SIZE
hello-world         latest              e9ffedc8c286        4 minutes ago
 194MB
```

5. Exécutez la nouvelle image. L'option `-p 80:80` mappe le port exposé 80 du conteneur au port 80 du système hôte. Pour en savoir plus sur docker run, accédez à Docker run reference.

```
docker run -t -i -p 80:80 hello-world
```

> **Note**
>
> La sortie du serveur Web Apache est affichée dans la fenêtre du terminal. Vous pouvez ignorer le message « `Could not reliably determine the fully qualified domain name` ».

6. Ouvrez un navigateur et pointez vers le serveur qui exécute Docker et qui héberge votre conteneur.

   - Si vous utilisez une instance EC2, il s'agit de la valeur de DNS public du serveur, c'est-à-dire la même adresse que celle que vous utilisez pour vous connecter à l'instance avec le protocole SSH. Assurez-vous que le groupe de sécurité de votre instance autorise le trafic entrant sur le port 80.
   - Si vous exécutez Docker localement, pointez votre navigateur vers http://localhost/.
   - Si vous l'utilisez docker-machine sur un ordinateur Windows ou Mac, recherchez l'adresse IP de la VirtualBox machine virtuelle hébergeant Docker à l'aide de la docker-machine ip commande, en remplaçant *machine-name par le nom* de la machine docker que vous utilisez.

     ```
     docker-machine ip machine-name
     ```

   Vous devriez voir une page web avec « Hello, World! » .
7. Arrêtez le conteneur Docker en appuyant sur Ctrl + c.

Étape 2 : Vous authentifier auprès de votre registre par défaut

Après avoir installé et configuré le AWS CLI, authentifiez la CLI Docker dans votre registre par défaut. Ainsi, la commande docker peut pousser et extraire des images avec Amazon ECR. AWS CLI Fournit une get-login-password commande pour simplifier le processus d'authentification.

Pour authentifier Docker auprès d'un registre Amazon ECR avec get-login-password, exécutez la commande. aws ecr get-login-password Lorsque vous passez le jeton d'authentification à la commande docker login, utilisez la valeur `AWS` pour le nom d'utilisateur et spécifiez l'URI de registre Amazon ECR auquel vous souhaitez vous authentifier. Si vous vous authentifiez sur plusieurs registres, vous devrez répéter la commande pour chacun d'eux.

> **Important**
>
> Si vous recevez une erreur, installez la dernière version de la CLI ou effectuez une mise à niveau vers cette version AWS CLI. Pour en savoir plus, consultez Installer la AWS Command Line Interface dans le guide de l'utilisateur AWS Command Line Interface .

- get-login-password (AWS CLI)

```
aws ecr get-login-password --region region | docker login --username AWS --password-
stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

- Obtenez ECR (LoginCommand)AWS Tools for Windows PowerShell

```
(Get-ECRLoginCommand).Password | docker login --username AWS --password-
stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

Étape 3 : Créer un référentiel

Maintenant que vous disposez d'une image à transmettre à Amazon ECR, vous devez créer un référentiel afin de la contenir. Dans cet exemple, vous créez un référentiel nommé `hello-repository` dans lequel vous pourrez transmettre l'image `hello-world:latest`. Pour créer un référentiel, exécutez la commande suivante :

```
aws ecr create-repository \
    --repository-name hello-repository \
    --region region
```

Étape 4 : Transmettre une image à Amazon ECR

Vous pouvez maintenant transmettre l'image au référentiel Amazon ECR que vous avez créé à la section précédente. Utilisez la docker CLI pour envoyer des images une fois que les conditions préalables suivantes sont remplies :

- La version minimale de docker est installée : 1.7.
- Le jeton d'autorisation Amazon ECR a été configuré avecdocker login.
- Le référentiel Amazon ECR existe et l'utilisateur dispose d'un accès lui permettant de transmettre des images dans le référentiel.

Une fois ces conditions remplies, vous pouvez transmettre l'image au référentiel qui vient d'être créé dans le registre par défaut de votre compte.

Étiqueter et transmettre une image à Amazon ECR

1. Répertoriez les images que vous avez stockées localement afin d'identifier l'image à étiqueter et à transmettre.

   ```
   docker images
   ```

   Sortie :

   ```
   REPOSITORY          TAG                 IMAGE ID            CREATED
    VIRTUAL SIZE
   hello-world         latest              e9ffedc8c286        4 minutes ago
    241MB
   ```

2. Étiquetez l'image à transmettre à votre référentiel.

   ```
   docker tag hello-world:latest aws_account_id.dkr.ecr.region.amazonaws.com/hello-
   repository
   ```

3. Transmettez l'image.

   ```
   docker push aws_account_id.dkr.ecr.region.amazonaws.com/hello-repository
   ```

   Sortie :

   ```
   The push refers to a repository [aws_account_id.dkr.ecr.region.amazonaws.com/hello-
   repository] (len: 1)
   e9ae3c220b23: Pushed
   a6785352b25c: Pushed
   0998bf8fb9e9: Pushed
   0a85502c06c9: Pushed
   latest: digest: sha256:215d7e4121b30157d8839e81c4e0912606fca105775bb0636EXAMPLE
    size: 6774
   ```

Étape 5 : Extraire une image d'Amazon ECR

Une fois que votre image a été transférée vers votre référentiel Amazon ECR, vous pouvez l'extraire d'autres emplacements. Utilisez la docker CLI pour extraire des images une fois que les conditions préalables suivantes sont remplies :

- La version minimale de docker est installée : 1.7.
- Le jeton d'autorisation Amazon ECR a été configuré avecdocker login.
- Le référentiel Amazon ECR existe et l'utilisateur dispose d'un accès lui permettant d'extraire des images du référentiel.

Une fois ces conditions remplies, vous pouvez extraire l'image. Pour extraire votre exemple d'image d'Amazon ECR, exécutez la commande suivante :

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/hello-repository:latest
```

Sortie :

```
latest: Pulling from hello-repository
0a85502c06c9: Pull complete
0998bf8fb9e9: Pull complete
a6785352b25c: Pull complete
e9ae3c220b23: Pull complete
Digest: sha256:215d7e4121b30157d8839e81c4e0912606fca105775bb0636EXAMPLE
Status: Downloaded newer image for aws_account_id.dkr.region.amazonaws.com/hello-
repository:latest
```

Étape 6 : Supprimer une image

Si vous n'avez plus besoin d'une image dans l'un de vos référentiels, vous pouvez la supprimer. Pour supprimer une image, spécifiez le référentiel dans lequel elle se trouve et une `imageDigest` valeur `imageTag` ou pour l'image. L'exemple suivant supprime une image du `hello-repository` référentiel avec la balise `latest` image. Pour supprimer votre exemple d'image du référentiel, exécutez la commande suivante :

```
aws ecr batch-delete-image \
      --repository-name hello-repository \
      --image-ids imageTag=latest \
      --region region
```

Étape 7 : Supprimer un référentiel

Si vous n'avez plus besoin d'un référentiel complet d'images, vous pouvez le supprimer. L'exemple suivant utilise l'`--force`indicateur pour supprimer un référentiel contenant des images. Pour supprimer un référentiel et toutes les images qu'il contient, exécutez la commande suivante :

```
aws ecr delete-repository \
      --repository-name hello-repository \
      --force \
      --region region
```

Optimisation des performances pour Amazon ECR

Vous pouvez utiliser les recommandations suivantes concernant les paramètres et les stratégies pour optimiser les performances lorsque vous utilisez Amazon ECR.

Utiliser Docker 1.10 et des versions ultérieures afin de bénéficier des chargements de couches simultanés

Les images Docker sont composées de couches qui constituent des étapes de création intermédiaires de l'image. Chaque ligne d'un fichier Docker crée un nouvelle couche. Lorsque vous utilisez Docker 1.10 et les versions ultérieures, Docker transmet par défaut autant de couches qu'il y a eu de chargements dans Amazon ECR, ce qui permet d'accélérer les temps de chargement.

Utiliser une image de base plus petite

Les images par défaut disponibles via Docker Hub peuvent contenir de nombreuses dépendances dont votre application n'a pas besoin. Nous vous conseillons d'utiliser une image plus petite créée et gérée par d'autres personnes de la communauté Docker, ou de créer votre propre image de base à l'aide d'une image de Docker réduite au minimum. Pour en savoir plus, consultez Créer une image de base dans la documentation Docker.

Placement des dépendances qui changent le moins plus tôt dans votre fichier Docker

Docker met en cache des couches, ce qui accélère les temps de création. S'il n'y a eu aucun changement sur une couche depuis la dernière création, Docker utilisera la version mise en cache au lieu de récréer la couche. Toutefois, chaque couche est dépendante des couches précédentes. Si une couche change, Docker recompilera non seulement cette couche, mais également toutes les couches ultérieures.

Afin de réduire le temps nécessaire à la recréation d'un fichier Docker et au rechargement des couches, pensez à placer les dépendances qui changent le moins souvent plus tôt dans votre fichier Docker. Placez les dépendances qui changent rapidement (par exemple, le code source de votre application) plus tard dans la pile.

Chaîner des commandes pour éviter le stockage de fichier inutile

Les fichiers intermédiaires créés sur une couche continuent à faire partie de cette couche, même s'ils sont supprimés dans une couche ultérieure. Prenez l'exemple suivant :

```
WORKDIR /tmp
```

```
RUN wget http://example.com/software.tar.gz
RUN wget tar -xvf software.tar.gz
RUN mv software/binary /opt/bin/myapp
RUN rm software.tar.gz
```

Dans cet exemple, les couches créées par la première et la deuxième commande RUN contiennent le fichier .tar.gz d'origine et l'ensemble de son contenu non compressé. Et ce, même si le fichier .tar.gz est supprimé par la quatrième commande RUN. Ces commandes peuvent être regroupées dans une seule instruction RUN afin d'éviter que ces fichiers inutiles fassent partie de l'image Docker finale :

```
WORKDIR /tmp
RUN wget http://example.com/software.tar.gz &&\
    wget tar -xvf software.tar.gz &&\
    mv software/binary /opt/bin/myapp &&\
    rm software.tar.gz
```

Utiliser le point de terminaison régional le plus proche

Vous pouvez réduire la latence d'extraction des images d'Amazon ECR en veillant à utiliser le point de terminaison régional le plus proche de l'emplacement d'exécution de votre application. Si votre application est exécutée sur une instance Amazon EC2, vous pouvez utiliser le code shell suivant afin d'obtenir la région de la zone de disponibilité de l'instance :

```
REGION=$(curl -s http://169.254.169.254/latest/meta-data/placement/availability-zone
 |\
    sed -n 's/\(\d*\)[a-zA-Z]*$/\1/p')
```

La région peut être transmise aux AWS CLI commandes à l'aide du --region paramètre ou définie comme région par défaut pour un profil à l'aide de la aws configure commande. Vous pouvez également définir la région lorsque vous passez des appels à l'aide du AWS SDK. Pour en savoir plus , consultez la documentation du kit SDK correspondant au langage de programmation utilisé.

Registre privé Amazon ECR

Un registre privé Amazon ECR héberge vos images de conteneur dans une architecture hautement disponible et évolutive. Vous pouvez utiliser votre registre pour gérer les référentiels d'images privés composés d'images et d'artefacts Docker et Open Container Initiative (OCI). Chaque compte AWS est fourni avec un registre privé Amazon ECR par défaut. Pour en savoir plus sur les registres publics Amazon ECR, consultez Registres publics dans le guide de l'utilisateur du registre de conteneur Amazon Elastic public.

Concepts de registre privé

- L'URL de votre registre privé par défaut est `https://aws_account_id.dkr.ecr.us-west-2.amazonaws.com`.
- Par défaut, votre compte dispose d'un accès en lecture et en écriture aux référentiels de votre registre privé. Cependant, les utilisateurs ont besoin d'autorisations pour appeler les API Amazon ECR et pour envoyer ou extraire des images vers et depuis vos référentiels privés. Amazon ECR fournit plusieurs politiques gérées pour contrôler l'accès des utilisateurs à différents niveaux. Pour plus d'informations, consultez Exemples de politiques basées sur l'identité du registre de conteneur Amazon Elastic.
- Vous devez authentifier votre client Docker auprès de votre registre privé afin de pouvoir utiliser les commandes docker push et docker pull pour transmettre et extraire les images vers et depuis les référentiels de ce registre. Pour plus d'informations, consultez Authentification du registre privé dans Amazon ECR.
- Les référentiels peuvent être contrôlés à l'aide de politiques d'accès utilisateur et de politiques de référentiel. Pour en savoir plus sur les politiques de référentiel, consultez Politiques relatives aux référentiels privés dans Amazon ECR.
- Les référentiels de votre registre privé peuvent être répliqués entre les régions de votre propre registre privé et entre des comptes distincts en configurant la réplication de votre registre privé. Pour plus d'informations, consultez Réplication d'images privées dans Amazon ECR.

Authentification du registre privé dans Amazon ECR

Vous pouvez utiliser le AWS Management Console AWS CLI, le ou les AWS SDK pour créer et gérer des référentiels privés. Vous pouvez également utiliser ces méthodes pour exécuter certaines actions sur les images, par exemple les répertorier sur une liste ou les supprimer. Ces clients utilisent des

méthodes AWS d'authentification standard. Bien que vous puissiez utiliser l'API Amazon ECR pour transmettre et extraire des images, vous utiliserez probablement plus souvent la CLI Docker ou une bibliothèque Docker propre à un langage.

La CLI Docker ne prend pas en charge les méthodes d'authentification IAM natives. Des étapes supplémentaires sont nécessaires pour qu'Amazon ECR puisse authentifier et autoriser les demandes push et pull de Docker.

Vous trouverez dans les sections suivantes les méthodes d'authentification de registre détaillées.

Utilisation de l'assistant d'informations d'identification Amazon ECR

Amazon ECR propose un assistant d'informations d'identification Docker qui facilite le stockage et l'utilisation des informations d'identification Docker lors de la transmission ou l'extraction d'images vers Amazon ECR. Pour connaître les étapes d'installation et de configuration, consultez Assistant d'informations d'identification Amazon ECR Docker.

> **Note**
>
> L'assistant d'informations d'identification Amazon ECR Docker ne prend pas en charge l'authentification multi-facteur (MFA) actuellement.

Utiliser un jeton d'autorisation

L'étendue d'autorisation d'un jeton d'autorisation correspond à celle du principal IAM utilisé pour récupérer le jeton d'authentification. Un jeton d'authentification est utilisé pour accéder à tout registre Amazon ECR auquel votre principal IAM a accès. Il est valide pendant 12 heures. Pour obtenir un jeton d'autorisation, vous devez utiliser l'opération GetAuthorizationTokenAPI pour récupérer un jeton d'autorisation codé en base64 contenant le nom d'utilisateur `AWS` et un mot de passe codé. La AWS CLI `get-login-password` commande simplifie cela en récupérant et en décodant le jeton d'autorisation que vous pouvez ensuite rediriger vers une docker login commande d'authentification.

Pour authentifier Docker dans un registre privé Amazon ECR avec get-login-password

- Pour authentifier Docker auprès d'un registre Amazon ECR avec get-login-password, exécutez la commande. aws ecr get-login-password Lorsque vous passez le jeton d'authentification à la commande docker login, utilisez la valeur `AWS` pour le nom d'utilisateur et spécifiez l'URI de

registre Amazon ECR auquel vous souhaitez vous authentifier. Si vous vous authentifiez sur plusieurs registres, vous devrez répéter la commande pour chacun d'eux.

> **Important**
>
> Si vous recevez une erreur, installez la dernière version de la CLI ou effectuez une mise à niveau vers cette version AWS CLI. Pour plus d'informations, consultez Installation d' AWS Command Line Interface dans le Guide de l'utilisateur AWS Command Line Interface .

- get-login-password (AWS CLI)

```
aws ecr get-login-password --region region | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

- Obtenez ECR (LoginCommand)AWS Tools for Windows PowerShell

```
(Get-ECRLoginCommand).Password | docker login --username AWS --password-
stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

Utiliser l'authentification API HTTP

Amazon ECR prend en charge l'API HTTP du registre Docker. Cependant, étant donné qu'Amazon ECR est un registre privé, vous devez fournir un jeton d'autorisation avec chaque demande HTTP. Vous pouvez ajouter un en-tête d'autorisation HTTP à l'aide de l'`-H`option for curl et transmettre le jeton d'autorisation fourni par la get-authorization-token AWS CLI commande.

S'authentifier auprès de l'API HTTP Amazon ECR

1. Récupérez un jeton d'autorisation avec le AWS CLI et définissez-le sur une variable d'environnement.

```
TOKEN=$(aws ecr get-authorization-token --output text --query
 'authorizationData[].authorizationToken')
```

2. Pour vous authentifier auprès de l'API, transmettez la variable `$TOKEN` à l'option `-H` de curl. Par exemple, la commande suivante répertorie les étiquettes d'image dans un référentiel Amazon

ECR. Pour en savoir plus, consultez la documentation de la référence API HTTP du registre Docker.

```
curl -i -H "Authorization: Basic $TOKEN"
 https://aws_account_id.dkr.ecr.region.amazonaws.com/v2/amazonlinux/tags/list
```

La sortie est la suivante :

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Date: Thu, 04 Jan 2018 16:06:59 GMT
Docker-Distribution-Api-Version: registry/2.0
Content-Length: 50
Connection: keep-alive

{"name":"amazonlinux","tags":["2017.09","latest"]}
```

Paramètres du registre privé dans Amazon ECR

Amazon ECR utilise des paramètres de registre privés pour configurer les fonctions au niveau du registre. Les paramètres du registre privé sont configurés séparément pour chaque région. Vous pouvez utiliser des paramètres de registre privés pour configurer les fonctions suivantes.

- Autorisations de registre : une politique d'autorisations de registre permet de contrôler la réplication et les autorisations de mise en cache par extraction. Pour plus d'informations, consultez Autorisations de registre privé dans Amazon ECR.
- Règles de mise en cache par extraction : une règle de mise en cache par extraction est utilisée pour mettre en cache les images d'un registre en amont dans votre registre privé Amazon ECR. Pour plus d'informations, consultez Synchroniser un registre en amont avec un registre privé Amazon ECR.
- Configuration de réplication : la configuration de réplication est utilisée pour contrôler si vos référentiels sont copiés dans les régions ou comptes AWS . Pour plus d'informations, consultez Réplication d'images privées dans Amazon ECR.
- Modèles de création de référentiels : un modèle de création de référentiel est utilisé pour définir les paramètres standard à appliquer lorsque de nouveaux référentiels sont créés par Amazon ECR en votre nom. Par exemple, les référentiels créés par une action de mise en cache par extraction.

Pour plus d'informations, consultez Modèles pour contrôler les référentiels créés lors d'une action d'extraction dans le cache.

- Configuration de l'analyse : par défaut, votre registre est activé pour une analyse de base. Vous pouvez activer l'analyse améliorée qui fournit un mode d'analyse automatisé et continu qui recherche les vulnérabilités des packages du système d'exploitation et du langage de programmation. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités logicielles dans Amazon ECR.

Autorisations de registre privé dans Amazon ECR

Amazon ECR utilise une politique de registre pour accorder des autorisations à un principal AWS au niveau du registre privé. Ces autorisations sont utilisées pour étendre l'accès aux fonctions de réplication et de la mise en cache par extraction.

Amazon ECR applique uniquement les autorisations suivantes au niveau du registre privé. Si d'autres actions sont ajoutées à la politique de registre, une erreur se produira.

- `ecr:ReplicateImage` : accorde l'autorisation à un autre compte, appelé registre source, pour répliquer ses images dans votre registre. Ceci est uniquement utilisé pour la réplication entre comptes.
- `ecr:BatchImportUpstreamImage` – Accorde l'autorisation de récupérer l'image externe et de l'importer dans votre registre privé.
- `ecr:CreateRepository` – Accorde l'autorisation de créer un référentiel dans un registre privé. Cette autorisation est requise si le référentiel stockant les images répliquées ou mises en cache n'existe pas déjà dans le registre privé.

> **Note**
>
> Bien qu'il soit possible d'ajouter l'action `ecr:*` à une politique d'autorisation de registre privé, il est considéré comme une bonne pratique de n'ajouter que les actions spécifiques requises pour la fonction que vous utilisez plutôt que d'utiliser un caractère générique.

Rubriques

- Exemples de politiques de registre privé pour Amazon ECR
- Octroi d'autorisations de registre pour la réplication entre comptes dans Amazon ECR

- Octroi d'autorisations de registre pour le cache d'extraction dans Amazon ECR

Exemples de politiques de registre privé pour Amazon ECR

Les exemples suivants illustrent des déclarations de politique que vous pouvez utiliser pour contrôler les autorisations octroyées aux utilisateurs sur votre registre Amazon ECR.

> **Note**
>
> Dans chaque exemple, si l'action `ecr:CreateRepository` est supprimée de votre instruction d'autorisation de registre, la réplication pourra toujours se produire. Toutefois, pour une réplication réussie, vous devez créer des référentiels portant le même nom dans votre compte.

Exemple : Autoriser l'utilisateur racine d'un compte source à répliquer tous les référentiels

La politique d'autorisation de registre suivante permet à l'utilisateur root d'un compte source de répliquer tous les référentiels.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/*"
            ]
        }
    ]
}
```

Exemple : autoriser les utilisateurs root à accéder à plusieurs comptes

La politique d'autorisation de registre suivante comporte deux déclarations. Chaque instruction permet à l'utilisateur root d'un compte source de répliquer tous les référentiels.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/*"
            ]
        },
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/*"
            ]
        }
    ]
}
```

Exemple : Autoriser l'utilisateur racine d'un compte source à répliquer tous les référentiels avec un préfixe **`prod-`**.

La politique d'autorisation de registre suivante permet à l'utilisateur root d'un compte source de répliquer tous les référentiels commençant par. `prod-`

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/prod-*"
            ]
        }
    ]
}
```

Octroi d'autorisations de registre pour la réplication entre comptes dans Amazon ECR

Le type de politique entre comptes est utilisé pour accorder des autorisations à un principal AWS , permettant la réplication des référentiels d'un registre source vers votre registre. Par défaut, vous avez l'autorisation de configurer la réplication inter-régions dans votre propre registre. Vous devez uniquement configurer la politique de registre si vous accordez à un autre compte l'autorisation de répliquer du contenu dans votre registre.

Une politique de registre doit octroyer l'autorisation pour l'action d'API `ecr:ReplicateImage`. Cette API est une API Amazon ECR interne qui peut répliquer des images entre régions ou comptes. Vous pouvez également octroyer l'autorisation pour l'autorisation `ecr:CreateRepository`, qui permet à Amazon ECR de créer des référentiels dans votre registre s'ils n'existent pas déjà. Si l'autorisation `ecr:CreateRepository` n'est pas octroyée, un référentiel portant le même nom que

le référentiel source doit être créé manuellement dans votre registre. Si aucun des deux n'est fait, la réplication échouera. Tout échec CreateRepository ou toute action d' ReplicateImage API apparaît dans CloudTrail.

Pour configurer une politique d'autorisations pour la réplication (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région dans laquelle configurer votre politique de registre.
3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Registry permissions (Autorisations du registre).
4. Dans la page Registry permissions (Autorisations de registre), choisissez Generate statement (Générer une instruction).
5. Effectuez les étapes suivantes pour définir votre déclaration de politique à l'aide du générateur de politique.

   a. Pour Policy type (Type de politique), choisissez Cross account policy (Politique entre comptes).
   b. Pour ID d'instruction, saisissez un ID d'instruction unique. Ce champ est utilisé comme `Sid` dans la politique de registre.
   c. Pour Comptes, saisissez les ID de compte pour chaque compte auquel vous souhaitez octroyer des autorisations. Lorsque vous précisez plusieurs ID de compte, séparez-les par une virgule.
6. Développez l'Aperçu de l'instruction de la politique pour consulter l'instruction de la politique d'autorisations de registre.
7. Après confirmation de la déclaration de politique, choisissez Ajouter à la politique pour enregistrer la politique dans votre registre.

Pour configurer une politique d'autorisations pour la réplication (AWS CLI)

1. Créez un fichier nommé `registry_policy.json` et remplissez-le avec une politique de registre.

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

```
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/*"
            ]
        }
    ]
}
```

2. Créez la politique de registre à l'aide du fichier de politique.

```
aws ecr put-registry-policy \
      --policy-text file://registry_policy.json \
      --region us-west-2
```

3. Récupérez la politique de votre registre pour confirmer.

```
aws ecr get-registry-policy \
      --region us-west-2
```

Octroi d'autorisations de registre pour le cache d'extraction dans Amazon ECR

Les autorisations du registre privé Amazon ECR peuvent être utilisées pour étendre les autorisations des entités IAM individuelles à utiliser la mise en cache par extraction. Si une entité IAM dispose de plus d'autorisations accordées par une politique IAM que celles accordées par la politique d'autorisations de registre, la politique IAM a la priorité.

Pour créer une politique d'autorisations de registre privée (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région dans laquelle vous souhaitez configurer votre instruction d'autorisations de registre privé.

3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Registry permissions (Autorisations du registre).
4. Dans la page Registry permissions (Autorisations de registre), choisissez Generate statement (Générer une instruction).
5. Pour chaque instruction de politique d'autorisations de mise en cache par extraction que vous souhaitez créer, procédez comme suit.

    a. Pour Policy type (Type de politique), choisissez Pull through cache policy (Politique de mise en cache par extraction).
    b. Pour Statement id (ID d'instruction), fournissez un nom pour l'instruction de politique de mise en cache par extraction.
    c. Pour IAM entities (Entités IAM), indiquez les utilisateurs, groupes ou rôles à inclure dans la politique.
    d. Pour Repository namespace (Espace de noms de référentiel), sélectionnez la règle de mise en cache par extraction à laquelle associer la politique.
    e. Pour Repository names (Noms de référentiel), spécifiez le nom de base du référentiel pour lequel appliquer la règle. Par exemple, si vous voulez spécifier le référentiel Amazon Linux sur Amazon ECR Public, le nom du référentiel sera `amazonlinux`.

Référentiels privés Amazon ECR

Un référentiel privé Amazon ECR contient vos images Docker, vos images Open Container Initiative (OCI) et vos artefacts compatibles avec OCI. Vous pouvez créer, surveiller et supprimer des référentiels d'images et définir des autorisations qui contrôlent qui peut y accéder à l'aide des opérations de l'API Amazon ECR ou de la section Référentiels de la console Amazon ECR. Amazon ECR s'intègre également à la CLI Docker, afin que vous puissiez transférer et extraire des images de vos environnements de développement vers vos référentiels.

Rubriques

Concepts de référentiel privé

- Par défaut, votre compte dispose d'un accès en lecture et en écriture aux référentiels de votre registre par défaut (*aws_account_id*.dkr.ecr.*region*.amazonaws.com). Toutefois, les utilisateurs ont besoin d'autorisations spécifiques pour effectuer des appels des API Amazon ECR et pour transmettre ou extraire des images depuis et vers vos référentiels. Amazon ECR fournit plusieurs politiques gérées pour contrôler l'accès des utilisateurs à différents niveaux. Pour plus d'informations, consultez Exemples de politiques basées sur l'identité du registre de conteneur Amazon Elastic.
- Les référentiels peuvent être contrôlés à l'aide de politiques d'accès utilisateur et de politiques de référentiel. Pour plus d'informations, consultez Politiques relatives aux référentiels privés dans Amazon ECR.
- Les noms des référentiels peuvent comporter des espaces de noms, que vous pouvez utiliser pour regrouper des référentiels similaires. Par exemple, si plusieurs équipes utilisent le même registre, l'équipe A pourra utiliser l'espace de noms `team-a`, tandis que l'équipe B ajoutera l'espace de noms `team-b`. En faisant cela, chaque équipe a sa propre image appelée `web-app` avec chaque

image préfacée avec l'espace de noms de l'équipe. Cette configuration permet que ces images de chaque équipe puissent être utilisées simultanément sans interférence. L'image de l'équipe A est `team-a/web-app`, et l'image de l'équipe B est `team-b/web-app`.

- Vos images peuvent être répliquées vers d'autres référentiels dans les régions de votre propre registre et entre les comptes. Pour ce faire, indiquez une configuration de réplication dans les paramètres de votre registre. Pour plus d'informations, consultez Paramètres du registre privé dans Amazon ECR.

Création d'un référentiel privé Amazon ECR pour stocker des images

Créez un référentiel privé Amazon ECR, puis utilisez-le pour stocker les images de vos conteneurs. Suivez les étapes suivantes pour créer un référentiel privé à l'aide de la AWS Management Console. Pour connaître les étapes de création d'un référentiel à l'aide du AWS CLI, voirÉtape 3 : Créer un référentiel.

Créer un référentiel (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région dans laquelle vous souhaitez créer votre référentiel.
3. Sur la page Référentiels, choisissez Dépôts privés, puis sélectionnez Créer un référentiel.
4. Pour Visibility settings (Paramètres de visibilité), vérifiez que Private (Privé) est sélectionné.
5. Pour Nom du référentiel, saisissez un nom unique pour votre référentiel. Le nom du référentiel peut être spécifié seul (par exemple `nginx-web-app`). Alternativement, il peut être précédé par un espace de noms pour regrouper le référentiel dans une catégorie (par exemple `project-a/nginx-web-app`).

> **Note**
>
> Le nom du référentiel peut contenir un maximum de 256 caractères. Le nom doit commencer par une lettre et peut uniquement contenir des lettres minuscules, des chiffres, des traits d'union, des traits de soulignement, des points et des barres obliques. L'utilisation d'un tiret double, d'un trait de soulignement double ou d'une double barre oblique n'est pas prise en charge.

6. Pour Immuabilité des étiquettes, choisissez le paramètre d'immuabilité des étiquettes pour le référentiel. Dans les référentiels configurés avec des étiquettes immuables, les étiquettes d'image ne peuvent pas être écrasées. Pour plus d'informations, consultez Empêcher le remplacement des balises d'image dans Amazon ECR.
7. Pour Numériser lors du transfert, bien que vous puissiez spécifier les paramètres d'analyse au niveau du référentiel pour l'analyse de base, il est recommandé de spécifier la configuration de l'analyse au niveau du registre privé. Spécifiez les paramètres d'analyse dans le registre privé qui vous permettent d'activer l'analyse améliorée ou l'analyse de base, ainsi que de définir des filtres pour spécifier quels référentiels seront analysés. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités logicielles dans Amazon ECR.
8. Pour le chiffrement KMS, choisissez d'activer ou non le chiffrement des images du référentiel à l'aide de AWS Key Management Service. Par défaut, lorsque le chiffrement KMS est activé, Amazon ECR utilise une Clé gérée par AWS (clé KMS) avec l'alias`aws/ecr`. Cette clé est créée dans votre compte la première fois que vous créez un référentiel avec le chiffrement KMS activé. Pour plus d'informations, consultez Chiffrement au repos.
9. Lorsque le chiffrement KMS est activé, sélectionnez Paramètres de chiffrement client (avancés) pour choisir votre propre clé KMS. Les clés KMS doivent être situées dans la même région que le cluster. Choisissez Créer une AWS KMS clé pour accéder à la AWS KMS console afin de créer votre propre clé.
10. Choisissez Créer un référentiel.

Étapes suivantes

Pour afficher les étapes à suivre pour transférer une image vers votre référentiel, sélectionnez le référentiel et choisissez Afficher les commandes push. Pour plus d'informations sur le transfert d'une image vers un référentiel, consultez Transférer une image vers un référentiel privé Amazon ECR.

Afficher le contenu et les détails d'un référentiel privé dans Amazon ECR

Après avoir créé un dépôt privé, vous pouvez consulter les informations le concernant dans AWS Management Console :

- Images stockées dans un référentiel

- Les informations sur chaque image stockée dans le référentiel, y compris la taille et le résumé SHA de chaque image
- La fréquence d'analyse spécifiée pour le contenu du référentiel
- Indique si le référentiel est associé à une règle de cache par extraction active
- Les paramètres de chiffrement pour le référentiel

> **Note**
>
> Depuis la version 1.9 de Docker, le client Docker compresse les couches d'images avant de les transmettre à un registre Docker V2. La sortie de la commande docker images affiche la taille de l'image non compressée. Par conséquent, n'oubliez pas que Docker peut renvoyer une image plus grande que l'image montrée dans la AWS Management Console.

Afficher les informations du référentiel (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région qui contient le référentiel à afficher.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Dans la page Repositories (Référentiels), choisissez l'onglet Private (Privé), puis choisissez le référentiel à afficher.
5. Sur la page des informations sur le référentiel, la console affiche par défaut la vue Images. Utilisez le menu de navigation pour afficher d'autres informations sur le référentiel.
   - Choisissez Summary (Récapitulatif) pour afficher les détails du référentiel et les données de comptage d'extraction du référentiel.
   - Choisissez Images pour afficher les informations relatives aux balises des images du référentiel. Pour afficher des informations supplémentaires sur l'image, sélectionnez la balise de l'image. Pour plus d'informations, consultez Afficher les détails d'une image dans Amazon ECR.

     Si vous souhaitez supprimer des images non étiquetées, vous pouvez cocher la case à gauche des référentiels à supprimer, puis choisir Supprimer. Pour plus d'informations, consultez Supprimer une image dans Amazon ECR.

- Choisissez Autorisations pour afficher les politiques de référentiel qui sont appliquées au référentiel. Pour plus d'informations, consultez Politiques relatives aux référentiels privés dans Amazon ECR.
- Choisissez Politique de cycle de vie pour afficher les règles de politique de cycle de vie qui sont appliquées au référentiel, ainsi que l'historique des événements du cycle de vie. Pour plus d'informations, consultez Automatisez le nettoyage des images en utilisant les politiques de cycle de vie d'Amazon ECR.
- Choisissez Étiquettes pour afficher les étiquettes de métadonnées appliquées au référentiel.

Supprimer un dépôt privé dans Amazon ECR

Si vous n'avez plus besoin d'un référentiel, vous pouvez le supprimer. Lorsque vous supprimez un référentiel dans le AWS Management Console, toutes les images qu'il contient sont également supprimées ; cela ne peut pas être annulé.

> **Important**
>
> Les images des référentiels supprimés sont également supprimées. Vous ne pouvez pas annuler cette opération.

Supprimer un référentiel (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région qui contient le référentiel à supprimer.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Dans la page Repositories (Référentiels), choisissez la page Private (Privé), puis sélectionnez le référentiel à supprimer et choisissez Delete (Supprimer).
5. Dans la fenêtre Supprimer ***`nom_référentiel`***, vérifiez que les référentiels sélectionnés doivent être supprimés, puis choisissez Supprimer.

Politiques relatives aux référentiels privés dans Amazon ECR

Amazon ECR utilise les autorisations basées sur les ressources pour contrôler l'accès aux référentiels. Les autorisations basées sur les ressources vous permettent de spécifier quels

utilisateurs ou rôles ont accès à un référentiel et quelles actions ils peuvent effectuer sur le référentiel. Par défaut, seul le AWS compte qui a créé le référentiel a accès au référentiel. Vous pouvez appliquer une politique de dépôt qui autorise un accès supplémentaire à votre dépôt.

Rubriques

Politiques de référentiel vs politiques IAM

Les politiques de référentiel Amazon ECR constituent un sous-ensemble de politiques IAM spécifiquement limitées et utilisées pour contrôler l'accès aux référentiels Amazon ECR individuels. Les politiques IAM sont généralement utilisées pour appliquer des autorisations pour l'ensemble du service Amazon ECR, mais elles peuvent également être utilisées pour contrôler l'accès à des ressources spécifiques.

Les politiques de référentiel Amazon ECR et les politiques IAM sont utilisées pour déterminer les actions qu'un utilisateur ou un rôle particulier peut effectuer sur un référentiel. Si un utilisateur ou un rôle est autorisé à effectuer une action via une politique de référentiel, mais se voit refuser l'autorisation via une politique IAM (ou inversement), l'action sera refusée. Un utilisateur ou un rôle doit être autorisé à effectuer une action par une politique de référentiel ou par une stratégie IAM, mais pas par les deux, pour que l'action soit autorisée.

> **Important**
>
> Amazon ECR exige que les utilisateurs aient l'autorisation d'effectuer des appels d'API `ecr:GetAuthorizationToken` via une politique IAM avant qu'ils puissent s'authentifier auprès d'un référentiel et transmettre ou extraire des images à partir d'un référentiel Amazon ECR. Amazon ECR fournit plusieurs politiques IAM gérées afin de contrôler l'accès utilisateur à différents niveaux. Pour en savoir plus, consultez Exemples de politiques basées sur l'identité du registre de conteneur Amazon Elastic.

Vous pouvez utiliser l'un ou l'autre de ces types de politique pour contrôler l'accès à vos référentiels, comme illustré dans les exemples suivants.

Cet exemple présente une politique de référentiel Amazon ECR qui autorise un utilisateur spécifique à décrire le référentiel et les images de ce référentiel.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ECRRepositoryPolicy",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::account-id:user/username"},
            "Action": [
                "ecr:DescribeImages",
                "ecr:DescribeRepositories"
            ]
        }
    ]
}
```

Cet exemple présente une politique IAM qui permet d'atteindre le même objectif que ci-dessus en délimitant la politique à un référentiel (spécifié par l'ARN complet du référentiel) à l'aide du paramètre de ressource. Pour en savoir plus sur le format Amazon Resource Name (ARN), consultez Ressources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeRepoImage",
            "Effect": "Allow",
            "Action": [
                "ecr:DescribeImages",
                "ecr:DescribeRepositories"
            ],
            "Resource": ["arn:aws:ecr:region:account-id:repository/repository-name"]
        }
    ]
}
```

Exemples de politiques relatives aux référentiels privés dans Amazon ECR

> **Important**
>
> Les exemples de politique de référentiel présentés sur cette page sont destinés à être appliqués aux référentiels privés Amazon ECR. Ils ne fonctionneront pas correctement s'ils sont utilisés directement avec un principal IAM, sauf s'ils sont modifiés pour spécifier le référentiel Amazon ECR comme ressource. Pour plus d'informations sur les paramètres des politiques de référentiel, consultez Définition d'une déclaration de politique de dépôt privé dans Amazon ECR.

Les politiques de référentiel Amazon ECR constituent un sous-ensemble de politiques IAM spécifiquement limitées et utilisées pour contrôler l'accès aux référentiels Amazon ECR individuels. Les politiques IAM sont généralement utilisées pour appliquer des autorisations pour l'ensemble du service Amazon ECR, mais elles peuvent également être utilisées pour contrôler l'accès à des ressources spécifiques. Pour plus d'informations, consultez Politiques de référentiel vs politiques IAM.

Les exemples de politique de référentiel suivants illustrent des déclarations d'autorisation que vous pouvez utiliser pour contrôler l'accès à vos référentiels privés Amazon ECR.

> **Important**
>
> Amazon ECR exige que les utilisateurs aient l'autorisation d'effectuer des appels d'API `ecr:GetAuthorizationToken` via une politique IAM avant qu'ils puissent s'authentifier auprès d'un référentiel et transmettre ou extraire des images à partir d'un référentiel Amazon ECR. Amazon ECR fournit plusieurs politiques IAM gérées afin de contrôler l'accès utilisateur à différents niveaux. Pour en savoir plus, consultez Exemples de politiques basées sur l'identité du registre de conteneur Amazon Elastic.

Exemple : Autoriser un ou plusieurs utilisateurs

La politique de référentiel suivante autorise un ou plusieurs utilisateurs à transmettre et extraire des images vers et depuis un référentiel.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPushPull",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:user/push-pull-user-1",
                    "arn:aws:iam::account-id:user/push-pull-user-2"
                ]
            },
            "Action": [
                "ecr:BatchGetImage",
                "ecr:BatchCheckLayerAvailability",
                "ecr:CompleteLayerUpload",
                "ecr:GetDownloadUrlForLayer",
                "ecr:InitiateLayerUpload",
                "ecr:PutImage",
                "ecr:UploadLayerPart"
            ]
        }
    ]
}
```

Exemple : autoriser un autre compte

La politique de référentiel suivante autorise un compte spécifique à transmettre des images.

> **Important**
>
> Le compte auquel vous octroyez des autorisations doit avoir activé la région dans laquelle vous créez la politique de référentiel, sinon une erreur se produira.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCrossAccountPush",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
```

```
            },
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:CompleteLayerUpload",
                "ecr:InitiateLayerUpload",
                "ecr:PutImage",
                "ecr:UploadLayerPart"
            ]
        }
    ]
}
```

La politique de référentiel suivante permet aux utilisateurs d'extraire des images (*pull-user-1* et *pull-user-2*) tout en fournissant un accès total à un autre utilisateur (*admin-user*).

> **Note**
>
> Pour les politiques de référentiel plus complexes qui ne sont actuellement pas prises en charge dans le AWS Management Console, vous pouvez appliquer la politique à l'aide de la set-repository-policy AWS CLI commande.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPull",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:user/pull-user-1",
                    "arn:aws:iam::account-id:user/pull-user-2"
                ]
            },
            "Action": [
                "ecr:BatchGetImage",
                "ecr:GetDownloadUrlForLayer"
            ]
        },
        {
            "Sid": "AllowAll",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "arn:aws:iam::account-id:user/admin-user"
            },
            "Action": [
                "ecr:*"
            ]
        }
    ]
}
```

Exemple : Refuser tout

La politique de référentiel suivante permet à tous les utilisateurs de tous les comptes d'extraire des images.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyPull",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "ecr:BatchGetImage",
                "ecr:GetDownloadUrlForLayer"
            ]
        }
    ]
}
```

Exemple : Restriction de l'accès à des adresses IP spécifiques

L'exemple suivant refuse des autorisations à tout utilisateur souhaitant effectuer des opérations Amazon ECR appliquées à un référentiel à partir d'une plage d'adresses spécifique.

La condition dans cette instruction identifie la plage `54.240.143.*` d'adresses Internet Protocol version 4 (IPv4) autorisées.

Le `Condition` bloc utilise les `NotIpAddress` conditions et la clé de `aws:SourceIp` condition, qui est une clé AWS de condition étendue. Pour obtenir plus d'informations sur les clés de condition, consultez la section Clés de contexte de condition globale AWS. Les valeurs IPv4 `aws:sourceIp`

font appel à la notation CIDR standard. Pour en savoir plus, consultez Opérateurs de condition d'adresse IP dans le guide de l'utilisateur IAM.

```
{
    "Version": "2012-10-17",
    "Id": "ECRPolicyId1",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "ecr:*",
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": "54.240.143.0/24"
                }
            }
        }
    ]
}
```

Exemple : autoriser un AWS service

La politique de référentiel suivante autorise l' AWS CodeBuild accès aux actions de l'API Amazon ECR nécessaires à l'intégration avec ce service. Lorsque vous utilisez l'exemple suivant, vous devez utiliser les clés de condition `aws:SourceArn` et `aws:SourceAccount` pour définir quelles ressources peuvent assumer ces autorisations. Pour plus d'informations, consultez l'exemple Amazon ECR CodeBuild dans le guide de l'AWS CodeBuild utilisateur.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"CodeBuildAccess",
         "Effect":"Allow",
         "Principal":{
            "Service":"codebuild.amazonaws.com"
         },
         "Action":[
            "ecr:BatchGetImage",
            "ecr:GetDownloadUrlForLayer"
         ],
```

```
         "Condition":{
            "ArnLike":{
               "aws:SourceArn":"arn:aws:codebuild:region:123456789012:project/project-
name"
            },
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            }
         }
      }
   ]
}
```

Définition d'une déclaration de politique de dépôt privé dans Amazon ECR

Vous pouvez ajouter une déclaration de politique d'accès à un référentiel dans le AWS Management Console en suivant les étapes ci-dessous. Vous pouvez ajouter plusieurs instructions de politique par référentiel. Pour obtenir des exemples de politiques, consultez Exemples de politiques relatives aux référentiels privés dans Amazon ECR.

> **Important**
>
> Amazon ECR exige que les utilisateurs aient l'autorisation d'effectuer des appels d'API `ecr:GetAuthorizationToken` via une politique IAM avant qu'ils puissent s'authentifier auprès d'un référentiel et transmettre ou extraire des images à partir d'un référentiel Amazon ECR. Amazon ECR fournit plusieurs politiques IAM gérées afin de contrôler l'accès utilisateur à différents niveaux. Pour en savoir plus, consultez Exemples de politiques basées sur l'identité du registre de conteneur Amazon Elastic.

Définir une instruction de politique de référentiel

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région qui contient le référentiel pour lequel vous souhaitez définir une instruction de politique.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Dans la page Référentiels, choisissez le référentiel pour lequel vous souhaitez définir une instruction de politique pour afficher le contenu du référentiel.

5. Dans la vue de liste des images du référentiel, dans le panneau de navigation, sélectionnez Autorisations, Modifier.

> **Note**
>
> Si vous ne voyez pas l'option Autorisations dans le panneau de navigation, vérifiez que vous êtes dans la vue de la liste des images du référentiel.

6. Dans la page Modifier des autorisations, choisissez Ajouter une instruction.
7. Pour Nom d'instruction, saisissez un nom pour l'instruction.
8. Pour Effet, choisissez si l'instruction de politique entraînera une autorisation ou un refus explicite.
9. Pour principal, choisissez l'étendue à laquelle s'applique l'instruction de politique. Pour en savoir plus, consultez AWS Éléments de politique JSON : principal dans le guide de l'utilisateur IAM.

   - Vous pouvez appliquer la déclaration à tous les AWS utilisateurs authentifiés en cochant la case Tout le monde (*).
   - Pour principal du service, indiquez le nom du principal du service (par exemple, `ecs.amazonaws.com`) pour appliquer l'instruction à un service particulier.
   - Pour les identifiants de AWS compte, spécifiez un numéro de AWS compte (par exemple,`111122223333`) pour appliquer la déclaration à tous les utilisateurs d'un AWS compte spécifique. Il est possible de préciser plusieurs comptes à l'aide d'une liste séparée par des virgules.

   > **Important**
   >
   > Le compte auquel vous octroyez des autorisations doit avoir activé la région dans laquelle vous créez la politique de référentiel, sinon une erreur se produira.

   - Pour les entités IAM, sélectionnez les rôles ou les utilisateurs de votre AWS compte auxquels appliquer la déclaration.

   > **Note**
   >
   > Pour les politiques de référentiel plus complexes qui ne sont actuellement pas prises en charge dans le AWS Management Console, vous pouvez appliquer la politique à l'aide de la set-repository-policy AWS CLI commande.

10. Pour Actions, choisissez l'étendue des opérations d'API Amazon ECR auxquelles l'instruction de politique doit s'appliquer dans la liste des opérations d'API individuelles.
11. Lorsque vous aurez terminé, choisissez Enregistrer pour définir la politique.
12. Répétez l'étape précédente pour chaque politique de référentiel à ajouter.

Marquage d'un référentiel privé dans Amazon ECR

Pour vous aider à gérer vos référentiels Amazon ECR, vous pouvez attribuer vos propres métadonnées à des référentiels Amazon ECR nouveaux ou existants à l'aide de balises de ressource. AWS Par exemple, vous pouvez définir un ensemble d'identifications pour les référentiels Amazon ECR de votre compte qui vous aide à suivre le propriétaire de chaque référentiel.

Principes de base des étiquettes

Les balises n'ont pas de signification sémantique pour Amazon ECR et sont interprétées strictement comme des chaînes de caractères. Les balises ne sont pas automatiquement affectées à vos ressources. Vous pouvez modifier les clés et valeurs de balise, et vous pouvez retirer des balises d'une ressource à tout moment. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur null. Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur. Si vous supprimez une ressource, ses balises sont également supprimées.

Vous pouvez utiliser des balises à l'aide de la console Amazon ECR, du AWS CLI, et de l'API Amazon ECR.

À l'aide de AWS Identity and Access Management (IAM), vous pouvez contrôler quels utilisateurs de votre AWS compte sont autorisés à créer, modifier ou supprimer des tags. Pour plus d'informations sur les balises dans les politiques IAM, consultezthe section called "Utilisation du contrôle d'accès basé sur les balises".

Identification de vos ressources pour facturation

Les balises que vous ajoutez à vos référentiels Amazon ECR sont utiles lorsque vous examinez l'allocation des coûts après les avoir activés dans votre rapport Coût et utilisation. Pour plus d'informations, consultez Rapports d'utilisation d'Amazon ECR.

Pour voir le coût de vos ressources combinées, vous pouvez organiser vos informations de facturation en fonction des ressources possédant les mêmes valeurs de clé d'étiquette. Par exemple,

vous pouvez étiqueter plusieurs ressources avec un nom d'application spécifique, puis organiser vos informations de facturation pour afficher le coût total de cette application dans plusieurs services. Pour en savoir plus sur la configuration d'un rapport de répartition des coûts avec des étiquettes, consultez Rapport d'allocation des coûts mensuel dans le guide de l'utilisateur AWS Billing .

> **Note**
>
> Si vous venez d'activer la création de rapports, les données du mois en cours peuvent être consultées après 24 heures.

Ajouter des balises à un référentiel privé dans Amazon ECR

Vous pouvez ajouter des balises à un dépôt privé.

Pour plus d'informations sur les noms et les meilleures pratiques relatives aux balises, consultez les sections Limites et exigences en matière de dénomination des balises et Bonnes pratiques du Guide de l'utilisateur AWS des ressources de balisage.

Ajouter des balises à un référentiel (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, sélectionnez la région à utiliser.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Sur la page Référentiels, cochez la case en regard du référentiel que vous voulez baliser.
5. Dans le menu Action, sélectionnez Balises du référentiel.
6. Sur la page Balises du référentiel, sélectionnez Ajouter des balises, Ajouter une balise.
7. Sur la page Modifier les balises du référentiel, spécifiez la clé et la valeur de chaque balise, puis choisissez Enregistrer.

Ajouter des balises à un référentiel (AWS CLI ou à une API)

Vous pouvez ajouter ou remplacer une ou plusieurs balises à l'aide de l'API AWS CLI ou d'une API.

- AWS CLI - tag-ressource
- Action de l'API - TagResource

Les exemples suivants montrent comment ajouter des balises à l'aide du AWS CLI.

Exemple 1 : étiqueter un dépôt

La commande suivante balise un référentiel.

```
aws ecr tag-resource \
     --resource-arn arn:aws:ecr:region:account_id:repository/repository_name \
     --tags Key=stack,Value=dev
```

Exemple 2 : étiqueter un dépôt avec plusieurs balises

La commande suivante ajoute trois balises à un référentiel.

```
aws ecr tag-resource \
     --resource-arn arn:aws:ecr:region:account_id:repository/repository_name \
     --tags Key=key1,Value=value1 Key=key2,Value=value2 Key=key3,Value=value3
```

Exemple 3 : Afficher la liste des balises d'un référentiel

La commande suivante répertorie les balises associées à un référentiel.

```
aws ecr list-tags-for-resource \
     --resource-arn arn:aws:ecr:region:account_id:repository/repository_name
```

Exemple 4 : création d'un référentiel et ajout d'une balise

La commande suivante permet de créer un référentiel nommé `test-repo` et d'ajouter une balise avec la clé `team` et la valeur `devs`.

```
aws ecr create-repository \
     --repository-name test-repo \
     --tags Key=team,Value=devs
```

Supprimer des balises d'un référentiel privé dans Amazon ECR

Vous pouvez supprimer des balises d'un dépôt privé.

Pour supprimer un tag d'un dépôt privé (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.

2. Dans la barre de navigation, sélectionnez la région à utiliser.
3. Sur la page Référentiels, cochez la case en regard du référentiel dont vous voulez supprimer une balise.
4. Dans le menu Action, sélectionnez Balises du référentiel.
5. Sur la page Balises du référentiel, sélectionnez Modifier.
6. Sur la page Modifier les balises du référentiel, sélectionnez Supprimer pour chaque balise que vous voulez supprimer, puis choisissez Enregistrer.

Pour supprimer un tag d'un dépôt privé (AWS CLI)

Vous pouvez supprimer une ou plusieurs balises à l'aide de l'API AWS CLI ou d'une API.

- AWS CLI - untag-resource
- Action de l'API - UntagResource

L'exemple suivant montre comment supprimer une balise d'un référentiel à l'aide du AWS CLI.

```
aws ecr untag-resource \
     --resource-arn arn:aws:ecr:region:account_id:repository/repository_name \
     --tag-keys tag_key
```

Images privées dans Amazon ECR

Amazon ECR stocke les images Docker, les images Open Container Initiative (OCI) et les artefacts compatibles OCI dans des référentiels privés. Vous pouvez utiliser la CLI Docker pour transmettre et extraire les images des référentiels.

Rubriques

Transférer une image vers un référentiel privé Amazon ECR

Vous pouvez transférer vos images Docker, listes manifestes, images OCI (Open Container Initiative) et artefacts compatibles vers vos référentiels privés.

Amazon ECR fournit également un moyen de répliquer vos images dans d'autres référentiels. En spécifiant une configuration de réplication dans les paramètres de votre registre privé, vous pouvez effectuer une réplication entre les régions de votre propre registre et sur différents comptes. Pour plus d'informations, consultez Paramètres du registre privé dans Amazon ECR.

Rubriques

- Transmission d'une image multi-architecture vers un référentiel privé Amazon ECR
- Transférer un graphique de Helm vers un référentiel privé Amazon ECR

Autorisations IAM pour transférer une image vers un référentiel privé Amazon ECR

Les utilisateurs ont besoin d'autorisations IAM pour transférer des images vers les référentiels privés Amazon ECR. Conformément à la meilleure pratique consistant à accorder le moindre privilège, vous pouvez accorder l'accès à un référentiel spécifique. Vous pouvez également accorder l'accès à tous les référentiels.

Un utilisateur doit s'authentifier auprès de chaque registre Amazon ECR auquel il souhaite envoyer des images en demandant un jeton d'autorisation. Amazon ECR fournit plusieurs politiques AWS gérées pour contrôler l'accès des utilisateurs à différents niveaux. Pour plus d'informations, consultez AWS politiques gérées pour Amazon Elastic Container Registry.

Vous pouvez également créer vos propres politiques IAM. La politique IAM suivante accorde les autorisations requises pour transférer une image vers un référentiel spécifique. Le référentiel doit être spécifié en tant qu'Amazon Resource Name (ARN) complet.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:CompleteLayerUpload",
                "ecr:UploadLayerPart",
                "ecr:InitiateLayerUpload",
                "ecr:BatchCheckLayerAvailability",
                "ecr:PutImage"
            ],
            "Resource": "arn:aws:ecr:region:111122223333:repository/repository-name"
        },
        {
            "Effect": "Allow",
            "Action": "ecr:GetAuthorizationToken",
            "Resource": "*"
        }
    ]
```

```
}
```

La politique IAM suivante accorde les autorisations requises pour transférer une image vers tous les référentiels.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:CompleteLayerUpload",
                "ecr:GetAuthorizationToken",
                "ecr:UploadLayerPart",
                "ecr:InitiateLayerUpload",
                "ecr:BatchCheckLayerAvailability",
                "ecr:PutImage"
            ],
            "Resource": "*"
        }
    ]
}
```

Transférer une image Docker vers un référentiel privé Amazon ECR

Vous pouvez envoyer vos images de conteneur vers un référentiel Amazon ECR à l'aide de la commande docker push.

Amazon ECR prend également en charge la création et le transfert de listes de manifestes Docker utilisées pour les images multi-architectures. Pour plus d'informations, veuillez consulter Transmission d'une image multi-architecture vers un référentiel privé Amazon ECR.

Pour transmettre une image Docker à un référentiel Amazon ECR

Le référentiel Amazon ECR doit exister avant que vous poussiez l'image. Pour plus d'informations, consultez the section called "Création d'un référentiel pour stocker des images".

1. Authentifiez le client Docker auprès du registre Amazon ECR dans lequel vous prévoyez de transmettre votre image. Vous devez obtenir des jetons d'authentification pour chaque registre utilisé ; les jetons sont valides pendant 12 heures. Pour plus d'informations, consultez Authentification du registre privé dans Amazon ECR.

Pour authentifier Docker dans un registre Amazon ECR, exécutez la commande aws ecr get-login-password. Lorsque vous passez le jeton d'authentification à la commande docker login, utilisez la valeur `AWS` pour le nom d'utilisateur et spécifiez l'URI de registre Amazon ECR auquel vous souhaitez vous authentifier. Si vous vous authentifiez sur plusieurs registres, vous devrez répéter la commande pour chacun d'eux.

> **Important**
>
> Si vous recevez une erreur, installez la dernière version de la CLI ou effectuez une mise à niveau vers cette version AWS CLI. Pour en savoir plus, consultez Installer la AWS Command Line Interface dans le guide de l'utilisateur AWS Command Line Interface .

```
aws ecr get-login-password --region region | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

2. Si le référentiel d'images n'existe pas dans le registre dans lequel vous souhaitez transmettre l'image, créez-le. Pour plus d'informations, consultez Création d'un référentiel privé Amazon ECR pour stocker des images.
3. Identifiez l'image à transmettre. Exécutez la commande docker images afin d'afficher la liste des images du conteneur du système.

   ```
   docker images
   ```

   Vous pouvez identifier une image avec la valeur *repository:tag* ou l'ID de l'image dans la sortie de commande obtenue.
4. Balisez l'image avec la combinaison registre Amazon ECR, référentiel et nom de balise d'image facultatif à utiliser. Le format du registre est *aws_account_id*.dkr.ecr.*us-west-2*.amazonaws.com. Le nom du référentiel doit correspondre au référentiel que vous avez créé pour l'image. Si vous omettez la balise de l'image, nous supposerons que c'est `latest`.

   L'exemple suivant balise une image locale avec l'ID *e9ae3c220b23* au format *aws_account_id*.dkr.ecr.*us-west-2*.amazonaws.com/my-repository:tag.

   ```
   docker tag e9ae3c220b23 aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-
   repository:tag
   ```

5. Transmettez l'image à l'aide de la commande docker push :

```
docker push aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository:tag
```

6. (Facultatif) Appliquez toute balise supplémentaire à l'image et transmettez ces balises à Amazon ECR en répétant Step 4 et Step 5.

Transmission d'une image multi-architecture vers un référentiel privé Amazon ECR

Vous pouvez transférer des images multi-architectures vers un référentiel Amazon ECR en créant et en diffusant des listes de manifestes Docker. Une liste manifeste est une liste d'images créée en spécifiant un ou plusieurs noms d'image. Dans la plupart des cas, la liste des manifestes est créée à partir d'images ayant la même fonction mais correspondant à des systèmes d'exploitation ou à des architectures différents. La liste manifeste n'est pas obligatoire. Pour en savoir plus, consultez manifeste docker.

Une liste manifeste peut être extraite ou référencée dans une définition de tâche Amazon ECS ou dans une spécification de pod Amazon EKS, comme d'autres images Amazon ECR.

Prérequis

- Dans votre CLI Docker, activez les fonctionnalités expérimentales. Pour plus d'informations sur les fonctionnalités expérimentales, consultez la section Fonctionnalités expérimentales dans la documentation Docker.
- Le référentiel Amazon ECR doit exister avant que vous poussiez l'image. Pour plus d'informations, consultez the section called “Création d'un référentiel pour stocker des images”.
- Les images doivent être transférées vers votre dépôt avant de créer le manifeste Docker. Pour en savoir plus sur la création d'une image, consultez Transférer une image Docker vers un référentiel privé Amazon ECR.

Transmettre une image Docker multi-architecture vers un référentiel Amazon ECR

1. Authentifiez le client Docker auprès du registre Amazon ECR dans lequel vous prévoyez de transmettre votre image. Vous devez obtenir des jetons d'authentification pour chaque registre utilisé ; les jetons sont valides pendant 12 heures. Pour plus d'informations, consultez Authentification du registre privé dans Amazon ECR.

Pour authentifier Docker dans un registre Amazon ECR, exécutez la commande aws ecr get-login-password. Lorsque vous passez le jeton d'authentification à la commande docker login, utilisez la valeur `AWS` pour le nom d'utilisateur et spécifiez l'URI de registre Amazon ECR auquel vous souhaitez vous authentifier. Si vous vous authentifiez sur plusieurs registres, vous devrez répéter la commande pour chacun d'eux.

> **Important**
>
> Si vous recevez une erreur, installez la dernière version de la CLI ou effectuez une mise à niveau vers cette version AWS CLI. Pour en savoir plus, consultez Installer la AWS Command Line Interface dans le guide de l'utilisateur AWS Command Line Interface .

```
aws ecr get-login-password --region region | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

2. Répertoriez les images de votre référentiel, en confirmant les balises d'image.

```
aws ecr describe-images --repository-name my-repository
```

3. Créez la liste manifeste Docker. La commande `manifest create` vérifie que les images référencées se trouvent déjà dans votre référentiel et crée le manifeste localement.

```
docker manifest create aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-
repository aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-
repository:image_one_tag aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-
repository:image_two
```

4. (Facultatif) Vérifiez la liste manifeste Docker. Cela vous permet de confirmer la taille et le résumé de chaque manifeste d'image référencé dans la liste manifeste.

```
docker manifest inspect aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-
repository
```

5. Transmettez la liste manifeste Docker à votre référentiel Amazon ECR.

```
docker manifest push aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository
```

Transférer un graphique de Helm vers un référentiel privé Amazon ECR

Vous pouvez transférer des artefacts de l'Open Container Initiative (OCI) vers un référentiel Amazon ECR. Pour voir un exemple de cette fonctionnalité, suivez les étapes ci-dessous pour transférer un graphique Helm vers Amazon ECR.

Pour plus d'informations sur l'utilisation de vos cartes Helm hébergées par Amazon ECR avec Amazon EKS, consultezInstallation d'un graphique Helm sur un cluster Amazon EKS.

Envoyer les Charts de Helm à un référentiel Amazon ECR

1. Installez la dernière version du Helm client. Ces étapes ont été écrites à l'aide de la version Helm `3.8.2`. Pour en savoir plus, consultez Installation Helm.
2. Pour créer les Charts de Helm de test, effectuez les étapes suivantes. Pour en savoir plus, consultez Documents Helm – Prise en main.

   a. Créer les Charts de Helm nommés `helm-test-chart`, puis effacez le contenu du répertoire `templates`.

   ```
   helm create helm-test-chart
   rm -rf ./helm-test-chart/templates/*
   ```

   b. Créez un ConfigMap dans le `templates` dossier.

   ```
   cd helm-test-chart/templates
   cat <<EOF > configmap.yaml
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: helm-test-chart-configmap
   data:
     myvalue: "Hello World"
   EOF
   ```

3. Empaquetez le graphique. La sortie contiendra le nom de fichier du graphique empaqueté que vous utilisez lorsque vous appuyez sur les Charts de Helm.

   ```
   cd ../..
   helm package helm-test-chart
   ```

   Sortie

```
Successfully packaged chart and saved it to: /Users/username/helm-test-chart-0.1.0.tgz
```

4. Créez un référentiel pour stocker les Charts de Helm. Le nom de votre référentiel doit correspondre au nom que vous avez utilisé lors de la création des Charts de Helm à l'étape 2. Pour plus d'informations, consultez Création d'un référentiel privé Amazon ECR pour stocker des images.

```
aws ecr create-repository \
     --repository-name helm-test-chart \
     --region us-west-2
```

5. Authentifiez votre Helm client auprès du registre Amazon ECR dans lequel vous prévoyez de transmettre l'image. Vous devez obtenir des jetons d'authentification pour chaque registre utilisé ; les jetons sont valides pendant 12 heures. Pour plus d'informations, consultez Authentification du registre privé dans Amazon ECR.

```
aws ecr get-login-password \
     --region us-west-2 | helm registry login \
     --username AWS \
     --password-stdin aws_account_id.dkr.ecr.us-west-2.amazonaws.com
```

6. Poussez les Charts de Helm à l'aide de la commande helm push. La sortie doit inclure l'URI du référentiel Amazon ECR et le résumé SHA.

```
helm push helm-test-chart-0.1.0.tgz oci://aws_account_id.dkr.ecr.us-west-2.amazonaws.com/
```

7. Décrivez les Charts de Helm.

```
aws ecr describe-images \
     --repository-name helm-test-chart \
     --region us-west-2
```

Dans la sortie, vérifiez que le paramètre `artifactMediaType` indique le type d'artefact approprié.

```
{
    "imageDetails": [
```

```
        {
            "registryId": "aws_account_id",
            "repositoryName": "helm-test-chart",
            "imageDigest":
 "sha256:dd8aebdda7df991a0ffe0b3d6c0cf315fd582cd26f9755a347a52adEXAMPLE",
            "imageTags": [
                "0.1.0"
            ],
            "imageSizeInBytes": 1620,
            "imagePushedAt": "2021-09-23T11:39:30-05:00",
            "imageManifestMediaType": "application/vnd.oci.image.manifest.v1+json",
            "artifactMediaType": "application/vnd.cncf.helm.config.v1+json"
        }
    ]
}
```

8. (Facultatif) Pour des étapes supplémentaires, installez l'outil de configuration Helm et commencez avec Amazon EKS. Pour plus d'informations, consultez Installation d'un graphique Helm sur un cluster Amazon EKS.

Signature d'une image stockée dans un référentiel privé Amazon ECR

Amazon ECR s'intègre AWS Signer pour vous permettre de signer les images de vos conteneurs. Vous pouvez stocker à la fois les images de vos conteneurs et les signatures dans vos référentiels privés.

Considérations

Les informations suivantes doivent être prises en compte lors de l'utilisation de la signature d'images Amazon ECR.

- Les signatures stockées dans votre référentiel sont prises en compte dans les quotas de service correspondant au nombre maximum d'images par référentiel. Pour plus d'informations, consultez Service Quotas Amazon ECR..
- Lorsque vous utilisez les stratégies de cycle de vie d'Amazon ECR, toute action provenant d'une règle qui vise à faire expirer ou à supprimer un index d'image OCI entraîne la suppression par Amazon ECR de toutes les signatures référencées par cet index d'image dans les 24 heures.

Prérequis

Avant de commencer, les prérequis suivants doivent être respectés.

- Installez et configurez la version la plus récente de l' AWS CLI. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI (langue française non garantie) dans le Guide de l'utilisateur AWS Command Line Interface .
- Installez la CLI Notation et le AWS Signer plugin pour Notation. Pour plus d'informations, consultez Prérequis pour la signature des images de conteneur (langue française non garantie) dans le Guide du développeur AWS Signer .
- Vous devez avoir une image de conteneur enregistrée dans un référentiel privé Amazon ECR à signer. Pour plus d'informations, consultez Transférer une image vers un référentiel privé Amazon ECR.

Configuration de l'authentification pour le client Notary

Avant de pouvoir créer une signature à l'aide de la CLI Notation, vous devez configurer le client afin qu'il puisse s'authentifier auprès d'Amazon ECR. Si Docker est installé sur le même hôte que le client Notation, ce dernier réutilisera la même méthode d'authentification que celle utilisée pour le client Docker. Les commandes Docker `login` et `logout` permettront aux commandes Notation `sign` et `verify` d'utiliser ces mêmes informations d'identification, sans que vous ayez à authentifier Notation séparément. Pour plus d'informations sur la configuration de votre client Notation pour l'authentification, consultez Authentication avec les registres conformes à l'OCI (français non garanti) dans la documentation du projet Notary

Si vous n'utilisez pas Docker ou un autre outil qui utilise des informations d'identification Docker, nous vous recommandons d'utiliser l'assistant des informations d'identification Amazon ECR Docker comme magasin d'informations d'identification. Pour plus d'informations sur l'installation et la configuration de l'assistant des informations d'identification Amazon ECR Docker, consultez la page Assistant des informations d'identification Amazon ECR Docker (français non garanti).

Signature d'une image

Les étapes suivantes peuvent être utilisées pour créer les ressources nécessaires pour signer une image de conteneur et stocker la signature dans un référentiel privé Amazon ECR. Notation signe les images à l'aide du hachage.

Pour signer une image

1. Créez un profil de AWS Signer signature à l'aide de la plateforme de `Notation-OCI-SHA384-ECDSA` signature. Vous pouvez spécifier une période de validité de signature à l'aide du paramètre `--signature-validity-period`. Cette valeur peut être spécifiée à l'aide de `DAYS`, `MONTHS` ou `YEARS`. Si aucune période de validité n'est spécifiée, la valeur par défaut de 135 mois est utilisée.

   ```
   aws signer put-signing-profile --profile-name ecr_signing_profile --platform-id
    Notation-OCI-SHA384-ECDSA
   ```

   > **Note**
   >
   > Le nom du profil de signature ne prend en charge que les caractères alphanumériques et le trait de soulignement (_).

2. Authentifiez le client Notation auprès de votre registre par défaut. L'exemple suivant utilise le AWS CLI pour authentifier la CLI Notation auprès d'un registre privé Amazon ECR.

   ```
   aws ecr get-login-password --region region | notation login --username AWS --
   password-stdin 111122223333.dkr.ecr.region.amazonaws.com
   ```

3. Utilisez l'interface de la ligne de commande Notation pour signer l'image, en spécifiant l'image à l'aide du nom du référentiel et du hachage SHA. Cela crée la signature et l'envoie vers le référentiel privé Amazon ECR dans lequel se trouve l'image qui est en train d'être signée.

   Dans l'exemple suivant, nous signons une image dans le référentiel `curl` avec le hachage SHA `sha256:ca78e5f730f9a789ef8c63bb55275ac12dfb9e8099e6EXAMPLE`.

   ```
   notation
    sign 111122223333.dkr.ecr.region.amazonaws.com/
   curl@sha256:ca78e5f730f9a789ef8c63bb55275ac12dfb9e8099e6EXAMPLE --plugin
    "com.amazonaws.signer.notation.plugin" --id "arn:aws:signer:region:111122223333:/
   signing-profiles/ecrSigningProfileName"
   ```

Étapes suivantes

Après avoir signé l'image de votre conteneur, vous pouvez vérifier la signature localement. Pour obtenir des instructions sur la vérification d'une image, voir Vérifier une image localement après signature dans le Guide du AWS Signer développeur

Supprimer une signature d'un référentiel privé Amazon ECR

Vous pouvez supprimer une signature d'un référentiel privé Amazon ECR. Lorsque vous créez et envoyez une signature à l'aide de la CLI Notation, un index d'image OCI est également créé dans votre référentiel Amazon ECR. L'API Amazon ECR ne prend pas en charge la suppression d'artefacts ou d'images auxquels fait référence un index d'image OCI. Voici donc les options disponibles pour nettoyer ces artefacts.

- (Recommandé) Vous pouvez utiliser la CLI ORAS pour supprimer l'artefact, et ORAS se chargera de mettre à jour ou de supprimer l'index d'image.
- Vous pouvez utiliser l'API ou la console Amazon ECR pour supprimer d'abord l'index d'image OCI, puis l'artefact référencé tel que la signature.

Lorsque vous utilisez le client ORAS pour supprimer des signatures et d'autres artefacts de type référence, ORAS gère l'index d'image OCI. ORAS supprime d'abord la référence à l'artefact de l'index, puis supprime le manifeste. La commande `oras manifest delete` peut être utilisée en faisant référence à l'index de l'artefact de signature.

Pour supprimer une signature à l'aide de l'ORAS CLI

1. Installez et configurez le client ORAS.

   Pour plus d'informations sur l'installation et la configuration du client ORAS, consultez la section Installation dans la documentation ORAS.
2. Pour supprimer une signature à l'aide de la CLI ORAS, exécutez la commande suivante :

```
oras manifest
 delete 111122223333.dkr.ecr.region.amazonaws.com/
repository_name@sha256:ca78e5f730f9a789ef8c63bb55275ac12dfb9e8099e6EXAMPLE
```

Afficher les détails d'une image dans Amazon ECR

Une fois que vous avez transféré une image dans votre dépôt, vous pouvez consulter les informations la concernant. Les détails inclus sont les suivants :

- URI de l'image
- Étiquettes de l'image
- Type de média de l'artefact
- Type de manifeste de l'image
- État de l'analyse
- Taille des images en Mo
- Date de transmission de l'image dans le référentiel
- État de la réplication

Afficher les détails de l'image (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région qui contient le référentiel contenant votre image.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Dans la page Référentiels, choisissez le référentiel à afficher.
5. Dans la page Repositories : ***repository_name***, choisissez l'image dont afficher les détails.

Extraction d'une image vers votre environnement local à partir d'un référentiel privé Amazon ECR

Si vous souhaitez exécuter une image Docker disponible dans Amazon ECR, vous pouvez l'extraire et la transmettre à votre environnement local à l'aide de la commande docker pull. Vous pouvez le faire depuis votre registre par défaut ou depuis un registre associé à un autre AWS compte.

Pour utiliser une image Amazon ECR dans une définition de tâche Amazon ECS, consultez Utiliser des images Amazon ECR avec Amazon ECS.

> **Important**
>
> Amazon ECR exige que les utilisateurs aient l'autorisation d'appeler l'API `ecr:GetAuthorizationToken` via une politique IAM avant qu'ils puissent s'authentifier auprès d'un référentiel et envoyer ou récupérer des images à partir d'un référentiel Amazon ECR. Amazon ECR fournit plusieurs politiques AWS gérées pour contrôler l'accès des utilisateurs à différents niveaux. Pour plus d'informations sur les politiques AWS gérées pour Amazon ECR, consultezAWS politiques gérées pour Amazon Elastic Container Registry.

Pour extraire une image Docker d'un référentiel Amazon ECR

1. Authentifiez votre client Docker auprès du registre Amazon ECR à partir duquel l'image doit être extraite. Vous devez obtenir des jetons d'authentification pour chaque registre utilisé ; les jetons sont valides pendant 12 heures. Pour plus d'informations, consultez Authentification du registre privé dans Amazon ECR.
2. (Facultatif) Identifiez l'image à extraire.
   - Vous pouvez consulter une liste des référentiels dans un registre avec la commande aws ecr describe-repositories :

     ```
     aws ecr describe-repositories
     ```

     L'exemple de registre ci-dessus comporte un référentiel nommé `amazonlinux`.
   - Vous pouvez décrire les images d'un référentiel à l'aide de la commande aws ecr describe-images :

     ```
     aws ecr describe-images --repository-name amazonlinux
     ```

     L'exemple de référentiel ci-dessus comporte une image balisée en tant que `latest` et `2016.09`, avec le hachage d'image `sha256:f1d4ae3f7261a72e98c6ebefe9985cf10a0ea5bd762585a43e0700ed99863807`.
3. Procédez à l'extraction de l'image à l'aide de la commande docker pull. Le format du nom de l'image doit être *registry*/*repository*[:*tag*] pour une extraction par balise ou *registry*/*repository*[@*digest*] pour une extraction par hachage.

   ```
   docker pull aws_account_id.dkr.ecr.us-west-2.amazonaws.com/amazonlinux:latest
   ```

> **Important**
>
> Si vous recevez un *`repository-url`* `not found: does not exist or no pull access` d'erreur, il se peut que vous deviez authentifier votre client Docker auprès d'Amazon ECR. Pour plus d'informations, consultez Authentification du registre privé dans Amazon ECR.

Extraction de l'image du conteneur Amazon Linux

L'image de conteneur Amazon Linux est créée à partir des mêmes composants logiciels que ceux inclus dans l'AMI Amazon Linux. L'image du conteneur Amazon Linux peut être utilisée dans n'importe quel environnement en tant qu'image de base pour les charges de travail Docker. Si vous utilisez l'AMI Amazon Linux pour des applications dans Amazon EC2, vous pouvez conteneuriser vos applications avec l'image du conteneur Amazon Linux.

Vous pouvez utiliser l'image du conteneur Amazon Linux dans votre environnement de développement local, puis pousser votre application à AWS utiliser Amazon ECS. Pour plus d'informations, consultez Utiliser des images Amazon ECR avec Amazon ECS.

L'image de conteneur Amazon Linux est disponible sur Amazon ECR Public et sur Docker Hub. Pour obtenir de l'aide concernant l'image du conteneur Amazon Linux, rendez-vous sur les forums des AWS développeurs.

Pour extraire l'image de conteneur Amazon Linux depuis Amazon ECR Public

1. Authentifiez votre client Docker dans votre registre Amazon Linux Public . Les jetons d'authentification sont valides pendant 12 heures. Pour plus d'informations, consultez Authentification du registre privé dans Amazon ECR.

   > **Note**
   >
   > Les commandes ecr-public sont disponibles dans la AWS CLI à partir de la version `1.18.1.187`, mais nous vous recommandons d'utiliser la dernière version de l' AWS CLI. Pour en savoir plus, consultez Installer la AWS Command Line Interface dans le guide de l'utilisateur AWS Command Line Interface .

```
aws ecr-public get-login-password --region us-east-1 | docker login --username AWS
 --password-stdin public.ecr.aws
```

La sortie est la suivante :

```
Login succeeded
```

2. Procédez à l'extraction de l'image de conteneur Amazon Linux à l'aide de la commande docker pull. Pour afficher l'image du conteneur Amazon Linux dans la galerie publique Amazon ECR, consultez Galerie publique Amazon ECR – amazonlinux.

```
docker pull public.ecr.aws/amazonlinux/amazonlinux:latest
```

3. (Facultatif) Exécutez le conteneur localement.

```
docker run -it public.ecr.aws/amazonlinux/amazonlinux /bin/bash
```

Pour extraire l'image de conteneur Amazon Linux de Docker Hub

1. Procédez à l'extraction de l'image de conteneur Amazon Linux à l'aide de la commande docker pull.

```
docker pull amazonlinux
```

2. (Facultatif) Exécutez le conteneur localement.

```
docker run -it amazonlinux:latest /bin/bash
```

Supprimer une image dans Amazon ECR

Si vous n'avez plus besoin d'une image, vous pouvez la supprimer du référentiel. Si vous n'avez plus besoin d'un référentiel, vous pouvez le supprimer totalement, ainsi que les images qu'il contient. Pour plus d'informations, consultez Supprimer un dépôt privé dans Amazon ECR.

Comme alternative à la suppression manuelle des images, vous pouvez créer des politiques de cycle de vie des référentiels qui permettent un contrôle accru sur la gestion du cycle de vie des images

dans vos référentiels. Les politiques de cycle de vie automatisent ce processus pour vous. Pour plus d'informations, consultez Automatisez le nettoyage des images en utilisant les politiques de cycle de vie d'Amazon ECR.

Supprimer une image (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région qui contient l'image à supprimer.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Dans la page Référentiels, choisissez le référentiel qui contient l'image à supprimer.
5. Dans la page Repositories: ***repository_name***, cochez la case située à gauche de l'image à supprimer, puis choisissez Supprimer.
6. Dans la boîte de dialogue Supprimer image(s), vérifiez que les images sélectionnées sont bien celles qui doivent être supprimées, puis choisissez Supprimer.

Supprimer une image (AWS CLI)

1. Répertoriez les images dans votre référentiel. Les images étiquetées auront à la fois un résumé d'image et une liste d'étiquettes associées. Les images non étiquetées n'auront qu'un résumé d'image.

```
aws ecr list-images \
     --repository-name my-repo
```

2. (Facultatif) Supprimez toutes les étiquettes non souhaitées pour l'image en spécifiant l'étiquette de l'image à supprimer. Lorsque vous aurez supprimé la dernière étiquette de l'image, cette dernière sera supprimée.

```
aws ecr batch-delete-image \
     --repository-name my-repo \
     --image-ids imageTag=tag1 imageTag=tag2
```

3. Supprimez une image étiquetée ou non étiquetée en spécifiant le résumé de l'image. Lorsque vous supprimez une image en référençant son hachage, l'image et toutes ses étiquettes sont supprimées.

```
aws ecr batch-delete-image \
     --repository-name my-repo \
```

```
     --image-ids imageDigest=sha256:4f70ef7a4d29e8c0c302b13e25962d8f7a0bd304EXAMPLE
```

Pour supprimer plusieurs images, vous pouvez spécifier plusieurs étiquettes d'image ou des résumées d'image dans la demande.

```
aws ecr batch-delete-image \
     --repository-name my-repo \
     --image-ids imageDigest=sha256:4f70ef7a4d29e8c0c302b13e25962d8f7a0bd304EXAMPLE
 imageDigest=sha256:f5t0e245ssffc302b13e25962d8f7a0bd304EXAMPLE
```

Modifier le balisage d'une image dans Amazon ECR

Avec les images Docker Image Manifest V2 Schéma 2, vous pouvez utiliser l'option `--image-tag` de la commande put-image pour réétiqueter une image existante. Vous pouvez réétiqueter une image sans la transmettre ni l'extraire avec Docker. Pour les images plus grandes, ce processus permet d'économiser une grande quantité de bande passante réseau et de temps nécessaires au réétiquetage d'une image.

Réétiqueter une image (AWS CLI)

Pour réétiqueter une image à l'aide du AWS CLI

1. Utilisez la commande batch-get-image pour obtenir le manifeste d'image pour l'image à réétiqueter et l'écrire dans un fichier. Dans cet exemple, le manifeste d'une image avec l'identification, *`latest`*, dans le référentiel, *`amazonlinux`*, est écrit dans une variable d'environnement nommée *`MANIFEST`*.

   ```
   MANIFEST=$(aws ecr batch-get-image --repository-name amazonlinux --image-ids
    imageTag=latest --output text --query 'images[].imageManifest')
   ```

2. Utilisez l'option `--image-tag` de la commande put-image afin de placer le manifeste de l'image dans Amazon ECR avec une nouvelle étiquette. Dans cet exemple, l'image est étiquetée sous la forme *`2017.03`*.

> **Note**
>
> Si l'`--image-tag`option n'est pas disponible dans votre version du AWS CLI, passez à la dernière version. Pour en savoir plus, consultez Installer la AWS Command Line Interface dans le guide de l'utilisateur AWS Command Line Interface .

```
aws ecr put-image --repository-name amazonlinux --image-tag 2017.03 --image-manifest "$MANIFEST"
```

3. Vérifiez que la nouvelle étiquette de l'image est attachée à l'image. Dans la sortie ci-dessous, l'image porte les étiquettes `latest` et `2017.03`.

```
aws ecr describe-images --repository-name amazonlinux
```

La sortie est la suivante :

```
{
    "imageDetails": [
        {
            "imageSizeInBytes": 98755613,
            "imageDigest":
 "sha256:8d00af8f076eb15a33019c2a3e7f1f655375681c4e5be157a26EXAMPLE",
            "imageTags": [
                "latest",
                "2017.03"
            ],
            "registryId": "aws_account_id",
            "repositoryName": "amazonlinux",
            "imagePushedAt": 1499287667.0
        }
    ]
}
```

Réétiqueter une image (AWS Tools for Windows PowerShell)

Pour réétiqueter une image à l'aide du AWS Tools for Windows PowerShell

1. Utilisez l'applet de commande Get-ECRImageBatch afin d'obtenir la description de l'image à réétiqueter et l'écrire dans une variable d'environnement. Dans cet exemple, une image portant l'étiquette *latest*, dans le référentiel *amazonlinux*, est écrite dans la variable d'environnement *$Image*.

   > **Note**
   >
   > Si l'applet de commande Get-ECRImageBatch n'est pas disponible sur votre système, consultez Configuration de AWS Tools for Windows PowerShell dans le guide de l'utilisateur AWS Tools for Windows PowerShell .

   ```
   $Image = Get-ECRImageBatch -ImageId @{ imageTag="latest" } -
   RepositoryName amazonlinux
   ```

2. Écrivez le manifeste de l'image dans la variable d'environnement *$Manifest*.

   ```
   $Manifest = $Image.Images[0].ImageManifest
   ```

3. Utilisez l'option `-ImageTag` de l'applet de commande Write-ECRImage afin de placer le manifeste de l'image dans Amazon ECR avec une nouvelle étiquette. Dans cet exemple, l'image est étiquetée sous la forme *2017.09*.

   ```
   Write-ECRImage -RepositoryName amazonlinux -ImageManifest $Manifest -
   ImageTag 2017.09
   ```

4. Vérifiez que la nouvelle étiquette de l'image est attachée à l'image. Dans la sortie ci-dessous, l'image porte les étiquettes `latest` et `2017.09`.

   ```
   Get-ECRImage -RepositoryName amazonlinux
   ```

   La sortie est la suivante :

   ```
   ImageDigest                                                             ImageTag
   -----------                                                             --------
   ```

```
sha256:359b948ea8866817e94765822787cd482279eed0c17bc674a7707f4256d5d497 latest
sha256:359b948ea8866817e94765822787cd482279eed0c17bc674a7707f4256d5d497 2017.09
```

Empêcher le remplacement des balises d'image dans Amazon ECR

Vous pouvez empêcher le remplacement des balises d'image en activant l'immuabilité des balises dans un référentiel. Une fois l'immuabilité des balises activée, l'`ImageTagAlreadyExistsException`erreur est renvoyée si vous envoyez une image avec une balise déjà présente dans le référentiel. L'immuabilité des balises affecte toutes les balises. Vous ne pouvez pas rendre certaines balises immuables alors que d'autres ne le sont pas.

Vous pouvez utiliser les AWS CLI outils AWS Management Console et pour définir la mutabilité des balises d'image pour un nouveau référentiel ou pour un référentiel existant. Pour créer un référentiel à l'aide des étapes de la console, voirCréation d'un référentiel privé Amazon ECR pour stocker des images.

Configuration de la mutabilité des balises d'image ()AWS Management Console

Pour définir la mutabilité des balises d'image

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région qui contient le référentiel à modifier.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Dans la page Repositories (Référentiels), choisissez la page Private (Privé), puis sélectionnez le référentiel à modifier et choisissez Edit (Modifier).
5. Pour Immuabilité des étiquettes, choisissez le paramètre d'immuabilité des étiquettes pour le référentiel. Dans les référentiels configurés avec des étiquettes immuables, les étiquettes d'image ne peuvent pas être écrasées. Pour plus d'informations, consultez Empêcher le remplacement des balises d'image dans Amazon ECR.
6. Pour Image scan settings (Paramètres d'analyse de l'image), bien que vous puissiez spécifier les paramètres d'analyse au niveau du référentiel pour l'analyse de base, il est recommandé de spécifier la configuration de l'analyse au niveau du registre privé. Spécifiez les paramètres d'analyse dans le registre privé qui vous permettent d'activer l'analyse améliorée ou l'analyse de

base, ainsi que de définir des filtres pour spécifier quels référentiels seront analysés. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités logicielles dans Amazon ECR.

7. Pour Encryption settings (Paramètres de chiffrement), il s'agit d'un champ de vue uniquement car les paramètres de chiffrement d'un référentiel ne peuvent pas être modifiés une fois le référentiel créé.
8. Choisissez Enregistrer pour mettre à jour les paramètres du référentiel.

Configuration de la mutabilité des balises d'image ()AWS CLI

Créer un référentiel avec des étiquettes immuables configurées

Utilisez l'une des commandes suivantes pour créer un référentiel d'images avec des étiquettes immuables configurées.

- create-repository (AWS CLI)

```
aws ecr create-repository --repository-name name --image-tag-mutability IMMUTABLE --
region us-east-2
```

- New-ECRRepository (AWS Tools for Windows PowerShell)

```
New-ECRRepository -RepositoryName name -ImageTagMutability IMMUTABLE -Region us-
east-2 -Force
```

Pour mettre à jour les paramètres de mutabilité des balises d'image pour un référentiel

Utilisez l'une des commandes suivantes pour mettre à jour les paramètres d'immuabilité des étiquettes d'image pour un référentiel existant.

- put-image-tag-mutability (AWS CLI)

```
aws ecr put-image-tag-mutability --repository-name name --image-tag-
mutability IMMUTABLE --region us-east-2
```

- Mutabilité Write-ECR () ImageTagAWS Tools for Windows PowerShell

```
Write-ECRImageTagMutability -RepositoryName name -ImageTagMutability IMMUTABLE -
Region us-east-2 -Force
```

Prise en charge du format de manifeste d'image de conteneur dans Amazon ECR

Amazon ECR prend en charge les formats suivants pour manifestes d'images de conteneur :

- Docker Image Manifest V2, Schéma 1 (utilisé avec la version 1.9 de Docker et les versions antérieures)
- Docker Image Manifest V2, Schéma 2 (utilisé avec la version 1.10 de Docker et les versions les plus récentes)
- Spécifications OCI (initiative de conteneur ouvert) (v1.0 et versions ultérieures)

La prise en charge de Docker Image Manifest V2, Schéma 2 offre la fonctionnalité suivante :

- Capacité d'utiliser plusieurs étiquettes par image.
- Prise en charge du stockage des images de conteneur Windows.

Conversion du manifeste d'image Amazon ECR

Lorsque vous procédez à la transmission ou à l'extraction des images vers et depuis Amazon ECR, le client moteur du conteneur (par exemple, Docker) communique avec le registre pour convenir du format de manifeste compris par le client et le registre à utiliser pour l'image.

Lorsque vous transmettez une image à Amazon ECR avec la version de Docker 1.9 ou version antérieure, le format du manifeste d'image est stocké en tant que Docker Image Manifest V2, Schéma 1. Lorsque vous transmettez une image à Amazon ECR avec la version de Docker 1.10 ou version plus récente, le format du manifeste d'image est stocké en tant que Docker Image Manifest V2, Schéma 2.

Lorsque vous procédez à l'extraction d'une image d'Amazon ECR par étiquette, renvoie le format du manifeste d'image stocké dans le référentiel. Le format est renvoyé uniquement si ce format est compris par le client. Si le format du manifeste d'image stocké n'est pas compris par le client,

Amazon ECR le convertit dans un format qui est compris par le client. Par exemple, si un client Docker 1.9 demande un manifeste d'image stocké en tant que Docker Image Manifest V2 Schéma 2, Amazon ECR renvoie le manifeste au format Docker Image Manifest V2 Schéma 1. Le tableau ci-dessous décrit les conversions disponibles prises en charge par Amazon ECR lorsqu'une image est extraite par étiquette :

Schéma demandé par le client	Transmis à ECR en tant que V2, schéma 1	Transmis à ECR en tant que V2, schéma 2	Transmis à ECR en tant qu'OCI
V2, schéma 1	Aucune conversion requise	Conversion à V2, schéma 1	Conversion à V2, schéma 1
V2, schéma 2	Aucune conversio n disponible, le client revient à V2, Schéma 1	Aucune conversion requise	Conversion à V2, schéma 2
OCI	Aucune conversion disponible	Conversion à OCI	Aucune conversion requise

Important

Si vous tirez une image par résumé, il n'y aura pas de conversion disponible. Votre client devra comprendre le format du manifeste d'image stocké dans Amazon ECR. Si vous demandez une image Docker Image Manifest V2, Schéma 2 par hachage sur un client Docker 1.9 ou antérieur, l'extraction de l'image échouera. Pour en savoir plus, consultez Compatibilité de registre dans la documentation Docker.

Dans cet exemple, si vous demandez la même image par étiquette, Amazon ECR convertira le manifeste d'image dans un format que le client pourra comprendre. L'extraction d'image a réussi.

Utiliser des images Amazon ECR avec Amazon ECS

Vous pouvez utiliser vos référentiels Amazon ECR privés pour héberger des images de conteneurs et des artefacts que vos tâches Amazon ECS peuvent extraire. Pour que cela fonctionne, l'agent de

conteneur Amazon ECS ou Fargate doit disposer des autorisations nécessaires pour créer les API `ecr:BatchGetImage`, `ecr:GetDownloadUrlForLayer` et `ecr:GetAuthorizationToken`.

Autorisations IAM requises

Le tableau suivant indique le rôle IAM à utiliser, pour chaque type de lancement, qui fournit les autorisations requises pour que vos tâches puissent être extraites d'un référentiel Amazon ECR privé. Amazon ECS fournit des politiques IAM gérées qui incluent les autorisations requises.

Type de lancement	Rôle IAM	AWS politique IAM gérée
Amazon ECS sur des instances Amazon EC2	Utilisez le rôle IAM de l'instance de conteneur, qui est associé à l'instance Amazon EC2 enregistrée dans votre cluster Amazon ECS. Pour plus d'informations, consultez la section consacrée au Rôle IAM d'instance de conteneur dans le Guide du développeur Amazon Elastic Container Servic	`AmazonEC2ContainerServiceforEC2Role` Pour plus d'informations, consultez AmazonEC2ContainerServiceforEC2Role dans le Guide du développeur Amazon Elastic Container Service
Amazon ECS sur Fargate	Utilisez le rôle IAM d'exécution des tâches auquel vous faites référence dans votre définition de tâche Amazon ECS. Pour de plus amples informations, veuillez consulter Rôle IAM d'exécution de tâche dans le Manuel du développeur Amazon Elastic Container Servic	`AmazonECSTaskExecutionRolePolicy` Pour plus d'informations, consultez AmazonECSTaskExecutionRolePolicy dans le Guide du développeur Amazon Elastic Container Service
Amazon ECS sur les instances externes	Utilisez le rôle IAM de l'instance de conteneur, qui est associé au serveur sur site ou à la machine virtuelle (VM) enregistrée vers votre	`AmazonEC2ContainerServiceforEC2Role` Pour plus d'informations, consultez AmazonEC2

Type de lancement	Rôle IAM	AWS politique IAM gérée
	cluster Amazon ECS. Pour plus d'informations, reportez-vous à la section consacrée au Rôle Amazon ECS d'instance de conteneur dans le Guide du développeur Amazon Elastic Container Servic	ContainerServiceforEC2Role dans le Guide du développeur Amazon Elastic Container Service

Important

Les politiques IAM AWS gérées contiennent des autorisations supplémentaires dont vous n'aurez peut-être pas besoin pour votre utilisation. Dans ce cas, il s'agit des autorisations minimales requises pour extraire des données d'un référentiel Amazon ECR privé.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchGetImage",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetAuthorizationToken"
            ],
            "Resource": "*"
        }
    ]
}
```

Spécifier une image Amazon ECR dans une définition de tâche Amazon ECS

Lorsque vous créez une définition de tâche Amazon ECS, vous pouvez spécifier une image de conteneur hébergée dans un référentiel Amazon ECR privé. Dans la définition de tâches, assurez-vous d'utiliser la dénomination `registry/repository:tag` complète pour vos images

Amazon ECR. Par exemple, *aws_account_id*.dkr.ecr.*region*.amazonaws.com/*my-repository*:*latest*.

L'extrait de définition de tâche suivant montre la syntaxe que vous utiliseriez pour spécifier une image de conteneur hébergée dans Amazon ECR pour votre définition de tâche Amazon ECS.

```
{
    "family": "task-definition-name",
    ...
    "containerDefinitions": [
        {
            "name": "container-name",
            "image": "aws_account_id.dkr.ecr.region.amazonaws.com/my-
repository:latest",
            ...
        }
    ],
    ...
}
```

Utiliser des images Amazon ECR avec Amazon EKS

Vous pouvez utiliser vos images Amazon ECR avec Amazon EKS.

Lorsque vous référencez une image à partir d'Amazon ECR, vous devez utiliser le nom complet `registry/repository:tag` de l'image. Par exemple, *aws_account_id*.dkr.ecr.*region*.amazonaws.com/*my-repository*:*latest*.

Autorisations IAM requises

Si vous avez des charges de travail Amazon EKS hébergées sur des nœuds gérés, des nœuds autogérés AWS Fargate, ou consultez les points suivants :

- Charges de travail Amazon EKS hébergées sur des nœuds gérés ou autogérés : le rôle IAM du nœud de travail Amazon EKS (`NodeInstanceRole`) est requis. Le rôle IAM de composant master Amazon EKS doit contenir les autorisations de politique IAM suivantes pour Amazon ECR.

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

```
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetAuthorizationToken"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Si vous avez utilisé `eksctl` les AWS CloudFormation modèles de Getting Started with Amazon EKS pour créer votre cluster et vos groupes de nœuds de travail, ces autorisations IAM sont appliquées par défaut au rôle IAM de votre nœud de travail.

- Charges de travail Amazon EKS hébergées sur AWS Fargate : utilisez le rôle d'exécution du module Fargate, qui autorise vos pods à extraire des images depuis des référentiels Amazon ECR privés. Pour plus d'informations, consultez Création d'un rôle d'exécution de pod Fargate.

Installation d'un graphique Helm sur un cluster Amazon EKS

Les cartes Helm hébergées dans Amazon ECR peuvent être installées sur vos clusters Amazon EKS.

Prérequis

- Installez la dernière version du Helm client. Ces étapes ont été écrites à l'aide de la version Helm `3.9.0`. Pour en savoir plus, consultez Installation Helm.
- Vous avez au moins une version `1.23.9` ou `2.6.3` du AWS CLI installé sur votre ordinateur. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI.
- Vous avez envoyé les Charts de Helm à votre référentiel Amazon ECR. Pour plus d'informations, consultez Transférer un graphique de Helm vers un référentiel privé Amazon ECR.
- Vous avez configuré le `kubectl` afin qu'il fonctionne avec Amazon EKS. Pour en savoir plus, consultez Créer un `kubeconfig` pour Amazon EKS dans le guide de l'utilisateur Amazon EKS. Si les commandes suivantes aboutissent pour votre cluster, votre configuration est correcte.

```
kubectl get svc
```

Pour installer un graphique Helm sur un cluster Amazon EKS

1. Authentifiez votre client Helm dans le registre Amazon ECR où vos Charts de Helm sont hébergés. Vous devez obtenir des jetons d'authentification pour chaque registre utilisé. Les jetons sont valides pendant 12 heures. Pour plus d'informations, consultez Authentification du registre privé dans Amazon ECR.

   ```
   aws ecr get-login-password \
        --region us-west-2 | helm registry login \
        --username AWS \
        --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
   ```

2. Installez le chart. *helm-test-chart*Remplacez-le par votre dépôt et *0.1.0* par le tag de votre graphique Helm.

   ```
   helm install ecr-chart-demo oci://aws_account_id.dkr.ecr.region.amazonaws.com/helm-test-chart --version 0.1.0
   ```

   La sortie doit être similaire à ceci : .

   ```
   NAME: ecr-chart-demo
   LAST DEPLOYED: Tue May 31 17:38:56 2022
   NAMESPACE: default
   STATUS: deployed
   REVISION: 1
   TEST SUITE: None
   ```

3. Vérifiez l'installation des Charts de Helm.

   ```
   helm list -n default
   ```

   Exemple de sortie :

   ```
   NAME            NAMESPACE       REVISION        UPDATED
        STATUS          CHART                   APP VERSION
   ```

```
ecr-chart-demo  default         1               2022-06-01 15:56:40.128669157 +0000
 UTC deployed        helm-test-chart-0.1.0   1.16.0
```

4. (Facultatif) Consultez les Charts de Helm installés `ConfigMap`.

```
kubectl describe configmap helm-test-chart-configmap
```

5. Lorsque vous aurez terminé, vous pourrez supprimer la version des Charts de Helm de votre cluster.

```
helm uninstall ecr-chart-demo
```

Scannez les images pour détecter les vulnérabilités logicielles dans Amazon ECR

La fonctionnalité de numérisation de base améliorée est disponible dans la version préliminaire d'Amazon ECR et est sujette à modification. Au cours de cette version préliminaire publique, vous ne pouvez utiliser le que AWS Management Console pour opter pour la version de numérisation de base améliorée.

La numérisation d'images Amazon ECR permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. Les types d'analyse suivants sont proposés.

> **Important**
>
> En basculant entre les versions de numérisation améliorée, de numérisation de base et de numérisation de base améliorée, les scans précédemment établis ne seront plus disponibles. Vous devrez à nouveau configurer vos scans. Toutefois, si vous revenez à votre version de numérisation précédente, les scans établis seront disponibles.

- Analyse améliorée – Amazon ECR s'intègre à Amazon Inspector pour fournir une analyse automatisée et continue de vos référentiels. Vos images de conteneur sont analysées à la fois pour les vulnérabilités des systèmes d'exploitation et des packages de langage de programmation. À mesure que de nouvelles vulnérabilités apparaissent, les résultats de l'analyse sont mis à jour et Amazon Inspector émet un événement EventBridge pour vous en informer. La numérisation améliorée fournit les avantages suivants :
  - Vulnérabilités liées aux packages du système d'exploitation et des langages
  - Deux fréquences de numérisation : scan en mode push et scan continu.
- Analyse de base —Amazon ECR propose deux versions de l'analyse de base qui utilisent la base de données Common Vulnerabilities and Exposures (CVEs) : la version GA actuelle qui utilise le projet open source Clair et une version récemment améliorée de la numérisation de base (en version préliminaire) qui utilise notre technologie native. AWS Avec l'analyse de base, vous configurez vos référentiels pour qu'ils soient analysés au moment de l'envoi (push) ou vous pouvez effectuer des analyses manuelles et Amazon ECR fournit une liste des résultats de l'analyse. La numérisation de base fournit les éléments suivants :

- Analyses du système d'exploitation.
- Deux fréquences de numérisation : manuelle et numérisation en mode push.

> **Important**
>
> La nouvelle version de l'analyse de base ne prend pas en charge `imageScanFindingsSummary` et `imageScanStatus` dans l'`DescribeImages`API. Pour les consulter, utilisez l'`DescribeImageScanFindings`API.

Filtres permettant de choisir les référentiels à analyser dans Amazon ECR

Lorsque vous configurez la numérisation d'images pour votre registre privé, vous pouvez utiliser des filtres pour choisir les référentiels à analyser.

Lorsque l'analyse de base est utilisée, vous pouvez spécifier des filtres d'analyse lors du transfert par push pour indiquer quels référentiels sont configurés pour effectuer une analyse d'image lorsque de nouvelles images sont transférées par push. La fréquence d'analyse sera définie sur manuelle pour tous les référentiels qui ne correspondent pas à un filtre d'analyse de base lors du transfert par push, ce qui signifie que pour effectuer une analyse, vous devez la déclencher manuellement.

Lorsque l'analyse améliorée est utilisée, vous pouvez spécifier des filtres distincts pour l'analyse lors du transfert par push et l'analyse continue. L'analyse sera désactivée pour tous les référentiels ne correspondant pas à un filtre d'analyse améliorée. Si vous utilisez l'analyse améliorée et spécifiez des filtres distincts pour l'analyse lors du transfert par push et l'analyse continue et qu'un même référentiel correspond aux critères des deux filtres, Amazon ECR applique le filtre d'analyse continue plutôt que le filtre d'analyse lors du transfert par push pour ce référentiel.

Filtrer les caractères génériques

Lorsqu'un filtre est spécifié, un filtre sans caractère générique correspondra à tous les noms de référentiel qui contiennent le filtre. Un filtre avec un caractère générique (*) correspond à tout nom de référentiel où le caractère générique remplace zéro ou plusieurs caractères dans le nom du référentiel.

Le tableau suivant fournit des exemples où les noms de référentiels sont exprimés sur l'axe horizontal et les exemples de filtres sont spécifiés sur l'axe vertical.

	prod	repo-prod	prod-repo	repo-prod-repo	prodrepo
prod	Oui	Oui	Oui	Oui	Oui
*prod	Oui	Oui	Non	Non	Non
prod*	Oui	Non	Oui	Non	Oui
prod	Oui	Oui	Oui	Oui	Oui
prod*repo	Non	Non	Oui	Non	Oui

Scannez les images pour détecter les vulnérabilités du système d'exploitation et des packages de langage de programmation dans Amazon ECR

L'analyse améliorée d'Amazon ECR est une intégration avec Amazon Inspector qui fournit une analyse de vulnérabilité pour vos images de conteneur. Vos images de conteneur sont analysées à la fois pour les vulnérabilités des systèmes d'exploitation et des packages de langage de programmation. Vous pouvez afficher les résultats de l'analyse directement avec Amazon ECR et avec Amazon Inspector. Pour plus d'informations sur Amazon Inspector, consultez Analyse des images de conteneur avec Amazon Inspector dans le Guide de l'utilisateur Amazon Inspector.

Avec l'analyse améliorée, vous pouvez choisir les référentiels qui sont configurés pour une analyse automatique et continue et ceux qui sont configurés pour une analyse sur demande. Cela se fait en définissant des filtres d'analyse.

Considérations relatives à l'analyse améliorée

Tenez compte des points suivants avant d'activer le scan amélioré Amazon ECR.

- L'utilisation de cette fonctionnalité n'entraîne aucun coût supplémentaire pour Amazon ECR, mais Amazon Inspector facture la numérisation de vos images. Pour plus d'informations, consultez la Tarification d'Amazon Inspector.
- L'analyse améliorée n'est pas prise en charge dans les régions suivantes :

  - Moyen-Orient (EAU) (`me-central-1`)
  - Asie-Pacifique (Hyderabad) (`ap-south-2`)
  - Israël (Tel Aviv) (`il-central-1`)
  - Asie-Pacifique (Melbourne) (`ap-southeast-4`)
  - Europe (Espagne) (`eu-south-2`)
- Amazon Inspector prend en charge l'analyse pour des systèmes d'exploitation spécifiques. Pour obtenir la liste complète, consultez Systèmes d'exploitation pris en charge – Analyse Amazon ECR dans le Guide de l'utilisateur Amazon Inspector.
- Amazon Inspector utilise un rôle IAM lié à un service, qui fournit les autorisations nécessaires pour fournir une analyse améliorée pour vos référentiels. Le rôle IAM lié à un service est créé automatiquement par Amazon Inspector lorsque l'analyse améliorée est activée pour votre registre privé. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon Inspector dans le Guide de l'utilisateur d'Amazon Inspector.
- Lorsque vous activez initialement la numérisation améliorée pour votre registre privé, Amazon Inspector reconnaît uniquement les images envoyées à Amazon ECR au cours des 30 derniers jours, sur la base de l'horodatage des images, ou extraites au cours des 90 derniers jours. Les images plus anciennes auront le statut d'analyse `SCAN_ELIGIBILITY_EXPIRED`. Si vous souhaitez que ces images soient analysées par Amazon Inspector, vous devez les envoyer à nouveau dans votre référentiel.
- Toutes les images transmises à Amazon ECR après l'activation de l'analyse améliorée sont analysées en continu pendant la durée configurée. Par défaut, la durée est Lifetime. Ce paramètre peut être configuré à l'aide de la console Amazon Inspector. Pour plus d'informations, consultez Modification de la durée de numérisation améliorée pour les images dans Amazon Inspector.
- Lorsque l'analyse améliorée est activée pour votre registre privé Amazon ECR, les référentiels correspondant aux filtres d'analyse sont analysés en utilisant uniquement l'analyse améliorée. Tous les référentiels qui ne correspondent pas à un filtre auront une fréquence d'analyse `Off` et ne seront pas analysés. Les analyses manuelles qui utilisent l'analyse améliorée ne sont pas prises en charge. Pour plus d'informations, consultez Filtres permettant de choisir les référentiels à analyser dans Amazon ECR.
- Si vous spécifiez des filtres distincts pour l'analyse lors du transfert par push et l'analyse continue et qu'un même référentiel correspond aux critères des deux filtres, Amazon ECR applique le filtre d'analyse continue plutôt que le filtre d'analyse lors du transfert par push pour ce référentiel.
- Lorsque le scan amélioré est activé, Amazon ECR envoie un événement EventBridge lorsque la fréquence d'analyse d'un référentiel est modifiée. Amazon Inspector émet des événements

EventBridge lorsqu'une numérisation initiale est terminée et lorsqu'un résultat de numérisation d'image est créé, mis à jour ou fermé.

Autorisations IAM requises pour une numérisation améliorée dans Amazon ECR

L'analyse améliorée d'Amazon ECR nécessite un rôle IAM lié à un service Amazon Inspector et le principal IAM qui active et utilise l'analyse améliorée doit avoir les autorisations nécessaires pour appeler les API d'Amazon Inspector nécessaires à l'analyse. Le rôle IAM lié à un service Amazon Inspector est créé automatiquement par Amazon Inspector lorsque l'analyse améliorée est activée pour votre registre privé. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon Inspector dans le Guide de l'utilisateur d'Amazon Inspector.

La politique IAM suivante accorde les autorisations requises pour activer et utiliser l'analyse améliorée. Elle comprend l'autorisation nécessaire à Amazon Inspector pour créer le rôle IAM lié à un service ainsi que les autorisations API d'Amazon Inspector nécessaires pour activer et désactiver l'analyse améliorée et récupérer les résultats de l'analyse.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector2:Enable",
                "inspector2:Disable",
                "inspector2:ListFindings",
                "inspector2:ListAccountPermissions",
                "inspector2:ListCoverage"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "inspector2.amazonaws.com"
```

```
                    ]
                }
            }
        }
    ]
}
```

Configuration de la numérisation améliorée pour les images dans Amazon ECR

Configurez l'analyse améliorée par région pour votre registre privé.

Vérifiez que vous disposez des autorisations IAM appropriées pour configurer le scan amélioré. Pour plus d'informations, veuillez consulter Autorisations IAM requises pour une numérisation améliorée dans Amazon ECR.

AWS Management Console

Pour activer l'analyse améliorée de votre registre privé

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région pour laquelle vous souhaitez définir la configuration d'analyse.
3. Dans le volet de navigation, choisissez Registre privé, Paramètres, Numérisation.
4. Sur la page Scanning configuration (Configuration de l'analyse), pour Scan type (Type d'analyse), choisissez Enhanced scanning (Analyse améliorée).

   Par défaut, lorsque l'option Analyse améliorée est sélectionnée, tous vos référentiels sont analysés en continu.
5. Pour choisir des référentiels spécifiques à analyser en continu, décochez la case Analyser en continu tous les référentiels, puis définissez vos filtres :

   Important

   Les filtres sans caractère générique correspondent à tous les noms de référentiel qui contiennent le filtre. Les filtres avec des caractères génériques (*) correspondent à un nom de référentiel où le caractère générique remplace zéro ou plusieurs

caractères dans le nom du référentiel. Pour voir des exemples illustrant le comportement des filtres, voirthe section called “Filtrer les caractères génériques”.

a. Entrez un filtre basé sur les noms des référentiels, puis choisissez Ajouter un filtre.

b. Décidez quels référentiels numériser lorsqu'une image est envoyée :

- Pour analyser tous les référentiels en mode push, sélectionnez Analyser en mode push tous les référentiels.
- Pour choisir des référentiels spécifiques à analyser en mode push, entrez un filtre basé sur les noms des référentiels, puis choisissez Ajouter un filtre.

6. Choisissez Enregistrer.
7. Répétez ces étapes dans chaque région dans laquelle vous voulez activer l'analyse améliorée.

AWS CLI

Utilisez la AWS CLI commande suivante pour activer l'analyse améliorée de votre registre privé à l'aide du AWS CLI. Vous pouvez spécifier des filtres d'analyse à l'aide de l'objet `rules`.

- put-registry-scanning-configuration (AWS CLI)

  L'exemple suivant active l'analyse améliorée pour votre registre privé. Par défaut, lorsqu'aucun `rules` n'est spécifié, Amazon ECR définit la configuration d'analyse sur une analyse continue pour tous les référentiels.

```
aws ecr put-registry-scanning-configuration \
     --scan-type ENHANCED \
     --region us-east-2
```

  L'exemple suivant active l'analyse améliorée pour votre registre privé et spécifie un filtre d'analyse. Le filtre d'analyse dans l'exemple active l'analyse continue pour tous les référentiels avec `prod` dans leur nom.

```
aws ecr put-registry-scanning-configuration \
     --scan-type ENHANCED \
     --rules '[{"repositoryFilters" : [{"filter":"prod","filterType" :
 "WILDCARD"}],"scanFrequency" : "CONTINUOUS_SCAN"}]' \
```

```
    --region us-east-2
```

L'exemple suivant active l'analyse améliorée pour votre registre privé et spécifie plusieurs filtres d'analyse. Les filtres d'analyse de l'exemple activent l'analyse continue pour tous les référentiels dont le nom contient `prod` et activent l'analyse lors de l'envoi (push) uniquement pour tous les autres référentiels.

```
aws ecr put-registry-scanning-configuration \
    --scan-type ENHANCED \
    --rules '[{"repositoryFilters" : [{"filter":"prod","filterType" :
 "WILDCARD"}],"scanFrequency" : "CONTINUOUS_SCAN"},{"repositoryFilters" :
 [{"filter":"*","filterType" : "WILDCARD"}],"scanFrequency" : "SCAN_ON_PUSH"}]' \
    --region us-west-2
```

Modification de la durée de numérisation améliorée pour les images dans Amazon Inspector

Vous pouvez modifier le nombre de jours pendant lesquels Amazon Inspector scanne en continu les images de vos référentiels privés Amazon ECR. Par défaut, lorsque l'analyse améliorée est activée pour votre registre privé Amazon ECR, le service Amazon Inspector surveille en permanence vos référentiels jusqu'à ce que l'image soit supprimée ou que l'analyse améliorée soit désactivée. La durée pendant laquelle Amazon Inspector analyse vos images peut être modifiée à l'aide des paramètres Amazon Inspector. Les durées d'analyse disponibles sont les suivantes : Durée de vie (par défaut), 180 jours, et 30 jours. Lorsque la durée d'analyse d'un référentiel est écoulée, l'état de l'analyse de `SCAN_ELIGIBILITY_EXPIRED` s'affiche quand vous répertoriez vos vulnérabilités d'analyse. Pour plus d'informations, consultez Modification de la durée de la nouvelle analyse automatisée Amazon ECR dans le Guide de l'utilisateur Amazon Inspector.

Pour modifier le paramètre de durée de l'analyse améliorée

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans la navigation de gauche, développez Settings (Paramètres), puis choisissez General (Général).
3. Sur la page Settings (Paramètres), sous ECR re-scan duration(Durée de la ré-analyse ECR), choisissez un paramètre, puis choisissezSave (Enregistrer).

EventBridge événements envoyés pour une analyse améliorée dans Amazon ECR

Lorsque le scan amélioré est activé, Amazon ECR envoie un événement EventBridge lorsque la fréquence d'analyse d'un référentiel est modifiée. Amazon Inspector envoie des événements EventBridge lorsqu'une numérisation initiale est terminée et lorsqu'un résultat de numérisation d'image est créé, mis à jour ou fermé.

Événement pour un changement de fréquence d'analyse d'un référentiel

Lorsque l'analyse améliorée est activée pour votre registre, l'événement suivant est envoyé par Amazon ECR lorsqu'il y a un changement avec une ressource dont l'analyse améliorée est activée. Cela inclut la création de nouveaux référentiels, la modification de la fréquence d'analyse d'un référentiel ou la création ou la suppression d'images dans des référentiels dont l'analyse améliorée est activée. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités logicielles dans Amazon ECR.

```
{
 "version": "0",
 "id": "0c18352a-a4d4-6853-ef53-0abEXAMPLE",
 "detail-type": "ECR Scan Resource Change",
 "source": "aws.ecr",
 "account": "123456789012",
 "time": "2021-10-14T20:53:46Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {
  "action-type": "SCAN_FREQUENCY_CHANGE",
  "repositories": [{
    "repository-name": "repository-1",
    "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-1",
    "scan-frequency": "SCAN_ON_PUSH",
    "previous-scan-frequency": "MANUAL"
   },
   {
    "repository-name": "repository-2",
    "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-2",
    "scan-frequency": "CONTINUOUS_SCAN",
    "previous-scan-frequency": "SCAN_ON_PUSH"
   },
   {
```

```
    "repository-name": "repository-3",
    "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-3",
    "scan-frequency": "CONTINUOUS_SCAN",
    "previous-scan-frequency": "SCAN_ON_PUSH"
   }
  ],
  "resource-type": "REPOSITORY",
  "scan-type": "ENHANCED"
 }
}
```

Événement pour une analyse initiale d'image (analyse améliorée)

Lorsque l'analyse améliorée est activée pour votre registre, l'événement suivant est envoyé par Amazon Inspector lorsque l'analyse initiale de l'image est terminée. Le paramètre `finding-severity-counts` ne retournera une valeur pour un niveau de gravité que s'il en existe un. Par exemple, si l'image ne contient pas de résultats au niveau `CRITICAL`, aucun nombre critique ne sera renvoyé. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités du système d'exploitation et des packages de langage de programmation dans Amazon ECR.

Modèle d'événement :

```
{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Scan"]
}
```

Exemple de sortie :

```
{
    "version": "0",
    "id": "739c0d3c-4f02-85c7-5a88-94a9EXAMPLE",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2021-12-03T18:03:16Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:ecr:us-east-2:123456789012:repository/amazon/amazon-ecs-sample"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
```

```
        "repository-name": "arn:aws:ecr:us-east-2:123456789012:repository/amazon/
amazon-ecs-sample",
        "finding-severity-counts": {
            "CRITICAL": 7,
            "HIGH": 61,
            "MEDIUM": 62,
            "TOTAL": 158
        },
        "image-digest":
 "sha256:36c7b282abd0186e01419f2e58743e1bf635808231049bbc9d77e5EXAMPLE",
        "image-tags": [
            "latest"
        ]
    }
}
```

Événement pour une mise à jour de découverte d'analyse d'image (analyse améliorée)

Lorsque l'analyse améliorée est activée pour votre registre, l'événement suivant est envoyé par Amazon Inspector lorsque la découverte d'analyse d'image est créée, mise à jour ou fermée. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités du système d'exploitation et des packages de langage de programmation dans Amazon ECR.

Modèle d'événement :

```
{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Finding"]
}
```

Exemple de sortie :

```
{
    "version": "0",
    "id": "42dbea55-45ad-b2b4-87a8-afaEXAMPLE",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2021-12-03T18:02:30Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:ecr:us-east-2:123456789012:repository/amazon/amazon-ecs-sample/
sha256:36c7b282abd0186e01419f2e58743e1bf635808231049bbc9d77eEXAMPLE"
```

```
    ],
    "detail": {
        "awsAccountId": "123456789012",
        "description": "In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT
 logic in packet.c has an integer overflow in a bounds check, enabling an attacker to
 specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted
 SSH server may be able to disclose sensitive information or cause a denial of service
 condition on the client system when a user connects to the server.",
        "findingArn": "arn:aws:inspector2:us-east-2:123456789012:finding/
be674aaddd0f75ac632055EXAMPLE",
        "firstObservedAt": "Dec 3, 2021, 6:02:30 PM",
        "inspectorScore": 6.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "adjustments": [],
                "cvssSource": "REDHAT_CVE",
                "score": 6.5,
                "scoreSource": "REDHAT_CVE",
                "scoringVector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N",
                "version": "3.0"
            }
        },
        "lastObservedAt": "Dec 3, 2021, 6:02:30 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 6.5,
                    "scoringVector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N",
                    "source": "REDHAT_CVE",
                    "version": "3.0"
                },
                {
                    "baseScore": 5.8,
                    "scoringVector": "AV:N/AC:M/Au:N/C:P/I:N/A:P",
                    "source": "NVD",
                    "version": "2.0"
                },
                {
                    "baseScore": 8.1,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
```

```
            "referenceUrls": [
                "https://access.redhat.com/errata/RHSA-2020:3915"
            ],
            "source": "REDHAT_CVE",
            "sourceUrl": "https://access.redhat.com/security/cve/CVE-2019-17498",
            "vendorCreatedAt": "Oct 16, 2019, 12:00:00 AM",
            "vendorSeverity": "Moderate",
            "vulnerabilityId": "CVE-2019-17498",
            "vulnerablePackages": [
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "name": "libssh2",
                    "packageManager": "OS",
                    "release": "12.amzn2.2",
                    "sourceLayerHash":
"sha256:72d97abdfae3b3c933ff41e39779cc72853d7bd9dc1e4800c5294dEXAMPLE",
                    "version": "1.4.3"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "Update all packages in the vulnerable packages section to
their latest versions."
            }
        },
        "resources": [
            {
                "details": {
                    "awsEcrContainerImage": {
                        "architecture": "amd64",
                        "imageHash":
"sha256:36c7b282abd0186e01419f2e58743e1bf635808231049bbc9d77e5EXAMPLE",
                        "imageTags": [
                            "latest"
                        ],
                        "platform": "AMAZON_LINUX_2",
                        "pushedAt": "Dec 3, 2021, 6:02:13 PM",
                        "registry": "123456789012",
                        "repositoryName": "amazon/amazon-ecs-sample"
                    }
                },
```

```
                "id": "arn:aws:ecr:us-east-2:123456789012:repository/amazon/amazon-ecs-
sample/sha256:36c7b282abd0186e01419f2e58743e1bf635808231049bbc9d77EXAMPLE",
                "partition": "N/A",
                "region": "N/A",
                "type": "AWS_ECR_CONTAINER_IMAGE"
            }
        ],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2019-17498 - libssh2",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Dec 3, 2021, 6:02:30 PM"
    }
}
```

Extraction des résultats pour des scans améliorés dans Amazon ECR

Vous pouvez récupérer les résultats de numérisation de la dernière numérisation d'image améliorée terminée, puis ouvrir les résultats dans Amazon Inspector pour obtenir plus de détails. Les vulnérabilités logicielles découvertes sont répertoriées par gravité sur la base de données CVE (Common Vulnerabilities and Exposures).

Pour en savoir plus sur le dépannage de certains problèmes courants lors de la numérisation des images, consultez Résolution des problèmes liés à la numérisation d'images dans Amazon ECR.

AWS Management Console

Suivez les étapes ci-dessous pour récupérer les résultats de numérisation d'images à l'aide de la AWS Management Console.

Pour récupérer les résultats de numérisation d'images

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région où votre référentiel existe.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Dans la page Référentiels, choisissez le référentiel qui contient l'image pour laquelle récupérer les résultats de numérisation.

5. Sur la page Images, sous la colonne Vulnerabilities (Vulnérabilités), sélectionnez See findings (Voir les résultats) pour l'image pour laquelle vous souhaitez récupérer les résultats d'analyse.
6. Pour obtenir plus de détails dans la console Amazon Inspector, choisissez le nom de la vulnérabilité dans la colonne Nom.

AWS CLI

Utilisez la AWS CLI commande suivante pour récupérer les résultats de numérisation d'images à l'aide du AWS CLI. Vous pouvez spécifier une image à l'aide de `imageTag` ou `imageDigest`, qui peuvent être obtenus à l'aide de la commande CLI list-images.

- describe-image-scan-findings (AWS CLI)

  L'exemple suivant utilise une étiquette d'image.

  ```
  aws ecr describe-image-scan-findings \
       --repository-name name \
       --image-id imageTag=tag_name \
       --region us-east-2
  ```

  L'exemple suivant utilise un résumé d'image.

  ```
  aws ecr describe-image-scan-findings \
       --repository-name name \
       --image-id imageDigest=sha256_hash \
       --region us-east-2
  ```

Scannez les images pour détecter les vulnérabilités du système d'exploitation dans Amazon ECR

La fonctionnalité de numérisation de base améliorée est disponible dans la version préliminaire d'Amazon ECR et est sujette à modification. Au cours de cette version préliminaire publique, vous ne pouvez utiliser le que AWS Management Console pour opter pour la version de numérisation de base améliorée.

Amazon ECR propose deux versions de l'analyse de base qui utilisent la base de données Common Vulnerabilities and Exposures (CVE) :

- La version GA actuelle qui utilise le projet open source Clair. Pour plus d'informations sur Clair, voir Clair on GitHub.
- La nouvelle version améliorée de la numérisation de base (en version préliminaire) qui utilise la technologie AWS native.

Amazon ECR utilise la gravité d'un CVE à partir de la source de distribution en amont, si elle est disponible. Dans le cas contraire, le score CVSS (Common Vulnerability Scoring System) est utilisé. Le score CVSS peut être utilisé pour obtenir l'évaluation de gravité de la vulnérabilité NVD. Pour en savoir plus, consultez NVD Vulnerability Gravity Ratings.

Les deux versions d'Amazon ECR Basic Scanning prennent en charge les filtres permettant de spécifier les référentiels à analyser en mode push. Tous les référentiels qui ne correspondent pas à un filtre de numérisation en mode push sont définis sur la fréquence d'analyse manuelle, ce qui signifie que vous devez démarrer l'analyse manuellement. Une image peut être numérisée une fois toutes les 24 heures. Les 24 heures incluent le scan initial sur push, si configuré, et tous les scans manuels.

Vous pouvez récupérer les derniers résultats de numérisation d'image achevée pour chaque image. Lorsqu'une numérisation d'image est terminée, Amazon ECR envoie un événement à Amazon EventBridge. Pour plus d'informations, consultez Événements Amazon ECR et EventBridge.

Support régional pour une numérisation de base améliorée

La version améliorée de la numérisation de base est prise en charge dans les régions suivantes :

- Asie-Pacifique (Hong Kong) (`ap-east-1`)
- Europe (Stockholm) (`eu-north-1`)
- Moyen-Orient (Bahreïn) (`me-south-1`)
- Asie-Pacifique (Mumbai) (`ap-south-1`)
- Europe (Paris) (`eu-west-3`)
- AWS GovCloud (USA Est) (`us-gov-east-1`)
- Afrique (Le Cap) (`af-south-1`)
- Asie-Pacifique (Jakarta) (`ap-southeast-3`)

- Europe (Francfort) (eu-central-1)
- Europe (Irlande) (eu-west-1)
- Amérique du Sud (Sao Paulo) (sa-east-1)
- USA Est (Ohio) (us-east-2)
- AWS GovCloud (US-Ouest) (us-gov-west-1)
- Asie-Pacifique (Tokyo) (ap-northeast-1)
- Asie-Pacifique (Séoul) (ap-northeast-2)
- Asie-Pacifique(Osaka) (ap-northeast-3)
- Europe (Milan) (eu-south-1)
- Europe (Londres) (eu-west-2)
- USA Est (Virginie du Nord) (us-east-1)
- Asie-Pacifique (Singapour) (ap-southeast-1)
- Asie-Pacifique (Sydney) (ap-southeast-2)
- Canada (Centre) (ca-central-1)
- USA Ouest (Californie du Nord) (us-west-1)
- USA Ouest (Oregon) (us-west-2)
- Europe (Zurich) (eu-central-2)

Support du système d'exploitation pour la numérisation de base et la numérisation de base améliorée

Pour des raisons de sécurité et pour garantir une couverture continue, nous vous recommandons de continuer à utiliser les versions prises en charge d'un système d'exploitation. Conformément à la politique du fournisseur, les systèmes d'exploitation abandonnés ne sont plus mis à jour avec des correctifs et, dans de nombreux cas, de nouveaux avis de sécurité ne sont plus publiés à leur sujet. En outre, certains fournisseurs suppriment les alertes de sécurité et les détections existantes de leurs flux lorsqu'un système d'exploitation concerné atteint la fin du support standard. Lorsqu'une distribution perd le support de son fournisseur, Amazon ECR peut ne plus prendre en charge son analyse pour détecter les vulnérabilités. Tous les résultats générés par Amazon ECR concernant un système d'exploitation abandonné doivent être utilisés à titre informatif uniquement. Vous trouverez ci-dessous la liste des systèmes d'exploitation et des versions actuellement pris en charge.

Système d'exploitation	Version
Alpine Linux (Alpine)	3,19
Alpine Linux (Alpine)	3,18
Alpine Linux (Alpine)	3,17
Alpine Linux (Alpine)	3,16
Amazon Linux 2 (AL2)	AL2
Amazon Linux 2023 (AL2023)	AL2023
CentOS Linux (CentOS)	7
Serveur Debian (Bookworm)	12
Serveur Debian (Bullseye)	11
Serveur Debian (Buster)	10
Oracle Linux (Oracle)	9
Oracle Linux (Oracle)	8
Oracle Linux (Oracle)	7
Ubuntu (Lunar)	23,04
Ubuntu (Jammy)	22.04 (LITRES)
Ubuntu (Focal)	20.04 (LITRES)
Ubuntu (Bionic)	18,04 (ESM)
Ubuntu (Xenial)	16,04 (ESM)
Ubuntu (Fidèle)	14,04 (ESM)
Red Hat Enterprise Linux (RHEL)	7

Système d'exploitation	Version
Red Hat Enterprise Linux (RHEL)	8
Red Hat Enterprise Linux (RHEL)	9

Configuration de la numérisation de base améliorée pour les images dans Amazon ECR

Une version améliorée de la numérisation de base d'Amazon ECR est désormais disponible en version préliminaire. La numérisation de base améliorée utilise une technologie AWS native.

Configurez une analyse de base améliorée par région pour votre dépôt privé. Pour obtenir la liste des régions qui prennent en charge l'analyse de base améliorée, reportez-vous à la sectionSupport régional pour une numérisation de base améliorée.

Pour activer l'analyse de base améliorée pour votre registre privé

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région pour laquelle vous souhaitez définir la configuration d'analyse.
3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Scanning (Analyse).
4. Sur la page de configuration de numérisation, pour le type de numérisation, choisissez Numérisation de base améliorée (en aperçu) - nouveau.
5. Par défaut, tous vos référentiels sont configurés pour une analyse manuelle. Vous pouvez éventuellement configurer l'analyse lors de l'envoi (push) en spécifiant des filtres d'analyse lors de l'envoi (push). Vous pouvez définir l'analyse lors de l'envoi (push) pour tous les référentiels ou pour des référentiels individuels. Pour plus d'informations, consultez Filtres permettant de choisir les référentiels à analyser dans Amazon ECR.

Configuration de la numérisation de base pour les images dans Amazon ECR

Par défaut, Amazon ECR active le scan de base pour tous les registres privés. Par conséquent, à moins que vous n'ayez modifié les paramètres de numérisation de votre registre privé, il n'est pas nécessaire d'activer le scan de base. La numérisation de base utilise le projet open source Clair.

Vous pouvez utiliser les étapes suivantes pour définir un ou plusieurs filtres de scan sur push.

Pour activer le scan de base pour votre registre privé

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région pour laquelle vous souhaitez définir la configuration d'analyse.
3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Scanning (Analyse).
4. Dans la page Scanning configuration (Configuration de l'analyse), pour Scan type (Type d'analyse), choisissez Basic scanning (Analyse de base).
5. Par défaut, tous vos référentiels sont configurés pour une analyse manuelle. Vous pouvez éventuellement configurer l'analyse lors de l'envoi (push) en spécifiant des filtres d'analyse lors de l'envoi (push). Vous pouvez définir l'analyse lors de l'envoi (push) pour tous les référentiels ou pour des référentiels individuels. Pour plus d'informations, consultez Filtres permettant de choisir les référentiels à analyser dans Amazon ECR.

Numérisation manuelle d'une image pour détecter les vulnérabilités du système d'exploitation dans Amazon ECR

Si vos référentiels ne sont pas configurés pour numériser en mode push, vous pouvez lancer manuellement des numérisations d'images. Une image peut être numérisée une fois toutes les 24 heures. Les 24 heures incluent le scan initial sur push, si configuré, et tous les scans manuels.

Pour en savoir plus sur le dépannage de certains problèmes courants lors de la numérisation des images, consultez Résolution des problèmes liés à la numérisation d'images dans Amazon ECR.

AWS Management Console

Suivez les étapes suivantes pour lancer la numérisation manuelle d'une image à l'aide de la AWS Management Console.

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région dans laquelle vous souhaitez créer votre référentiel.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Dans la page Référentiels, choisissez le référentiel qui contient l'image à numériser.

5. Dans la page Images sélectionnez l'image à numériser, puis choisissez Numériser.

AWS CLI

- start-image-scan (AWS CLI)

  L'exemple suivant utilise une étiquette d'image.

```
aws ecr start-image-scan --repository-name name --image-id imageTag=tag_name --
region us-east-2
```

  L'exemple suivant utilise un résumé d'image.

```
aws ecr start-image-scan --repository-name name --image-id imageDigest=sha256_hash
 --region us-east-2
```

AWS Tools for Windows PowerShell

- Recherche Get-ECR () ImageScanAWS Tools for Windows PowerShell

  L'exemple suivant utilise une étiquette d'image.

```
Start-ECRImageScan -RepositoryName name -ImageId_ImageTag tag_name -Region us-
east-2 -Force
```

  L'exemple suivant utilise un résumé d'image.

```
Start-ECRImageScan -RepositoryName name -ImageId_ImageDigest sha256_hash -
Region us-east-2 -Force
```

Extraction des résultats pour les scans de base dans Amazon ECR

Vous pouvez récupérer les résultats de numérisation de la dernière numérisation d'image de base terminée. Les vulnérabilités logicielles découvertes sont répertoriées par gravité sur la base de données CVE (Common Vulnerabilities and Exposures).

Pour en savoir plus sur le dépannage de certains problèmes courants lors de la numérisation des images, consultez Résolution des problèmes liés à la numérisation d'images dans Amazon ECR.

AWS Management Console

Suivez les étapes ci-dessous pour récupérer les résultats de numérisation d'images à l'aide de la AWS Management Console.

Pour récupérer les résultats de numérisation d'images

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région dans laquelle vous souhaitez créer votre référentiel.
3. Dans le panneau de navigation, choisissez Référentiels.
4. Dans la page Référentiels, choisissez le référentiel qui contient l'image pour laquelle récupérer les résultats de numérisation.
5. Dans la page Images, sous la colonne Vulnérabilités sélectionnez Détails de l'image pour récupérer les résultats de la numérisation.

AWS CLI

Utilisez la AWS CLI commande suivante pour récupérer les résultats de numérisation d'images à l'aide du AWS CLI. Vous pouvez spécifier une image à l'aide de `imageTag` ou `imageDigest`, qui peuvent être obtenus à l'aide de la commande CLI list-images.

- describe-image-scan-findings (AWS CLI)

  L'exemple suivant utilise une étiquette d'image.

  ```
  aws ecr describe-image-scan-findings --repository-name name --image-id
   imageTag=tag_name --region us-east-2
  ```

  L'exemple suivant utilise un résumé d'image.

  ```
  aws ecr describe-image-scan-findings --repository-name name --image-id
   imageDigest=sha256_hash --region us-east-2
  ```

AWS Tools for Windows PowerShell

- Recherche Get-ECR () ImageScanAWS Tools for Windows PowerShell

L'exemple suivant utilise une étiquette d'image.

```
Get-ECRImageScanFinding -RepositoryName name -ImageId_ImageTag tag_name -
Region us-east-2
```

L'exemple suivant utilise un résumé d'image.

```
Get-ECRImageScanFinding -RepositoryName name -ImageId_ImageDigest sha256_hash -
Region us-east-2
```

Résolution des problèmes liés à la numérisation d'images dans Amazon ECR

Les échecs de numérisation d'images suivants sont les plus courants. Vous pouvez consulter les erreurs de ce type dans la console Amazon ECR en affichant les détails de l'image, via l'API ou AWS CLI en utilisant l'`DescribeImageScanFindings`API.

UnsupportedImageErreur

Vous pouvez recevoir une erreur `UnsupportedImageError` lors de la tentative d'effectuer une analyse de base sur une image créée à l'aide d'un système d'exploitation pour lequel Amazon ECR ne prend pas en charge l'analyse de base d'images. Amazon ECR prend en charge l'analyse des vulnérabilités de paquets pour les principales versions des distributions Amazon Linux, Amazon Linux 2, Debian, Ubuntu, CentOS, Oracle Linux, Alpine et RHEL Linux. Une fois qu'une distribution perd le support de son fournisseur, Amazon ECR peut ne plus prendre en charge la recherche de vulnérabilités. Amazon ECR ne prend pas en charge l'analyse d'images créées à partir de l'image Docker scratch.

> **Important**
>
> Lorsque vous utilisez l'analyse améliorée, Amazon Inspector prend en charge l'analyse pour des systèmes d'exploitation et des types de médias spécifiques. Pour obtenir la liste complète, veuillez consulter la rubrique Systèmes d'exploitation et types de médias pris en charge dans le Guide de l'utilisateur Amazon Inspector.

Un niveau de gravité `UNDEFINED` est renvoyé

Vous pouvez recevoir un résultat d'analyse dont le niveau de gravité est `UNDEFINED`. Les raisons les plus courantes sont les suivantes :

- La source CVE n'a pas attribué de priorité à la vulnérabilité.
- La vulnérabilité a reçu une priorité non reconnue par Amazon ECR.

Pour déterminer la gravité et la description d'une vulnérabilité, vous pouvez afficher le CVE directement à partir de la source.

Présentation des statuts d'analyse **`SCAN_ELIGIBILITY_EXPIRED`**

Lorsque l'analyse améliorée à l'aide d'Amazon Inspector est activée pour votre registre privé et que vous consultez les vulnérabilités d'analyse, vous pouvez voir un état d'analyse de `SCAN_ELIGIBILITY_EXPIRED`. Les raisons les plus courantes sont les suivantes :

- Lorsque vous activez pour la première fois l'analyse améliorée pour votre registre privé, Amazon Inspector ne reconnaît que les images envoyées à Amazon ECR au cours des 30 derniers jours, en fonction de l'horodatage de l'image. Les images plus anciennes auront le statut d'analyse `SCAN_ELIGIBILITY_EXPIRED`. Si vous souhaitez que ces images soient analysées par Amazon Inspector, vous devez les envoyer à nouveau dans votre référentiel.
- Si la durée de ré-analyse ECR est modifiée dans la console Amazon Inspector et que ce délai est écoulé, l'état d'analyse de l'image devient `inactive` avec un code de motif de `expired`, et toutes les résulats associées à l'image sont programmées pour être fermées. Cela a pour effet que la console Amazon ECR indique l'état d'analyse comme `SCAN_ELIGIBILITY_EXPIRED`.

Synchroniser un registre en amont avec un registre privé Amazon ECR

À l'aide des règles de cache d'extraction, vous pouvez synchroniser le contenu d'un registre en amont avec votre registre privé Amazon ECR.

Amazon ECR prend actuellement en charge la création de règles de mise en cache par extraction pour les registres en amont suivants.

- Docker Hub, Microsoft Azure Container Registry, GitHub Container Registry et GitLab Container Registry (authentification requise)
- Amazon ECR Public, le registre d'images de conteneur Kubernetes et Quay (ne nécessitent pas d'authentification)

Pour GitLab Container Registry, Amazon ECR prend en charge le pull through cache uniquement avec l' GitLab software-as-a-service offre GitLab .com.

Pour les registres en amont qui nécessitent une authentification, vous devez conserver vos informations d'identification de manière AWS Secrets Manager secrète. La console Amazon ECR vous permet de créer facilement le secret Secrets Manager pour chacun des registres en amont authentifiés. Pour plus d'informations sur la création d'un secret Secrets Manager à l'aide de la console Secrets Manager, consultezStockage AWS Secrets Manager secret des informations d'identification de votre référentiel en amont.

Après avoir créé une règle de mise en cache par extraction pour le registre en amont, il suffit d'extraire une image de ce registre en amont en utilisant l'URI de votre registre privé Amazon ECR. Amazon ECR crée ensuite un référentiel et met cette image en cache dans votre registre privé. Lors de vos requêtes d'extraction ultérieures de l'image mise en cache avec une balise donnée, Amazon ECR vérifie dans le registre en amont s'il existe une nouvelle version de l'image avec cette balise spécifique et tente de mettre à jour l'image dans votre registre privé au moins une fois toutes les 24 heures.

Modèles de création de référentiels

Amazon ECR a ajouté la prise en charge des modèles de création de référentiels, actuellement en version préliminaire, qui vous donne le contrôle nécessaire pour spécifier les configurations initiales pour les nouveaux référentiels créés par Amazon ECR en votre nom à l'aide de règles de mise

en cache par extraction. Chaque modèle contient un préfixe d'espace de noms de référentiel qui est utilisé pour faire correspondre les nouveaux référentiels à un modèle spécifique. Les modèles peuvent spécifier la configuration de tous les paramètres du référentiel, y compris les politiques d'accès basées sur les ressources, l'immuabilité des balises, le chiffrement et les politiques de cycle de vie. Les paramètres d'un modèle de création de référentiel ne sont appliqués que lors de la création du référentiel et n'ont aucun effet sur les référentiels existants ou les référentiels créés à l'aide d'une autre méthode. Pour plus d'informations, consultez Modèles pour contrôler les référentiels créés lors d'une action d'extraction dans le cache.

Considérations relatives à l'utilisation des règles du cache d'extraction

Tenez compte des points suivants lorsque vous utilisez les règles de cache d'extraction d'Amazon ECR.

- La création de règles de mise en cache par extraction n'est pas prise en charge dans les régions suivantes.
  - Chine (Beijing) (`cn-north-1`)
  - Chine (Ningxia) (`cn-northwest-1`)
  - AWS GovCloud (USA Est) (`us-gov-east-1`)
  - AWS GovCloud (US-Ouest) (`us-gov-west-1`)
- AWS Lambda ne prend pas en charge l'extraction d'images de conteneurs depuis Amazon ECR à l'aide d'une règle de cache d'extraction.
- Lors de l'extraction d'images à l'aide de la mise en cache par extraction, les points de terminaison de service FIPS d'Amazon ECR ne sont pas pris en charge la première fois qu'une image est extraite. L'utilisation des points de terminaison de service FIPS d'Amazon ECR fonctionne cependant pour les extractions suivantes.
- Lorsqu'une image mise en cache est extraite via l'URI du registre privé Amazon ECR, les extractions d'image sont initiées par des AWS adresses IP. Cela garantit que l'extraction de l'image n'est pas comptabilisée dans les quotas de taux d'extraction implémenté par le registre en amont.
- Lorsqu'une image mise en cache est extraite via l'URI du registre privé Amazon ECR, Amazon ECR vérifie le référentiel en amont au moins une fois toutes les 24 heures afin de s'assurer que l'image mise en cache est la dernière version. S'il existe une image plus récente dans le registre en amont, Amazon ECR tente de mettre à jour l'image mise en cache. Ce délai est basé sur la dernière extraction de l'image mise en cache.

- Si Amazon ECR ne peut pas mettre à jour l'image depuis le registre en amont pour une raison quelconque et que l'image est extraite, la dernière image mise en cache sera quand même extraite.
- Lors de la création du secret Secrets Manager qui contient les informations d'identification du registre en amont, le nom du secret doit utiliser le préfixe `ecr-pullthroughcache/`. Le secret doit également se trouver dans le même compte et dans la même région que ceux dans lesquels est créée la règle de mise en cache par extraction.
- Lorsqu'une image multi-architecture est extraite à l'aide d'une règle mise en cache par extraction, la liste de manifestes et chaque image référencée dans la liste de manifestes sont extraites vers le référentiel Amazon ECR. Si vous ne souhaitez extraire qu'une architecture spécifique, vous pouvez extraire l'image en utilisant le résumé d'image ou l'identification associée à l'architecture plutôt que l'identification associée à la liste de manifestes.
- Amazon ECR utilise un rôle IAM lié à un service, qui fournit les autorisations nécessaires à Amazon ECR pour créer le référentiel, récupérer la valeur du secret Secrets Manager pour l'authentification et transmettre l'image mise en cache en votre nom. Le rôle IAM lié à un service est créé automatiquement lorsqu'une règle de mise en cache par extraction est créée. Pour plus d'informations, consultez Rôle lié à un service Amazon ECR pour la mise en cache par extraction.
- Par défaut, l'utilisateur, le principal IAM qui extrait l'image mise en cache a les autorisations qui lui sont accordées par sa politique IAM. Vous pouvez utiliser la politique d'autorisations du registre privé Amazon ECR pour étendre les autorisations d'une entité IAM. Pour plus d'informations, consultez Utilisation des autorisations de registre.
- Les référentiels Amazon ECR créés à l'aide du flux de travail de mise en cache par extraction sont traités comme tout autre référentiel Amazon ECR. Toutes les fonctions du référentiel, telles que la réplication et l'analyse d'images, sont prises en charge.
- Lorsqu'Amazon ECR crée un nouveau référentiel en votre nom à l'aide d'une action de mise en cache par extraction, les paramètres par défaut suivants sont appliqués au référentiel, sauf s'il existe un modèle de création de référentiel correspondant. Vous pouvez utiliser un modèle de création de référentiel pour définir les paramètres appliqués aux référentiels créés par Amazon ECR en votre nom. Pour plus d'informations, consultez Modèles pour contrôler les référentiels créés lors d'une action d'extraction dans le cache.
  - Immuabilité des balises : désactivée, les balises sont mutables et peuvent être remplacées.
  - Chiffrement : on utilise le chiffrement par défaut `AES256`.
  - Autorisations du référentiel : omises, aucune politique d'autorisation de référentiel n'est appliquée.
  - Politique de cycle de vie : omise, aucune politique de cycle de vie n'est appliquée.

  - Balises de ressource : omises, aucune balise de ressource n'est appliquée.
- L'activation de l'immuabilité des balises d'image pour des référentiels à l'aide d'une règle de mise en cache par extraction empêchera Amazon ECR de mettre à jour les images à l'aide de la même balise.
- Lorsqu'une image est extraite à l'aide de la règle du cache d'extraction pour la première fois, un itinéraire vers Internet peut être nécessaire. Dans certaines circonstances, un itinéraire vers Internet est nécessaire, il est donc préférable de configurer un itinéraire pour éviter toute défaillance. Ainsi, si vous avez configuré Amazon ECR pour utiliser un point de terminaison AWS PrivateLink VPC d'interface, vous devez vous assurer que le premier pull dispose d'un itinéraire vers Internet. Pour ce faire, vous pouvez créer un sous-réseau public dans le même VPC, avec une passerelle Internet, puis acheminer tout le trafic sortant vers Internet depuis leur sous-réseau privé vers le sous-réseau public. Les extractions d'image suivantes à l'aide de la règle de cache d'extraction ne l'exigent pas. Pour de plus amples informations, consultez Exemples d'options de routage dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Autorisations IAM requises pour synchroniser un registre en amont avec un registre privé Amazon ECR

Outre les autorisations d'API Amazon ECR nécessaires pour s'authentifier auprès d'un registre privé et pour transférer et extraire des images, les autorisations supplémentaires suivantes sont nécessaires pour utiliser efficacement les règles de mise en cache par extraction.

- `ecr:CreatePullThroughCacheRule` – Accorde l'autorisation de créer une règle de cache par extraction. Cette autorisation doit être accordée via une politique IAM basée sur l'identité.
- `ecr:BatchImportUpstreamImage` – Accorde l'autorisation de récupérer l'image externe et de l'importer dans votre registre privé. Cette autorisation peut être accordée à l'aide de la politique d'autorisation du registre privé, d'une politique IAM basée sur l'identité ou de la politique d'autorisations de référentiel basée sur les ressources. Pour plus d'informations sur l'utilisation d'autorisations de référentiel, consultez Politiques relatives aux référentiels privés dans Amazon ECR.
- `ecr:CreateRepository` – Accorde l'autorisation de créer un référentiel dans un registre privé. Cette autorisation est requise si le référentiel stockant les images mises en cache n'existe pas déjà. Cette autorisation peut être accordée soit par une politique IAM basée sur l'identité, soit par la politique d'autorisation du registre privé.

- `ecr:TagResource` : accorde l'autorisation d'ajouter des balises de métadonnées à une ressource Amazon ECR. Cette autorisation n'est requise que si vous extrayez une image qui utilise une règle de mise en cache par extraction associée à un modèle de création de référentiel configuré pour ajouter des balises de ressources au référentiel. Cette autorisation doit être accordée via une politique IAM basée sur l'identité.

Utilisation des autorisations de registre

Les autorisations du registre privé Amazon ECR peuvent être utilisées pour étendre les autorisations des entités IAM individuelles à utiliser la mise en cache par extraction. Si une entité IAM dispose de plus d'autorisations accordées par une politique IAM que celles accordées par la politique d'autorisations de registre, la politique IAM a la priorité. Par exemple, si un utilisateur dispose des autorisations `ecr:*`, aucune autorisation supplémentaire n'est nécessaire au niveau du registre.

Pour créer une politique d'autorisations de registre privée (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région dans laquelle vous souhaitez configurer votre instruction d'autorisations de registre privé.
3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Registry permissions (Autorisations du registre).
4. Dans la page Registry permissions (Autorisations de registre), choisissez Generate statement (Générer une instruction).
5. Pour chaque instruction de politique d'autorisations de mise en cache par extraction que vous souhaitez créer, procédez comme suit.

    a. Pour Policy type (Type de politique), choisissez Pull through cache policy (Politique de mise en cache par extraction).

    b. Pour Statement id (ID d'instruction), fournissez un nom pour l'instruction de politique de mise en cache par extraction.

    c. Pour IAM entities (Entités IAM), indiquez les utilisateurs, groupes ou rôles à inclure dans la politique.

    d. Pour Repository namespace (Espace de noms de référentiel), sélectionnez la règle de mise en cache par extraction à laquelle associer la politique.

e. Pour Repository names (Noms de référentiel), spécifiez le nom de base du référentiel pour lequel appliquer la règle. Par exemple, si vous voulez spécifier le référentiel Amazon Linux sur Amazon ECR Public, le nom du référentiel sera `amazonlinux`.

Pour créer une politique d'autorisations de registre privée (AWS CLI)

Utilisez la AWS CLI commande suivante pour spécifier les autorisations de registre privé à l'aide du AWS CLI.

1. Créez un fichier local nommé `ptc-registry-policy.json` avec le contenu de la politique de référentiel. L'exemple suivant accorde à `ecr-pull-through-cache-user` l'autorisation de créer un référentiel et d'extraire une image depuis Amazon ECR Public, qui est la source en amont associée à la règle de cache par extraction précédemment créée.

```
{
  "Sid": "PullThroughCacheFromReadOnlyRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ecr-pull-through-cache-user"
  },
  "Action": [
    "ecr:CreateRepository",
    "ecr:BatchImportUpstreamImage"
  ],
  "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/ecr-public/*"
}
```

> **Important**
>
> L'autorisation `ecr-CreateRepository` n'est requise que si le référentiel stockant les images mises en cache n'existe pas déjà. Par exemple, si l'action de création du référentiel et les actions d'extraction d'image sont effectuées par des IAM principaux distincts tels qu'un administrateur et un développeur.

2. Utilisation de la commande put-registry-policy pour définir la politique de registre.

```
aws ecr put-registry-policy \
     --policy-text file://ptc-registry.policy.json
```

Étapes suivantes

Une fois que vous êtes prêt à commencer à utiliser les règles de mise en cache par extraction, procédez comme suit.

- Créez une règle de mise en cache par extraction. Pour plus d'informations, consultez Création d'une règle de cache d'extraction dans Amazon ECR.
- Créez un modèle de création de référentiel. Un modèle de création de référentiel vous permet de définir les paramètres à utiliser pour les nouveaux référentiels créés par Amazon ECR en votre nom lors d'une action de mise en cache par extraction. Pour plus d'informations, consultez Modèles pour contrôler les référentiels créés lors d'une action d'extraction dans le cache.

Création d'une règle de cache d'extraction dans Amazon ECR

Pour chaque registre en amont contenant des images que vous souhaitez mettre en cache dans votre registre privé Amazon ECR, vous devez créer une règle de cache d'extraction.

Pour les registres en amont qui nécessitent une authentification, vous devez stocker les informations d'identification dans un secret Secrets Manager. Vous pouvez utiliser un secret existant ou en créer un nouveau. Vous pouvez créer le secret Secrets Manager dans la console Amazon ECR ou dans la console Secrets Manager. Pour créer un secret Secrets Manager à l'aide de la console Secrets Manager au lieu de la console Amazon ECR, consultezStockage AWS Secrets Manager secret des informations d'identification de votre référentiel en amont.

Prérequis

- Vérifiez que vous disposez des autorisations IAM appropriées pour créer des règles de cache d'extraction. Pour plus d'informations, veuillez consulter Autorisations IAM requises pour synchroniser un registre en amont avec un registre privé Amazon ECR.
- Pour les registres en amont qui nécessitent une authentification : si vous souhaitez utiliser un secret existant, vérifiez que le secret Secrets Manager répond aux exigences suivantes :
  - Le nom du secret commence par`ecr-pullthroughcache/`. Affiche AWS Management Console uniquement les secrets de Secrets Manager avec le `ecr-pullthroughcache/` préfixe.
  - Le compte et la région dans lesquels se trouve le secret doivent correspondre au compte et à la région dans lesquels se trouve la règle de cache d'extraction.

Pour créer une règle de mise en cache par extraction (AWS Management Console)

Les étapes suivantes montrent comment créer une règle de mise en cache par extraction et un secret Secrets Manager à l'aide de la console Amazon ECR. Pour créer un secret à l'aide de la console Secrets Manager, consultezStockage AWS Secrets Manager secret des informations d'identification de votre référentiel en amont.

Pour Amazon ECR Public, le registre de conteneur Kubernetes ou Quay

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région pour laquelle vous souhaitez configurer les paramètres de votre registre privé.
3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Pull through cache (Mise en cache par extraction).
4. Sur la page Pull through cache configuration (Configuration de la mise en cache par extraction), cliquez sur Add rule (Ajouter une règle).
5. Sur la page Étape 1 : Spécifier une source pour Registre, choisissez Amazon ECR Public, Kubernetes ou Quay dans la liste des registres en amont, puis choisissez Suivant.
6. Sur la page Étape 2 : Spécifier une destination pour le Préfixe du référentiel Amazon ECR, spécifiez le préfixe d'espace de noms du référentiel à utiliser lors de la mise en cache des images extraites du registre public source, puis choisissez Suivant. Par défaut, un espace de noms est renseigné mais un espace de noms personnalisé peut également être spécifié.
7. Sur la page Étape 3 : Vérifier et créer, vérifiez la configuration de la règle de mise en cache par extraction, puis choisissez Créer.
8. Répétez l'étape précédente pour chaque mise en cache par extraction que vous souhaitez créer. Les règles de mise en cache par extraction sont créées séparément pour chaque région.

Pour Docker Hub

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région pour laquelle vous souhaitez configurer les paramètres de votre registre privé.
3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Pull through cache (Mise en cache par extraction).

4. Sur la page Pull through cache configuration (Configuration de la mise en cache par extraction), cliquez sur Add rule (Ajouter une règle).
5. Sur la page Étape 1 : Spécifier une source pour Registre, choisissez Docker Hub, Suivant.
6. Sur la page Étape 2 : Configuration de l'authentification pour les Informations d'identification en amont, vous devez stocker vos informations d'identification pour Docker Hub dans un sectret AWS Secrets Manager . Vous pouvez spécifier un secret existant ou utiliser la console Amazon ECR pour créer un nouveau secret.

   a. Pour utiliser un secret existant, choisissez Utiliser un AWS secret existant. Pour Nom du secret, utilisez le menu déroulant pour sélectionner votre secret existant, puis choisissez Suivant.

      > **Note**
      >
      > Affiche AWS Management Console uniquement les secrets de Secrets Manager dont le nom utilise le `ecr-pullthroughcache/` préfixe. Le secret doit également se trouver dans le même compte et dans la même région que ceux dans lesquels est créée la règle de mise en cache par extraction.

   b. Pour créer un nouveau secret, choisissez Créer un secret AWS , procédez comme suit, puis choisissez Suivant.

      i. Pour le Nom du secret, spécifiez un nom descriptif pour le secret. Les noms des secrets doivent contenir entre 1 et 512 caractères Unicode.

      ii. Pour le Nom d'utilisateur Docker Hub, spécifiez votre nom d'utilisateur Docker Hub.

      iii. Pour le Jeton d'accès Docker Hub, spécifiez votre jeton d'accès Docker Hub. Pour plus d'informations sur la création d'un jeton d'accès Docker Hub, consultez la section Création et gestion des jetons d'accès dans la documentation Docker.

7. Sur la page Étape 3 : Spécifier une destination pour le Préfixe du référentiel Amazon ECR, spécifiez l'espace de noms du référentiel à utiliser lors de la mise en cache des images extraites du registre public source, puis choisissez Suivant.

   Par défaut, un espace de noms est renseigné mais un espace de noms personnalisé peut également être spécifié.

8. Sur la page Étape 4 : Vérifier et créer, vérifiez la configuration de la règle de mise en cache par extraction, puis choisissez Créer.

9. Répétez l'étape précédente pour chaque mise en cache par extraction que vous souhaitez créer. Les règles de mise en cache par extraction sont créées séparément pour chaque région.

Pour le registre des GitHub conteneurs

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région pour laquelle vous souhaitez configurer les paramètres de votre registre privé.
3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Pull through cache (Mise en cache par extraction).
4. Sur la page Pull through cache configuration (Configuration de la mise en cache par extraction), cliquez sur Add rule (Ajouter une règle).
5. À l'étape 1 : Spécifier une page source, pour Registry, choisissez GitHub Container Registry, Next.
6. Sur la page Étape 2 : Configuration de l'authentification, pour les informations d'identification Upstream, vous devez enregistrer vos informations d'authentification pour GitHub Container Registry dans un AWS Secrets Manager secret. Vous pouvez spécifier un secret existant ou utiliser la console Amazon ECR pour créer un nouveau secret.

   a. Pour utiliser un secret existant, choisissez Utiliser un AWS secret existant. Pour Nom du secret, utilisez le menu déroulant pour sélectionner votre secret existant, puis choisissez Suivant.

      > **Note**
      >
      > Affiche AWS Management Console uniquement les secrets de Secrets Manager dont le nom utilise le `ecr-pullthroughcache/` préfixe. Le secret doit également se trouver dans le même compte et dans la même région que ceux dans lesquels est créée la règle de mise en cache par extraction.

   b. Pour créer un nouveau secret, choisissez Créer un secret AWS , procédez comme suit, puis choisissez Suivant.

      i. Pour le Nom du secret, spécifiez un nom descriptif pour le secret. Les noms des secrets doivent contenir entre 1 et 512 caractères Unicode.

ii. Pour le nom d'utilisateur du registre des GitHub conteneurs, spécifiez votre nom d'utilisateur du registre des GitHub conteneurs.

iii. Pour le GitHub jeton d'accès au registre des GitHub conteneurs, spécifiez votre jeton d'accès au registre des conteneurs. Pour plus d'informations sur la création d'un jeton d' GitHub accès, consultez la section Gestion de vos jetons d'accès personnels dans la GitHub documentation.

7. Sur la page Étape 3 : Spécifier une destination pour le Préfixe du référentiel Amazon ECR, spécifiez l'espace de noms du référentiel à utiliser lors de la mise en cache des images extraites du registre public source, puis choisissez Suivant.

   Par défaut, un espace de noms est renseigné mais un espace de noms personnalisé peut également être spécifié.

8. Sur la page Étape 4 : Vérifier et créer, vérifiez la configuration de la règle de mise en cache par extraction, puis choisissez Créer.

9. Répétez l'étape précédente pour chaque mise en cache par extraction que vous souhaitez créer. Les règles de mise en cache par extraction sont créées séparément pour chaque région.

Pour Microsoft Azure Container Registry

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.

2. Dans la barre de navigation, choisissez la région pour laquelle vous souhaitez configurer les paramètres de votre registre privé.

3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Pull through cache (Mise en cache par extraction).

4. Sur la page Pull through cache configuration (Configuration de la mise en cache par extraction), cliquez sur Add rule (Ajouter une règle).

5. Sur la page Étape 1 : Spécifier une source, procédez comme suit.

   a. Pour Registre, choisissez Microsoft Azure Container Registry

   b. Pour URL du registre source, spécifiez le nom de votre Microsoft Azure Container Registry, puis choisissez Suivant.

> **Important**
>
> Il vous suffit de spécifier le préfixe, car le suffixe `.azurecr.io` est complété en votre nom.

6. Sur la page Étape 2 : Configuration de l'authentification pour les Informations d'identification en amont, vous devez stocker vos informations d'identification pour Microsoft Azure Container Registry dans un sectret AWS Secrets Manager . Vous pouvez spécifier un secret existant ou utiliser la console Amazon ECR pour créer un nouveau secret.

   a. Pour utiliser un secret existant, choisissez Utiliser un AWS secret existant. Pour Nom du secret, utilisez le menu déroulant pour sélectionner votre secret existant, puis choisissez Suivant.

   > **Note**
   >
   > Affiche AWS Management Console uniquement les secrets de Secrets Manager dont le nom utilise le `ecr-pullthroughcache/` préfixe. Le secret doit également se trouver dans le même compte et dans la même région que ceux dans lesquels est créée la règle de mise en cache par extraction.

   b. Pour créer un nouveau secret, choisissez Créer un secret AWS , procédez comme suit, puis choisissez Suivant.

      i. Pour le Nom du secret, spécifiez un nom descriptif pour le secret. Les noms des secrets doivent contenir entre 1 et 512 caractères Unicode.

      ii. Pour le Nom d'utilisateur Microsoft Azure Container Registry, spécifiez votre nom d'utilisateur Microsoft Azure Container Registry.

      iii. Pour le Jeton d'accès à Microsoft Azure Container Registry, spécifiez votre jeton d'accès à Microsoft Azure Container Registry. Pour plus d'informations sur la création d'un jeton d'accès à Microsoft Azure Container Registry, consultez la section Créer un jeton - portail dans la documentation Microsoft Azure.

7. Sur la page Étape 3 : Spécifier une destination pour le Préfixe du référentiel Amazon ECR, spécifiez l'espace de noms du référentiel à utiliser lors de la mise en cache des images extraites du registre public source, puis choisissez Suivant.

Par défaut, un espace de noms est renseigné mais un espace de noms personnalisé peut également être spécifié.

8. Sur la page Étape 4 : Vérifier et créer, vérifiez la configuration de la règle de mise en cache par extraction, puis choisissez Créer.
9. Répétez l'étape précédente pour chaque mise en cache par extraction que vous souhaitez créer. Les règles de mise en cache par extraction sont créées séparément pour chaque région.

Pour le registre des GitLab conteneurs

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région pour laquelle vous souhaitez configurer les paramètres de votre registre privé.
3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Pull through cache (Mise en cache par extraction).
4. Sur la page Pull through cache configuration (Configuration de la mise en cache par extraction), cliquez sur Add rule (Ajouter une règle).
5. À l'étape 1 : Spécifier une page source, pour Registry, choisissez GitLab Container Registry, Next.
6. Sur la page Étape 2 : Configuration de l'authentification, pour les informations d'identification Upstream, vous devez enregistrer vos informations d'authentification pour GitLab Container Registry dans un AWS Secrets Manager secret. Vous pouvez spécifier un secret existant ou utiliser la console Amazon ECR pour créer un nouveau secret.

    a. Pour utiliser un secret existant, choisissez Utiliser un AWS secret existant. Pour Nom du secret, utilisez le menu déroulant pour sélectionner votre secret existant, puis choisissez Suivant. Pour plus d'informations sur la création d'un secret Secrets Manager à l'aide de la console Secrets Manager, consultez Stockage AWS Secrets Manager secret des informations d'identification de votre référentiel en amont.

    > **Note**
    >
    > Affiche AWS Management Console uniquement les secrets de Secrets Manager dont le nom utilise le `ecr-pullthroughcache/` préfixe. Le secret doit également

se trouver dans le même compte et dans la même région que ceux dans lesquels est créée la règle de mise en cache par extraction.

b. Pour créer un nouveau secret, choisissez Créer un secret AWS , procédez comme suit, puis choisissez Suivant.

   i. Pour le Nom du secret, spécifiez un nom descriptif pour le secret. Les noms des secrets doivent contenir entre 1 et 512 caractères Unicode.

   ii. Pour le nom d'utilisateur du registre des GitLab conteneurs, spécifiez votre nom d'utilisateur du registre des GitLab conteneurs.

   iii. Pour le GitLab jeton d'accès au registre des GitLab conteneurs, spécifiez votre jeton d'accès au registre des conteneurs. Pour plus d'informations sur la création d'un jeton d'accès au registre des GitLab conteneurs, voir Jetons d'accès personnels, jetons d'accès de groupe ou jetons d'accès au projet dans la GitLab documentation.

7. Sur la page Étape 3 : Spécifier une destination pour le Préfixe du référentiel Amazon ECR, spécifiez l'espace de noms du référentiel à utiliser lors de la mise en cache des images extraites du registre public source, puis choisissez Suivant.

   Par défaut, un espace de noms est renseigné mais un espace de noms personnalisé peut également être spécifié.

8. Sur la page Étape 4 : Vérifier et créer, vérifiez la configuration de la règle de mise en cache par extraction, puis choisissez Créer.

9. Répétez l'étape précédente pour chaque mise en cache par extraction que vous souhaitez créer. Les règles de mise en cache par extraction sont créées séparément pour chaque région.

Pour créer une règle de mise en cache par extraction (AWS CLI)

Utilisez la AWS CLI commande create-pull-through-cache-rule pour créer une règle de cache d'extraction pour un registre privé Amazon ECR. Pour de registres en amont qui nécessitent une authentification, vous devez stocker les informations d'identification dans un secret Secrets Manager. Pour créer un secret à l'aide de la console Secrets Manager, consultezStockage AWS Secrets Manager secret des informations d'identification de votre référentiel en amont.

Les exemples suivants sont fournis pour chaque registre en amont pris en charge.

Pour Amazon ECR Public

L'exemple suivant crée une règle de mise en cache par extraction pour le registre public Amazon ECR. Il spécifie un préfixe de référentiel de `ecr-public`, ce qui fait que chaque référentiel créé à l'aide de la règle de mise en cache par extraction aura le schéma de dénomination de `ecr-public/`*`upstream-repository-name`*.

```
aws ecr create-pull-through-cache-rule \
     --ecr-repository-prefix ecr-public \
     --upstream-registry-url public.ecr.aws \
     --region us-east-2
```

Pour le registre de conteneurs Kubernetes

L'exemple suivant crée une règle de mise en cache par extraction pour le registre public Kubernetes. Il spécifie un préfixe de référentiel de `kubernetes`, ce qui fait que chaque référentiel créé à l'aide de la règle de mise en cache par extraction aura le schéma de dénomination de `kubernetes/`*`upstream-repository-name`*.

```
aws ecr create-pull-through-cache-rule \
     --ecr-repository-prefix kubernetes \
     --upstream-registry-url registry.k8s.io \
     --region us-east-2
```

Pour Quay

L'exemple suivant crée une règle de mise en cache par extraction pour le registre public Quay. Il spécifie un préfixe de référentiel de `quay`, ce qui fait que chaque référentiel créé à l'aide de la règle de mise en cache par extraction aura le schéma de dénomination de `quay/`*`upstream-repository-name`*.

```
aws ecr create-pull-through-cache-rule \
     --ecr-repository-prefix quay \
     --upstream-registry-url quay.io \
     --region us-east-2
```

Pour Docker Hub

L'exemple suivant crée une règle de mise en cache par extraction pour le registre Docker Hub. Il spécifie un préfixe de référentiel de `docker-hub`, ce qui fait que chaque référentiel créé à

l'aide de la règle de mise en cache par extraction aura le schéma de dénomination de `docker-hub/`*`upstream-repository-name`*. Vous devez spécifier l'Amazon Resource Name (ARN) complet du secret contenant vos informations d'identification Docker Hub.

```
aws ecr create-pull-through-cache-rule \
     --ecr-repository-prefix docker-hub \
     --upstream-registry-url registry-1.docker.io \
     --credential-arn arn:aws:secretsmanager:us-east-2:111122223333:secret:ecr-
pullthroughcache/example1234 \
     --region us-east-2
```

Pour le registre des GitHub conteneurs

L'exemple suivant crée une règle de cache d'extraction pour le registre des GitHub conteneurs. Il spécifie un préfixe de référentiel de `docker-hub`, ce qui fait que chaque référentiel créé à l'aide de la règle de mise en cache par extraction aura le schéma de dénomination de `github/`*`upstream-repository-name`*. Vous devez spécifier le nom Amazon Resource Name (ARN) complet du secret contenant vos informations d'identification du registre des GitHub conteneurs.

```
aws ecr create-pull-through-cache-rule \
     --ecr-repository-prefix github \
     --upstream-registry-url ghcr.io \
     --credential-arn arn:aws:secretsmanager:us-east-2:111122223333:secret:ecr-
pullthroughcache/example1234 \
     --region us-east-2
```

Pour Microsoft Azure Container Registry

L'exemple suivant crée une règle de cache d'extraction pour le Microsoft Azure Container Registry. Il spécifie un préfixe de référentiel de `azure`, ce qui fait que chaque référentiel créé à l'aide de la règle de mise en cache par extraction aura le schéma de dénomination de `azure/`*`upstream-repository-name`*. Vous devez spécifier l'Amazon Resource Name (ARN) complet du secret contenant vos informations d'identification Azure Container Registry.

```
aws ecr create-pull-through-cache-rule \
     --ecr-repository-prefix azure \
     --upstream-registry-url myregistry.azurecr.io \
     --credential-arn arn:aws:secretsmanager:us-east-2:111122223333:secret:ecr-
pullthroughcache/example1234 \
     --region us-east-2
```

Pour le registre des GitLab conteneurs

L'exemple suivant crée une règle de cache d'extraction pour le registre des GitLab conteneurs. Il spécifie un préfixe de référentiel de `gitlab`, ce qui fait que chaque référentiel créé à l'aide de la règle de mise en cache par extraction aura le schéma de dénomination de `gitlab/`*`upstream-repository-name`*. Vous devez spécifier le nom Amazon Resource Name (ARN) complet du secret contenant vos informations d'identification du registre des GitLab conteneurs.

```
aws ecr create-pull-through-cache-rule \
     --ecr-repository-prefix gitlab \
     --upstream-registry-url registry.gitlab.com \
     --credential-arn arn:aws:secretsmanager:us-east-2:111122223333:secret:ecr-
pullthroughcache/example1234 \
     --region us-east-2
```

Étapes suivantes

Après avoir créé vos règles de cache d'extraction, les étapes suivantes sont les suivantes :

- Créez un modèle de création de référentiel. Un modèle de création de référentiel vous permet de définir les paramètres à utiliser pour les nouveaux référentiels créés par Amazon ECR en votre nom lors d'une action de mise en cache par extraction. Pour plus d'informations, consultez Modèles pour contrôler les référentiels créés lors d'une action d'extraction dans le cache.
- Validez vos règles de mise en cache par extraction. Lors de la validation d'une règle de mise en cache par extraction, Amazon ECR établit une connexion réseau avec le registre en amont, vérifie qu'il peut accéder au secret Secrets Manager contenant les informations d'identification du registre en amont et que l'authentification a été réussie. Pour plus d'informations, consultez Validation des règles de cache d'extraction dans Amazon ECR.
- Commencez à utiliser vos règles de mise en cache par extraction. Pour plus d'informations, consultez Extraction d'une image à l'aide d'une règle de cache d'extraction dans Amazon ECR.

Modèles pour contrôler les référentiels créés lors d'une action d'extraction dans le cache

La fonctionnalité de modèle de création de référentiel est disponible en version préliminaire pour Amazon ECR et est sujette à changement. Au cours de cette version préliminaire publique, seuls

les AWS Management Console peuvent être utilisés pour gérer vos modèles de création de référentiels.

Utilisez les modèles de création de référentiels Amazon ECR pour définir les paramètres des référentiels créés par Amazon ECR en votre nom lors d'une action d'extraction dans le cache. Les paramètres d'un modèle de création de référentiel ne sont appliqués que lors de la création du référentiel et n'ont aucun effet sur les référentiels existants ou les référentiels créés à l'aide d'une autre méthode.

Les modèles de création de référentiels ne sont pas pris en charge dans les régions suivantes :

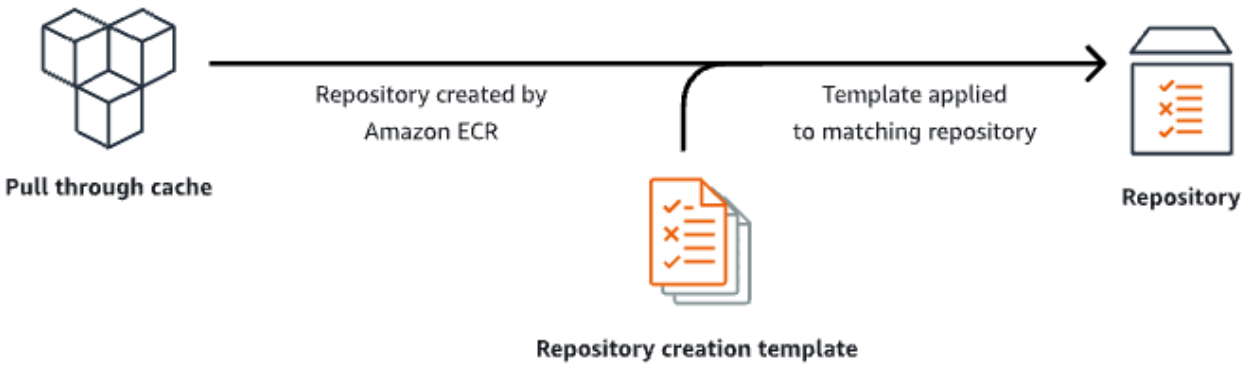
- Chine (Beijing) (`cn-north-1`)
- Chine (Ningxia) (`cn-northwest-1`)
- AWS GovCloud (USA Est) (`us-gov-east-1`)
- AWS GovCloud (US-Ouest) (`us-gov-west-1`)

Fonctionnement des modèles de création de référentiels

Parfois, Amazon ECR doit créer un nouveau référentiel privé en votre nom. Par exemple, la première fois que vous utilisez une règle de mise en cache par extraction pour récupérer le contenu d'un référentiel en amont et le stocker dans votre registre privé Amazon ECR. Lorsqu'aucun modèle de création de référentiel ne correspond à votre règle de mise en cache par extraction, Amazon ECR utilise les paramètres par défaut pour le nouveau référentiel. Ces paramètres par défaut incluent la désactivation de l'immuabilité des balises, l'utilisation du chiffrement `AES-256` et l'absence d'application de politiques de référentiel ou de cycle de vie.

L'utilisation d'un modèle de création de référentiel avec un préfixe correspondant à une règle de mise en cache par extraction vous permet de définir les paramètres qu'Amazon ECR applique aux nouveaux référentiels créés par le biais de l'action de mise en cache par extraction. Vous pouvez définir l'immuabilité des balises, la configuration du chiffrement, les autorisations des référentiels, la politique de cycle de vie et les balises de ressource pour les nouveaux référentiels.

Le schéma suivant illustre le flux de travail qu'Amazon ECR utilise lorsqu'un modèle de création de référentiel est utilisé.



Vous trouverez ci-dessous une description détaillée de chaque paramètre d'un modèle de création de référentiel.

Préfixe

Le préfixe est le préfixe de l'espace de noms du référentiel à associer au modèle. Les paramètres définis dans ce modèle seront appliqués à tous les référentiels créés à l'aide de ce préfixe. Par exemple, le préfixe de `prod` s'appliquerait à tous les référentiels commençant par `prod/`. De la même façon, le préfixe de `prod/team` s'appliquerait à tous les référentiels commençant par `prod/team/`.

Pour appliquer un modèle à tous les référentiels de votre registre auxquels aucun modèle de création n'est associé, vous pouvez utiliser ROOT comme préfixe.

> **Important**
>
> Il y a toujours un / supposé/appliqué à la fin du préfixe. Si vous spécifiez `ecr-public` comme préfixe, Amazon ECR le traite comme `ecr-public/`. Lorsque vous utilisez une règle de mise en cache par extraction, le préfixe de référentiel que vous spécifiez lors de la création de la règle est également celui que vous devez spécifier comme préfixe de modèle de création de référentiel.

Description

Cette description du modèle est facultative et est utilisée pour décrire l'objectif du modèle de création de référentiel.

Version du modèle

La version du modèle de création de référentiel à utiliser. Actuellement, la seule version du modèle prise en charge est TV1.

Version de configuration

La version de configuration du référentiel, le modèle à utiliser. Chaque modèle doit inclure une configuration de référentiel. La version de configuration par défaut est CV1 et comprend les paramètres de mutabilité des balises d'image, de politique de référentiel et de politique de cycle de vie.

Mutabilité d'une étiquette d'image

Le paramètre de mutabilité des balises à utiliser pour les référentiels créés à l'aide du modèle. Si ce paramètre est omis, le paramètre par défaut MUTABLE sera utilisé, ce qui permettra le remplacement des balises d'image. Il est recommandé d'utiliser ce paramètre pour les modèles utilisés pour les référentiels créés par des actions de mise en cache par extraction. Cela permet à Amazon ECR de mettre à jour les images mises en cache lorsque les balises sont identiques.

Si on spécifie IMMUABLE, toutes les balises d'image du référentiel seront immuables, ce qui les empêchera d'être remplacées.

Configuration de chiffrement

La Configuration de chiffrement à utiliser pour les référentiels créés à l'aide du modèle.

Si vous utilisez le type de chiffrement KMS, le contenu du référentiel sera chiffré à l'aide du chiffrement côté serveur avec une clé AWS Key Management Service stockée dans AWS KMS. Lorsque vous chiffrez vos données, vous pouvez soit utiliser la AWS KMS clé AWS gérée par défaut pour Amazon ECR, soit spécifier votre propre AWS KMS clé, que vous avez déjà créée. AWS KMS Pour plus d'informations, consultez la section Protection des données à l'aide du chiffrement côté serveur avec une AWS Key Management Service clé stockée dans AWS Key Management Service (SSE-KMS) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Si vous utilisez le type de chiffrement AES256, Amazon ECR utilise le chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3, ce qui chiffre les images dans le référentiel à l'aide d'un algorithme de chiffrement AES-256. Pour plus d'informations, consultez la section Protection des données à l'aide du chiffrement côté serveur avec les clés de chiffrement gérés par Amazon S3 (SSE-S3) dans le Guide de l'utilisateur Amazon Simple Storage Service.

Autorisations du référentiel

La Politique de référentiel à appliquer aux référentiels créés à l'aide du modèle. Une politique de référentiel utilise les autorisations basées sur les ressources pour contrôler l'accès à un référentiel. Les autorisations basées sur les ressources vous permettent de spécifier les utilisateurs ou rôles IAM qui ont accès à un référentiel et quelles sont les actions qui peuvent être exécutées. Par défaut, seul le AWS compte qui a créé le référentiel a accès à un référentiel. Vous pouvez appliquer un document de politique qui accorde ou refuse des autorisations supplémentaires à votre référentiel. Pour plus d'informations, consultez Politiques relatives aux référentiels privés dans Amazon ECR.

Politique de cycle de vie de référentiel

La politique de cycle de vie à utiliser pour les référentiels créés à l'aide du modèle. Une politique de cycle de vie vous permette de contrôler la gestion du cycle de vie des images d'un référentiel privé. Une politique de cycle de vie est un ensemble d'une ou plusieurs règles, où chaque règle définit une action pour Amazon ECR. Cela fournit un moyen d'automatiser le nettoyage des images de conteneur en faisant expirer des images selon l'ancienneté ou le décompte. Pour plus d'informations, consultez Automatisez le nettoyage des images en utilisant les politiques de cycle de vie d'Amazon ECR.

Balises de ressources

Les balises de ressource sont des métadonnées à appliquer au référentiel afin de mieux les classer et les organiser. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez.

Autorisations IAM pour créer des modèles de création de référentiels

Les autorisations suivantes sont nécessaires pour qu'un principal IAM puisse gérer les modèles de création de référentiels. Cette autorisation doit être accordée à l'aide d'une politique IAM basée sur l'identité.

- `ecr:CreateRepositoryCreationTemplate` : accorde l'autorisation de créer un modèle de création de référentiel.
- `ecr:DeleteRepositoryCreationTemplate` : accorde l'autorisation de supprimer un modèle de création de référentiel.

- `ecr:PutLifecyclePolicy` : accorde l'autorisation de créer une politique de cycle de vie et de l'appliquer à un référentiel. Cette autorisation n'est requise que si le modèle de création de référentiel inclut une politique de cycle de vie.
- `ecr:SetRepositoryPolicy` : accorde l'autorisation de créer une politique d'autorisation pour un référentiel. Cette autorisation n'est requise que si le modèle de création de référentiel inclut une politique de référentiel.
- `ecr:TagResource` : accorde l'autorisation d'ajouter des balises de métadonnées à une ressource. Cette autorisation n'est requise que si le modèle de création de référentiel inclut des balises de ressource.

Création d'un modèle de création de référentiel dans Amazon ECR

Vous pouvez créer un modèle de création de référentiel pour définir les paramètres à utiliser pour les référentiels créés par Amazon ECR en votre nom lors des actions de mise en cache par extraction. Une fois le modèle de création de référentiel créé, les paramètres seront appliqués à tous les nouveaux référentiels créés lors des actions de capture du cache. Cela n'a aucun effet sur les référentiels créés précédemment.

Pour créer un modèle de création de référentiel (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région dans laquelle créer le modèle de création de référentiel.
3. Dans le volet de navigation, choisissez Registre privé, Modèles de création de référentiels.
4. Sur la page Modèles de création de référentiels, choisissez Créer un modèle.
5. Sur la page Étape 1 : définir le modèle, pour Détails du modèle, choisissez Un préfixe spécifique pour appliquer le modèle à un préfixe d'espace de noms de référentiel spécifique ou choisissez N'importe quel préfixe dans votre registre ECR pour appliquer le modèle à tous les référentiels qui ne correspondent à aucun autre modèle dans la région.

    a. Si vous choisissez Un préfixe spécifique pour Préfixe, spécifiez le préfixe de l'espace de noms du référentiel auquel appliquer le modèle. Il y a toujours un `/` supposé/appliqué à la fin du préfixe. Par exemple, le préfixe de `prod` s'appliquerait à tous les référentiels commençant par `prod/`. De la même façon, le préfixe de `prod/team` s'appliquerait à tous les référentiels commençant par `prod/team/`.

b. Si vous choisissez N'importe quel préfixe dans votre registre ECR, le Préfixe sera défini sur `ROOT`.

6. Pour Description du modèle, spécifiez une description facultative pour le modèle, puis choisissez Suivant.
7. Sur la page Étape 2 : ajouter une configuration de création de référentiel, spécifiez la configuration des paramètres de référentiel à appliquer aux référentiels créés à l'aide du modèle.

   a. Pour Mutabilité des balises d'image, choisissez le paramètre mutabilité des balises à utiliser. Pour plus d'informations, consultez Empêcher le remplacement des balises d'image dans Amazon ECR.

      Lorsque Mutable est sélectionné, les balises d'image peuvent être remplacées. Il est recommandé d'utiliser ce paramètre pour les modèles utilisés pour les référentiels créés par des actions de mise en cache par extraction. Cela permet à Amazon ECR de mettre à jour les images mises en cache lorsque les balises sont identiques.

      Lorsque Immuable est sélectionné, les balises d'image ne peuvent pas être remplacées. Une fois que le référentiel est configuré pour balises immuables, un message d'erreur `ImageTagAlreadyExistsException` sera renvoyé en cas de tentative de transmettre une image avec une balise qui existe déjà dans le référentiel. Lorsque l'immuabilité des identifications est activée pour un référentiel, cela affecte toutes les identifications et vous ne pouvez pas rendre certaines d'entre elles inaltérables alors que d'autres ne le sont pas.

   b. Pour la configuration du chiffrement, choisissez le paramètre de chiffrement à utiliser. Pour plus d'informations, consultez Chiffrement au repos.

      Lorsque AES-256 est sélectionné, Amazon ECR utilise le chiffrement côté serveur avec des clés de chiffrement gérées par Amazon Simple Storage Service, ce qui chiffre vos données au repos à l'aide d'un algorithme de chiffrement AES-256 standard du secteur. Ceci est offert sans frais supplémentaires.

      Lorsque AWS KMS est sélectionné, Amazon ECR utilise le chiffrement côté serveur avec des clés stockées dans AWS Key Management Service ().AWS KMS Lorsque vous chiffrez vos données, vous pouvez soit utiliser la clé AWS gérée par défaut, qui est gérée par Amazon ECR, soit spécifier votre propre AWS KMS clé, appelée clé gérée par le client. AWS KMS

> **Note**
>
> Les paramètres de chiffrement pour un référentiel ne peuvent pas être modifiés une fois celui-ci créé.

c. Pour les autorisations de référentiel, spécifiez la politique d'autorisation de référentiel à appliquer aux référentiels créés à l'aide de ce modèle. Vous pouvez éventuellement utiliser le menu déroulant pour sélectionner l'un des exemples JSON pour les cas d'utilisation les plus fréquents. Pour plus d'informations, consultez Politiques relatives aux référentiels privés dans Amazon ECR.

d. Pour la politique de cycle de vie de référentiel, spécifiez la politique de cycle de vie de référentiel à appliquer aux référentiels créés à l'aide de ce modèle. Vous pouvez éventuellement utiliser le menu déroulant pour sélectionner l'un des exemples JSON pour les cas d'utilisation les plus fréquents. Pour plus d'informations, consultez Automatisez le nettoyage des images en utilisant les politiques de cycle de vie d'Amazon ECR.

e. Pour les AWS balises de référentiel, spécifiez les métadonnées, sous forme de paires clé-valeur, à associer aux référentiels créés à l'aide de ce modèle, puis choisissez Next. Pour plus d'informations, consultez Marquage d'un référentiel privé dans Amazon ECR.

8. Sur la page Étape 3 : vérifier et créer, passez en revue les paramètres que vous avez spécifiés pour le modèle de création de référentiel. Choisissez l'option Modifier pour effectuer des changements. Une fois que vous avez terminé, choisissez Créer.

Supprimer un modèle de création de référentiel dans Amazon ECR

Vous pouvez supprimer un modèle de création de référentiel une fois que vous avez fini de l'utiliser. Une fois le modèle de création de référentiel supprimé, les paramètres par défaut de tous les référentiels créés lors d'une action d'extraction du cache seront appliqués.

Pour supprimer un modèle de création de référentiel (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région dans laquelle se trouve le modèle de création de référentiel à supprimer.
3. Dans le volet de navigation, choisissez Registre privé, Modèles de création de référentiels.

4. Sur la page Modèles de création de référentiels, sélectionnez le modèle de création de référentiel à supprimer.
5. Dans le menu déroulant Actions, choisissez Supprimer.

Validation des règles de cache d'extraction dans Amazon ECR

Après avoir créé une règle de cache d'extraction, pour les registres en amont qui nécessitent une authentification, vous pouvez vérifier que la règle fonctionne correctement. Lors de la validation d'une règle de cache d'extraction, Amazon ECR établit une connexion réseau avec le registre en amont, vérifie qu'il peut accéder au secret Secrets Manager contenant les informations d'identification du registre en amont et vérifie que l'authentification a réussi.

Avant de commencer à utiliser vos règles de cache d'extraction, vérifiez que vous disposez des autorisations IAM appropriées. Pour plus d'informations, consultez Autorisations IAM requises pour synchroniser un registre en amont avec un registre privé Amazon ECR.

Pour valider une règle de mise en cache par extraction (AWS Management Console)

Les étapes suivantes montrent comment valider une règle de mise en cache par extraction à l'aide de la console Amazon ECR.

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région contenant la règle de mise en cache par extraction à valider.
3. Dans le panneau de navigation, choisissez Private registry (Registre privé), Pull through cache (Mise en cache par extraction).
4. Sur la page Configuration de la mise en cache par extraction, sélectionnez la règle de mise en cache par extraction à valider. Utilisez ensuite le menu déroulant Actions et choisissez Afficher les détails.
5. Sur la page des détails de la règle de mise en cache par extraction, utilisez le menu déroulant Actions et choisissez Vérifier l'authentification. Amazon ECR affichera une bannière avec le résultat.
6. Répétez ces étapes pour chaque règle de mise en cache par extraction que vous souhaitez valider.

Pour valider une règle de mise en cache par extraction (AWS CLI)

La AWS CLI commande validate-pull-through-cache-rule est utilisée pour valider une règle de cache d'extraction pour un registre privé Amazon ECR. L'exemple suivant utilise le préfixe d'espace de noms `ecr-public`. Remplacez cette valeur par la valeur du préfixe de la règle de mise en cache par extraction à valider.

```
aws ecr validate-pull-through-cache-rule \
     --ecr-repository-prefix ecr-public \
     --region us-east-2
```

Dans la réponse, le paramètre `isValid` indique si la validation a réussi ou non. Si `true`, Amazon ECR a pu accéder au registre en amont et l'authentification a réussi. Si `false`, un problème est survenu et la validation a échoué. Le paramètre `failure` indique la cause.

Extraction d'une image à l'aide d'une règle de cache d'extraction dans Amazon ECR

Les exemples suivants montrent la syntaxe de commande à utiliser lors de l'extraction d'une image à l'aide d'une règle de mise en cache par extraction. Si vous recevez une erreur lors de l'extraction d'une image en amont à l'aide d'une règle de cache par extraction, consultez Résolution des problèmes liés au cache d'extraction dans Amazon ECR pour connaître les erreurs les plus courantes et leurs solutions.

Avant de commencer à utiliser vos règles de cache d'extraction, vérifiez que vous disposez des autorisations IAM appropriées. Pour plus d'informations, consultez Autorisations IAM requises pour synchroniser un registre en amont avec un registre privé Amazon ECR.

> **Note**
>
> Les exemples suivants utilisent les valeurs d'espace de noms du référentiel Amazon ECR par défaut qu'il utilise. AWS Management Console Assurez-vous que vous utilisez l'URI du référentiel privé Amazon ECR que vous avez configuré.

Pour Amazon ECR Public

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/ecr-public/repository_name/
image_name:tag
```

Registre de conteneurs Kubernetes

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/kubernetes/repository_name/
image_name:tag
```

Quay

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/quay/repository_name/
image_name:tag
```

Docker Hub

Pour les images officielles de Docker Hub :

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/docker-hub/
library/image_name:tag
```

> **Note**
>
> Pour les images officielles de Docker Hub, le préfixe `/library` doit être inclus. Pour tous les autres référentiels Docker Hub, vous devez omettre le préfixe `/library`.

Pour toutes les autres images de Docker Hub :

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/docker-hub/repository_name/
image_name:tag
```

GitHub Registre des conteneurs

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/github/repository_name/
image_name:tag
```

Microsoft Azure Container Registry

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/azure/repository_name/
image_name:tag
```

GitLab Registre des conteneurs

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/gitlab/repository_name/
image_name:tag
```

Stockage AWS Secrets Manager secret des informations d'identification de votre référentiel en amont

Lorsque vous créez une règle de mise en cache par extraction pour un référentiel en amont qui nécessite une authentification, vous devez stocker les informations d'identification dans un secret Secrets Manager. L'utilisation d'un secret Secrets Manager peut entraîner des frais. Pour en savoir plus, consultez AWS Secrets Manager Tarification.

Les procédures suivantes expliquent comment créer un secret Secrets Manager pour chaque référentiel en amont pris en charge. Vous pouvez éventuellement utiliser le flux de travail de création de règles de mise en cache par extraction dans la console Amazon ECR pour créer le secret au lieu de le créer à l'aide de la console Secrets Manager. Pour plus d'informations, consultez Création d'une règle de cache d'extraction dans Amazon ECR.

Docker Hub

Pour créer un secret Secrets Manager pour vos informations d'identification Docker Hub (AWS Management Console)

1. Ouvrez la console Secrets Manager à l'adresse https://console.aws.amazon.com/secretsmanager/.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sur la page Choisir un type de secret, procédez comme suit.
   a. Pour Secret type (Type de secret), choisissez Other type of secret (Autre type de secret).
   b. Dans les paires clé/valeur, créez deux lignes pour vos informations d'identification Docker Hub. Vous pouvez stocker jusqu'à 65 536 octets dans le secret.

i. Pour la première paire clé/valeur, spécifiez `username` comme clé et votre nom d'utilisateur Docker Hub comme valeur.

ii. Pour la deuxième paire clé/valeur, spécifiez `accessToken` comme clé et votre jeton d'accès Docker Hub comme valeur. Pour plus d'informations sur la création d'un jeton d'accès Docker Hub, consultez la section Création et gestion des jetons d'accès dans la documentation Docker.

c. Pour la clé de chiffrement, conservez la valeur par défaut de AWS KMS key aws/secretsmanager, puis choisissez Suivant. L'utilisation de cette clé n'entraîne aucun coût. Pour plus d'informations, consultez la section Chiffrement et déchiffrement de secret dans Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

> **Important**
>
> Vous devez utiliser la clé de chiffrement par défaut `aws/secretsmanager` pour chiffrer votre secret. Amazon ECR ne prend pas en charge l'utilisation d'une clé gérée par le client (CMK) pour cela.

4. Sur la page Configurer le secret, procédez comme suit.

a. Saisissez un Secret name (Nom de secret) descriptif et une Description. Les noms des secrets doivent contenir entre 1 et 512 caractères Unicode et être préfixés par `ecr-pullthroughcache/`.

> **Important**
>
> Amazon ECR affiche AWS Management Console uniquement les secrets de Secrets Manager dont les noms utilisent le `ecr-pullthroughcache/` préfixe.

b. (Facultatif) Dans la section Tags (Balises), vous pouvez ajouter une ou plusieurs balises à votre secret. Pour les stratégies de balisage, consultez la Balise secrets Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager . Ne stockez pas les informations sensibles dans des balises car elles ne sont pas chiffrées.

c. (Facultatif) Dans Resource permissions (Permission de la ressource), pour ajouter une stratégie de ressources à votre secret, choisissez Edit permissions (Modification des autorisations). Pour plus d'informations, consultez la rubrique Attacher une politique

d'autorisation à un secret Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

d. (Facultatif) Dans Répliquer le secret, pour répliquer votre secret vers un autre Région AWS, choisissez Répliquer le secret. Vous pouvez reproduire votre secret maintenant ou revenir et le répliquer ultérieurement. Pour plus d'informations, consultez la rubrique Réplication d'un secret vers d'autres régions dans le Guide de l'utilisateur AWS Secrets Manager .

e. Choisissez Suivant.

5. (Facultatif) Dans la page Configure rotation (Configurer la rotation), vous pouvez activer la rotation automatique. Vous pouvez également garder la rotation désactivée pour l'instant, puis l'activer plus tard. Pour plus d'informations, consultez la rubrique Rotation des secrets Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager . Choisissez Suivant.

6. Dans la page Review (Révision), passez en revue vos paramètres, puis choisissez Store (Stocker).

   Secrets Manager revient à la liste des secrets. Si votre nouveau secret n'apparaît pas, choisissez le bouton d'actualisation.

GitHub Container Registry

Pour créer un secret Secrets Manager pour vos informations d'identification du registre des GitHub conteneurs (AWS Management Console)

1. Ouvrez la console Secrets Manager à l'adresse https://console.aws.amazon.com/secretsmanager/.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sur la page Choisir un type de secret, procédez comme suit.

   a. Pour Secret type (Type de secret), choisissez Other type of secret (Autre type de secret).

   b. Dans les paires clé/valeur, créez deux lignes pour vos GitHub informations d'identification. Vous pouvez stocker jusqu'à 65 536 octets dans le secret.

      i. Pour la première paire clé/valeur, spécifiez `username` comme clé et votre GitHub nom d'utilisateur comme valeur.

      ii. Pour la deuxième paire clé/valeur, spécifiez `accessToken` comme clé et votre jeton GitHub d'accès comme valeur. Pour plus d'informations sur la création d'un jeton d'

GitHub accès, consultez la section Gestion de vos jetons d'accès personnels dans la GitHub documentation.

c. Pour la clé de chiffrement, conservez la valeur par défaut de AWS KMS key aws/secretsmanager, puis choisissez Suivant. L'utilisation de cette clé n'entraîne aucun coût. Pour plus d'informations, consultez la section Chiffrement et déchiffrement de secret dans Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

> **Important**
>
> Vous devez utiliser la clé de chiffrement par défaut `aws/secretsmanager` pour chiffrer votre secret. Amazon ECR ne prend pas en charge l'utilisation d'une clé gérée par le client (CMK) pour cela.

4. Sur la page Configure secret (Configurer le secret), procédez comme suit :

a. Saisissez un Secret name (Nom de secret) descriptif et une Description. Les noms des secrets doivent contenir entre 1 et 512 caractères Unicode et être préfixés par `ecr-pullthroughcache/`.

> **Important**
>
> Amazon ECR affiche AWS Management Console uniquement les secrets de Secrets Manager dont les noms utilisent le `ecr-pullthroughcache/` préfixe.

b. (Facultatif) Dans la section Tags (Balises), vous pouvez ajouter une ou plusieurs balises à votre secret. Pour les stratégies de balisage, consultez la Balise secrets Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager . Ne stockez pas les informations sensibles dans des balises car elles ne sont pas chiffrées.

c. (Facultatif) Dans Resource permissions (Permission de la ressource), pour ajouter une stratégie de ressources à votre secret, choisissez Edit permissions (Modification des autorisations). Pour plus d'informations, consultez la rubrique Attacher une politique d'autorisation à un secret Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

d. (Facultatif) Dans Répliquer le secret, pour répliquer votre secret vers un autre Région AWS, choisissez Répliquer le secret. Vous pouvez reproduire votre secret maintenant ou revenir et le répliquer ultérieurement. Pour plus d'informations, consultez la rubrique

Réplication d'un secret vers d'autres régions dans le Guide de l'utilisateur AWS Secrets Manager .

e. Choisissez Suivant.

5. (Facultatif) Dans la page Configure rotation (Configurer la rotation), vous pouvez activer la rotation automatique. Vous pouvez également garder la rotation désactivée pour l'instant, puis l'activer plus tard. Pour plus d'informations, consultez la rubrique Rotation des secrets Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager . Choisissez Suivant.
6. Dans la page Review (Révision), passez en revue vos paramètres, puis choisissez Store (Stocker).

   Secrets Manager revient à la liste des secrets. Si votre nouveau secret n'apparaît pas, choisissez le bouton d'actualisation.

Microsoft Azure Container Registry

Pour créer un secret Secrets Manager pour vos informations d'identification Microsoft Azure Container Registry (AWS Management Console)

1. Ouvrez la console Secrets Manager à l'adresse https://console.aws.amazon.com/secretsmanager/.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sur la page Choisir un type de secret, procédez comme suit.

   a. Pour Secret type (Type de secret), choisissez Other type of secret (Autre type de secret).

   b. Dans les paires clé/valeur, créez deux lignes pour vos informations d'identification Microsoft Azure. Vous pouvez stocker jusqu'à 65 536 octets dans le secret.

      i. Pour la première paire clé/valeur, spécifiez `username` comme clé et votre nom d'utilisateur Microsoft Azure Container Registry comme valeur.

      ii. Pour la deuxième paire clé/valeur, spécifiez `accessToken` comme clé et votre jeton d'accès Microsoft Azure Container Registry comme valeur. Pour plus d'informations sur la création d'un jeton d'accès à Microsoft Azure, consultez la section Créer un jeton - portail dans la documentation Microsoft Azure.

   c. Pour la clé de chiffrement, conservez la valeur par défaut de AWS KMS key aws/secretsmanager, puis choisissez Suivant. L'utilisation de cette clé n'entraîne aucun coût.

Pour plus d'informations, consultez la section Chiffrement et déchiffrement de secret dans Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

> **Important**
>
> Vous devez utiliser la clé de chiffrement par défaut `aws/secretsmanager` pour chiffrer votre secret. Amazon ECR ne prend pas en charge l'utilisation d'une clé gérée par le client (CMK) pour cela.

4. Sur la page Configure secret (Configurer le secret), procédez comme suit :

   a. Saisissez un Secret name (Nom de secret) descriptif et une Description. Les noms des secrets doivent contenir entre 1 et 512 caractères Unicode et être préfixés par `ecr-pullthroughcache/`.

   > **Important**
   >
   > Amazon ECR affiche AWS Management Console uniquement les secrets de Secrets Manager dont les noms utilisent le `ecr-pullthroughcache/` préfixe.

   b. (Facultatif) Dans la section Tags (Balises), vous pouvez ajouter une ou plusieurs balises à votre secret. Pour les stratégies de balisage, consultez la Balise secrets Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager . Ne stockez pas les informations sensibles dans des balises car elles ne sont pas chiffrées.

   c. (Facultatif) Dans Resource permissions (Permission de la ressource), pour ajouter une stratégie de ressources à votre secret, choisissez Edit permissions (Modification des autorisations). Pour plus d'informations, consultez la rubrique Attacher une politique d'autorisation à un secret Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

   d. (Facultatif) Dans Répliquer le secret, pour répliquer votre secret vers un autre Région AWS, choisissez Répliquer le secret. Vous pouvez reproduire votre secret maintenant ou revenir et le répliquer ultérieurement. Pour plus d'informations, consultez la rubrique Réplication d'un secret vers d'autres régions dans le Guide de l'utilisateur AWS Secrets Manager .

   e. Choisissez Suivant.

5. (Facultatif) Dans la page Configure rotation (Configurer la rotation), vous pouvez activer la rotation automatique. Vous pouvez également garder la rotation désactivée pour l'instant,

puis l'activer plus tard. Pour plus d'informations, consultez la rubrique Rotation des secrets Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager . Choisissez Suivant.

6. Dans la page Review (Révision), passez en revue vos paramètres, puis choisissez Store (Stocker).

   Secrets Manager revient à la liste des secrets. Si votre nouveau secret n'apparaît pas, choisissez le bouton d'actualisation.

GitLab Container Registry

Pour créer un secret Secrets Manager pour vos informations d'identification du registre des GitLab conteneurs (AWS Management Console)

1. Ouvrez la console Secrets Manager à l'adresse https://console.aws.amazon.com/secretsmanager/.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sur la page Choisir un type de secret, procédez comme suit.

   a. Pour Secret type (Type de secret), choisissez Other type of secret (Autre type de secret).

   b. Dans les paires clé/valeur, créez deux lignes pour vos GitLab informations d'identification. Vous pouvez stocker jusqu'à 65 536 octets dans le secret.

      i. Pour la première paire clé/valeur, spécifiez `username` comme clé et votre nom d'utilisateur de GitLab Container Registry comme valeur.

      ii. Pour la deuxième paire clé/valeur, spécifiez `accessToken` comme clé et votre jeton d'accès au registre des GitLab conteneurs comme valeur. Pour plus d'informations sur la création d'un jeton d'accès au registre des GitLab conteneurs, voir Jetons d'accès personnels, jetons d'accès de groupe ou jetons d'accès au projet dans la GitLab documentation.

   c. Pour la clé de chiffrement, conservez la valeur par défaut de AWS KMS key aws/secretsmanager, puis choisissez Suivant. L'utilisation de cette clé n'entraîne aucun coût. Pour plus d'informations, consultez la section Chiffrement et déchiffrement de secret dans Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

> **Important**
>
> Vous devez utiliser la clé de chiffrement par défaut `aws/secretsmanager` pour chiffrer votre secret. Amazon ECR ne prend pas en charge l'utilisation d'une clé gérée par le client (CMK) pour cela.

4. Sur la page Configure secret (Configurer le secret), procédez comme suit :

   a. Saisissez un Secret name (Nom de secret) descriptif et une Description. Les noms des secrets doivent contenir entre 1 et 512 caractères Unicode et être préfixés par `ecr-pullthroughcache/`.

   > **Important**
   >
   > Amazon ECR affiche AWS Management Console uniquement les secrets de Secrets Manager dont les noms utilisent le `ecr-pullthroughcache/` préfixe.

   b. (Facultatif) Dans la section Tags (Balises), vous pouvez ajouter une ou plusieurs balises à votre secret. Pour les stratégies de balisage, consultez la Balise secrets Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager . Ne stockez pas les informations sensibles dans des balises car elles ne sont pas chiffrées.

   c. (Facultatif) Dans Resource permissions (Permission de la ressource), pour ajouter une stratégie de ressources à votre secret, choisissez Edit permissions (Modification des autorisations). Pour plus d'informations, consultez la rubrique Attacher une politique d'autorisation à un secret Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager .

   d. (Facultatif) Dans Répliquer le secret, pour répliquer votre secret vers un autre Région AWS, choisissez Répliquer le secret. Vous pouvez reproduire votre secret maintenant ou revenir et le répliquer ultérieurement. Pour plus d'informations, consultez la rubrique Réplication d'un secret vers d'autres régions dans le Guide de l'utilisateur AWS Secrets Manager .

   e. Choisissez Suivant.

5. (Facultatif) Dans la page Configure rotation (Configurer la rotation), vous pouvez activer la rotation automatique. Vous pouvez également garder la rotation désactivée pour l'instant, puis l'activer plus tard. Pour plus d'informations, consultez la rubrique Rotation des secrets Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager . Choisissez Suivant.

6. Dans la page Review (Révision), passez en revue vos paramètres, puis choisissez Store (Stocker).

   Secrets Manager revient à la liste des secrets. Si votre nouveau secret n'apparaît pas, choisissez le bouton d'actualisation.

Résolution des problèmes liés au cache d'extraction dans Amazon ECR

Voici les erreurs les plus courantes que vous pouvez recevoir lors de l'extraction d'une image en amont à l'aide d'une règle de cache par extraction.

Le référentiel n'existe pas

Une erreur indiquant que le référentiel n'existe pas résulte le plus souvent du fait que le référentiel n'existe pas dans votre registre privé Amazon ECR ou du fait que l'autorisation `ecr:CreateRepository` n'est pas accordée à l'IAM principal qui extrait l'image en amont. Pour résoudre cette erreur, vous devez vérifier que l'URI du référentiel dans votre commande d'extraction est correct, que les autorisations IAM requises sont accordées à l'IAM principal qui extrait l'image en amont ou que le référentiel de l'image en amont vers laquelle vous souhaitez effectuer le transfert est créé dans votre registre privé Amazon ECR avant d'effectuer l'extraction d'image en amont. Pour plus d'informations sur les autorisations IAM requises, consultez Autorisations IAM requises pour synchroniser un registre en amont avec un registre privé Amazon ECR

Voici un exemple de cette erreur.

```
Error response from daemon: repository 111122223333.dkr.ecr.us-east-1.amazonaws.com/
ecr-public/amazonlinux/amazonlinux not found: name unknown: The repository with
 name 'ecr-public/amazonlinux/amazonlinux' does not exist in the registry with id
 '111122223333'
```

L'image demandée n'a pas été trouvée

Une erreur indiquant que l'image est introuvable résulte le plus souvent du fait que l'image n'existe pas dans votre registre privé Amazon ECR en amont ou du fait que l'autorisation `ecr:BatchImportUpstreamImage` n'est pas accordée à l'IAM principal qui extrait l'image en amont mais que le référentiel existe déjà dans votre registre privé Amazon ECR. Pour résoudre

cette erreur, vous devez vérifier que le nom de l'image en amont et celui de la balise de l'image sont corrects et qu'ils existent, et que les autorisations IAM requises sont accordées à l'IAM principal qui extrait l'image en amont. Pour plus d'informations sur les autorisations IAM requises, consultez Autorisations IAM requises pour synchroniser un registre en amont avec un registre privé Amazon ECR.

Voici un exemple de cette erreur.

```
Error response from daemon: manifest for 111122223333.dkr.ecr.us-
east-1.amazonaws.com/ecr-public/amazonlinux/amazonlinux:latest not found: manifest
 unknown: Requested image not found
```

403 Interdit lors de l'extraction depuis un dépôt Docker Hub

Lorsque vous extrayez un référentiel Docker Hub étiqueté comme image officielle Docker, vous devez l'inclure `/library/` dans l'URI que vous utilisez. Par exemple, *`aws_account_id`*`.dkr.ecr.`*`region`*`.amazonaws.com/docker-hub/`**`library/`***`image_name:tag`*. Si vous omettez `/library/` pour les images officielles de Docker Hub, une erreur `403 Forbidden` sera renvoyée lorsque vous tenterez d'extraire l'image à l'aide d'une règle de mise en cache par extraction. Pour plus d'informations, consultez Extraction d'une image à l'aide d'une règle de cache d'extraction dans Amazon ECR.

Voici un exemple de cette erreur.

```
Error response from daemon: failed to resolve reference "111122223333.dkr.ecr.us-
west-2.amazonaws.com/docker-hub/amazonlinux:2023": pulling from host
 111122223333.dkr.ecr.us-west-2.amazonaws.com failed with status code [manifests
 2023]: 403 Forbidden
```

Réplication d'images privées dans Amazon ECR

Vous pouvez configurer votre registre privé Amazon ECR pour prendre en charge la réplication de vos référentiels. Amazon ECR prend en charge la réplication inter-régions et inter-comptes. Pour que la réplication inter-comptes se produise, le compte de destination doit configurer une politique d'autorisations de registre pour autoriser la réplication à partir du registre source. Pour plus d'informations, consultez Autorisations de registre privé dans Amazon ECR.

Rubriques

Considérations relatives à la réplication d'images privées

Les informations suivantes doivent être prises en compte lors de l'utilisation de la réplication d'images privées.

- Seul le contenu du référentiel envoyé vers un référentiel après la configuration de la réplication est répliqué. Tout contenu préexistant dans un référentiel n'est pas répliqué. Une fois la réplication configurée pour un référentiel, Amazon ECR synchronise la destination et la source.
- Le nom du référentiel restera le même pour toutes les régions et tous les comptes une fois la réplication effectuée. Amazon ECR ne prend pas en charge la modification du nom du référentiel pendant la réplication.
- La première fois que vous configurez votre registre privé pour la réplication, Amazon ECR crée un rôle IAM lié à un service en votre nom. Le rôle IAM lié à un service octroie au service de réplication Amazon ECR l'autorisation dont il a besoin pour créer des référentiels et répliquer des images dans votre registre. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon ECR.
- Pour que la réplication inter-comptes se produise, la destination du registre privé doit octroyer au registre source l'autorisation de répliquer ses images. Pour ce faire, définissez une politique d'autorisations de registre privé. Pour plus d'informations, consultez Autorisations de registre privé dans Amazon ECR.
- Si la politique d'autorisation d'un registre privé est modifiée pour supprimer une autorisation, toutes les réplications en cours précédemment octroyées peuvent se terminer.

- Pour que la réplication entre régions ait lieu, les comptes source et de destination doivent être intégrés à la région avant toute action de réplication au sein ou vers cette région. Pour plus d'informations, consultez Gestion des régions AWS dans le Référence générale d'Amazon Web Services.
- La réplication entre régions n'est pas prise en charge entre les AWS partitions. Par exemple, un référentiel dans `us-west-2` ne peut pas être répliqué vers `cn-north-1`. Pour plus d'informations sur AWS les partitions, consultez la section Format ARN dans le manuel de référence AWS général.
- La configuration de réplication d'un registre privé peut contenir jusqu'à 25 destinations uniques pour toutes les règles, avec un maximum de 10 règles au total. Chaque règle peut contenir jusqu'à 100 filtres. Cela permet de préciser des règles distinctes pour les référentiels contenant des images utilisées pour la production et le test, par exemple.
- La configuration de réplication prend en charge le filtrage des référentiels dans un registre privé qui sont répliqués en indiquant un préfixe de référentiel. Pour voir un exemple, consultez Exemple : Configuration de la réplication inter-régions à l'aide d'un filtre de référentiel.
- Une action de réplication ne se produit qu'une fois par poussée d'image. Par exemple, si vous avez configuré la réplication inter-régions à partir de `us-west-2` sur `us-east-1` et à partir de `us-east-1` sur `us-east-2`, une image poussée vers `us-west-2` répliquera uniquement sur `us-east-1`, elle ne se répliquera pas à nouveau sur `us-east-2`. Ce comportement s'applique à la fois à la réplication inter-régions et inter-comptes.
- La majorité des images se répliquent en moins de 30 minutes, mais dans de rares cas, la réplication peut prendre plus de temps.
- La réplication du registre n'effectue aucune action de suppression. Les images et les référentiels répliqués peuvent être supprimés manuellement lorsqu'ils ne sont plus utilisés.
- Les politiques de référentiel, notamment les politiques IAM et les politiques de cycle de vie, ne sont pas répliquées et n'ont aucun effet autre que sur le référentiel pour lequel elles sont définies.
- Les paramètres du référentiel ne sont pas répliqués. Les paramètres d'immuabilité des étiquettes, d'analyse des images et de chiffrement KMS sont désactivés par défaut sur tous les référentiels créés en raison d'une action de réplication. Le paramètre d'immuabilité des étiquettes et de numérisation des images pourra être modifié après la création du référentiel. Toutefois, le paramètre s'appliquera uniquement aux images poussées après la modification du paramètre.
- Si l'immuabilité des étiquettes est activée sur un référentiel et qu'une image qui utilise la même étiquette qu'une image existante est répliquée, l'image sera répliquée, mais elle ne contiendra pas l'étiquette dupliquée. Cela pourrait entraîner le non-étiquetage de l'image.

Exemples de réplication d'images privées pour Amazon ECR

Les exemples suivants montrent des cas d'utilisation courants de la réplication d'images privées. Si vous configurez la réplication à l'aide du AWS CLI, vous pouvez utiliser les exemples JSON comme point de départ lorsque vous créez votre fichier JSON. Si vous configurez la réplication à l'aide du AWS Management Console, vous verrez un JSON similaire lorsque vous examinerez votre règle de réplication sur la page Révision et envoi.

Exemple : configuration de la réplication inter-régions sur une même région de destination

L'exemple suivant illustre la configuration de la réplication inter-régions dans un registre unique. Cet exemple suppose que votre ID de compte est `111122223333` et que vous indiquez cette configuration de réplication dans une région autre que `us-west-2`.

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "us-west-2",
                    "registryId": "111122223333"
                }
            ]
        }
    ]
}
```

Exemple : Configuration de la réplication inter-régions à l'aide d'un filtre de référentiel

L'exemple suivant illustre la configuration de la réplication inter-régions pour les référentiels qui correspondent à une valeur de nom de préfixe. Cet exemple suppose que votre ID de compte est `111122223333`, que vous indiquez cette configuration de réplication dans une région autre que `us-west-1` et dispose de référentiels avec un préfixe de `prod`.

```
{
 "rules": [{
```

```
  "destinations": [{
   "region": "us-west-1",
   "registryId": "111122223333"
  }],
  "repositoryFilters": [{
   "filter": "prod",
   "filterType": "PREFIX_MATCH"
  }]
 }]
}
```

Exemple : Configuration de la réplication inter-régions vers plusieurs régions de destination

L'exemple suivant illustre la configuration de la réplication inter-régions dans un registre unique. Cet exemple suppose que votre ID de compte est `111122223333` et que vous indiquez cette configuration de réplication dans une région autre que `us-west-1` ou `us-west-2`.

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "us-west-1",
                    "registryId": "111122223333"
                },
                {
                    "region": "us-west-2",
                    "registryId": "111122223333"
                }
            ]
        }
    ]
}
```

Exemple : Configuration de la réplication inter-comptes

L'exemple suivant illustre la configuration de la réplication inter-comptes pour votre registre. Cet exemple configure la réplication vers le compte `444455556666`et vers la région `us-west-2`.

> **Important**
>
> Pour que la réplication inter-comptes se produise, le compte de destination doit configurer une politique d'autorisations de registre pour autoriser la réplication. Pour plus d'informations, consultez Autorisations de registre privé dans Amazon ECR.

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "us-west-2",
                    "registryId": "444455556666"
                }
            ]
        }
    ]
}
```

Exemple : Spécification de plusieurs règles dans une configuration

L'image suivante présente un exemple de configuration de plusieurs règles de réplication pour votre registre. Cet exemple configure la réplication pour le compte *111122223333* avec une seule règle qui réplique les référentiels avec un préfixe de `prod` vers la région `us-west-2` et les référentiels avec un préfixe de `test` vers la région `us-east-2`. Une configuration de réplication peut contenir jusqu'à 10 règles, chaque règle indiquant jusqu'à 25 destinations.

```
{
 "rules": [{
   "destinations": [{
    "region": "us-west-2",
    "registryId": "111122223333"
   }],
   "repositoryFilters": [{
    "filter": "prod",
    "filterType": "PREFIX_MATCH"
   }]
  },
  {
```

```
    "destinations": [{
     "region": "us-east-2",
     "registryId": "111122223333"
    }],
    "repositoryFilters": [{
     "filter": "test",
     "filterType": "PREFIX_MATCH"
    }]
   }
  ]
}
```

Configuration de la réplication d'images privées dans Amazon ECR

Configurez la réplication par région pour votre registre privé. Vous pouvez configurer la réplication entre régions ou entre comptes.

Pour obtenir des exemples sur la manière dont la réplication est couramment utilisée, consultez Exemples de réplication d'images privées pour Amazon ECR.

Configurer les paramètres de réplication du registre (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région pour laquelle vous souhaitez configurer les paramètres de réplication du registre.
3. Dans le panneau de navigation, choisissez Registre de schémas.
4. Dans la page Registre privé, dans la section Réplication, choisissez Modifier.
5. Dans la page Réplication, choisissez Ajouter une règle de réplication.
6. Dans la page Types de destination, choisissez si vous souhaitez activer la réplication inter-régions, la réplication inter-comptes ou les deux, puis choisissez Suivant.
7. Si la réplication inter-régions est activée, alors pour Configuration des régions de destination, choisissez une ou plusieurs régions de destination, puis choisissez Suivant.
8. Si la réplication inter-comptes est activée, alors pour Réplication inter-comptes, choisissez le paramètre de réplication inter-comptes pour le registre. Pour Compte de destination, saisissez l'ID de compte pour le compte de destination et une ou plusieurs régions de destination à répliquer. Choisissez Compte de destination + pour configurer des comptes supplémentaires en tant que destinations de réplication.

> **Important**
>
> Pour que la réplication inter-comptes se produise, le compte de destination doit configurer une politique d'autorisations de registre pour autoriser la réplication. Pour plus d'informations, consultez Autorisations de registre privé dans Amazon ECR.

9. (Facultatif) Dans l'onglet Ajouter des filtres, indiquez un ou plusieurs filtres pour la règle de réplication, puis choisissez Ajouter. Répétez cette étape pour chaque filtre que vous souhaitez associer à l'action de réplication. Un filtre doit être spécifié en tant que préfixe de nom de référentiel. Si aucun filtre n'est ajouté, le contenu de tous les référentiels est répliqué. Choisissez Suivant lorsque tous les filtres auront été ajoutés.
10. Dans la page Examen et soumission, examinez la configuration de la règle de réplication, puis choisissez Soumettre une règle.

Configurer les paramètres de réplication du registre (AWS CLI)

1. Créez un fichier JSON contenant les règles de réplication à définir pour votre registre. Une configuration de réplication peut contenir jusqu'à 10 règles, avec jusqu'à 25 destinations uniques pour toutes les règles et 100 filtres par règle. Pour configurer la réplication inter-régions dans votre propre compte, indiquez votre propre ID de compte. Pour obtenir plus d'exemples, consultez Exemples de réplication d'images privées pour Amazon ECR.

```
{
 "rules": [{
  "destinations": [{
   "region": "destination_region",
   "registryId": "destination_accountId"
  }],
  "repositoryFilters": [{
   "filter": "repository_prefix_name",
   "filterType": "PREFIX_MATCH"
  }]
 }]
}
```

2. Créez une configuration de réplication pour votre registre.

```
aws ecr put-replication-configuration \
```

```
    --replication-configuration file://replication-settings.json \
    --region us-west-2
```

3. Confirmez les paramètres de votre registre.

```
aws ecr describe-registry \
    --region us-west-2
```

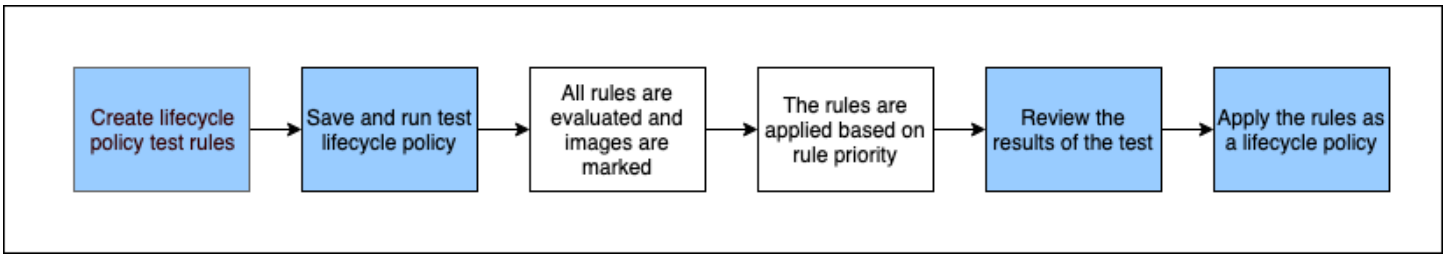
Automatisez le nettoyage des images en utilisant les politiques de cycle de vie d'Amazon ECR

Les politiques de cycle de vie Amazon ECR vous permettent de contrôler la gestion du cycle de vie des images d'un référentiel privé. Une politique de cycle de vie contient une ou plusieurs règles, et chaque règle définit une action pour Amazon ECR. Selon les critères d'expiration définis dans la politique de cycle de vie, les images expirent en fonction de leur âge ou de leur nombre dans les 24 heures. Lorsqu'Amazon ECR exécute une action basée sur une politique de cycle de vie, cette action est capturée en tant qu'événement dans AWS CloudTrail. Pour plus d'informations, consultez Journalisation des actions Amazon ECR avec AWS CloudTrail.

Fonctionnement des politiques de cycle de vie

Une politique de cycle de vie se compose d'une ou de plusieurs règles qui déterminent quelles sont images d'un référentiel qui doivent expirer. Lorsque vous envisagez d'utiliser des politiques de cycle de vie, il est important d'afficher l'aperçu de la politique de cycle de vie pour confirmer quelles sont les images que la politique de cycle de vie doit faire expirer avant de l'appliquer à un référentiel. Une fois qu'une politique de cycle de vie est appliquée à un référentiel, vous pouvez vous attendre à ce que les images concernées expireront dans les 24 heures après avoir satisfait aux critères d'expiration. Lorsque Amazon ECR exécute une action basée sur une stratégie de cycle de vie, elle est capturée en tant qu'événement dans AWS CloudTrail. Pour plus d'informations, consultez Journalisation des actions Amazon ECR avec AWS CloudTrail.

Le diagramme suivant illustre un flux de travail de la politique du cycle de vie.



1. Créez une ou plusieurs règles de test.
2. Enregistrez les règles de test et exécutez l'aperçu.
3. L'évaluateur de la politique de cycle de vie examine toutes les règles et marque les images auxquelles chaque règle doit s'appliquer.

4. L'évaluateur de la politique de cycle de vie applique ensuite les règles, en fonction de la priorité de la règle, et affiche les images du référentiel définies comme expirées.
5. Examinez les résultats du test, en vérifiant que les images marquées comme ayant expiré correspondent à ce que vous souhaitiez faire expirer.
6. Appliquez les règles de test en tant que politique de cycle de vie du référentiel.
7. Après avoir créé la politique de cycle de vie, vous pouvez vous attendre à ce que les images concernées expireront dans les 24 heures après avoir satisfait aux critères d'expiration.

Règles d'évaluation de la politique de cycle de vie

Cet évaluateur de politique de cycle de vie analyse le code JSON en texte brut de la politique de cycle de vie, évalue toutes les règles, puis applique ces règles aux images en fonction de la priorité des règles dans le référentiel. Ce qui suit explique la logique de l'évaluateur de la politique de cycle de vie plus en détails. Pour obtenir des exemples, consultez Exemples de politiques de cycle de vie dans Amazon ECR.

- Toutes les règles sont évaluées en même temps, quelle que soit la priorité de la règle. Lorsque l'évaluation de toutes les règles est terminée, les règles sont ensuite appliquées en fonction de leur priorité.
- Une image est expirée par exactement des règles un ou zéro.
- Une image qui correspond aux exigences d'étiquetage d'une règle ne peut pas être expirée par une règle avec une priorité plus basse.
- Les règles ne peuvent jamais marquer des images auxquelles correspondent des règles de priorité plus haute, mais elles peuvent quand même les identifier si elles n'ont pas expiré.
- L'ensemble de règles doit contenir un ensemble unique de préfixes d'étiquette.
- Une seule règle est autorisée à sélectionner des images non étiquetées.
- Si une image est référencée par une liste de manifestes, elle ne peut pas expirer sans que la liste des manifestes ne soit d'abord supprimée.
- L'expiration est toujours classée par `pushed_at_time`, et les images plus anciennes expirent toujours avant les images plus récentes.
- Une règle de politique de cycle de vie peut spécifier soit `tagPatternList`, soit `tagPrefixList`, mais pas les deux. Cependant, une politique de cycle de vie peut contenir plusieurs règles dans lesquelles différentes règles utilisent à la fois des listes de modèles et de préfixes.

- Les paramètres `tagPatternList` ou `tagPrefixList` ne peuvent être utilisés que si `tagStatus` est `tagged`.
- Lors de l'utilisation de `tagPatternList`, une image fait l'objet d'une correspondance si elle correspond au filtre de caractère générique. Par exemple, si un filtre `prod*` est appliqué, l'image correspond aux référentiels dont le nom commence par `prod`, tel que `prod`, `prod1` ou `production-team1`. De même, si un filtre `*prod*` est appliqué, l'image correspond aux référentiels dont le nom contient une valeur `prod`, telle que `repo-production` ou `prod-team`.

  > **Important**
  >
  > Il existe une limite maximale de quatre caractères génériques (*) par chaîne. Par exemple, `["*test*1*2*3", "test*1*2*3*"]` est valide mais `["test*1*2*3*4*5*6"]` ne l'est pas.

- Lorsque vous utilisez `tagPrefixList`, une image fait l'objet d'une correspondance si toutes les balises dans la valeur `tagPrefixList` correspondent à une des balises de l'image.
- Le paramètre `countUnit` est uniquement utilisé si `countType` a pour valeur `sinceImagePushed`.
- Avec `countType = imageCountMoreThan`, les images sont triées de la plus récente à la plus ancienne en fonction de la valeur de `pushed_at_time`, et toutes les images supérieures au décompte indiqué expirent.
- Avec `countType = sinceImagePushed`, toutes les images dont la valeur de `pushed_at_time` est plus ancienne que le nombre de jours indiqué en fonction de `countNumber` expirent.

Création d'un aperçu de la politique de cycle de vie dans Amazon ECR

Vous pouvez utiliser un aperçu de la politique de cycle de vie pour voir l'impact d'une politique de cycle de vie sur un référentiel d'images avant de l'appliquer. Il est recommandé d'effectuer un aperçu avant d'appliquer une politique de cycle de vie à un référentiel.

> **Note**
>
> Si vous utilisez la réplication Amazon ECR pour créer des copies d'un référentiel dans différentes régions ou comptes, notez qu'une politique de cycle de vie ne peut agir que sur les référentiels de la région dans laquelle il a été créé. Par conséquent, si la réplication est

activée, vous pouvez envisager de créer une politique de cycle de vie dans chaque région et chaque compte vers lesquels vous répliquez vos référentiels.

Créer une politique de cycle de vie (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région qui contient le référentiel sur lequel exécuter un aperçu de la politique de cycle de vie.
3. Dans le volet de navigation, sous Registre privé, choisissez Référentiels.
4. Sur la page Référentiels privés, sélectionnez un référentiel et utilisez le menu déroulant Actions pour choisir les Politiques de cycle de vie.
5. Sur la page des règles de la politique de cycle de vie du référentiel, choisissez Modifier les règles de test, Créer une règle.
6. Spécifiez les détails suivants pour chaque règle de politique de cycle de vie de test.

    a. Pour Priorité d'une règle, saisissez un nombre pour la priorité de la règle. La priorité d'une règle détermine l'ordre dans lequel les règles de politique de cycle de vie sont appliquées.

    b. Pour Description de la règle, saisissez une description pour la règle de la politique de cycle de vie.

    c. Pour Statut d'image, choisissez Balisée (correspondance par caractère générique), Balisée (correspondance par préfixe), Non balisée ou Toute.

    d. Si vous choisissez Balisée (correspondance par caractère générique) pour Statut d'image, vous pouvez alors spécifier une liste de balises d'image avec un caractère générique (*) sur lesquelles prendre des mesures conformément à votre politique de cycle de vie pour Spécifier les balises pour la correspondance par caractère générique. Par exemple, si vos images sont balisées comme `prod`, `prod1`, `prod2`, et ainsi de suite, vous devrez spécifier `prod*` afin d'appliquer des mesures à toutes les images. Si vous précisez plusieurs étiquettes, seules les images portant toutes les étiquettes précisées seront sélectionnées.

    > **Important**
    >
    > Il existe une limite maximale de quatre caractères génériques (*) par chaîne. Par exemple, `["*test*1*2*3", "test*1*2*3*"]` est valide mais `["test*1*2*3*4*5*6"]` ne l'est pas.

e. Si vous choisissez Balisée (correspondance par préfixe) pour Statut d'image, vous pouvez alors spécifier une liste de balises d'image sur lesquelles prendre des mesures conformément à votre politique de cycle de vie pour Spécifier les balises pour la correspondance par préfixe.

f. Pour Critères de correspondance, choisissez Depuis la transmission de l'image ou Décompte d'images supérieur à, puis spécifiez une valeur.

g. Choisissez Enregistrer.

7. Créez des règles de politique de cycle de vie de test supplémentaires en répétant les étapes 5 à 7.
8. Pour exécuter l'aperçu de la politique de cycle de vie, choisissez Enregistrer et exécuter le test.
9. Sous Correspondances d'images pour les règles de cycle de vie test), vérifiez l'impact de l'aperçu de votre politique de cycle de vie.
10. Si les résultats de l'aperçu sont satisfaisants, choisissez Appliquer la politique de cycle de vie pour créer une politique de cycle de vie avec les règles indiquées. Après avoir créé une politique de cycle de vie, les images concernées expireront dans les 24 heures.
11. Si vous n'êtes pas satisfait des résultats de l'aperçu, vous pouvez supprimer une ou plusieurs règles de cycle de vie du test et créer une ou plusieurs règles pour les remplacer, puis répéter le test.

Création d'une politique de cycle de vie pour un référentiel dans Amazon ECR

Utilisez une politique de cycle de vie pour créer un ensemble de règles qui expirent les images de référentiel non utilisées. Après avoir créé une politique de cycle de vie, les images concernées expirent dans les 24 heures.

> **Note**
>
> Si vous utilisez la réplication Amazon ECR pour créer des copies d'un référentiel dans différentes régions ou comptes, notez qu'une politique de cycle de vie ne peut agir que sur les référentiels de la région dans laquelle il a été créé. Par conséquent, si la réplication est activée, vous pouvez envisager de créer une politique de cycle de vie dans chaque région et chaque compte vers lesquels vous répliquez vos référentiels.

Prérequis

Bonne pratique : créez un aperçu de la politique de cycle de vie pour vérifier que les images expirées conformément à vos règles de politique de cycle de vie correspondent à vos attentes. Pour obtenir des instructions, veuillez consulter Création d'un aperçu de la politique de cycle de vie dans Amazon ECR.

Créer une politique de cycle de vie (AWS Management Console)

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/repositories.
2. Dans la barre de navigation, choisissez la région qui contient le référentiel sur lequel créer une politique de cycle de vie.
3. Dans le volet de navigation, sous Registre privé, choisissez Référentiels.
4. Sur la page Référentiels privés, sélectionnez un référentiel et utilisez le menu déroulant Actions pour choisir les Politiques de cycle de vie.
5. Sur la page des règles de la politique de cycle de vie du référentiel, choisissez Créer une règle.
6. Saisissez les détails suivants pour votre règle de politique de cycle de vie.

    a. Pour Priorité d'une règle, saisissez un nombre pour la priorité de la règle. La priorité d'une règle détermine l'ordre dans lequel les règles de politique de cycle de vie sont appliquées.

    b. Pour Description de la règle, saisissez une description pour la règle de la politique de cycle de vie.

    c. Pour Statut d'image, choisissez Balisée (correspondance par caractère générique), Balisée (correspondance par préfixe), Non balisée ou Toute.

    d. Si vous choisissez Balisée (correspondance par caractère générique) pour Statut d'image, vous pouvez alors spécifier une liste de balises d'image avec un caractère générique (*) sur lesquelles prendre des mesures conformément à votre politique de cycle de vie pour Spécifier les balises pour la correspondance par caractère générique. Par exemple, si vos images sont balisées comme `prod`, `prod1`, `prod2`, et ainsi de suite, vous devrez spécifier `prod*` afin d'appliquer des mesures à toutes les images. Si vous précisez plusieurs étiquettes, seules les images portant toutes les étiquettes précisées seront sélectionnées.

> **Important**
>
> Il existe une limite maximale de quatre caractères génériques (*) par chaîne. Par exemple, `["*test*1*2*3", "test*1*2*3*"]` est valide mais `["test*1*2*3*4*5*6"]` ne l'est pas.

e. Si vous choisissez Balisée (correspondance par préfixe) pour Statut d'image, vous pouvez alors spécifier une liste de balises d'image sur lesquelles prendre des mesures conformément à votre politique de cycle de vie pour Spécifier les balises pour la correspondance par préfixe.

f. Pour Critères de correspondance, choisissez Depuis la transmission de l'image ou Décompte d'images supérieur à, puis spécifiez une valeur.

g. Choisissez Enregistrer.

7. Créez des règles de politique de cycle de vie supplémentaires en répétant les étapes 5 à 7.

Créer une politique de cycle de vie (AWS CLI)

1. Obtenez le nom du référentiel pour lequel créer la politique de cycle de vie.

```
aws ecr describe-repositories
```

2. Créez un fichier local nommé `policy.json` avec le contenu de la politique de cycle de vie. Pour obtenir des exemples de politiques de cycle de vie, consultez Exemples de politiques de cycle de vie dans Amazon ECR.

3. Créez une politique de cycle de vie en indiquant le nom du référentiel, puis référencez le fichier JSON de la politique de cycle de vie que vous avez créé.

```
aws ecr put-lifecycle-policy \
      --repository-name repository-name \
      --lifecycle-policy-text file://policy.json
```

Exemples de politiques de cycle de vie dans Amazon ECR

Vous trouverez ci-dessous des exemples de politiques de cycle de vie illustrant la syntaxe.

Pour plus d'informations sur les propriétés des politiques, consultezPropriétés de la politique de cycle de vie dans Amazon ECR. Pour obtenir des instructions sur la création d'une politique de cycle de vie à l'aide du AWS CLI, consultezCréer une politique de cycle de vie (AWS CLI).

Modèle de politique de cycle de vie

Le contenu de votre politique de cycle de vie est évalué avant d'être associé à un référentiel. Voici le modèle de syntaxe JSON pour la politique de cycle de vie.

```
{
        "rules": [
            {
                "rulePriority": integer,
                "description": "string",
                "selection": {
                    "tagStatus": "tagged"|"untagged"|"any",
                    "tagPatternList": list<string>,
                    "tagPrefixList": list<string>,
                    "countType": "imageCountMoreThan"|"sinceImagePushed",
                    "countUnit": "string",
                    "countNumber": integer
                },
                "action": {
                    "type": "expire"
                }
            }
        ]
    }
```

Filtrer sur l'ancienneté des images

Voici un exemple de syntaxe d'une politique de cycle de vie qui fait expirer les images qui ont une balise commençant par `prod` à l'aide d'une `tagPatternList` de `prod*` qui ont également plus de 14 jours d'ancienneté.

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Expire images older than 14 days",
            "selection": {
                "tagStatus": "tagged",
```

```
                "tagPatternList": ["prod*"],
                "countType": "sinceImagePushed",
                "countUnit": "days",
                "countNumber": 14
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

Filtrer sur le décompte d'images

Voici un exemple de syntaxe d'une politique de cycle de vie qui conserve uniquement une image non balisée et fait expirer toutes les autres.

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Keep only one untagged image, expire all others",
            "selection": {
                "tagStatus": "untagged",
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

Filtrer sur plusieurs règles

Les exemples suivants utilisent plusieurs règles dans une politique de cycle de vie. Des exemples de référentiel et de politique de cycle de vie sont fournis avec une explication du résultat.

Exemple A

Contenu du référentiel :

- Image A, Taglist: ["beta-1", "prod-1"], Transmise : il y a 10 jours
- Image B, Taglist: ["beta-2", "prod-2"], Transmise : il y a 9 jours
- Image C, Taglist: ["beta-3"], Transmise : il y a 8 jours

Texte de la politique de cycle de vie :

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["prod*"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        },
        {
            "rulePriority": 2,
            "description": "Rule 2",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["beta*"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La logique de cette politique de cycle de vie serait :

- La règle 1 identifie les images étiquetées avec le préfixe `prod`. Elle doit marquer les images, en commençant par la plus ancienne, jusqu'à ce qu'il reste une image qui corresponde, ou moins. Elle marque l'image A pour expiration.
- La règle 2 identifie les images étiquetées avec le préfixe `beta`. Elle doit marquer les images, en commençant par la plus ancienne, jusqu'à ce qu'il reste une image qui corresponde, ou moins. Elle marque l'image A et l'image B pour expiration. Cependant, l'image A a déjà été examinée par la règle 1 et, si l'image B expirait, cela violerait la règle 1. L'image B est donc ignorée.
- Résultat : L'image A est expirée.

Exemple B

Il s'agit du même référentiel que dans l'exemple précédent, mais l'ordre de priorité des règles est modifié pour illustrer le résultat.

Contenu du référentiel :

- Image A, Taglist: ["beta-1", "prod-1"], Transmise : il y a 10 jours
- Image B, Taglist: ["beta-2", "prod-2"], Transmise : il y a 9 jours
- Image C, Taglist: ["beta-3"], Transmise : il y a 8 jours

Texte de la politique de cycle de vie :

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["beta*"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        },
        {
            "rulePriority": 2,
```

```
            "description": "Rule 2",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["prod*"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La logique de cette politique de cycle de vie serait :

- La règle 1 identifie les images étiquetées avec le préfixe `beta`. Elle doit marquer les images, en commençant par la plus ancienne, jusqu'à ce qu'il reste une image qui corresponde, ou moins. Elle examine les trois images, et marque l'image A et l'image B pour expiration.
- La règle 2 identifie les images étiquetées avec le préfixe `prod`. Elle doit marquer les images, en commençant par la plus ancienne, jusqu'à ce qu'il reste une image qui corresponde, ou moins. Elle n'examine aucune image, car toutes les images disponibles ont déjà été examinées par la règle 1. Elle ne marque donc aucune image supplémentaire.
- Résultat : Les images A et B sont expirées.

Filtrer sur plusieurs étiquettes dans une seule règle

Les exemples suivants indiquent la syntaxe de la politique de cycle de vie pour plusieurs modèles de balises dans une seule règle. Des exemples de référentiel et de politique de cycle de vie sont fournis avec une explication du résultat.

Exemple A

Lorsque plusieurs modèles de balises sont indiqués dans une seule règle, les images doivent correspondre à tous les modèles de balises répertoriés.

Contenu du référentiel :

- Image A, Taglist: ["alpha-1"], Transmise : il y a 12 jours
- Image B, Taglist: ["beta-1"], Transmise : il y a 11 jours

- Image C, Taglist: ["alpha-2", "beta-2"],Transmise : il y a 10 jours
- Image D, Taglist: ["alpha-3"], Transmise : il y a 4 jours
- Image E, Taglist: ["beta-3"], Transmise : il y a 3 jours
- Image F, Taglist: ["alpha-4", "beta-4"],Transmise : il y a 2 jours

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["alpha*", "beta*"],
                "countType": "sinceImagePushed",
                "countNumber": 5,
                "countUnit": "days"
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La logique de cette politique de cycle de vie serait :

- La règle 1 identifie les images balisées par les préfixes `alpha` et `beta`. Elle examine les images C et F. Elle doit marquer les images de plus de cinq jours, ce qui est le cas de l'image C.
- Résultat : L'image C est expirée.

Exemple B

L'exemple suivant montre que des étiquettes ne sont pas exclusives.

Contenu du référentiel :

- Image A, Taglist: ["alpha-1", "beta-1", "gamma-1"], Transmise : il y a 10 jours
- Image B, Taglist: ["alpha-2", "beta-2"], Transmise : il y a 9 jours

- Image C, Taglist: ["alpha-3", "beta-3", "gamma-2"], Transmise : il y a 8 jours

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["alpha*", "beta*"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La logique de cette politique de cycle de vie serait :

- La règle 1 identifie les images balisées par les préfixes `alpha` et `beta`. Elle examine toutes les images. Elle doit marquer les images, en commençant par la plus ancienne, jusqu'à ce qu'il reste une image qui corresponde, ou moins. Elle marque les images A et B pour expiration.
- Résultat : Les images A et B sont expirées.

Filtrer sur toutes les images

Les exemples de politique de cycle de vie suivants indiquent toutes les images avec différents filtres. Des exemples de référentiel et de politique de cycle de vie sont fournis avec une explication du résultat.

Exemple A

Voici la syntaxe d'une politique de cycle de vie qui applique toutes les règles, mais conserve uniquement une image et fait expirer toutes les autres.

Contenu du référentiel :

- Image A, Taglist: ["alpha-1"], Transmise : il y a 4 jours
- Image B, Taglist: ["beta-1"], Transmise : il y a 3 jours
- Image C, Taglist: [], Transmise : il y a 2 jours
- Image D, Taglist: ["alpha-2"], Transmise : il y a 1 jour

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "any",
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La logique de cette politique de cycle de vie serait :

- La règle 1 identifie toutes les images. Elle examine les images A, B, C et D. Elle doit faire expirer toutes les images, à l'exception de la plus récente. Elle marque les images A, B et C pour expiration.
- Résultat : Les images A, B et C expirent.

Exemple B

L'exemple suivant illustre une politique de cycle de vie qui combine tous les types de règles dans une seule politique.

Contenu du référentiel :

- Image A, Taglist: ["alpha-1", "beta-1"], Transmise : il y a 4 jours
- Image B, Taglist: [], Transmise : il y a 3 jours

- Image C, Taglist: ["alpha-2"],Transmise : il y a 2 jours
- Image D, Taglist: ["git hash"], Transmise : il y a 1 jour
- Image E, Taglist: [], Transmise : il y a 1 jour

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["alpha"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        },
        {
            "rulePriority": 2,
            "description": "Rule 2",
            "selection": {
                "tagStatus": "untagged",
                "countType": "sinceImagePushed",
                "countUnit": "days",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        },
        {
            "rulePriority": 3,
            "description": "Rule 3",
            "selection": {
                "tagStatus": "any",
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
```

```
            }
        }
    ]
}
```

La logique de cette politique de cycle de vie serait :

- La règle 1 identifie les images étiquetées avec le préfixe `alpha`. Elle identifie les images A et C. Elle doit conserver l'image la plus récente et marquer les autres pour expiration. Elle marque l'image A pour expiration.
- La règle 2 identifie les images non étiquetées. Elle identifie les images B et E. Elle doit marquer toutes les images datant de plus d'un jour pour expiration. Elle marque l'image B pour expiration.
- La règle 3 identifie toutes les images. Elle identifie les images A, B, C, D et E. Elle doit conserver l'image la plus récente et marquer les autres pour expiration. Cependant, elle ne peut pas marquer les images A, B, C ou E, car elles ont été identifiées par des règles de priorité plus haute. Elle marque l'image D pour expiration.
- Résultat : Les images A, B et D expirent.

Propriétés de la politique de cycle de vie dans Amazon ECR

Les politiques de cycle de vie présentent les propriétés suivantes.

Pour consulter des exemples de politiques relatives au cycle de vie, consultezExemples de politiques de cycle de vie dans Amazon ECR. Pour obtenir des instructions sur la création d'une politique de cycle de vie à l'aide du AWS CLI, consultezCréer une politique de cycle de vie (AWS CLI).

Priorité de la règle

`rulePriority`

Type : entier

Obligatoire : oui

Définit l'ordre dans lequel les règles sont évaluées, de la priorité la plus basse à la plus haute. Une règle de politique de cycle de vie avec une priorité de 1 est appliquée en premier, une règle avec une priorité de 2 est appliquée ensuite, et ainsi de suite. Lorsque vous ajoutez des règles à une politique de cycle de vie, vous devez attribuer à chacune une valeur unique

de `rulePriority`. Les valeurs n'ont pas besoin d'être séquentielles entre les règles d'une politique. Une règle avec une valeur `tagStatus` de `any` doit avoir la valeur la plus élevée pour `rulePriority` et être évaluée en dernier.

Description

`description`

Type : chaîne

Obligatoire : non

(Facultatif) Décrit l'objectif d'une règle dans une politique de cycle de vie.

État de l'étiquetage

`tagStatus`

Type : chaîne

Obligatoire : oui

Détermine si la règle de la politique de cycle de vie que vous ajoutez précise une étiquette pour une image. Les options acceptables sont `tagged`, `untagged` ou `any`. Si vous précisez `any`, la règle s'appliquera à toutes les images évaluées par la règle. Si vous précisez `tagged`, vous devrez également indiquer une valeur `tagPrefixList`. Si vous précisez `untagged`, vous devrez omettre `tagPrefixList`.

Liste des modèles de balises

`tagPatternList`

Type : list[string]

Obligatoire : oui, si `tagStatus` est défini sur balisé et `tagPrefixList` n'est pas spécifiée

Lors de la création d'une politique de cycle de vie pour les images balisées, il est recommandé d'utiliser une `tagPatternList` pour spécifier les balises à expirer. Précisez une liste séparée par des virgules de modèles de balises d'image pouvant contenir des caractères génériques (`*`)

sur lesquels exécuter une action avec votre politique de cycle de vie. Par exemple, si vos images sont balisées comme `prod`, `prod1`, `prod2`, et ainsi de suite, vous devrez utiliser le modèle de balise `prod*` pour les spécifier toutes. Si vous précisez plusieurs étiquettes, seules les images portant toutes les étiquettes précisées seront sélectionnées.

> **Important**
>
> Il existe une limite maximale de quatre caractères génériques (*) par chaîne. Par exemple, `["*test*1*2*3", "test*1*2*3*"]` est valide mais `["test*1*2*3*4*5*6"]` ne l'est pas.

Liste des préfixes d'étiquette

`tagPrefixList`

Type : list[string]

Obligatoire : oui, si `tagStatus` est défini sur balisé et `tagPatternList` n'est pas spécifiée

Uniquement utilisé si vous avez spécifié `"tagStatus": "tagged"` et que vous ne spécifiez pas une `tagPatternList`. Vous devez préciser une liste séparée par des virgules de préfixes d'étiquette d'image sur lesquels exécuter une action avec votre politique de cycle de vie. Par exemple, si vos images sont étiquetées comme `prod`, `prod1`, `prod2`, et ainsi de suite, vous devrez utiliser le préfixe d'étiquette `prod` pour toutes les préciser. Si vous précisez plusieurs étiquettes, seules les images portant toutes les étiquettes précisées seront sélectionnées.

Type de décompte

`countType`

Type : chaîne

Obligatoire : oui

Indiquez un type de décompte à appliquer aux images.

Si `countType` est défini sur `imageCountMoreThan`, vous précisez également `countNumber` pour créer une règle qui définit une limite sur le nombre d'images existant dans votre référentiel.

Si `countType` est défini sur `sinceImagePushed`, vous précisez également `countUnit` et `countNumber` pour indiquer une limite de temps sur le nombre d'images existant dans votre référentiel.

Unité de décompte

`countUnit`

Type : chaîne

Obligatoire : oui, uniquement si `countType` est défini sur `sinceImagePushed`

Précisez une unité de décompte `days` pour indiquer celle-ci comme unité de temps, en plus de `countNumber`, qui est le nombre de jours.

Cela doit uniquement être précisé lorsque `countType` est `sinceImagePushed` ; une erreur se produira si vous précisez une unité de décompte lorsque `countType` a n'importe quelle autre valeur.

Chiffre du décompte

`countNumber`

Type : entier

Obligatoire : oui

Précisez un chiffre de décompte. Les valeurs acceptables sont des entiers positifs (`0` n'est pas une valeur acceptée).

Si le paramètre `countType` utilisé est `imageCountMoreThan`, la valeur sera le nombre maximal d'images que vous souhaitez conserver dans votre référentiel. Si le paramètre `countType` utilisé est `sinceImagePushed`, la valeur sera la limite d'ancienneté maximale pour vos images.

Action

`type`

Type : chaîne

Obligatoire : oui

Précisez un type d'action. La valeur prise en charge est `expire`.

Sécurité dans le registre de conteneur Amazon Elastic

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

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

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

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lorsque vous utiliser Amazon ECR. Les rubriques suivantes vous expliquent comment configurer Amazon ECR afin de répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Amazon ECR.

Rubriques

Gestion des identités et des accès au registre de conteneur Amazon Elastic

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 ECR. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

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

Utilisateur du service – Si vous utilisez le service Amazon ECR pour accomplir votre tâche, votre administrateur vous fournira les informations d'identification et les autorisations nécessaires. Vous pourriez avoir besoin d'autorisations supplémentaires si vous utilisez davantage de fonctions Amazon ECR. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonction dans Amazon ECR, consultez Dépannage de l'identité et de l'accès au registre de conteneur Amazon Elastic.

Administrateur du service – Si vous êtes le responsable des ressources Amazon ECR de votre entreprise, vous bénéficiez probablement d'un accès total à Amazon ECR. C'est à vous de

déterminer les fonctionnalités et les ressources Amazon ECR auxquelles vos utilisateurs des services pourront accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour découvrir la façon dont votre entreprise peut utiliser IAM avec Amazon ECR, consultez Fonctionnement du registre de conteneur Amazon Elastic avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être obtenir des informations sur la façon dont vous pouvez écrire des politiques pour la gestion des accès à Amazon ECR. Pour afficher des exemples de politiques basées sur l'identité Amazon ECR que vous pouvez utiliser dans IAM, consultez Exemples de politiques basées sur l'identité du registre de conteneur Amazon Elastic.

Authentification par des identités

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

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

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

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

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

Compte AWS utilisateur root

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

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

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

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

des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

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

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

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

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

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal

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

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

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

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

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

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

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de

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

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

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

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou

un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

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

Fonctionnement du registre de conteneur Amazon Elastic avec IAM

Avant d'utiliser IAM pour gérer les accès à Amazon ECR, vous devez comprendre quelles sont les fonctions IAM qui peuvent être utilisées avec Amazon ECR. Pour obtenir une vue d'ensemble de la manière dont Amazon ECR 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 les identités Amazon ECR
- Politiques basées sur les ressources Amazon ECR
- Autorisation basée sur les balises Amazon ECR
- Rôles IAM Amazon ECR

Politiques basées sur les identités Amazon ECR

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 ECR est compatible avec 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 politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de politique dans Amazon ECR utilisent le préfixe suivant avant l'action : `ecr:`. Par exemple, pour accorder à une personne l'autorisation de créer un référentiel Amazon ECR à l'aide de l'opération d'API `CreateRepository` Amazon ECR, vous devez inclure l'action `ecr:CreateRepository` dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Amazon ECR 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": [
      "ecr:action1",
      "ecr: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": "ecr:Describe*"
```

Pour afficher la liste des actions Amazon ECR, consultez Actions, ressources et clés de condition pour le registre de conteneur Amazon Elastic 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": "*"
```

Une ressource de référentiel Amazon ECR possède l'ARN suivant :

```
arn:${Partition}:ecr:${Region}:${Account}:repository/${Repository-name}
```

Pour plus d'informations sur le format des ARN, consultez Amazon Resource Names (ARN) et AWS Service Namespaces.

Par exemple, pour spécifier le référentiel `my-repo` dans la région `us-east-1` dans votre instruction, utilisez l'ARN suivant :

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
```

Pour spécifier tous les référentiels qui appartiennent à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/*"
```

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 ECR et de leurs ARN, consultez Ressources définies par le registre de conteneur Amazon Elastic dans le guide de l'utilisateur IAM. Pour connaître les actions avec lesquelles vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par le registre de conteneur Amazon Elastic.

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 ECR 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.

La plupart des actions Amazon ECR prennent en charge les clés de condition `aws:ResourceTag` et `ecr:ResourceTag`. Pour plus d'informations, consultez Utilisation du contrôle d'accès basé sur les balises.

Pour afficher la liste des clés de condition Amazon ECR, consultez Clés de condition définies par le registre de conteneur Amazon Elastic 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 le registre de conteneur Amazon Elastic.

Exemples

Pour voir des exemples de politiques Amazon ECR basées sur l'identité, consultez Exemples de politiques basées sur l'identité du registre de conteneur Amazon Elastic.

Politiques basées sur les ressources Amazon ECR

Les politiques basées sur les ressources sont des documents de politique JSON précisant les actions qu'un principal spécifié peut effectuer sur la ressource Amazon ECR et dans quelles conditions. Amazon ECR prend en charge les politiques d'autorisation basées sur les ressources pour les référentiels Amazon ECR. Les politiques basées sur les ressources permettent d'accorder une autorisation à d'autres comptes en fonction des ressources. Vous pouvez également utiliser une politique basée sur une ressource pour autoriser un service AWS à accéder à vos référentiels Amazon ECR.

Pour permettre un accès comptes multiples, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource se trouvent dans des AWS comptes différents, vous devez également accorder à l'entité principale l'autorisation d'accéder à la ressource. Accordez l'autorisation en attachant une stratégie basée sur les identités à l'entité. Toutefois, si une stratégie basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre stratégie basée sur l'identité n'est requise. Pour en savoir plus, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le guide de l'utilisateur IAM.

Le service Amazon ECR prend en charge un seul type de politique basée sur une ressource, nommée politique de référentiel, qui est attachée à un référentiel Cette politique définit les entités principales (comptes, utilisateurs, rôles et utilisateurs fédérés) qui peuvent effectuer des actions sur

le référentiel. Pour savoir comment attacher une politique basée sur les ressources à un référentiel, consultez Politiques relatives aux référentiels privés dans Amazon ECR.

> **Note**
>
> Dans une politique de référentiel Amazon ECR, l'élément de stratégie`Sid` prend en charge les caractères et les espaces supplémentaires qui ne sont pas pris en charge dans les politiques IAM.

Exemples

Pour consulter des exemples de politiques basées sur les ressources ,Amazon ECR, consultez Exemples de politiques relatives aux référentiels privés dans Amazon ECR.

Autorisation basée sur les balises Amazon ECR

Vous pouvez rattacher des balises aux ressources Amazon ECR ou transmettre des balises dans une demande à Amazon ECR. Pour contrôler l'accès basé sur des balises, vous devez fournir les informations de balises dans l'élément de condition d'une politique utilisant les clés de condition `ecr:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`. Pour en savoir plus sur le balisage des ressources Amazon ECR, consultez Marquage d'un référentiel privé dans Amazon ECR.

Pour visualiser un exemple de politique basée sur l'identité permettant de limiter l'accès à une ressource en fonction des balises de cette ressource, consultez Utilisation du contrôle d'accès basé sur les balises.

Rôles IAM Amazon ECR

Un rôle IAM est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utiliser des informations d'identification temporaires avec Amazon ECR

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 ECR est compatible avec l'utilisation des informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Amazon ECR prend en charge les rôles liés à un service. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon ECR.

Exemples de politiques basées sur l'identité du registre de conteneur Amazon Elastic

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources Amazon ECR. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

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

Pour plus de détails sur les actions et les types de ressources définis par Amazon ECR, y compris le format des ARN pour chacun des types de ressources, consultez Actions, ressources et clés de condition pour Amazon Elastic Container Registry dans la Référence de l'autorisation de service.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utiliser la console Amazon ECR
- Autoriser les utilisateurs à afficher leurs propres autorisations

- Accéder à un seul référentiel Amazon ECR

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Amazon ECR 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.

Utiliser la console Amazon ECR

Pour accéder à la console du registre de conteneur Amazon Elastic, vous devez disposer d'un jeu minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon ECR de votre AWS compte. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Pour garantir que ces entités peuvent toujours utiliser la console Amazon ECR, ajoutez la politique `AmazonEC2ContainerRegistryReadOnly` AWS gérée aux entités. Pour en savoir plus, consultez Ajouter des autorisations à un utilisateur dans le guide de l'utilisateur IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:ListImages",
                "ecr:DescribeImages",
                "ecr:BatchGetImage",
                "ecr:GetLifecyclePolicy",
                "ecr:GetLifecyclePolicyPreview",
                "ecr:ListTagsForResource",
                "ecr:DescribeImageScanFindings"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Autoriser les utilisateurs à 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": "*"
        }
    ]
}
```

Accéder à un seul référentiel Amazon ECR

Dans cet exemple, vous souhaitez accorder à un utilisateur de votre AWS compte l'accès à l'un de vos référentiels Amazon ECR. `my-repo` Vous souhaitez également autoriser l'utilisateur à transférer, tirer et lister des images.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListImagesInRepository",
         "Effect":"Allow",
         "Action":[
            "ecr:ListImages"
         ],
         "Resource":"arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
      },
      {
         "Sid":"GetAuthorizationToken",
         "Effect":"Allow",
         "Action":[
            "ecr:GetAuthorizationToken"
         ],
         "Resource":"*"
      },
      {
         "Sid":"ManageRepositoryContents",
         "Effect":"Allow",
         "Action":[
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:ListImages",
                "ecr:DescribeImages",
```

```
                "ecr:BatchGetImage",
                "ecr:InitiateLayerUpload",
                "ecr:UploadLayerPart",
                "ecr:CompleteLayerUpload",
                "ecr:PutImage"
            ],
            "Resource":"arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
        }
    ]
}
```

Utilisation du contrôle d'accès basé sur les balises

L'action d' CreateRepository API Amazon ECR vous permet de spécifier des balises lorsque vous créez le référentiel. Pour plus d'informations, consultez Marquage d'un référentiel privé dans Amazon ECR.

Pour permettre aux utilisateurs d'attribuer des balises aux référentiels au moment de la création, ils doivent avoir les autorisations d'utiliser l'action qui crée la ressource (par exemple, `ecr:CreateRepository`). Si les balises sont spécifiées dans l'action de création de ressources, Amazon effectue une autorisation supplémentaire sur l'action `ecr:CreateRepository` pour vérifier si les utilisateurs sont autorisés à créer des balises.

Vous pouvez utiliser le contrôle d'accès basé sur des balises via des politiques IAM. Voici quelques exemples.

La politique suivante autorise uniquement un utilisateur à créer ou baliser un référentiel en tant que `key=environment,value=dev`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedRepository",
            "Effect": "Allow",
            "Action": [
                "ecr:CreateRepository"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:RequestTag/environment": "dev"
                }
            }
        },
        {
            "Sid": "AllowTagRepository",
            "Effect": "Allow",
            "Action": [
                "ecr:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "dev"
                }
            }
        }
    ]
}
```

La politique suivante autorise un utilisateur à accéder à tous les référentiels, sauf s'ils ont été balisés en tant que `key=environment,value=prod`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ecr:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ecr:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecr:ResourceTag/environment": "prod"
                }
            }
        }
    ]
}
```

AWS politiques gérées pour Amazon Elastic Container Registry

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.

Amazon ECR fournit plusieurs politiques gérées que vous pouvez associer aux identités IAM ou aux instances Amazon EC2. Ces politiques gérées permettent différents niveaux de contrôle sur l'accès aux ressources Amazon ECR et aux opérations d'API. Pour en savoir plus sur chaque opération d'API mentionnée dans ces politiques, consultezActions dans la Référence de l'API du registre de conteneur Amazon Elastic.

Rubriques

- AmazonEC2ContainerRegistryFullAccess
- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryReadOnly
- AWSECRPullThroughCache_ServiceRolePolicy
- ECRReplicationServiceRolePolicy
- Amazon ECR met à jour les politiques AWS gérées

AmazonEC2ContainerRegistryFullAccess

Vous pouvez attacher la politique AmazonEC2ContainerRegistryFullAccess à vos identités IAM.

Vous pouvez utiliser cette politique gérée comme point de départ pour créer votre propre politique IAM en fonction de vos besoins spécifiques. Par exemple, vous pouvez créer une politique spécifique pour fournir à un utilisateur ou à un rôle un accès administrateur total pour gérer l'utilisation d'Amazon ECR. La fonctionnalité Politiques de cycle de vie Amazon ECR permet aux clients de spécifier la gestion du cycle de vie des images dans un référentiel. Les événements liés à la politique de cycle de vie sont signalés en tant qu' CloudTrail événements. Amazon ECR est intégré à Amazon ECR AWS CloudTrail afin d'afficher les événements relatifs à votre politique de cycle de vie directement dans la console Amazon ECR. La politique gérée IAM AmazonEC2ContainerRegistryFullAccess l'autorisation cloudtrail:LookupEvents afin de faciliter ce comportement.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- ecr – Accorde aux mandataires un accès total à toutes les API Amazon ECR.
- cloudtrail— Permet aux principaux de consulter les événements de gestion ou les événements AWS CloudTrail Insights capturés par CloudTrail.

La politique AmazonEC2ContainerRegistryFullAccess est la suivante.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:*",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "replication.ecr.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

AmazonEC2ContainerRegistryPowerUser

Vous pouvez attacher la politique AmazonEC2ContainerRegistryPowerUser à vos identités IAM.

Cette politique accorde des autorisations d'administration qui permettent aux utilisateurs IAM de lire et d'écrire dans des référentiels, mais elle ne leur permet pas de supprimer des référentiels ni de modifier les documents de la politique qui leur sont appliqués.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- ecr– Permet aux identités de lire et d'écrire dans les référentiels, ainsi que de lire les politiques de cycle de vie. Les mandataires ne sont pas autorisées à supprimer des référentiels ni à modifier les politiques de cycle de vie qui leur sont appliquées.

La politique AmazonEC2ContainerRegistryPowerUser est la suivante.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetRepositoryPolicy",
                "ecr:DescribeRepositories",
```

```
                "ecr:ListImages",
                "ecr:DescribeImages",
                "ecr:BatchGetImage",
                "ecr:GetLifecyclePolicy",
                "ecr:GetLifecyclePolicyPreview",
                "ecr:ListTagsForResource",
                "ecr:DescribeImageScanFindings",
                "ecr:InitiateLayerUpload",
                "ecr:UploadLayerPart",
                "ecr:CompleteLayerUpload",
                "ecr:PutImage"
            ],
            "Resource": "*"
        }
    ]
}
```

AmazonEC2ContainerRegistryReadOnly

Vous pouvez attacher la politique AmazonEC2ContainerRegistryReadOnly à vos identités IAM.

Cette politique accorde des autorisations qui permettent un accès en lecture seule à Amazon ECR. Cela inclut la possibilité de répertorier les référentiels et les images dans les référentiels. Elle offre également la possibilité d'extraire des images depuis Amazon ECR avec la CLI Docker.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- ecr – permet aux mandataires de lire les référentiels et leurs politiques de cycle de vie respectives.

La politique AmazonEC2ContainerRegistryReadOnly est la suivante.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetRepositoryPolicy",
```

```
                "ecr:DescribeRepositories",
                "ecr:ListImages",
                "ecr:DescribeImages",
                "ecr:BatchGetImage",
                "ecr:GetLifecyclePolicy",
                "ecr:GetLifecyclePolicyPreview",
                "ecr:ListTagsForResource",
                "ecr:DescribeImageScanFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSECRPullThroughCache_ServiceRolePolicy

Vous ne pouvez pas attacher la politique IAM gérée `AWSECRPullThroughCache_ServiceRolePolicy` à vos entités IAM. Cette politique est attachée à un rôle lié à un service qui permet à Amazon ECR de transférer des images vers vos référentiels via le flux de travail de mise en cache par extraction. Pour plus d'informations, consultez Rôle lié à un service Amazon ECR pour la mise en cache par extraction.

ECRReplicationServiceRolePolicy

Vous ne pouvez pas attacher la politique IAM gérée `ECRReplicationServiceRolePolicy` à vos entités IAM. Cette politique est attachée à un rôle lié à un service qui permet à Amazon ECR d'effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon ECR.

Amazon ECR met à jour les politiques AWS gérées

Consultez les informations relatives aux mises à jour apportées aux politiques AWS gérées pour Amazon ECR depuis le moment où ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS sur la page de l'historique des documents Amazon ECR.

Modification	Description	Date
AWSECRPullThroughCache_ServiceRolePolicy –	Amazon ECR a ajouté de nouvelles autorisations à	15 novembre 2023

Modification	Description	Date
Mise à jour d'une stratégie existante	la politique `AWSECRPullThroughCache_ServiceRolePolicy` . Ces autorisations permettent à Amazon ECR de récupérer le contenu chiffré d'un secret de Secrets Manager. Cela est nécessaire lors de l'utilisation d'une règle de mise en cache par extraction pour mettre en cache des images provenant d'un registre en amont qui nécessite une authentification.	
AWSECRPullThroughCache_ServiceRolePolicy : nouvelle politique	Amazon ECR a ajouté une nouvelle politique. Cette politique est associée au rôle lié à un service `AWSServiceRoleForECRPullThroughCache` pour la fonction de mise en cache par extraction.	29 novembre 2021
ECR ReplicationServiceRolePolicy — Nouvelle politique	Amazon ECR a ajouté une nouvelle politique. Cette politique est associée au rôle lié à un service `AWSServiceRoleForECRReplication` pour la fonction de réplication.	4 décembre 2020

Modification	Description	Date
AmazonEC2 Container Registry FullAccess — Mise à jour d'une politique existante	Amazon ECR a ajouté de nouvelles autorisations à la politique `AmazonEC2ContainerRegistryFullAccess`. Ces autorisations permettent aux mandataires de créer un rôle lié au service Amazon ECR.	4 décembre 2020
AmazonEC2 Container Registry ReadOnly — Mise à jour d'une politique existante	Amazon ECR a ajouté de nouvelles autorisations à la politique `AmazonEC2ContainerRegistryReadOnly` qui permettent aux mandataires de lire les politiques de cycle de vie, de répertorier les balises et de décrire les résultats de l'analyse des images.	10 décembre 2019
AmazonEC2 Container Registry PowerUser — Mise à jour d'une politique existante	Amazon ECR a ajouté de nouvelles autorisations à la politique `AmazonEC2ContainerRegistryPowerUser`. Elles permettent aux mandataires de lire les politiques de cycle de vie, de répertorier les balises et de décrire les résultats de l'analyse des images.	10 décembre 2019

Modification	Description	Date
AmazonEC2 Container Registry FullAccess — Mise à jour d'une politique existante	Amazon ECR a ajouté de nouvelles autorisations à la politique `AmazonEC2ContainerRegistryFullAccess`. Ils permettent aux directeurs de rechercher les événements de gestion ou les événements AWS CloudTrail Insights capturés par CloudTrail.	le 10 novembre 2017
AmazonEC2 Container Registry ReadOnly — Mise à jour d'une politique existante	Amazon ECR a ajouté de nouvelles autorisations à la politique `AmazonEC2ContainerRegistryReadOnly`. Elles permettent aux mandataires de décrire les images Amazon ECR.	11 octobre 2016
AmazonEC2 Container Registry PowerUser — Mise à jour d'une politique existante	Amazon ECR a ajouté de nouvelles autorisations à la politique `AmazonEC2ContainerRegistryPowerUser`. Elles permettent aux mandataires de décrire les images Amazon ECR.	11 octobre 2016

Modification	Description	Date
Amazon EC2 Container Registry ReadOnly — Nouvelle politique	Amazon ECR a ajouté une nouvelle politique qui accorde des autorisations en lecture seule à Amazon ECR. Ces autorisations offrent la possibilité de répertorier les référentiels et les images dans les référentiels. Elles offrent également la possibilité d'extraire des images depuis Amazon ECR à l'aide de la CLI Docker.	21 décembre 2015
Amazon EC2 Container Registry PowerUser — Nouvelle politique	Amazon ECR a ajouté une nouvelle politique qui accorde des autorisations d'administration permettant aux utilisateurs de lire et d'écrire dans des référentiels, mais elle ne leur permet pas de supprimer des référentiels ni de modifier les documents de la politique qui leur sont appliqués.	21 décembre 2015
Amazon EC2 Container Registry FullAccess — Nouvelle politique	Amazon ECR a ajouté une nouvelle politique. Cette politique accorde à un accès total à Amazon ECR.	21 décembre 2015
Amazon ECR a commencé à assurer le suivi des modifications	Amazon ECR a commencé à suivre les modifications apportées aux politiques AWS gérées.	24 juin 2021

Utilisation des rôles liés à un service pour Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) AWS Identity and Access Management utilise des rôles liés à un service (IAM) pour fournir les autorisations nécessaires à l'utilisation des fonctionnalités de réplication et d'extraction du cache. Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon ECR. Le rôle lié au service est prédéfini par Amazon ECR. Il comprend toutes les autorisations dont le service a besoin pour prendre en charge les fonctions de réplication et de mise en cache par extraction pour votre registre privé. Après avoir configuré la réplication ou la mise en cache par extraction pour votre registre, un rôle lié à un service est créé automatiquement en votre nom. Pour plus d'informations, consultez Paramètres du registre privé dans Amazon ECR.

Un rôle lié à un service simplifie la configuration de la réplication et de la mise en cache par extraction avec Amazon ECR. En effet, son utilisation vous évite de devoir ajouter manuellement toutes les autorisations requises. Amazon ECR définit les autorisations de ses rôles liés à un service et, sauf indication contraire, seul Amazon ECR peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. La politique d'autorisations ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer le rôle lié à un service correspondant uniquement après avoir désactivé la réplication ou la mise en cache par extraction dans votre registre. Cela vous permet de ne pas supprimer par inadvertance les autorisations dont Amazon ECR a besoin pour ces fonctions.

Pour obtenir des informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Dans cette page de liens, recherchez les services qui comportent un Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter la documentation du rôle lié à un service, pour ce service.

Rubriques

Régions prises en charge pour les rôles liés à un service Amazon ECR

Amazon ECR prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service Amazon ECR est disponible. Pour en savoir plus sur la disponibilité de la région Amazon ECR, consultez Régions et Points de terminaison AWS.

Rôle lié à un service Amazon ECR pour la réplication

Amazon ECR utilise un rôle lié à un service nommé AWSServiceRoleForECRReplicationqui permet à Amazon ECR de répliquer des images sur plusieurs comptes.

Autorisations du rôle lié à un service pour Amazon ECR

Le rôle AWSServiceRoleForECRReplication lié à un service fait confiance aux services suivants pour assumer le rôle :

- `replication.ecr.amazonaws.com`

La politique d'autorisations liée au rôle `ECRReplicationServiceRolePolicy` permet à Amazon ECR d'utiliser les actions suivantes sur les ressources :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Le `ReplicateImage` est une API interne qu'Amazon ECR utilise pour la réplication et qui ne peut pas être appelée directement.

Vous devez configurer les autorisations de manière à autoriser une entité IAM (comme un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour en savoir plus, consultez Autorisations des rôles liés à un service dans le guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Amazon ECR

Vous n'avez pas besoin de créer manuellement un rôle lié au service Amazon ECR. Lorsque vous configurez les paramètres de réplication pour votre registre dans le AWS Management Console, le AWS CLI, ou l' AWS API, Amazon ECR crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous devez le recréer, vous pourrez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous configurez les paramètres de réplication pour votre registre, Amazon ECR recrée automatiquement le rôle lié à un service.

Modification d'un rôle lié à un service pour Amazon ECR

Amazon ECR n'autorise pas la modification manuelle du rôle lié au AWSServiceRoleForECRReplication 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 en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression du rôle lié à un service pour Amazon ECR

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, aucune entité inutilisée n'est surveillée ou gérée activement. Toutefois, vous devez supprimer la configuration de réplication de votre registre dans chaque région avant de pouvoir supprimer manuellement le rôle lié à un service.

> **Note**
>
> Si vous essayez de supprimer des ressources alors que le service Amazon ECR utilise toujours les rôles, votre action de suppression pourrait échouer. Si cela se produit, attendez quelques minutes et réessayez.

Pour supprimer les ressources Amazon ECR utilisées par AWSServiceRoleForECRReplication

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, sélectionnez la région dans laquelle votre configuration de réplication est définie.
3. Dans le panneau de navigation, choisissez Registre de schémas.
4. Dans la page Registre privé, dans la section Configuration de réplication, choisissez Modifier.

5. Pour supprimer toutes vos règles de réplication, choisissez Tout supprimer. Cette étape nécessite une confirmation.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForECRReplicationservice. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Rôle lié à un service Amazon ECR pour la mise en cache par extraction

Amazon ECR utilise un rôle lié à un service nommé AWSServiceRoleForECRPullThroughCachequi autorise Amazon ECR à effectuer des actions en votre nom pour effectuer des actions d'extraction dans le cache. Pour plus d'informations sur la mise en cache par extraction, consultez Synchroniser un registre en amont avec un registre privé Amazon ECR.

Autorisations du rôle lié à un service pour Amazon ECR

Le rôle AWSServiceRoleForECRPullThroughCachelié à un service fait confiance au service suivant pour assumer le rôle.

- `pullthroughcache.ecr.amazonaws.com`

Détails de l'autorisation

La politique d'autorisations `AWSECRPullThroughCache_ServiceRolePolicy` est attachée au rôle lié à un service. Cette politique gérée accorde à Amazon ECR l'autorisation d'effectuer les actions suivantes. Pour plus d'informations, consultez `AWSECRPullThroughCache_ServiceRolePolicy`.

- `ecr` : permet au service Amazon ECR de transférer des images vers un référentiel privé.
- `secretsmanager:GetSecretValue`— Permet au service Amazon ECR de récupérer le contenu chiffré d'un AWS Secrets Manager secret. Cela est nécessaire lors de l'utilisation d'une règle de mise en cache par extraction pour mettre en cache des images provenant d'un registre en amont qui nécessite une authentification dans votre registre privé. Cette autorisation s'applique uniquement aux secrets portant le préfixe de nom `ecr-pullthroughcache/`.

La politique `AWSECRPullThroughCache_ServiceRolePolicy` contient le JSON suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ECR",
            "Effect": "Allow",
            "Action": [
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:InitiateLayerUpload",
                "ecr:UploadLayerPart",
                "ecr:CompleteLayerUpload",
                "ecr:PutImage"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SecretsManager",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

Vous devez configurer les autorisations de manière à autoriser une entité IAM (comme un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Amazon ECR

Vous n'avez pas besoin de créer manuellement le rôle lié à un service Amazon ECR pour la mise en cache par extraction. Lorsque vous créez une règle de cache d'extraction pour votre registre privé dans le AWS Management Console, le AWS CLI ou l' AWS API, Amazon ECR crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous devez le recréer, vous pourrez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez une règle de mise en cache par extraction pour votre registre privé, Amazon ECR crée à nouveau le rôle lié à un service pour vous s'il n'existe pas déjà.

Modification d'un rôle lié à un service pour Amazon ECR

Amazon ECR n'autorise pas la modification manuelle du rôle lié au AWSServiceRoleForECRPullThroughCacheservice. Après la création du rôle lié à un service, vous ne pouvez pas modifier le nom du rôle car diverses entités pourraient y faire référence. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression du rôle lié à un service pour Amazon ECR

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, aucune entité inutilisée n'est surveillée ou gérée activement. Toutefois, vous devez supprimer les règles de mise en cache par extraction pour votre registre dans chaque région avant de pouvoir supprimer manuellement le rôle lié à un service.

> **Note**
>
> Si vous essayez de supprimer des ressources alors que le service Amazon ECR utilise toujours le rôle, votre action de suppression peut échouer. Si cela se produit, attendez quelques minutes et réessayez.

Pour supprimer des ressources Amazon ECR utilisées par le rôle lié à un service AWSServiceRoleForECRPullThroughCache

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans la barre de navigation, choisissez la région où vos règles de mise en cache par extraction sont créées.
3. Dans le panneau de navigation, choisissez Registre de schémas.
4. Dans la page Registre privé, dans la section Configuration de la mise en cache par extraction, choisissez Modifier.

5. Pour chaque règle de cache d'extraction que vous avez créée, sélectionnez la règle, puis choisissez Supprimer la règle.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForECRPullThroughCacheservice. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Dépannage de l'identité et de l'accès au registre de conteneur Amazon Elastic

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon ECR et IAM.

Rubriques

- Je ne suis pas autorisé à exécuter une action dans Amazon ECR
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon ECR

Je ne suis pas autorisé à exécuter une action dans Amazon ECR

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `ecr:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ecr:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `ecr:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon ECR.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans Amazon ECR. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon ECR

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

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon ECR est compatible avec ces fonctions, consultez Fonctionnement du registre de conteneur Amazon Elastic avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès inter-comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le guide de l'utilisateur IAM.

Protection des données dans Amazon ECR

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Amazon Elastic Container Service. 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 ECS ou une autre entreprise Services AWS à l'aide de la console, de l'API ou AWS des 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 au repos

Amazon ECR stocke les images dans des compartiments Amazon S3 gérés par Amazon ECR. Par défaut, Amazon ECR utilise le chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3, ce qui chiffre vos données au repos à l'aide d'un algorithme de chiffrement AES-256. Ceci ne nécessite aucune action de votre part et est fourni sans frais supplémentaires. Pour en savoir plus, consultez la section Protection des données à l'aide du chiffrement côté serveur avec des clés de chiffrement (SSE-S3) gérées par Amazon S3 dans le guide de l'utilisateur Amazon Simple Storage Service.

Pour mieux contrôler le chiffrement de vos référentiels Amazon ECR, vous pouvez utiliser le chiffrement côté serveur avec des clés KMS stockées dans (). AWS Key Management Service AWS KMS Lorsque vous chiffrez vos données, vous pouvez soit utiliser la clé par défaut Clé gérée par AWS, qui est gérée par Amazon ECR, soit spécifier votre propre clé KMS (appelée clé gérée par le client). AWS KMS Pour plus d'informations, consultez la section Protection des données à l'aide du chiffrement côté serveur avec des clés KMS stockées dans AWS KMS (SSE-KMS) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Chaque référentiel Amazon ECR dispose d'une configuration de chiffrement, qui est définie lors de la création du référentiel. Vous pouvez utiliser des configurations de chiffrement différentes dans chaque référentiel. Pour plus d'informations, consultez Création d'un référentiel privé Amazon ECR pour stocker des images.

Lorsqu'un référentiel est créé avec AWS KMS le chiffrement activé, une clé KMS est utilisée pour chiffrer le contenu du référentiel. De plus, Amazon ECR ajoute une AWS KMS subvention à la clé KMS avec le référentiel Amazon ECR comme bénéficiaire principal.

Ce qui suit fournit des informations de haut niveau afin de comprendre la façon dont Amazon ECR est intégré à AWS KMS pour chiffrer et déchiffrer vos référentiels :

1. Lors de la création d'un référentiel, Amazon ECR envoie un DescribeKeyappel AWS KMS pour valider et récupérer le nom de ressource Amazon (ARN) de la clé KMS spécifiée dans la configuration de chiffrement.
2. Amazon ECR envoie deux CreateGrantdemandes pour créer des autorisations sur la clé KMS AWS KMS afin de permettre à Amazon ECR de chiffrer et de déchiffrer les données à l'aide de la clé de données.
3. Lorsque vous envoyez une image, une demande de GenerateDataclé est envoyée pour AWS KMS spécifier la clé KMS à utiliser pour chiffrer la couche d'image et le manifeste.
4. AWS KMS génère une nouvelle clé de données, la chiffre sous la clé KMS spécifiée et envoie la clé de données chiffrée à stocker avec les métadonnées de la couche d'image et le manifeste d'image.
5. Lors de l'extraction d'une image, une demande de déchiffrement est envoyée à AWS KMS, spécifiant la clé de données cryptée.
6. AWS KMS déchiffre la clé de données chiffrée et envoie la clé de données déchiffrée à Amazon S3.
7. La clé de données est utilisée pour déchiffrer la couche d'image avant la couche d'image en cours d'extraction.
8. Lorsqu'un référentiel est supprimé, Amazon ECR envoie deux RetireGrantdemandes AWS KMS pour annuler les subventions créées pour le référentiel.

Considérations

Les points suivants doivent être pris en compte lors de l'utilisation du AWS KMS chiffrement avec Amazon ECR.

- Si vous créez votre référentiel Amazon ECR avec le chiffrement KMS et que vous ne spécifiez pas de clé KMS, Amazon ECR utilise un Clé gérée par AWS alias `aws/ecr` par défaut. Cette clé KMS sera créée dans votre compte la première fois que vous créerez un référentiel avec le chiffrement KMS activé.
- Lorsque vous utilisez le chiffrement KMS avec votre propre clé KMS, la clé doit exister dans la même région que votre référentiel.
- Les octrois créés par Amazon ECR en votre nom ne doivent pas être révoqués. Si vous révoquez l'autorisation qui autorise Amazon ECR à utiliser les AWS KMS clés de votre compte, Amazon ECR ne pourra pas accéder à ces données, chiffrer les nouvelles images envoyées au référentiel ou les déchiffrer lorsqu'elles sont extraites. Lorsque vous révoquez un octroi pour Amazon ECR, le changement est immédiat. Pour révoquer les droits d'accès, vous devez supprimez le référentiel plutôt que de révoquer l'octroi. Lorsqu'un référentiel est supprimé, Amazon ECR retire les octrois en votre nom.
- L'utilisation des AWS KMS clés entraîne un coût. Pour en savoir plus, consultez AWS Key Management Service Tarification.

Autorisations IAM requises

Lorsque vous créez ou supprimez un référentiel Amazon ECR avec un chiffrement côté serveur à l'aide de AWS KMS, les autorisations requises dépendent de la clé KMS spécifique que vous utilisez.

Autorisations IAM requises lors de l'utilisation du Clé gérée par AWS pour Amazon ECR

Par défaut, lorsque AWS KMS le chiffrement est activé pour un référentiel Amazon ECR mais qu'aucune clé KMS n'est spécifiée, la clé Clé gérée par AWS pour Amazon ECR est utilisée. Lorsque la clé KMS AWS gérée pour Amazon ECR est utilisée pour chiffrer un référentiel, tout principal autorisé à créer un référentiel peut également activer le AWS KMS chiffrement du référentiel. Toutefois, le principal IAM qui supprime le référentiel doit avoir l'autorisation `kms:RetireGrant`. Cela permet de retirer les subventions qui ont été ajoutées à la AWS KMS clé lors de la création du référentiel.

L'exemple de politique IAM suivant peut être ajouté en tant que politique intégrée à un utilisateur pour s'assurer qu'il dispose des autorisations minimales nécessaires pour supprimer un référentiel dont le chiffrement est activé. La clé KMS utilisée pour chiffrer le référentiel peut être spécifiée à l'aide du paramètre de ressource.

```
{
```

```
    "Version": "2012-10-17",
    "Id": "ecr-kms-permissions",
    "Statement": [
        {
            "Sid": "AllowAccessToRetireTheGrantsAssociatedWithTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:RetireGrant"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/b8d9ae76-080c-4043-92EXAMPLE"
        }
    ]
}
```

Autorisations IAM requises pour l'utilisation d'une clé gérée par le client

Lors de la création d'un référentiel dont le AWS KMS chiffrement est activé à l'aide d'une clé gérée par le client, des autorisations sont requises pour la politique de clés KMS et la politique IAM pour l'utilisateur ou le rôle qui crée le référentiel.

Lorsque vous créez votre propre clé KMS, vous pouvez utiliser la politique de clé AWS KMS par défaut créée ou vous pouvez spécifier la vôtre. Pour garantir que la clé gérée par le client reste gérable par le propriétaire du compte, la politique clé relative à la clé KMS doit autoriser toutes les AWS KMS actions pour l'utilisateur root du compte. Des autorisations étendues supplémentaires peuvent être ajoutées à la politique de clé, mais au minimum l'utilisateur racine doit être autorisé à gérer la clé KMS. Pour autoriser l'utilisation de la clé KMS uniquement pour les demandes provenant d'Amazon ECR, vous pouvez utiliser la clé de ViaService condition kms : avec la `ecr.<region>.amazonaws.com` valeur.

L'exemple de politique de clé suivant donne au AWS compte (utilisateur root) propriétaire de la clé KMS un accès complet à la clé KMS. Pour plus d'informations sur cet exemple de politique clé, voir Autoriser l'accès au AWS compte et activer les politiques IAM dans le Guide du AWS Key Management Service développeur.

```
{
    "Version": "2012-10-17",
    "Id": "ecr-key-policy",
    "Statement": [
        {
            "Sid": "EnableIAMUserPermissions",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

L'utilisateur IAM, le rôle IAM ou le AWS compte qui crée vos référentiels doit disposer de l'`kms:DescribeKey`autorisation `kms:CreateGrant``kms:RetireGrant`, et en plus des autorisations Amazon ECR nécessaires.

> **Note**
>
> L'autorisation `kms:RetireGrant` doit être ajoutée à la politique IAM de l'utilisateur ou du rôle créant le référentiel. Les autorisations `kms:CreateGrant` et `kms:DescribeKey`peuvent être ajoutées à la politique de clé pour la clé KMS ou à la politique IAM de l'utilisateur ou du rôle créant le référentiel. Pour plus d'informations sur le fonctionnement AWS KMS des autorisations, voir Autorisations d'AWS KMS API : référence aux actions et aux ressources dans le guide du AWS Key Management Service développeur.

L'exemple de politique IAM suivant peut être ajouté en tant que politique intégrée à un utilisateur pour s'assurer qu'il dispose des autorisations minimales nécessaires pour créer un référentiel avec le chiffrement activé et supprimer le référentiel lorsqu'il aura terminé. La AWS KMS key utilisée pour chiffrer le référentiel peut être spécifiée à l'aide du paramètre de ressource.

```
{
    "Version": "2012-10-17",
    "Id": "ecr-kms-permissions",
    "Statement": [
        {
            "Sid":
 "AllowAccessToCreateAndRetireTheGrantsAssociatedWithTheKeyAsWellAsDescribeTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:RetireGrant",
```

```
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/b8d9ae76-080c-4043-92EXAMPLE"
        }
    ]
}
```

Autoriser un utilisateur à répertorier les clés KMS dans la console lors de la création d'un référentiel

Lorsque vous utilisez la console Amazon ECR pour créer un référentiel, vous pouvez octroyer des autorisations afin de permettre à un utilisateur de répertorier les clés KMS gérées par le client dans la région lors de l'activation du chiffrement pour le référentiel. L'exemple de politique IAM suivant indique les autorisations nécessaires pour répertorier vos clés KMS et alias lors de l'utilisation de la console.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  }
}
```

Surveillance de l'interaction Amazon ECR avec AWS KMS

Vous pouvez l'utiliser AWS CloudTrail pour suivre les demandes qu'Amazon ECR envoie en votre AWS KMS nom. Les entrées du CloudTrail journal contiennent une clé contextuelle de chiffrement qui les rend plus facilement identifiables.

Contexte de chiffrement Amazon ECR

Un contexte de chiffrement est un ensemble de paires clé-valeur qui contiennent des données non secrètes arbitraires. Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, lie AWS KMS cryptographiquement le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez transmettre le même contexte de chiffrement.

Dans ses demandes GenerateDataKey and Decrypt adressées à AWS KMS, Amazon ECR utilise un contexte de chiffrement avec deux paires nom-valeur qui identifient le référentiel et le compartiment Amazon S3 utilisés. Voici un exemple : Les noms ne varient pas, mais les valeurs de contexte de chiffrement combinées sont différentes pour chaque valeur.

```
"encryptionContext": {
    "aws:s3:arn": "arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/
sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df",
    "aws:ecr:arn": "arn:aws:ecr:us-west-2:111122223333:repository/repository-name"
}
```

Vous pouvez utiliser le contexte de chiffrement pour identifier ces opérations cryptographiques dans les enregistrements et journaux d'audit, tels que AWS CloudTrailAmazon CloudWatch Logs, et comme condition d'autorisation dans les politiques et les autorisations.

Le contexte de chiffrement Amazon ECR se compose de deux paires nom-valeur.

- aws:s3:arn – La première paire nom-valeur identifie le compartiment. La clé est `aws:s3:arn`. La valeur est l'Amazon Resource Name (ARN) du compartiment Amazon S3.

  ```
  "aws:s3:arn": "ARN of an Amazon S3 bucket"
  ```

  Par exemple, si l'ARN du compartiment est `arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df`, le contexte de chiffrement devra inclure la paire suivante.

  ```
  "arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df"
  ```

- aws:ecr:arn – La deuxième paire nom-valeur identifie l'Amazon Resource Name (ARN) du référentiel. La clé est `aws:ecr:arn`. La valeur est l'ARN du référentiel.

  ```
  "aws:ecr:arn": "ARN of an Amazon ECR repository"
  ```

  Par exemple, si l'ARN du référentiel est `arn:aws:ecr:us-west-2:111122223333:repository/repository-name`, le contexte de chiffrement devra inclure la paire suivante.

```
"aws:ecr:arn": "arn:aws:ecr:us-west-2:111122223333:repository/repository-name"
```

Résolution des problèmes

Lorsque vous supprimez un référentiel Amazon ECR avec la console, si le référentiel est supprimé correctement, mais qu'Amazon ECR ne parvient pas à retirer les octrois ajoutés à votre clé KMS pour votre référentiel, vous recevrez l'erreur suivante.

```
The repository [{repository-name}] has been deleted successfully but the grants created
 by the kmsKey [{kms_key}] failed to be retired
```

Dans ce cas, vous pouvez retirer vous-même les AWS KMS subventions pour le dépôt.

Pour annuler manuellement les AWS KMS subventions accordées à un dépôt

1. Répertoriez les autorisations pour la AWS KMS clé utilisée pour le référentiel. La valeur `key-id` est incluse dans l'erreur que vous recevez de la console. Vous pouvez également utiliser la `list-keys` commande pour répertorier à la fois les clés KMS Clés gérées par AWS et les clés KMS gérées par le client dans une région spécifique de votre compte.

   ```
   aws kms list-grants \
        --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc
        --region us-west-2
   ```

   La sortie inclut un `EncryptionContextSubset` avec l'Amazon Resource Name (ARN) de votre référentiel. Cela peut être utilisé pour déterminer quel octroi ajouté à la clé est celui que vous souhaitez retirer. La valeur `GrantId` sera utilisée lors de la suppression de l'octroi à l'étape suivante.

2. Retirez chaque subvention pour la AWS KMS clé ajoutée au référentiel. Remplacez la valeur pour *`GrantId`*par l'ID de la subvention indiqué dans le résultat de l'étape précédente.

   ```
   aws kms retire-grant \
        --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc \
        --grant-id GrantId \
        --region us-west-2
   ```

Validation de conformité pour le registre de conteneur Amazon Elastic

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

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

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  > **Note**
  >
  > Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).

- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Sécurité de l'infrastructure dans le registre de conteneur Amazon Elastic

En tant que service géré, Amazon Elastic Container Registry est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon ECR via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

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

Vous pouvez appeler ces opérations d'API à partir de n'importe quel emplacement sur le réseau, mais Amazon ECR prend en charge les politiques d'accès basées sur les ressources, ce qui peut inclure des restrictions en fonction de l'adresse IP source. Vous pouvez également utiliser des politiques Amazon ECR pour contrôler l'accès à partir de points de terminaison Amazon Virtual Private Cloud (Amazon VPC) ou de VPC spécifiques. En fait, cela isole l'accès réseau à une ressource Amazon ECR donnée uniquement du VPC spécifique au sein du réseau. AWS Pour plus d'informations, consultez Points de terminaison VPC de l'interface Amazon ECR ()AWS PrivateLink.

Points de terminaison VPC de l'interface Amazon ECR ()AWS PrivateLink

Vous pouvez améliorer le niveau de sécurité de votre VPC en configurant Amazon ECR de façon à utiliser un point de terminaison d'un VPC d'interface. Les points de terminaison VPC sont alimentés par AWS PrivateLink une technologie qui vous permet d'accéder en privé aux API Amazon ECR via des adresses IP privées. AWS PrivateLink restreint tout le trafic réseau entre votre VPC et Amazon ECR vers le réseau Amazon. Vous n'avez pas besoin d'une passerelle Internet, d'un périphérique NAT ni d'une passerelle privée virtuelle.

Pour plus d'informations sur AWS PrivateLink les points de terminaison VPC, consultez la section Points de terminaison VPC dans le guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de terminaison d'un VPC Amazon ECR

Avant de configurer les points de terminaison d'un VPC pour Amazon ECR, vous devez tenir compte des considérations suivantes.

- Pour autoriser vos tâches Amazon ECS hébergées sur des instances Amazon EC2 à extraire des images privées à partir d'Amazon ECR, veillez à créer également les points de terminaison d'un VPC d'interface pour Amazon ECS. Pour plus d'informations, consultez Interface VPC Endpoints (AWS PrivateLink) dans le manuel Amazon Elastic Container Service Developer Guide.

  > **Important**
  >
  > Les tâches Amazon ECS hébergées sur Fargate ne nécessitent pas de points de terminaison d'un VPC d'interface Amazon ECS.

- Les tâches Amazon ECS hébergées sur Fargate et utilisant la version `1.3.0` de la plateforme Linux ou une version antérieure nécessitent uniquement le point de terminaison d'un VPC Amazon ECR com.amazonaws.***region***.ecr.dkr et le point de terminaison de la passerelle Amazon S3 pour tirer parti de cette fonctionnalité.
- Les tâches Amazon ECS hébergées sur Fargate et utilisant la version `1.4.0` ou ultérieure de la plateforme Linux nécessitent à la fois les points de terminaison d'un VPC Amazon ECR com.amazonaws.***region***.ecr.dkr et com.amazonaws.***region***.ecr.api et le point de terminaison de passerelle Amazon S3 pour tirer parti de cette fonctionnalité.
- Les tâches Amazon ECS hébergées sur Fargate et utilisant la version `1.0.0` ou ultérieure de la plateforme Windows nécessitent à la fois les points de terminaison d'un VPC Amazon ECR com.amazonaws.***region***.ecr.dkr et com.amazonaws.***region***.ecr.api et le point de terminaison de passerelle Amazon S3 pour tirer parti de cette fonctionnalité.
- Les tâches Amazon ECS hébergées sur Fargate qui extrait des images de conteneur à partir d'Amazon ECR peuvent limiter l'accès au VPC spécifique utilisé par ces tâches et au point de terminaison d'un VPC utilisé par le service en ajoutant des clés de condition à au rôle IAM d'exécution de la tâche. Pour en savoir plus, consultez Autorisations IAM facultatives pour les tâches Fargate qui extraient des images Amazon ECR sur les points de terminaison d'interface dans le guide du développeur du service de conteneur Amazon Elastic.
- Les tâches Amazon ECS hébergées sur Fargate qui extraient des images de conteneurs d'Amazon ECR qui utilisent également le pilote de journal pour envoyer des informations de journal à Logs nécessitent `awslogs` le CloudWatch point de terminaison CloudWatch VPC Logs. Pour plus d'informations, consultez Création du point de terminaison CloudWatch Logs.
- Le groupe de sécurité attaché au point de terminaison d'un VPC doit autoriser les connexions entrantes sur le port 443 à partir du sous-réseau privé du VPC.
- Les points de terminaison d'un VPC ne prennent pas en charge les demandes inter-régions pour le moment. Veillez à créer vos points de terminaison d'un VPC dans la même région que celle où vous souhaitez envoyer vos appels d'API à Amazon ECR.
- À l'heure actuelle, les points de terminaison d'un VPC ne prennent pas en charge les référentiels publics Amazon ECR. Envisagez d'utiliser une règle de mise en cache par extraction pour héberger l'image publique dans un référentiel privé situé dans la même région que le point de terminaison d'un VPC. Pour plus d'informations, consultez Synchroniser un registre en amont avec un registre privé Amazon ECR.
- Les points de terminaison VPC ne prennent en charge que le AWS DNS fourni via Amazon Route 53. Si vous souhaitez utiliser votre propre DNS, vous pouvez utiliser le transfert DNS conditionnel. Pour en savoir plus, consultez Jeux d'options DHCP dans le guide de l'utilisateur Amazon VPC.

- Si vos conteneurs ont des connexions existantes vers Amazon S3, leurs connexions peuvent être brièvement interrompues lorsque vous ajoutez le point de terminaison de passerelle Amazon S3. Si vous souhaitez éviter cette interruption, créez un VPC qui utilise le point de terminaison de passerelle Amazon S3, puis migrez votre cluster Amazon ECS et ses conteneurs dans le nouveau VPC.
- Lorsqu'une image est extraite à l'aide d'une règle de mise en cache par extraction pour la première fois, si vous avez configuré Amazon ECR pour utiliser un point de terminaison d'un VPC d'interface à l'aide de AWS PrivateLink , vous devez créer un sous-réseau public dans le même VPC, avec une passerelle NAT, puis acheminer tout le trafic sortant vers l'Internet depuis leur sous-réseau privé vers la passerelle NAT afin que l'extraction fonctionne. Les extractions d'images suivantes ne nécessitent pas cela. Pour plus d'informations, consultez la section Scénario : Accéder à Internet depuis un sous-réseau privé dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Considérations relatives aux images Windows

Les images basées sur le système d'exploitation Windows contiennent des artefacts dont la distribution est restreinte par la licence. Par défaut, lorsque vous poussez des images Windows vers un référentiel Amazon ECR, les couches qui contiennent ces artefacts ne sont pas poussées, car elles sont considérées comme des couches étrangères. Lorsque les artefacts sont fournis par Microsoft, les couches étrangères sont récupérées à partir de l'infrastructure Microsoft Azure. Pour cette raison, afin de permettre à vos conteneurs d'extraire ces couches étrangères d'Azure, des étapes supplémentaires sont nécessaires au-delà de la création des points de terminaison d'un VPC.

Il est possible de remplacer ce comportement lorsque vous poussez des images Windows vers Amazon ECR à l'aide de la clé `--allow-nondistributable-artifacts` dans le démon Docker. Lorsqu'il est activé, cet indicateur envoie les couches sous licence vers Amazon ECR, ce qui permet d'extraire ces images d'Amazon ECR via le point de terminaison d'un VPC, sans qu'un accès supplémentaire à Azure soit requis.

> **Important**
>
> L'utilisation de l'indicateur `--allow-nondistributable-artifacts` n'exclut pas votre obligation de respecter les termes de la licence d'image de base du conteneur Windows ; vous ne pouvez pas publier du contenu Windows pour une redistribution publique ou tierce. L'utilisation dans votre propre environnement est autorisée.

Pour activer l'utilisation de cet indicateur pour votre installation Docker, vous devez modifier le fichier de configuration du démon Docker qui, en fonction de votre installation Docker, peut généralement être configuré dans le menu des paramètres ou des préférences sous l'onglet Moteur Docker ou en modifiant directement le fichier `C:\ProgramData\docker\config\daemon.json`.

Voici un exemple de configuration de la configuration requise. Remplacez la valeur par l'URI du référentiel vers lequel vous poussez les images.

```
{
    "allow-nondistributable-artifacts": [
        "111122223333.dkr.ecr.us-west-2.amazonaws.com"
    ]
}
```

Après avoir modifié le fichier de configuration du démon Docker, vous devrez redémarrer le démon Docker avant de tenter de pousser votre image. Confirmez que la transmission a fonctionné en vérifiant que la couche de base a fait l'objet d'une transmission de type push vers votre référentiel.

> **Note**
>
> Les couches de base des images Windows sont volumineuses. La taille de la couche entraînera un délai de transmission plus long et des coûts de stockage supplémentaires dans Amazon ECR pour ces images. Pour ces raisons, nous vous recommandons d'utiliser cette option uniquement lorsqu'elle est strictement nécessaire pour réduire les temps de création et les coûts de stockage continus. Par exemple, la taille de l'image `mcr.microsoft.com/windows/servercore`est d'environ 1,7 Go lorsqu'elle est compressée dans Amazon ECR.

Créer des points de terminaison d'un VPC pour Amazon ECR

Pour créer des points de terminaison d'un VPC pour le service Amazon ECR, utilisez la procédure Créer un point de terminaison d'interface que vous trouverez dans le gui de l'utilisateur Amazon VPC.

Les tâches Amazon ECS hébergées sur des instances Amazon EC2 nécessitent des points de terminaison Amazon ECR et le point de terminaison de passerelle Amazon S3.

Les tâches Amazon ECS hébergées sur Fargate et utilisant la version `1.4.0` de la plateforme ou version ultérieure nécessitent à la fois les points de terminaison d'un VPC Amazon ECR et les points de terminaison de la passerelle Amazon S3.

Les tâches Amazon ECS hébergées sur Fargate qui utilisent la version `1.3.0` de la plateforme ou une version antérieure nécessitent uniquement le point de terminaison d'un VPC Amazon ECR com.amazonaws.*region*.ecr.dkr et les points de terminaison de la passerelle Amazon S3.

> **Note**
>
> L'ordre dans lequel les points de terminaison sont créés n'a pas d'importance.

com.amazonaws.*region*.ecr.dkr

Ce point de terminaison est utilisé pour les API de registre Docker. Les commandes du client Docker telles que `push` et `pull` utilisent ce point de terminaison.

Lorsque vous créez ce point de terminaison, vous devez activer un nom d'hôte DNS privé. Pour ce faire, assurez-vous que l'option Activer le nom DNS privé est sélectionnée dans la console Amazon VPC lorsque vous créez le point de terminaison d'un VPC.

com.amazonaws.*region*.ecr.api

> **Note**
>
> La *région* spécifiée représente l'identifiant de région d'une AWS région prise en charge par Amazon ECR, telle que `us-east-2` la région USA Est (Ohio).

Ce point de terminaison est utilisé pour les appels à l'API Amazon ECR. Les actions d'API telles que `DescribeImages` et `CreateRepository` vont jusqu'à ce point de terminaison.

Lorsque ce point de terminaison est créé, vous avez la possibilité d'activer un nom d'hôte DNS privé. Activez ce nom d'hôte en sélectionnant Activer le nom de DNS privé dans la console VPC lorsque vous créez le point de terminaison d'un VPC. Si vous activez un nom d'hôte DNS privé pour le point de terminaison VPC, mettez à jour votre SDK AWS CLI ou optez pour la dernière version afin qu'il ne soit pas nécessaire de spécifier une URL de point de terminaison lors de l'utilisation du SDK AWS CLI .

Si vous activez un nom d'hôte DNS privé et que vous utilisez un SDK ou une AWS CLI version publiée avant le 24 janvier 2019, vous devez utiliser le `--endpoint-url` paramètre pour spécifier les points de terminaison de l'interface. L'exemple suivant montre le format de l'URL du point de terminaison.

```
aws ecr create-repository --repository-name name --endpoint-url https://
api.ecr.region.amazonaws.com
```

Si vous n'activez pas un nom d'hôte DNS privé pour le point de terminaison d'un VPC, vous devrez utiliser le paramètre `--endpoint-url` en spécifiant l'ID du point de terminaison de VPC pour le point de terminaison d'interface. L'exemple suivant montre le format de l'URL du point de terminaison.

```
aws ecr create-repository --repository-name name --endpoint-url
 https://VPC_endpoint_ID.api.ecr.region.vpce.amazonaws.com
```

Créer le point de terminaison de la passerelle Amazon S3

Pour que vos tâches Amazon ECS puissent extraire des images privées d'Amazon ECR, vous devez créer un point de terminaison de passerelle pour Amazon S3. Le point de terminaison de passerelle est obligatoire, car Amazon ECR utilise Amazon S3 pour stocker vos couches d'images. Lorsque vos conteneurs téléchargent des images depuis Amazon ECR, ils doivent accéder à Amazon ECR pour obtenir le manifeste d'image et à Amazon S3 pour télécharger les couches d'image réelles. Voici l'Amazon Resource Name (ARN) du compartiment Amazon S3 contenant les couches pour chaque image Docker.

```
arn:aws:s3:::prod-region-starport-layer-bucket/*
```

Utilisez la procédure Créer un point de terminaison de passerelle dans le guide de l'utilisateur Amazon VPC pour créer le point de terminaison de la passerelle Amazon S3 suivant pour Amazon ECR. Lorsque vous créez le point de terminaison, veillez à sélectionner les tables de routage pour votre VPC.

com.amazonaws.*region*.s3

Le point de terminaison de la passerelle Amazon S3 utilise un document de politique IAM pour limiter l'accès au service. Vous pouvez utiliser la politique Accès total en raison des restrictions que vous avez placées dans les rôles IAM de votre tâche, ou si d'autres politiques utilisateur IAM restent applicables au-dessus de cette politique. Si vous souhaitez limiter l'accès au compartiment Amazon S3 aux autorisations minimales requises pour utiliser Amazon ECR, consultez Autorisations minimales relatives aux compartiments Amazon S3 pour Amazon ECR.

Autorisations minimales relatives aux compartiments Amazon S3 pour Amazon ECR

Le point de terminaison de la passerelle Amazon S3 utilise un document de politique IAM pour limiter l'accès au service. Pour accorder uniquement les autorisations minimales de compartiment Amazon S3 pour Amazon ECR, limitez l'accès au compartiment Amazon S3 utilisé par Amazon ECR lorsque vous créez le document de politique IAM pour le point de terminaison.

Le tableau suivant décrit les autorisations de la politique de compartiment Amazon S3 requises par Amazon ECR.

Autorisation	Description
`arn:aws:s3:::prod-` *`region`* `-starport-layer-bucket/*`	Fournit l'accès au compartiment Amazon S3 contenant les couches pour chaque image Docker. Représente l'identifiant de région d'une région AWS prise en charge par Amazon ECR, telle que `us-east-2` pour la région USA Est (Ohio).

Exemple

L'exemple suivant montre comment fournir l'accès aux compartiments Amazon S3 requis pour les opérations Amazon ECR.

```
{
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::prod-region-starport-layer-bucket/*"]
    }
  ]
}
```

Création du point de terminaison CloudWatch Logs

Les tâches Amazon ECS utilisant le type de lancement Fargate qui utilisent un VPC sans passerelle Internet et qui utilisent également le pilote de journal pour envoyer des informations de journal à Logs nécessitent que vous créiez **`awslogs`** le fichier CloudWatch com.amazonaws. point de terminaison CloudWatch VPC de l'interface ***`region`*** .logs. Pour plus d'informations, consultez la section Utilisation CloudWatch des journaux avec les points de terminaison VPC de l'interface dans le guide de l'utilisateur Amazon CloudWatch Logs.

Créer une politique de point de terminaison pour vos points de terminaison d'un VPC Amazon ECR

Une politique de point de terminaison d'un VPC est une politique de ressource IAM que vous attachez à un point de terminaison lorsque vous le créez ou le modifiez. Si vous n'attachez pas de politique lorsque vous créez un point de AWS terminaison, associez une politique par défaut qui permet un accès complet au service. Une stratégie de point de terminaison n'annule pas et ne remplace pas les stratégies utilisateur ou les stratégies propres au service. Il s'agit d'une politique distincte qui contrôle l'accès depuis le point de terminaison jusqu'au service spécifié. Les politiques de point de terminaison doivent être écrites au format JSON. Pour en savoir plus, consultez Contrôle de l'accès aux services avec des points de terminaison d'un VPC dans le guide de l'utilisateur Amazon VPC.

Nous vous recommandons de créer une politique de ressource IAM unique et de l'attacher aux deux points de terminaison d'un VPC Amazon ECR.

Voici un exemple de politique de point de terminaison pour l'API Amazon ECR. Cette politique permet à un rôle IAM spécifique d'extraire des images depuis Amazon ECR.

```
{
 "Statement": [{
  "Sid": "AllowPull",
  "Principal": {
   "AWS": "arn:aws:iam::1234567890:role/role_name"
  },
  "Action": [
   "ecr:BatchGetImage",
   "ecr:GetDownloadUrlForLayer",
                   "ecr:GetAuthorizationToken"
  ],
  "Effect": "Allow",
```

```
  "Resource": "*"
 }]
}
```

L'exemple de politique de point de terminaison suivant empêche la suppression d'un référentiel spécifié.

```
{
 "Statement": [{
   "Sid": "AllowAll",
   "Principal": "*",
   "Action": "*",
   "Effect": "Allow",
   "Resource": "*"
  },
  {
   "Sid": "PreventDelete",
   "Principal": "*",
   "Action": "ecr:DeleteRepository",
   "Effect": "Deny",
   "Resource": "arn:aws:ecr:region:1234567890:repository/repository_name"
  }
 ]
}
```

L'exemple de politique de point de terminaison suivant combine les deux exemples précédents en une seule politique.

```
{
 "Statement": [{
   "Sid": "AllowAll",
   "Effect": "Allow",
   "Principal": "*",
   "Action": "*",
   "Resource": "*"
  },
  {
   "Sid": "PreventDelete",
   "Effect": "Deny",
   "Principal": "*",
   "Action": "ecr:DeleteRepository",
   "Resource": "arn:aws:ecr:region:1234567890:repository/repository_name"
```

```
  },
  {
   "Sid": "AllowPull",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::1234567890:role/role_name"
   },
   "Action": [
    "ecr:BatchGetImage",
    "ecr:GetDownloadUrlForLayer",
                          "ecr:GetAuthorizationToken"
   ],
   "Resource": "*"
  }
 ]
}
```

Pour modifier la politique de point de terminaison d'un VPC pour Amazon ECR

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Si vous n'avez pas encore créé les points de terminaison d'un VPC pour Amazon ECR, consultez Créer des points de terminaison d'un VPC pour Amazon ECR.
4. Sélectionnez le point de terminaison d'un VPC Amazon ECR auquel ajouter une politique, puis choisissez l'onglet Politique dans la partie inférieure de l'écran.
5. Choisissez Modifier la politique, puis apportez les modifications souhaitées à la politique.
6. Choisissez Enregistrer pour enregistrer la politique.

Sous-réseaux partagés

Vous ne pouvez pas créer, décrire, modifier ou supprimer des points de terminaison d'un VPC dans des sous-réseaux qui sont partagés avec vous. Toutefois, vous pouvez utiliser les points de terminaison d'un VPC dans les sous-réseaux qui sont partagés avec vous.

Prévention du cas de figure de l'adjoint désorienté 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 la confusion des 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` ou `aws:SourceAccount` dans les politiques de ressources afin de limiter les autorisations à la ressource octroyées par Amazon ECR à un autre service. 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.

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:`*`servicename`*`:`*`region`*`:`*`123456789012`*`:*`.

Si la valeur `aws:SourceArn` ne contient pas l'ID du compte, tel qu'un ARN de compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations.

La valeur de `aws:SourceArn` doit être ResourceDescription.

L'exemple suivant montre comment vous pouvez utiliser les clés de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et les clés de contexte dans une politique de référentiel Amazon ECR pour autoriser l' AWS CodeBuild accès aux actions de l'API Amazon ECR nécessaires à l'intégration à ce service, tout en évitant le problème de confusion lié aux adjoints.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"CodeBuildAccess",
         "Effect":"Allow",
         "Principal":{
            "Service":"codebuild.amazonaws.com"
         },
```

```
         "Action":[
            "ecr:BatchGetImage",
            "ecr:GetDownloadUrlForLayer"
         ],
         "Condition":{
            "ArnLike":{
               "aws:SourceArn":"arn:aws:codebuild:region:123456789012:project/project-
name"
            },
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            }
         }
      }
   ]
}
```

Surveiller Amazon ECR

Vous pouvez surveiller l'utilisation de l'API Amazon ECR avec Amazon CloudWatch, qui collecte et traite les données brutes d'Amazon ECR pour en faire des indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pendant une période de deux semaines afin que vous puissiez accéder aux informations historiques et avoir une idée plus précise de votre utilisation des API. Les données métriques Amazon ECR sont automatiquement envoyées par intervalles CloudWatch d'une minute. Pour plus d'informations CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Amazon ECR fournit des métriques basées sur l'utilisation de votre API en ce qui concerne les actions d'autorisation, de transmission d'image et d'extraction d'image.

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon ECR et de vos AWS solutions. Nous vous recommandons de collecter des données de surveillance à partir des ressources qui constituent votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. Avant de commencer à surveiller Amazon ECR, vous devez cependant créer un plan de surveillance qui contient les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

L'étape suivante consiste à établir une référence de performances Amazon ECR normales dans votre environnement, en mesurant la performance à différents moments et dans différentes conditions de charge. Lorsque vous surveillez Amazon ECR, conservez les données de l'historique de surveillance afin de pouvoir les comparer aux nouvelles données de performances, d'identifier les modèles de performances normales et les anomalies de performances, et de concevoir des méthodes pour résoudre les problèmes.

Rubriques

- Visualiser vos quotas de service et définir des alarmes

- Métriques d'utilisation Amazon ECR
- Rapports d'utilisation d'Amazon ECR
- Métriques de référentiel Amazon ECR
- Événements Amazon ECR et EventBridge
- Journalisation des actions Amazon ECR avec AWS CloudTrail

Visualiser vos quotas de service et définir des alarmes

Vous pouvez utiliser la CloudWatch console pour visualiser vos quotas de service et comparer votre utilisation actuelle aux quotas de service. Vous pouvez également définir des alarmes afin d'être averti lorsque vous approchez un quota.

Visualiser un quota de service et définir éventuellement une alarme

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, choisissez Métriques.
3. Sous l'onglet Toutes les métriques, choisissez Utilisation, puis choisissez Par ressource AWS .

   La liste des métriques d'utilisation des Service Quotas s'affiche.
4. Cochez la case en regard de l'une des métriques.

   Le graphique indique votre utilisation actuelle de cette AWS ressource.
5. Pour ajouter votre quota de service au graphique, procédez comme suit :

   a. Sélectionnez l'onglet Graphed metrics (Graphiques des métriques).

   b. Choisissez Math expression (Expression mathématique), puis Start with an empty expression (Commencer par une expression vide). Ensuite, dans la nouvelle ligne, sous Détails, saisissez **`SERVICE_QUOTA(m1)`**.

      Une nouvelle ligne est ajoutée au graphique avec le quota de service de la ressource représentée dans la métrique.
6. Pour afficher votre utilisation actuelle sous forme de pourcentage du quota, ajoutez une nouvelle expression ou modifiez l'expression SERVICE_QUOTA actuelle. Pour la nouvelle expression, utilisez **`m1/60/SERVICE_QUOTA(m1)*100`**
7. (Facultatif) Pour définir une alerte qui vous avertit si vous approchez du quota de service, procédez comme suit :

a. Sur la ligne **`m1/60/SERVICE_QUOTA(m1)*100`**, sous Actions, choisissez l'icône d'alarme. Elle ressemble à une cloche.

   La page de création d'alerte s'affiche.

b. Sous Conditions, vérifiez que le Threshold type (Type de seuil) est Static (Statique) et que Whenever Expression1 is (Lorsque Expression1 est) est défini sur Greater (Supérieur). Sous than (à), entrez **`80`**. Cela crée une alerte qui passe à l'état alerte lorsque votre utilisation dépasse 80 % du quota.

c. Choisissez Suivant.

d. Dans la page suivante, sélectionnez une rubrique Amazon SNS ou créez-en une nouvelle. Cette rubrique est notifiée lorsque l'alarme passe à l'état ALARME. Ensuite, choisissez Suivant.

e. Dans la page suivante, saisissez le nom et la description de l'alarme, puis choisissez Suivant.

f. Choisissez Créer une alarme.

Métriques d'utilisation Amazon ECR

Vous pouvez utiliser les statistiques CloudWatch d'utilisation pour obtenir une visibilité sur l'utilisation des ressources par votre compte. Utilisez ces indicateurs pour visualiser l'utilisation actuelle de vos services sur CloudWatch des graphiques et des tableaux de bord.

Les métriques d'utilisation d'Amazon ECR correspondent aux quotas AWS de service. Vous pouvez configurer des alarmes qui vous alertent lorsque votre utilisation approche d'un quota de service. Pour en savoir plus sur les quotas de service par défaut d'Amazon ECR, consultez Service Quotas Amazon ECR..

Amazon ECR publie les métriques suivantes dans l'espace de noms `AWS/Usage`.

Métrique	Description
`CallCount`	Nombre d'appels d'action d'API depuis votre compte. Les ressources sont définies par les dimensions associées à la métrique.

Métrique	Description
	La statistique la plus utile pour cette métrique est `SUM`, qui représente la somme des valeurs de tous les contributeurs pendant la période définie.

Les dimensions suivantes permettent d'affiner les métriques d'utilisation publiées par Amazon ECR.

Dimension	Description
`Service`	Nom du AWS service contenant la ressource. Pour les métriques d'utilisation d'Amazon ECR, la valeur de cette dimension est `ECR`.
`Type`	Type d'entité faisant l'objet d'un rapport. Actuellement, la seule valeur valide pour les métriques d'utilisation d'Amazon ECR est `API`.
`Resource`	Type de ressource en cours d'exécution. Actuellement, Amazon ECR renvoie des informations sur l'utilisation de votre API pour les actions d'API suivantes. • GetAuthorizationToken • BatchCheckLayerAvailability • InitiateLayerUpload • UploadLayerPart • CompleteLayerUpload • PutImage • BatchGetImage • GetDownloadUrlForLayer
`Class`	Classe de ressource suivie. Actuellement, Amazon ECR n'utilise pas la dimension Class.

Rapports d'utilisation d'Amazon ECR

AWS fournit un outil de reporting gratuit appelé Cost Explorer qui vous permet d'analyser le coût et l'utilisation de vos ressources Amazon ECR.

Utilisez Cost Explorer pour afficher les graphiques de votre utilisation et de vos coûts. Vous pouvez afficher les données des 13 mois précédents et prévoir vos dépenses pour les trois prochains mois. Vous pouvez utiliser Cost Explorer pour afficher des modèles de vos dépenses en ressources AWS au fil du temps, identifier les domaines qui méritent d'être approfondis et connaître les tendances que vous pouvez utiliser pour comprendre vos coûts. Vous pouvez également préciser des plages de temps pour les données et afficher des données temporelles par jour ou par mois.

Les données de métriques de vos rapports sur les coûts et l'utilisation illustrent l'utilisation dans l'ensemble de vos référentiels Amazon ECR. Pour plus d'informations, consultez Identification de vos ressources pour facturation.

Pour plus d'informations sur la création d'un rapport sur les AWS coûts et l'utilisation, consultez le rapport sur les AWS coûts et l'utilisation dans le guide de AWS Billing l'utilisateur.

Métriques de référentiel Amazon ECR

Amazon ECR envoie les statistiques du nombre d'appels du référentiel à Amazon CloudWatch. Les données métriques Amazon ECR sont automatiquement envoyées par tranches CloudWatch d'une minute. Pour plus d'informations CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Rubriques

- CloudWatch Indicateurs habilitants
- Métriques et dimensions disponibles
- Afficher les métriques Amazon ECR à l'aide de la console CloudWatch

CloudWatch Indicateurs habilitants

Amazon ECR envoie des métriques de référentiel automatiquement pour tous les référentiels. Il n'est pas nécessaire d'effectuer des étapes manuelles.

Métriques et dimensions disponibles

Les sections suivantes répertorient les métriques et les dimensions qu'Amazon ECR envoie à Amazon CloudWatch.

Métriques Amazon ECR

Amazon ECR fournit des métriques pour vous permettre de contrôler vos référentiels. Vous pouvez mesurer le nombre d'extractions.

L'espace de noms `AWS/ECR` inclut les métriques suivantes.

`RepositoryPullCount`

Le nombre total d'extractions pour les images dans le référentiel.

Dimensions valides : `RepositoryName`.

Statistiques valides : Moyenne, Minimum, Maximum, Somme, Nombre d'échantillons. La statistique la plus utile est Sum (Somme).

Unité : Entier.

Dimensions pour les métriques Amazon ECR

Les métriques Amazon ECR utilisent l'espace de noms `AWS/ECR` et fournissent des métriques pour les dimensions suivantes.

`RepositoryName`

Cette dimension filtre les données que vous demandez pour toutes les images de conteneur dans un référentiel spécifié.

Afficher les métriques Amazon ECR à l'aide de la console CloudWatch

Vous pouvez consulter les métriques du référentiel Amazon ECR sur la CloudWatch console. La CloudWatch console fournit un affichage précis et personnalisable de vos ressources. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Pour afficher les métriques dans la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans la navigation de gauche, choisissez Metrics (Métriques), All metrics (Toutes les métriques).
3. Dans l'onglet Browse (Parcourir), sous AWS Namespaces (Espaces de noms), choisissez ECR.
4. Choisissez les métriques à afficher. Les métriques de référentiel sont définies comme ECR > Repository Metrics (ECR > Métriques de référentiel).

Événements Amazon ECR et EventBridge

Amazon vous EventBridge permet d'automatiser vos AWS services et de répondre automatiquement aux événements du système tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour indiquer quels événements vous intéressent et inclure les actions automatisées à effectuer quand un événement correspond à une règle. Les actions pouvant être déclenchées automatiquement sont les suivantes :

- Ajouter des événements à des groupes de CloudWatch journaux dans Logs
- Invoquer une fonction AWS Lambda
- Appel de la fonctionnalité Exécuter la commande d'Amazon EC2
- Relais de l'événement à Amazon Kinesis Data Streams
- Activation d'une machine à AWS Step Functions états
- Notification d'une rubrique Amazon SNS ou d'une file d'attente Amazon SQS

Pour plus d'informations, consultez Getting Started with Amazon EventBridge dans le guide de EventBridge l'utilisateur Amazon.

Exemples d'événements d'Amazon ECR

Voici des exemples d'événements à partir d'Amazon ECR. Les événements sont générés dans la mesure du possible.

Événement pour un transfert d'image terminée

L'événement suivant est envoyé lorsque chaque transfert d'image est terminé. Pour plus d'informations, consultez Transférer une image Docker vers un référentiel privé Amazon ECR.

```
{
    "version": "0",
    "id": "13cde686-328b-6117-af20-0e5566167482",
    "detail-type": "ECR Image Action",
    "source": "aws.ecr",
    "account": "123456789012",
    "time": "2019-11-16T01:54:34Z",
    "region": "us-west-2",
    "resources": [],
    "detail": {
        "result": "SUCCESS",
        "repository-name": "my-repository-name",
        "image-digest":
 "sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
        "action-type": "PUSH",
        "image-tag": "latest"
    }
}
```

Événement pour une action de mise en cache par extraction

L'événement suivant est envoyé lorsqu'une action de mise en cache par extraction est tentée. Pour plus d'informations, consultez Synchroniser un registre en amont avec un registre privé Amazon ECR.

```
{
    "version": "0",
    "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
    "detail-type": "ECR Pull Through Cache Action",
    "source": "aws.ecr",
    "account": "123456789012",
    "time": "2023-02-29T02:36:48Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:ecr:us-west-2:123456789012:repository/docker-hub/alpine"
    ],
    "detail": {
        "rule-version": "1",
        "sync-status": "SUCCESS",
        "ecr-repository-prefix": "docker-hub",
        "repository-name": "docker-hub/alpine",
        "upstream-registry-url": "public.ecr.aws",
        "image-tag": "3.17.2",
```

```
        "image-digest":
 "sha256:4aa08ef415aecc80814cb42fa41b658480779d80c77ab15EXAMPLE",
    }
}
```

Événement pour une analyse d'image terminée (analyse de base)

Lorsque l'analyse de base est activée pour votre registre, l'événement suivant est envoyé lorsque chaque analyse d'image est terminée. Le paramètre `finding-severity-counts` ne retournera une valeur pour un niveau de gravité que s'il en existe un. Par exemple, si l'image ne contient pas de résultats au niveau `CRITICAL`, aucun nombre critique ne sera renvoyé. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités du système d'exploitation dans Amazon ECR.

> **Note**
>
> Pour plus de détails sur les événements qu'Amazon Inspector émet lorsque l'analyse améliorée est activée, consultez EventBridge événements envoyés pour une analyse améliorée dans Amazon ECR.

```
{
    "version": "0",
    "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
    "detail-type": "ECR Image Scan",
    "source": "aws.ecr",
    "account": "123456789012",
    "time": "2019-10-29T02:36:48Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:123456789012:repository/my-repository-name"
    ],
    "detail": {
        "scan-status": "COMPLETE",
        "repository-name": "my-repository-name",
        "finding-severity-counts": {
        "CRITICAL": 10,
        "MEDIUM": 9
      },
        "image-digest":
 "sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
```

```
        "image-tags": []
    }
}
```

Événement pour une notification de changement sur une ressource dont l'analyse améliorée est activée (analyse améliorée)

Lorsque l'analyse améliorée est activée pour votre registre, l'événement suivant est envoyé par Amazon ECR lorsqu'il y a un changement avec une ressource dont l'analyse améliorée est activée. Cela inclut la création de nouveaux référentiels, la modification de la fréquence d'analyse d'un référentiel ou la création ou la suppression d'images dans des référentiels dont l'analyse améliorée est activée. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités logicielles dans Amazon ECR.

```
{
 "version": "0",
 "id": "0c18352a-a4d4-6853-ef53-0ab8638973bf",
 "detail-type": "ECR Scan Resource Change",
 "source": "aws.ecr",
 "account": "123456789012",
 "time": "2021-10-14T20:53:46Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {
  "action-type": "SCAN_FREQUENCY_CHANGE",
  "repositories": [{
    "repository-name": "repository-1",
    "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-1",
    "scan-frequency": "SCAN_ON_PUSH",
    "previous-scan-frequency": "MANUAL"
   },
   {
    "repository-name": "repository-2",
    "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-2",
    "scan-frequency": "CONTINUOUS_SCAN",
    "previous-scan-frequency": "SCAN_ON_PUSH"
   },
   {
    "repository-name": "repository-3",
    "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-3",
    "scan-frequency": "CONTINUOUS_SCAN",
    "previous-scan-frequency": "SCAN_ON_PUSH"
```

```
    }
   ],
   "resource-type": "REPOSITORY",
   "scan-type": "ENHANCED"
  }
}
```

Événement pour une suppression d'image

L'événement suivant est envoyé lorsqu'une image est supprimée. Pour plus d'informations, consultez Supprimer une image dans Amazon ECR.

```
{
    "version": "0",
    "id": "dd3b46cb-2c74-f49e-393b-28286b67279d",
    "detail-type": "ECR Image Action",
    "source": "aws.ecr",
    "account": "123456789012",
    "time": "2019-11-16T02:01:05Z",
    "region": "us-west-2",
    "resources": [],
    "detail": {
        "result": "SUCCESS",
        "repository-name": "my-repository-name",
        "image-digest":
 "sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
        "action-type": "DELETE",
        "image-tag": "latest"
    }
}
```

Journalisation des actions Amazon ECR avec AWS CloudTrail

Amazon ECR 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 ECR. CloudTrail capture les actions Amazon ECR suivantes sous forme d'événements :

- Tous les appels d'API, notamment les appels à partir de la console Amazon ECR
- Toutes les actions effectuées en raison des paramètres de chiffrement sur vos référentiels
- Toutes les actions entreprises en vertu des règles de politique de cycle de vie, qu'elles réussissent ou qu'elles échouent

> **Important**
>
> En raison des limites de taille des CloudTrail événements individuels, pour les actions politiques relatives au cycle de vie impliquant l'expiration de 10 images ou plus, Amazon ECR envoie plusieurs événements à CloudTrail. En outre, Amazon ECR inclut un maximum de 100 identifications par image.

Lorsqu'un suivi est créé, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon ECR. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. En utilisant ces informations, vous pouvez déterminer la demande qui a été envoyée à Amazon ECR, l'adresse IP source, qui a effectué la demande, quand, ainsi que d'autres informations.

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

Informations Amazon ECR dans CloudTrail

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

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour Amazon ECR, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Si vous créez un journal d'activité dans la console, vous pourrez l'appliquer à une seule région ou à toutes les régions. Le journal enregistre les événements dans la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez :

- Création d'un parcours pour votre AWS compte
- AWS intégrations de services avec journaux CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail

- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions de l'API Amazon ECR sont enregistrées CloudTrail et documentées dans le manuel Amazon Elastic Container Registry API Reference. Lorsque vous effectuez des tâches courantes, des sections sont générées dans les fichiers CloudTrail journaux pour chaque action d'API faisant partie de cette tâche. Par exemple, lorsque vous créez un référentiel`GetAuthorizationToken`, `CreateRepository` et que `SetRepositoryPolicy` des sections sont générées dans les fichiers CloudTrail journaux. Lorsque vous transférez une image vers un référentiel, les sections `InitiateLayerUpload`, `UploadLayerPart`, `CompleteLayerUpload` et `PutImage` sont générées. Lorsque vous extrayez une image, les sections `GetDownloadUrlForLayer` et `BatchGetImage` sont générées. Pour obtenir des exemples de ces tâches courantes, consultez CloudTrail exemples de saisie de journal.

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

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été faite par un autre AWS service

Pour plus d'informations, consultez l'`CloudTrailuserIdentity`élément.

Présentation des entrées des fichiers journaux Amazon ECR

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

CloudTrail exemples de saisie de journal

Vous trouverez ci-dessous des exemples de saisie de CloudTrail journal pour quelques tâches Amazon ECR courantes.

> **Note**
>
> Ces exemples ont été mis en forme pour faciliter la lecture. Dans un fichier CloudTrail journal, toutes les entrées et tous les événements sont concaténés sur une seule ligne. En outre, cet exemple se limite à une seule entrée Amazon ECR. Dans un véritable fichier CloudTrail journal, vous pouvez voir les entrées et les événements de plusieurs AWS services.

Rubriques

Exemple : Créer une action de référentiel

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateRepository`action.

```
{
    "eventVersion": "1.04",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
        "arn": "arn:aws:sts::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-07-11T21:54:07Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            }
```

```
        }
    },
    "eventTime": "2018-07-11T22:17:43Z",
    "eventSource": "ecr.amazonaws.com",
    "eventName": "CreateRepository",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "203.0.113.12",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "repositoryName": "testrepo"
    },
    "responseElements": {
        "repository": {
            "repositoryArn": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
            "repositoryName": "testrepo",
            "repositoryUri": "123456789012.dkr.ecr.us-east-2.amazonaws.com/testrepo",
            "createdAt": "Jul 11, 2018 10:17:44 PM",
            "registryId": "123456789012"
        }
    },
    "requestID": "cb8c167e-EXAMPLE",
    "eventID": "e3c6f4ce-EXAMPLE",
    "resources": [
        {
            "ARN": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
            "accountId": "123456789012"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Exemple : action d' AWS KMS CreateGrant API lors de la création d'un référentiel Amazon ECR

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l' AWS KMS CreateGrant action à effectuer lors de la création d'un référentiel Amazon ECR avec le chiffrement KMS activé. Pour chaque dépôt créé avec le chiffrement KMS activé, vous devriez voir apparaître deux entrées de CreateGrant journal CloudTrail.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
```

```
        "principalId": "AIDAIEP6W46J43IG7LXAQ",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "sessionIssuer": {

            },
            "webIdFederationData": {

            },
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-06-10T19:22:10Z"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2020-06-10T19:22:10Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "203.0.113.12",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "keyId": "4b55e5bf-39c8-41ad-b589-18464af7758a",
        "granteePrincipal": "ecr.us-west-2.amazonaws.com",
        "operations": [
            "GenerateDataKey",
            "Decrypt"
        ],
        "retiringPrincipal": "ecr.us-west-2.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {
                "aws:ecr:arn": "arn:aws:ecr:us-west-2:123456789012:repository/testrepo"
            }
        }
    },
    "responseElements": {
        "grantId": "3636af9adfee1accb67b83941087dcd45e7fadc4e74ff0103bb338422b5055f3"
    },
    "requestID": "047b7dea-b56b-4013-87e9-a089f0f6602b",
    "eventID": "af4c9573-c56a-4886-baca-a77526544469",
```

```
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:123456789012:key/4b55e5bf-39c8-41ad-
b589-18464af7758a"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Exemple : Action de transmission d'image

L'exemple suivant montre une entrée de CloudTrail journal illustrant une image push qui utilise l'`PutImage`action.

> **Note**
>
> Lorsque vous insérez une image, vous verrez `InitiateLayerUpload` également des `CompleteLayerUpload` références et des références dans les CloudTrail journaux. `UploadLayerPart`

```
{
    "eventVersion": "1.04",
    "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
    "arn": "arn:aws:sts::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "userName": "Mary_Major",
  "sessionContext": {
   "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2019-04-15T16:42:14Z"
   }
  }
 },
 "eventTime": "2019-04-15T16:45:00Z",
```

```
 "eventSource": "ecr.amazonaws.com",
 "eventName": "PutImage",
 "awsRegion": "us-east-2",
 "sourceIPAddress": "203.0.113.12",
 "userAgent": "console.amazonaws.com",
 "requestParameters": {
  "repositoryName": "testrepo",
  "imageTag": "latest",
  "registryId": "123456789012",
  "imageManifest": "{\n   \"schemaVersion\": 2,\n   \"mediaType\": \"application/
vnd.docker.distribution.manifest.v2+json\",\n   \"config\": {\n      \"mediaType\":
 \"application/vnd.docker.container.image.v1+json\",\n      \"size\": 5543,\n
 \"digest\": \"sha256:000b9b805af1cdb60628898c9f411996301a1c13afd3dbef1d8a16ac6dbf503a
\"\n   },\n   \"layers\": [\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 43252507,\n
 \"digest\": \"sha256:3b37166ec61459e76e33282dda08f2a9cd698ca7e3d6bc44e6a6e7580cdeff8e
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 846,\n         \"digest
\": \"sha256:504facff238fde83f1ca8f9f54520b4219c5b8f80be9616ddc52d31448a044bd
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 615,\n         \"digest
\": \"sha256:ebbcacd28e101968415b0c812b2d2dc60f969e36b0b08c073bf796e12b1bb449\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 850,\n         \"digest
\": \"sha256:c7fb3351ecad291a88b92b600037e2435c84a347683d540042086fe72c902b8a
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 168,\n         \"digest\":
 \"sha256:2e3debadcbf7e542e2aefbce1b64a358b1931fb403b3e4aeca27cb4d809d56c2\"\n      },
\n      {\n         \"mediaType\": \"application/vnd.docker.image.rootfs.diff.tar.gzip
\",\n         \"size\": 37720774,\n         \"digest\":
 \"sha256:f8c9f51ad524d8ae9bf4db69cd3e720ba92373ec265f5c390ffb21bb0c277941\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 30432107,\n
 \"digest\": \"sha256:813a50b13f61cf1f8d25f19fa96ad3aa5b552896c83e86ce413b48b091d7f01b
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 197,\n         \"digest
\": \"sha256:7ab043301a6187ea3293d80b30ba06c7bf1a0c3cd4c43d10353b31bc0cecfe7d
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 154,\n         \"digest
\": \"sha256:67012cca8f31dc3b8ee2305e7762fee20c250513effdedb38a1c37784a5a2e71\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 176,\n         \"digest
\": \"sha256:3bc892145603fffc9b1c97c94e2985b4cb19ca508750b15845a5d97becbd1a0e
\"\n      },\n      {\n         \"mediaType\": \"application/
```

```
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 183,\n         \"digest
\": \"sha256:6f1c79518f18251d35977e7e46bfa6c6b9cf50df2a79d4194941d95c54258d18\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 212,\n         \"digest
\": \"sha256:b7bcfbc2e2888afebede4dd1cd5eebf029bb6315feeaf0b56e425e11a50afe42\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 212,\n         \"digest\":
 \"sha256:2b220f8b0f32b7c2ed8eaafe1c802633bbd94849b9ab73926f0ba46cdae91629\"\n      }\n
   ]\n}"
 },
 "responseElements": {
  "image": {
   "repositoryName": "testrepo",
   "imageManifest": "{\n   \"schemaVersion\": 2,\n   \"mediaType\": \"application/
vnd.docker.distribution.manifest.v2+json\",\n   \"config\": {\n      \"mediaType\":
 \"application/vnd.docker.container.image.v1+json\",\n      \"size\": 5543,\n
 \"digest\": \"sha256:000b9b805af1cdb60628898c9f411996301a1c13afd3dbef1d8a16ac6dbf503a
\"\n   },\n   \"layers\": [\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 43252507,\n
 \"digest\": \"sha256:3b37166ec61459e76e33282dda08f2a9cd698ca7e3d6bc44e6a6e7580cdeff8e
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 846,\n         \"digest
\": \"sha256:504facff238fde83f1ca8f9f54520b4219c5b8f80be9616ddc52d31448a044bd
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 615,\n         \"digest
\": \"sha256:ebbcacd28e101968415b0c812b2d2dc60f969e36b0b08c073bf796e12b1bb449\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 850,\n         \"digest
\": \"sha256:c7fb3351ecad291a88b92b600037e2435c84a347683d540042086fe72c902b8a
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 168,\n         \"digest\":
 \"sha256:2e3debadcbf7e542e2aefbce1b64a358b1931fb403b3e4aeca27cb4d809d56c2\"\n      },
\n      {\n         \"mediaType\": \"application/vnd.docker.image.rootfs.diff.tar.gzip
\",\n         \"size\": 37720774,\n         \"digest\":
 \"sha256:f8c9f51ad524d8ae9bf4db69cd3e720ba92373ec265f5c390ffb21bb0c277941\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 30432107,\n
 \"digest\": \"sha256:813a50b13f61cf1f8d25f19fa96ad3aa5b552896c83e86ce413b48b091d7f01b
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 197,\n         \"digest
\": \"sha256:7ab043301a6187ea3293d80b30ba06c7bf1a0c3cd4c43d10353b31bc0cecfe7d
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 154,\n         \"digest
\": \"sha256:67012cca8f31dc3b8ee2305e7762fee20c250513effdedb38a1c37784a5a2e71\"\n
```

```
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 176,\n         \"digest
\": \"sha256:3bc892145603fffc9b1c97c94e2985b4cb19ca508750b15845a5d97becbd1a0e
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 183,\n         \"digest
\": \"sha256:6f1c79518f18251d35977e7e46bfa6c6b9cf50df2a79d4194941d95c54258d18\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 212,\n         \"digest
\": \"sha256:b7bcfbc2e2888afebede4dd1cd5eebf029bb6315feeaf0b56e425e11a50afe42\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 212,\n         \"digest\":
 \"sha256:2b220f8b0f32b7c2ed8eaafe1c802633bbd94849b9ab73926f0ba46cdae91629\"\n      }\n
   ]\n}",
   "registryId": "123456789012",
   "imageId": {
    "imageDigest":
 "sha256:98c8b060c21d9adbb6b8c41b916e95e6307102786973ab93a41e8b86d1fc6d3e",
    "imageTag": "latest"
   }
  }
 },
 "requestID": "cf044b7d-5f9d-11e9-9b2a-95983139cc57",
 "eventID": "2bfd4ee2-2178-4a82-a27d-b12939923f0f",
 "resources": [{
  "ARN": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
  "accountId": "123456789012"
 }],
 "eventType": "AwsApiCall",
 "recipientAccountId": "123456789012"
}
```


Exemple : Action d'extraction d'image

L'exemple suivant montre une entrée de CloudTrail journal qui illustre une extraction d'image utilisant l'`BatchGetImage`action.

> **Note**
>
> Lorsque vous extrayez une image, si vous ne l'avez pas déjà en local, vous verrez également `GetDownloadUrlForLayer` des références dans les CloudTrail journaux.

```
{
    "eventVersion": "1.04",
    "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
    "arn": "arn:aws:sts::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "userName": "Mary_Major",
  "sessionContext": {
   "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2019-04-15T16:42:14Z"
   }
  }
 },
 "eventTime": "2019-04-15T17:23:20Z",
 "eventSource": "ecr.amazonaws.com",
 "eventName": "BatchGetImage",
 "awsRegion": "us-east-2",
 "sourceIPAddress": "203.0.113.12",
 "userAgent": "console.amazonaws.com",
 "requestParameters": {
  "imageIds": [{
   "imageTag": "latest"
  }],
  "acceptedMediaTypes": [
   "application/json",
   "application/vnd.oci.image.manifest.v1+json",
   "application/vnd.oci.image.index.v1+json",
   "application/vnd.docker.distribution.manifest.v2+json",
   "application/vnd.docker.distribution.manifest.list.v2+json",
   "application/vnd.docker.distribution.manifest.v1+prettyjws"
  ],
  "repositoryName": "testrepo",
  "registryId": "123456789012"
 },
 "responseElements": null,
 "requestID": "2a1b97ee-5fa3-11e9-a8cd-cd2391aeda93",
 "eventID": "c84f5880-c2f9-4585-9757-28fa5c1065df",
 "resources": [{
  "ARN": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
  "accountId": "123456789012"
```

```
 }],
 "eventType": "AwsApiCall",
 "recipientAccountId": "123456789012"
}
```

Exemple : Action de politique de cycle de vie d'image

L'exemple suivant montre une entrée de CloudTrail journal qui montre quand une image a expiré en raison d'une règle de politique de cycle de vie. Ce type d'événement peut être localisé en filtrant le `PolicyExecutionEvent` pour le champ du nom d'événement.

> **Important**
>
> En raison des limites de taille des CloudTrail événements individuels, pour les actions politiques relatives au cycle de vie impliquant l'expiration de 10 images ou plus, Amazon ECR envoie plusieurs événements à CloudTrail. En outre, Amazon ECR inclut un maximum de 100 identifications par image.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2020-03-12T20:22:12Z",
    "eventSource": "ecr.amazonaws.com",
    "eventName": "PolicyExecutionEvent",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "9354dd7f-9aac-4e9d-956d-12561a4923aa",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:ecr:us-west-2:123456789012:repository/testrepo",
            "accountId": "123456789012",
            "type": "AWS::ECR::Repository"
        }
    ],
```

```
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "repositoryName": "testrepo",
        "lifecycleEventPolicy": {
            "lifecycleEventRules": [
                {
                    "rulePriority": 1,
                    "description": "remove all images > 2",
                    "lifecycleEventSelection": {
                        "tagStatus": "Any",
                        "tagPrefixList": [],
                        "countType": "Image count more than",
                        "countNumber": 2
                    },
                    "action": "expire"
                }
            ],
            "lastEvaluatedAt": 0,
            "policyVersion": 1,
            "policyId": "ceb86829-58e7-9498-920c-aa042e33037b"
        },
        "lifecycleEventImageActions": [
            {
                "lifecycleEventImage": {
                    "digest":
"sha256:ddba4d27a7ffc3f86dd6c2f92041af252a1f23a8e742c90e6e1297bfa1bc0c45",
                    "tagStatus": "Tagged",
                    "tagList": [
                        "alpine"
                    ],
                    "pushedAt": 1584042813000
                },
                "rulePriority": 1
            },
            {
                "lifecycleEventImage": {
                    "digest":
"sha256:6ab380c5a5acf71c1b6660d645d2cd79cc8ce91b38e0352cbf9561e050427baf",
                    "tagStatus": "Tagged",
                    "tagList": [
                        "centos"
                    ],
                    "pushedAt": 1584042842000
```

```
                },
                "rulePriority": 1
            }
        ]
    }
}
```

Utilisation d'Amazon ECR avec un SDK AWS

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. Chaque SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

Documentation SDK	Exemples de code
AWS SDK for C++	AWS SDK for C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK for Go	AWS SDK for Go exemples de code
AWS SDK for Java	AWS SDK for Java exemples de code
AWS SDK for JavaScript	AWS SDK for JavaScript exemples de code
Kit AWS SDK pour Kotlin	Kit AWS SDK pour Kotlin exemples de code
AWS SDK for .NET	AWS SDK for .NET exemples de code
AWS SDK for PHP	AWS SDK for PHP exemples de code
AWS Tools for PowerShell	Outils pour des exemples PowerShell de code
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) exemples de code
AWS SDK for Ruby	AWS SDK for Ruby exemples de code
Kit AWS SDK pour Rust	Kit AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
Kit AWS SDK pour Swift	Kit AWS SDK pour Swift exemples de code

Exemple de disponibilité

Vous n'avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Provide feedback (Fournir un commentaire) en bas de cette page.

Exemples de code pour Amazon ECR à l'aide de kits SDK AWS

Les exemples de code suivants montrent comment utiliser Amazon ECR avec un kit de développement AWS logiciel (SDK).

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés et dans des exemples interservices.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon ECR avec un SDK AWS. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

- Actions pour Amazon ECR à l'aide de kits SDK AWS
  - Utilisation DescribeRepositories avec un AWS SDK ou une CLI
  - Utilisation ListImages avec un AWS SDK ou une CLI

Actions pour Amazon ECR à l'aide de kits SDK AWS

Les exemples de code suivants montrent comment effectuer des actions Amazon ECR individuelles avec des AWS SDK. Ces extraits appellent l'API Amazon ECR et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour une liste complète, consultez le manuel Amazon Elastic Container Registry (Amazon ECR) API Reference.

Exemples

- Utilisation DescribeRepositories avec un AWS SDK ou une CLI
- Utilisation ListImages avec un AWS SDK ou une CLI

Utilisation **`DescribeRepositories`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DescribeRepositories`.

CLI

AWS CLI

Pour décrire les référentiels d'un registre

Cet exemple décrit les référentiels du registre par défaut d'un compte.

Commande :

```
aws ecr describe-repositories
```

Sortie :

```
{
    "repositories": [
        {
            "registryId": "012345678910",
            "repositoryName": "ubuntu",
            "repositoryArn": "arn:aws:ecr:us-west-2:012345678910:repository/
ubuntu"
        },
        {
            "registryId": "012345678910",
            "repositoryName": "test",
            "repositoryArn": "arn:aws:ecr:us-west-2:012345678910:repository/test"
        }
    ]
}
```

- Pour plus de détails sur l'API, voir DescribeRepositoriesla section Référence des AWS CLI commandes.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn show_repos(client: &aws_sdk_ecr::Client) -> Result<(),
 aws_sdk_ecr::Error> {
    let rsp = client.describe_repositories().send().await?;

    let repos = rsp.repositories();

    println!("Found {} repositories:", repos.len());

    for repo in repos {
        println!("  ARN:  {}", repo.repository_arn().unwrap());
        println!("  Name: {}", repo.repository_name().unwrap());
    }

    Ok(())
}
```

- Pour plus de détails sur l'API, voir DescribeRepositoriesla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon ECR avec un SDK AWS. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListImages`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`ListImages`.

CLI

AWS CLI

Pour répertorier les images d'un référentiel

L'`list-images`exemple suivant affiche la liste des images du `cluster-autoscaler` référentiel.

```
aws ecr list-images \
    --repository-name cluster-autoscaler
```

Sortie :

```
{
    "imageIds": [
        {
            "imageDigest":
 "sha256:99c6fb4377e9a420a1eb3b410a951c9f464eff3b7dbc76c65e434e39b94b6570",
            "imageTag": "v1.13.8"
        },
        {
            "imageDigest":
 "sha256:99c6fb4377e9a420a1eb3b410a951c9f464eff3b7dbc76c65e434e39b94b6570",
            "imageTag": "v1.13.7"
        },
        {
            "imageDigest":
 "sha256:4a1c6567c38904384ebc64e35b7eeddd8451110c299e3368d2210066487d97e5",
            "imageTag": "v1.13.6"
        }
    ]
}
```

- Pour plus de détails sur l'API, voir ListImagesla section Référence des AWS CLI commandes.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn show_images(
    client: &aws_sdk_ecr::Client,
    repository: &str,
) -> Result<(), aws_sdk_ecr::Error> {
    let rsp = client
        .list_images()
        .repository_name(repository)
        .send()
        .await?;

    let images = rsp.image_ids();

    println!("found {} images", images.len());

    for image in images {
        println!(
            "image: {}:{}",
            image.image_tag().unwrap(),
            image.image_digest().unwrap()
        );
    }

    Ok(())
}
```

- Pour plus de détails sur l'API, voir ListImagesla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon ECR avec un SDK AWS. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Service Quotas Amazon ECR.

Le tableau suivant fournit les quotas de service par défaut pour Amazon Elastic Container Registry (Amazon ECR).

Nom	Par défaut	Ajusta	Description
Filtres par règle dans une configuration de réplication	Chaque Région prise en charge : 100	Non	Nombre maximum de filtres par règle dans une configuration de réplicati on.
Images par référentiel	Chaque Région prise en charge : 10 000	Oui	Nombre maximal d'images par référentiel
Parties de couche	Chaque Région prise en charge : 4 200	Non	Nombre maximal de parties de couche Ceci s'applique uniquement si vous utilisez directeme nt des actions d'API Amazon ECR pour lancer des chargements de plusieurs parties pour des opérations de transfert d'images.
Durée de la stratégie de cycle de vie	Chaque Région prise en charge : 30 720	Non	Nombre maximal de caractères dans une stratégie de cycle de vie.
Taille maximale de la partie de couche	Chaque Région prise en charge : 10	Non	Taille maximale (Mio) d'une partie de couche. Ceci s'appliqu e uniquement si vous utilisez directeme nt des actions d'API

Nom	Par défaut	Ajusta	Description
			Amazon ECR pour lancer des chargements de plusieurs parties pour des opérations de transfert d'images.
Taille maximale de couche	Chaque Région prise en charge : 52 000	Non	Taille maximale (Mio) d'une couche.
Taille minimale de la partie de couche	Chaque région prise en charge : 5	Non	Taille minimale (Mio) d'une partie de couche. Ceci s'applique uniquement si vous utilisez directeme nt des actions d'API Amazon ECR pour lancer des chargements de plusieurs parties pour des opérations de transfert d'images.
Règles de mise en cache par extraction par registre	Chaque région prise en charge : 50	Non	Nombre maximum de règles de mise en cache par extraction.

Nom	Par défaut	Ajusta	Description
Taux de demandes BatchChec kLayerAvailability	Chaque Région prise en charge : 1 000 par seconde	Oui	Le nombre maximum de demandes BatchChec kLayerAvailability que vous pouvez effectuer par seconde dans la région actuelle. Lorsqu'un e image est transféré e vers un référentiel, chaque couche d'image est examinée afin de vérifier si elle a déjà été chargée. Si c'est le cas, la couche d'image est ignorée.
Taux de demandes BatchGetImage	Chaque Région prise en charge : 2 000 par seconde	Oui	Le nombre maximum de demandes BatchGetI mage que vous pouvez effectuer par seconde dans la région actuelle. Lorsqu'une image est extraite, l'API BatchGetI mage est appelée une fois pour récupérer le manifeste d'image. Si vous demandez d'augmenter un quota pour cette API, vérifiez également votre utilisati on de GetDownlo adUrlForLayer.

Nom	Par défaut	Ajusta	Description
Taux de demandes CompleteLayerUpload	Chaque Région prise en charge : 100 par seconde	Oui	Le nombre maximum de demandes CompleteLayerUpload que vous pouvez effectuer par seconde dans la région actuelle. Lorsqu'une image est transférée, l'API CompleteLayerUpload est appelée une fois par couche d'image pour vérifier que le chargement est terminé.
Taux de demandes GetAuthorizationToken	Chaque Région prise en charge : 500 par seconde	Oui	Le nombre maximum de demandes GetAuthorizationToken que vous pouvez effectuer par seconde dans la région actuelle.

Nom	Par défaut	Ajusta	Description
Taux de demandes GetDownloadUrlForLayer	Chaque Région prise en charge : 3 000 par seconde	Oui	Le nombre maximum de demandes GetDownloadUrlForLayer que vous pouvez effectuer par seconde dans la région actuelle. Lorsqu'une image est extraite, l'API GetDownloadUrlForLayer est appelée une fois pour chaque couche d'image qui n'est pas déjà mise en cache. Si vous demandez d'augmenter un quota pour cette API, vérifiez également votre utilisation de BatchGetImage.
Taux de demandes InitiateLayerUpload	Chaque Région prise en charge : 100 par seconde	Oui	Le nombre maximum de demandes InitiateLayerUpload que vous pouvez effectuer par seconde dans la région actuelle. Lorsqu'une image est transférée, l'API InitiateLayerUpload est appelée une fois par couche d'image qui n'a pas encore été chargée. L'action d'API BatchCheckLayerAvailability détermine si une couche d'image a été chargée ou non.

Nom	Par défaut	Ajusta	Description
Taux de demandes PutImage	Chaque Région prise en charge : 10 par seconde	Oui	Le nombre maximum des demandes PutImage que vous pouvez effectuer par seconde dans la région actuelle. Lorsqu'une image est transférée et que toutes les nouvelles couches d'image ont été chargées, l'API PutImage est appelée une fois pour créer ou mettre à jour le manifeste d'image et les balises associées à l'image.
Taux de demandes UploadLayerPart	Chaque Région prise en charge : 500 par seconde	Oui	Le nombre maximum de demandes UploadLayerPart que vous pouvez effectuer par seconde dans la région actuelle. Lorsqu'une image est transférée, chaque nouvelle couche d'image est téléchargée en plusieurs parties et l'API UploadLayerPart est appelée une fois pour chaque nouvelle partie de couche d'image.
Taux de numérisation d'images	Chaque Région prise en charge : 1	Non	Nombre maximal d'images numérisées par image et par 24 heures.

Nom	Par défaut	Ajusta	Description
Référentiels enregistrés	Chaque Région prise en charge : 10 000	Oui	Le nombre maximum de référentiels que vous pouvez créer dans ce compte dans la région actuelle.
Règles par politique de cycle de vie	Chaque région prise en charge : 50	Non	Nombre maximal de règles dans une politique de cycle de vie
Règles par configuration de réplication	Chaque Région prise en charge : 10	Non	Le nombre maximum de règles dans une configuration de réplication.
Balises par image	Chaque Région prise en charge : 1 000	Non	Nombre maximal de balises par image.
Destinations uniques pour toutes les règles dans une configuration de réplication	Chaque Région prise en charge : 25	Non	Le nombre maximum de destinations uniques pour toutes les règles dans une configuration de réplication.

Gestion de vos quotas de service Amazon ECR dans la AWS Management Console

Amazon ECR est intégré à Service Quotas, un service AWS qui vous permet d'afficher et de gérer vos quotas à partir d'un emplacement central. Pour en savoir plus sur Service Quotas, consultez Qu'est-ce que Service Quotas ? dans le Guide de l'utilisateur Service Quotas.

Service Quotas facilite la recherche de la valeur de tous les quotas de service Amazon ECR.

Afficher les quotas de service Amazon ECR (AWS Management Console)

1. Ouvrez la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/.

2. Dans le panneau de navigation, choisissez Services AWS.
3. Dans la liste AWSServices, recherchez et sélectionnez Amazon Elastic Container Registry (Amazon ECR).

   Dans la liste Service quotas vous pouvez voir le nom du quota de service, la valeur appliquée (le cas échéant), le quota AWS par défaut et si la valeur du quota est réglable.
4. Pour afficher des informations supplémentaires sur un quota de service, notamment la description, choisissez le nom du quota.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le guide de l'utilisateur Service Quotas.

Créer une alarme CloudWatch pour surveiller les métriques d'utilisation d'API

Amazon ECR fournit des métriques d'utilisation CloudWatch qui correspondent aux quotas de service AWS pour chacune des API impliquées dans les actions d'authentification de registre, de transmission d'image et d'extraction d'image. Dans la console Service Quotas, vous pouvez afficher votre utilisation sur un graphique et configurer des alarmes qui vous alertent lorsque votre utilisation approche un quota de service. Pour de plus amples informations, veuillez consulter Métriques d'utilisation Amazon ECR.

Suivez les étapes ci-dessous pour créer une alarme CloudWatch basée sur l'une des métriques d'utilisation de l'API Amazon ECR.

Pour créer une alarme en fonction de vos quotas d'utilisation Amazon ECR (AWS Management Console)

1. Ouvrez la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/.
2. Dans le panneau de navigation, choisissez Services AWS.
3. Dans la liste Services AWS, recherchez et sélectionnez Amazon Elastic Container Registry (Amazon ECR).
4. Dans la listeService quotas, sélectionnez le quota d'utilisation Amazon ECR pour lequel vous souhaitez créer une alarme.
5. Dans la section Amazon CloudWatch Events, sélectionnez Create (Créer).

6. Pour Alarm threshold (Seuil d'alarme), choisissez le pourcentage de la valeur de quota appliquée que vous souhaitez définir comme valeur d'alarme.
7. Pour Nom de l'alarme, saisissez un nom pour l'alarme, puis choisissez Créer.

Dépannage d'Amazon ECR

Ce chapitre vous aide à trouver des informations de diagnostic pour Amazon ECR et fournit des étapes de résolution des problèmes courants et des messages d'erreur.

Rubriques

Résolution des commandes Docker et des problèmes liés à l'utilisation d'Amazon ECR

Dans certains cas, l'exécution d'une commande Docker sur Amazon ECR peut générer un message d'erreur. Vous trouverez ci-après la présentation de certains messages d'erreur courants et des résolutions potentielles.

Rubriques

Les journaux Docker ne contiennent pas les messages d'erreur attendus

Pour commencer à déboguer tout problème lié à Docker, commencez par activer la sortie de débogage Docker sur le démon Docker exécuté sur vos instances hôtes. Si vous utilisez des images extraites d'Amazon ECR sur des instances de conteneur Amazon ECS, consultez la section Configuration de la sortie détaillée du démon Docker dans le manuel Amazon Elastic Container Service Developer Guide.

Erreur : « Filesystem Verification Failed » ou « 404: Image Not Found » lors de l'extraction d'une image d'un référentiel Amazon ECR

Il est possible que vous receviez l'erreur `Filesystem verification failed` lorsque vous utilisez la commande docker pull afin d'extraire une image d'un référentiel Amazon ECR avec Docker 1.9 ou une version ultérieure. Il est possible que vous receviez l'erreur `404: Image not found` lorsque vous utilisez des versions Docker antérieures à 1.9.

Quelques motifs possibles et leurs explications figurent ci-dessous :

Le disque local est plein

- Si le disque local sur lequel vous exécutez docker pull est plein, le hachage SHA-1 qui est calculé sur le fichier local peut être différent de celui calculé par Amazon ECR. Vérifiez que le disque local dispose d'un espace libre suffisant pour stocker l'image Docker transmise. Vous pouvez également supprimer d'anciennes images afin de libérer de l'espace pour les nouvelles. Utilisez la commande docker images pour afficher une liste de toutes les images Docker téléchargées localement, ainsi que de leurs tailles.

Le client ne peut pas se connecter au référentiel distant en raison d'une erreur de réseau

- Les appels à un référentiel Amazon ECR requièrent une connexion à Internet fonctionnelle. Vérifiez vos paramètres réseau et assurez-vous que les autres outils et applications peuvent accéder aux ressources sur Internet. Si vous exécutez docker pull sur une instance Amazon EC2 dans un sous-réseau privé, vérifiez que le sous-réseau offre un acheminement vers Internet. Utilisez un serveur de traduction d'adresses réseau (NAT) ou une passerelle NAT gérée.

  Pour l'instant, les appels d'un référentiel Amazon ECR ont également besoin d'un accès réseau via le pare-feu de votre entreprise à Amazon Simple Storage Service (Amazon S3). Si votre organisation utilise un logiciel de pare-feu ou un appareil NAT qui autorise les points de terminaison de service, vérifiez que les points de terminaison de service Amazon S3 de votre région actuelle sont autorisés.

  Si vous utilisez Docker derrière un proxy HTTP, vous pouvez configurer Docker avec les paramètres de proxy appropriés. Pour en savoir plus, consultez Proxy HTTP dans la documentation Docker.

Erreur : « Filesystem Layer Verification Failed » lors de l'extraction d'images d'Amazon ECR

Il est possible que vous receviez l'erreur `image image-name not found` lors de l'extraction d'images à l'aide de la commande docker pull. Si vous inspectez les journaux de Docker, vous verrez peut-être une erreur similaire à ce qui suit :

```
filesystem layer verification failed for digest sha256:2b96f...
```

Cette erreur indique qu'une ou plusieurs couches de votre image n'ont pas pu être téléchargées. Quelques motifs possibles et leurs explications figurent ci-dessous :

Vous utilisez une version plus ancienne de Docker

> Cette erreur peut se produire dans un petit pourcentage des cas lors de l'utilisation d'une version de Docker antérieure à 1.10. Dans ce cas, mettez à niveau le client Docker vers la version 1.10 ou une version ultérieure.

Votre client a rencontré une erreur de réseau ou de disque

> Un disque plein ou un problème de réseau peuvent empêcher le téléchargement d'une ou de plusieurs couches, comme nous l'avons vu pour le message `Filesystem verification failed`. Suivez les recommandations ci-dessus pour veiller à ce que votre système de fichiers ne soit pas plein et à autoriser l'accès à Amazon S3 depuis votre réseau.

Erreurs HTTP 403 ou « no basic auth credentials » lors de la transmission au référentiel

Vous êtes susceptible de recevoir une erreur `HTTP 403 (Forbidden)` ou le message d'erreur no `basic auth credentials` des commandes docker push ou docker pull, même si vous vous êtes authentifié correctement auprès de Docker à l'aide de la commande aws ecr get-login-password. Voici quelques causes connues de ce problème :

Vous vous êtes authentifié auprès d'une région différente

> Les demandes d'authentification sont liées à des régions spécifiques et ne peuvent pas être utilisées d'une région à l'autre. Par exemple, si vous obtenez un jeton d'autorisation de la région USA Ouest (Oregon), vous ne pourrez pas l'utiliser pour vous authentifier auprès des référentiels

de la région USA Est (Virginie du Nord). Pour résoudre le problème, vérifiez que vous avez récupéré un jeton d'authentification à partir de la région dans laquelle votre référentiel se trouve. Pour plus d'informations, consultez the section called "Authentification de registre".

Vous vous êtes authentifié pour effectuer une transmission vers un référentiel pour lequel vous n'avez pas d'autorisations

Vous n'avez pas les autorisations nécessaires pour effectuer une transmission vers le référentiel. Pour plus d'informations, consultez Politiques relatives aux référentiels privés dans Amazon ECR.

Votre jeton a expiré

La période d'expiration du jeton d'autorisation par défaut pour les jetons obtenus à l'aide de l'opération `GetAuthorizationToken` est de 12 heures.

Bogue dans le gestionnaire des informations d'identification `wincred`

Certaines versions de Docker pour Windows utilisent un gestionnaire des informations d'identification nommé `wincred`, qui ne gère pas correctement la commande de connexion de Docker produite par aws ecr get-login-password (pour plus d'informations, consultez https://github.com/docker/docker/issues/22910). Vous pouvez exécuter la commande de connexion de Docker qui est générée, mais lorsque vous tentez de transmettre ou d'extraire des images, ces commandes échouent. Vous pouvez contourner ce bogue en supprimant le schéma `https://` de l'argument de registre dans la commande de connexion de Docker sortie d'aws ecr get-login-password. Voici un exemple de commande de connexion Docker sans le schéma HTTPS.

```
docker login -u AWS -p <password> <aws_account_id>.dkr.ecr.<region>.amazonaws.com
```

Dépannage des messages d'erreur Amazon ECR

Dans certains cas, un appel d'API que vous avez lancé par le biais de la console Amazon ECR se termine AWS CLI par un message d'erreur. Vous trouverez ci-après la présentation de certains messages d'erreur courants et des résolutions potentielles.

HTTP 429 : trop de requêtes ou ThrottleException

Vous pouvez recevoir une `429: Too Many Requests` erreur ou une erreur suite à une `ThrottleException` ou plusieurs actions Amazon ECR ou à un ou plusieurs appels d'API. Cela indique que vous avez appelé un seul point de terminaison dans Amazon ECR à plusieurs reprises

au cours d'une période de temps limitée et que vos demandes se retrouvent limitées. La limitation se produit lorsque des appels d'un seul point de terminaison par un seul utilisateur dépassent un seuil donné au cours d'une période de temps donnée.

Chaque opération d'API dans Amazon ECR est associée à des limitations de débit. Par exemple, la limitation de l'action `GetAuthorizationToken` est fixée à 20 transactions par seconde (TPS), avec une rafale pouvant atteindre 200 TPS autorisée. Dans chaque région, chaque compte reçoit un compartiment qui peut stocker jusqu'à 200 crédits `GetAuthorizationToken`. Ces crédits sont réapprovisionnés au rythme de 20 par seconde. Si votre compartiment contient 200 crédits, vous pouvez réaliser 200 transactions d'API `GetAuthorizationToken` par seconde pendant une seconde, puis soutenir 20 transactions par seconde indéfiniment. Pour plus d'informations sur les limites de débit pour les API Amazon ECR, consultezService Quotas Amazon ECR..

Pour gérer les erreurs de limitation, implémentez une fonction de nouvelle tentative avec une interruption incrémentielle dans votre code. Pour plus d'informations, consultez la section Comportement des tentatives dans le Guide de référence AWS des SDK et des outils. Une autre option consiste à demander une augmentation de la limite de débit, ce que vous pouvez faire à l'aide de la console Service Quotas. Pour plus d'informations, consultez Gestion de vos quotas de service Amazon ECR dans la AWS Management Console.

HTTP 403 : « User [arn] is not authorized to perform [operation] »

Vous êtes susceptible de recevoir l'erreur suivante lorsque vous tentez d'effectuer une action avec Amazon ECR :

```
$ aws ecr get-login-password
A client error (AccessDeniedException) occurred when calling the GetAuthorizationToken
 operation:
    User: arn:aws:iam::account-number:user/username is not authorized to perform:
    ecr:GetAuthorizationToken on resource: *
```

Cette erreur indique que l'utilisateur n'est pas autorisé à utiliser Amazon ECR ou que les autorisations dont il dispose n'ont pas été configurées correctement. Si vous effectuez des actions liées au référentiel Amazon ECR, vérifiez plus particulièrement si l'utilisateur dispose des autorisations nécessaires pour accéder à ce référentiel. Pour en savoir plus sur la création et la vérification des autorisations pour Amazon ECR, consultez Gestion des identités et des accès au registre de conteneur Amazon Elastic.

HTTP 404 : « Repository Does Not Exist »

Si vous spécifiez un référentiel Docker Hub qui n'existe pas, Docker Hub le créera automatiquement. Avec Amazon ECR, les nouveaux référentiels doivent être créés explicitement avant de pouvoir être utilisés. Cela évite que de nouveaux référentiels soient créés accidentellement (par exemple, en raison de fautes de frappe) et vous permet également de veiller à ce qu'une politique d'accès de sécurité appropriée soit attribuée explicitement à tout nouveau référentiel. Pour plus d'informations sur la création des référentiels, consultez Référentiels privés Amazon ECR.

Erreur : impossible d'effectuer une connexion interactive à partir d'un appareil autre que TTY

Si vous recevez le message d'erreur `Cannot perform an interactive login from a non TTY device`, les étapes de dépannage suivantes devraient vous aider.

- Vérifiez que vous utilisez AWS CLI la version 2 et que vous ne disposez pas d'une version conflictuelle de la AWS CLI version 1 sur votre système. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI.
- Vérifiez que vous avez configuré votre compte AWS CLI avec des informations d'identification valides. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI.
- Vérifiez que la syntaxe de votre AWS CLI commande est correcte.

Historique du document

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version d'Amazon ECR. Nous mettons aussi la documentation à jour régulièrement pour prendre en compte les commentaires qui nous sont envoyés.

Modification	Description	Date
Ajout de la réplication entre régions et entre comptes dans les régions chinoises	Amazon ECR a ajouté la prise en charge de la région chinoise pour le filtrage des référentiels répliqués.	15 mai 2024
Ajout d' GitLab un registre de conteneurs pour parcourir les règles de cache	Amazon ECR a ajouté la prise en charge de la création de règles de cache d'extraction pour le registre des GitLab conteneurs.	8 mai 2024
Mise à jour de la politique de cycle de vie d'Amazon ECR pour ajouter la prise en charge de l'utilisation de caractères génériques	Amazon ECR a ajouté une prise en charge pour les caractères génériques dans une politique de cycle de vie grâce à l'utilisation du paramètre `tagPatternList` dans une règle de politique de cycle de vie. Pour plus d'informations, consultez Automatisez le nettoyage des images en utilisant les politiques de cycle de vie d'Amazon ECR.	18 décembre 2023
Modèles de création de référentiels Amazon ECR	Amazon ECR a ajouté une prise en charge pour les modèles de création de référentiels. Pour plus d'informations, consultez Modèles pour contrôler les référentiels créés lors d'une action d'extraction dans le cache.	15 novembre 2023
Ajout d'une mise en cache par extraction d'Amazon ECR pris en charge pour les registres en amont authentifiés	Amazon ECR a ajouté une pris en charge pour l'utilisation de registres en amont qui nécessitent une authentification pour vos règles de mise en cache par extraction. Pour plus d'informations, consultez	15 novembre 2023

Modification	Description	Date
	Synchroniser un registre en amont avec un registre privé Amazon ECR.	
AWSECRPullThroughCache_ServiceRolePolicy – Mise à jour d'une politique existante	Amazon ECR a ajouté de nouvelles autorisations à la politique `AWSECRPullThroughCache_ServiceRolePolicy` . Ces autorisations permettent à Amazon ECR de récupérer le contenu chiffré d'un secret de Secrets Manager. Cela est nécessaire lors de l'utilisation d'une règle de mise en cache par extraction pour mettre en cache des images provenant d'un registre en amont qui nécessite une authentification.	15 novembre 2023
Signature d'image Amazon ECR	Amazon ECR et AWS Signer ajout de la prise en charge de la création et de l'envoi de signatures d'images de conteneurs à l'aide du client Notary. Pour plus d'informations, consultez Signature d'une image stockée dans un référentiel privé Amazon ECR.	6 juin 2023
Ajout d'un registre de conteneurs Kubernetes pour consulter les règles de mise en cache par extraction	Amazon ECR a ajouté la prise en charge de la création de règles de mise en cache par extraction pour le registre de conteneurs Kubernetes. Pour plus d'informations, consultez Synchroniser un registre en amont avec un registre privé Amazon ECR.	1 juin 2023
Prise en charge de la durée de numérisation améliorée Amazon ECR	Amazon Inspector a ajouté la prise en charge de la définition de la durée pendant laquelle vos référentiels sont surveillés lorsque la numérisation améliorée est activée. Pour plus d'informations, consultez Modification de la durée de numérisation améliorée pour les images dans Amazon Inspector.	28 juin 2022
Amazon ECR envoie les statistiques du nombre d'extractions du référentiel à Amazon CloudWatch	Amazon ECR envoie les statistiques du nombre d'appels du référentiel à Amazon CloudWatch. Pour plus d'informations, consultez Métriques de référentiel Amazon ECR.	6 janvier 2022

Modification	Description	Date
Prise en charge étendue de la réplication	Amazon ECR a ajouté une prise en charge pour le filtrage des référentiels répliqués. Pour plus d'informations, consultez Réplication d'images privées dans Amazon ECR.	21 septembre 2021
AWS politiques gérées pour Amazon ECR	Amazon ECR a ajouté de la documentation sur les politiques AWS gérées. Pour plus d'informations, consultez AWS politiques gérées pour Amazon Elastic Container Registry.	24 juin 2021
Réplication inter-régions et inter-comptes	Amazon ECR a ajouté une prise en charge pour la configuration des paramètres de réplication de votre registre privé. Pour plus d'informations, consultez Paramètres du registre privé dans Amazon ECR.	8 décembre 2020
Prise en charge des artefacts OCI	Amazon ECR a ajouté une prise en charge pour pousser et tirer les artefacts OCI (Open Container Initiative). Un nouveau paramètre `artifactMediaType` a été ajouté à la réponse d'API `DescribeImages` pour indiquer le type d'artefact. Pour plus d'informations, consultez Transférer un graphique de Helm vers un référentiel privé Amazon ECR.	24 août 2020
Chiffrement au repos	Amazon ECR a ajouté une prise en charge pour la configuration du chiffrement de vos référentiels à l'aide du chiffrement côté serveur avec des clés gérées par le client stockées dans AWS Key Management Service (AWS KMS). Pour plus d'informations, consultez Chiffrement au repos.	29 juillet 2020

Modification	Description	Date
Images multi-architecture	Amazon ECR a ajouté une prise en charge pour la création et la transmission des listes manifeste Docker utilisées pour les images multi-architecture. Pour plus d'informations, consultez Transmission d'une image multi-architecture vers un référentiel privé Amazon ECR.	28 avril 2020
Métriques d'utilisation Amazon ECR	Amazon ECR a ajouté des statistiques CloudWatch d'utilisation qui fournissent une visibilité sur l'utilisation des ressources de votre compte. Vous avez également la possibilité de créer des CloudWatch alarmes à partir de la console Service Quotas CloudWatch et de la console Service Quotas pour recevoir des alertes lorsque votre utilisation approche le quota de service appliqué. Pour plus d'informations, consultez Métriques d'utilisation Amazon ECR.	28 février 2020
Service Quotas Amazon ECR mis à jour	Mise à jour des quotas de service Amazon ECR pour inclure des quotas par API. Pour plus d'informations, consultez Service Quotas Amazon ECR..	19 février 2020
Commande `get-login-password` ajoutée	Prise en charge ajoutée pour la get-login-password, qui fournit une méthode simple et sécurisée permettant de récupérer un jeton d'autorisation. Pour plus d'informations, consultez Utiliser un jeton d'autorisation.	4 février 2020

Modification	Description	Date
Numérisation d'images	Prise en charge ajoutée pour la numérisation d'images, ce qui permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. Amazon ECR utilise la base de données CVE(Common Vulnerabilities and Exposures) du projet open source CoreOS Clair et vous fournit la liste des résultats de la numérisation. Pour plus d'informations, consultez Scannez les images pour détecter les vulnérabilités logicielles dans Amazon ECR.	24 oct. 2019
Politique de point de terminaison d'un VPC	Prise en charge ajoutée pour la définition d'une politique IAM relative aux points de terminaison d'un VPC d'interface Amazon ECR. Pour plus d'informations, consultez Créer une politique de point de terminaison pour vos points de terminaison d'un VPC Amazon ECR.	26 septembre 2019
Caractère immuable des étiquettes d'image	Prise en charge ajoutée pour la configuration du caractère immuable d'un référentiel afin qu'il ne soit pas possible d'écraser les étiquettes d'image. Pour plus d'informations, consultez Empêcher le remplacement des balises d'image dans Amazon ECR.	25 juillet 2019
Points de terminaison d'un VPC d'interface (AWS PrivateLink)	Ajout de la prise en charge de la configuration des points de terminaison VPC d'interface alimentés par. AWS PrivateLink Cela vous permet de créer une connexion privée entre votre VPC et Amazon ECR sans avoir besoin d'un accès Internet, via une instance NAT, une connexion VPN ou AWS Direct Connect. Pour plus d'informations, consultez Points de terminaison VPC de l'interface Amazon ECR ()AWS PrivateLink.	25 janvier 2019

Modification	Description	Date
Étiquette des ressources	Amazon ECR a ajouté une prise en charge pour l'ajout d'étiquettes de métadonnées dans vos référentiels. Pour plus d'informations, consultez Marquage d'un référentiel privé dans Amazon ECR.	18 décembre 2018
Changement de nom Amazon ECR	Le registre de conteneur Amazon Elastic est renommé (anciennement, Amazon EC2 Container Registry).	21 novembre 2017
Politiques de cycle de vie	Les politiques de cycle de vie Amazon ECR vous permettent de préciser la gestion du cycle de vie des images dans un référentiel. Pour plus d'informations, consultez Automatisez le nettoyage des images en utilisant les politiques de cycle de vie d'Amazon ECR.	11 octobre 2017
Amazon ECR prend en charge le manifeste 2, schéma 2 d'image Docker	Amazon ECR prend désormais en charge le manifeste V2, schéma 2 d'image Docker (utilisé avec la version 1.10 de Docker et les versions les plus récentes). Pour plus d'informations, consultez Prise en charge du format de manifeste d'image de conteneur dans Amazon ECR.	27 janvier 2017
Disponibilité générale d'Amazon ECR	Amazon Elastic Container Registry (Amazon ECR) est un service de registre Docker AWS géré qui est sécurisé, évolutif et fiable.	21 décembre 2015

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.