aws

Guida per l'utente

Amazon ECR

Versione API 2015-09-21

Amazon ECR: Guida per l'utente

Table of Contents

Che cos'è Amazon Elastic Container Registry?

Amazon Elastic Container Registry (Amazon ECR) è un servizio di registro delle immagini container gestito AWS che offre sicurezza, scalabilità e affidabilità. Amazon ECR supporta i repository privati con autorizzazioni basate sulle risorse utilizzando AWS IAM. In tal modo, gli utenti specificati o le istanze Amazon EC2 possono accedere ai repository e alle immagini dei container. È possibile utilizzare la CLI preferita per inviare, estrarre e gestire le immagini Docker, le immagini OCI (Open Container Initiative) e i manufatti compatibili con OCI.

> **Note**
>
> Amazon ECR supporta anche repository di immagini di container pubblici. Per maggiori informazioni, consulta Che cos'è Amazon ECR Public nella Guida per l'utente di Amazon ECR Public.

Il team di servizi dei container AWS mantiene una roadmap pubblica su GitHub. Contiene informazioni sulle attività su cui stanno stanno lavorando i team e consente a tutti i clienti AWS di dare un feedback diretto. Per ulteriori informazioni, consulta Roadmap dei container AWS.

Componenti di Amazon ECR

Amazon ECR contiene i componenti seguenti:

Registro

Viene fornito un registro privato Amazon ECR a ogni account AWS; puoi creare uno o più repository nel registro e archiviare in questi repository immagini Docker, immagini Open Container Initiative (OCI) e artefatti OCI compatibili. Per ulteriori informazioni, consulta Registro privato Amazon ECR.

Token di autorizzazione

Per inviare ed estrarre le immagini, il tuo client deve prima autenticarsi in un registro privato Amazon ECR come utente AWS. Per ulteriori informazioni, consulta Autenticazione del registro privato.

Archivio

Un repository Amazon ECR contiene le immagini Docker, le immagini Open Container Initiative (OCI) e gli artefatti compatibili con OCI. Per ulteriori informazioni, consulta Repository Amazon ECR privati.

Policy del repository

Puoi controllare l'accesso ai repository e al contenuto presente in questi attraverso le policy del repository. Per ulteriori informazioni, consulta Policy del repository privato.

Immagine

Puoi inviare ed estrarre le immagini del container ai tuoi repository. Puoi utilizzare queste immagini localmente sul tuo sistema di sviluppo oppure nelle definizioni di attività Amazon ECS e nelle specifiche pod Amazon EKS. Per ulteriori informazioni, consulta Utilizzo delle immagini Amazon ECR con Amazon ECS e Utilizzo delle immagini Amazon ECR con Amazon EKS.

Caratteristiche di Amazon ECR

Amazon ECR offre le seguenti caratteristiche:

- Le policy relative al ciclo di vita consentono di gestire il ciclo di vita delle immagini nei repository. Definisci le regole che determinano la pulizia delle immagini inutilizzate. È possibile testare le regole prima di applicarle al repository. Per ulteriori informazioni, consulta Policy del ciclo di vita.
- La scansione delle immagini aiuta a identificare le vulnerabilità del software nelle immagini del container. Ogni repository può essere configurato per la scansione su invio. In tal modo viene eseguita la scansione di ogni nuova immagine inserita nel repository. È quindi possibile recuperare i risultati della scansione delle immagini. Per ulteriori informazioni, consulta Scansione delle immagini.
- La replica tra regioni e account consente di disporre più facilmente delle immagini quando è necessario. La configurazione è come un'impostazione del registro ed è per ogni specifica regione. Per ulteriori informazioni, consulta Impostazioni dei registri privati.
- Le regole di cache pull-through forniscono un modo per memorizzare nel registro privato Amazon ECR la cache dei repository di un registro upstream. Utilizzando una regola di cache pull-through, Amazon ECR si rivolgerà periodicamente al registro upstream per garantire che l'immagine memorizzata nella cache nel registro privato Amazon ECR sia aggiornata. Per ulteriori informazioni, consulta Utilizzo delle regole della cache pull-through.

Nozioni di base su Amazon ECR

Per utilizzare Amazon ECR, è necessario avere la giusta configurazione per l'installazione della AWS Command Line Interface e del Docker. Per ulteriori informazioni, consulta Configurazione con Amazon ECR e Utilizzo di Amazon ECR con il AWS CLI.

Prezzi di Amazon ECR

Con Amazon ECR, si paga solo per la quantità di dati archiviati nei repository e per il trasferimento dei dati dagli invii e dalle estrazioni di immagini. Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon ECR.

Configurazione con Amazon ECR

Se ti sei registrato per AWS e hai già usato Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS), sei quasi in grado di usare Amazon ECR. Il processo di configurazione per i due servizi è simile in quanto Amazon ECR è un'estensione di tali servizi. Quando utilizzi AWS CLI con Amazon ECR, ti consigliamo di usare una versione di AWS CLI che supporti le più recenti funzionalità di Amazon ECR. Se una caratteristica di Amazon ECR non è supportata in AWS CLI, esegui l'aggiornamento alla versione più recente. Per ulteriori informazioni, vedere http://aws.amazon.com/cli/.

Completa le seguenti attività per impostare l'invio di un'immagine container ad Amazon ECR per la prima volta. Se hai già completato queste fasi, puoi ignorarle e procedere con la fase successiva.

Registrarsi per creare un Account AWS

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Per registrarsi a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Al termine del processo di registrazione, riceverai un'e-mail di conferma da AWS. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

Dopo aver effettuato la registrazione di un Account AWS, proteggi Utente root dell'account AWS, abilita AWS IAM Identity Center e crea un utente amministratore in modo da non utilizzare l'utente root per le attività quotidiane.

Protezione dell'Utente root dell'account AWS

1. Accedi alla AWS Management Console come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email del Account AWS. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accesso come utente root della Guida per l'utente di Accedi ad AWS.
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per ricevere istruzioni, consulta Abilitazione di un dispositivo MFA virtuale per l'utente root dell'Account AWS (console) nella Guida per l'utente IAM.

Creazione di un utente amministratore

1. Abilita IAM Identity Center

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center.
2. In Centro identità AWS IAM, assegna l'accesso amministrativo a un utente amministrativo.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come origine di identità, consulta Configure user access with the default IAM Identity Center directory nella Guida per l'utente di AWS IAM Identity Center.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta Accedere al portale di accesso AWS nella Guida per l'utente Accedi ad AWS.

Nozioni di base su Amazon ECR utilizzando il AWS Management Console

Inizia a utilizzare Amazon ECR creando un repository nella console Amazon ECR. La console Amazon ECR fornisce le istruzioni dettagliate per iniziare a creare il primo repository.

Prima di iniziare, devi accertarti di aver completato le fasi in Configurazione con Amazon ECR.

Per creare un repository di immagini

Un repository è il posto in cui si memorizzano le immagini Docker o Open Container Initiative (OCI) in Amazon ECR. Ogni volta che si invia o si estrae un'immagine da Amazon ECR, è necessario specificare il repository e la posizione del registro per indicare dove inviare l'immagine o da dove estrarla.

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Seleziona Get Started (Inizia).
3. Per Visibility settings (Impostazioni di visibilità), scegliere Private (Privato).
4. Per Repository names (Nomi dei repository), specificare il nome di base per il repository.
5. Per Tag immutability (Immutabilità dei tag), scegliere l'impostazione di mutabilità dei tag per il repository. I repository configurati con tag immutabili impediscono la sovrascrittura dei tag immagine. Per ulteriori informazioni, consulta Mutabilità dei tag immagine.
6. Per Scan on push (Scansione su push), scegliere l'impostazione di scansione delle immagini per il repository. I repository configurati per la scansione su invio avviano una scansione dell'immagine ogni volta che un'immagine viene inviata, altrimenti le scansioni devono essere avviate manualmente.

   > **Important**
   >
   > La configurazione di scansione delle immagini a livello di repository è stata resa obsoleta a favore della configurazione a livello di registro. Per ulteriori informazioni, consulta Scansione delle immagini.

7. Per KMS encryption (Crittografia KMS), scegli se abilitare la crittografia lato server utilizzando chiavi AWS KMS memorizzate nel servizio AWS Key Management Service. Per ulteriori informazioni sull'utilizzo di questa caratteristica, consulta Crittografia dei dati a riposo.

8. Scegliere Create repository (Crea repository).

Creazione, aggiunta di tag e push di un'immagine Docker

In questa sezione della procedura guidata, puoi utilizzare la CLI Docker per aggiungere un tag a un'immagine locale esistente (che hai creato da un Dockerfile o hai estratto da un altro registro, come il Docker Hub), quindi inviare l'immagine con tag al registro Amazon ECR. Per i passaggi più dettagliati sull'utilizzo della CLI Docker, consulta Utilizzo di Amazon ECR con il AWS CLI.

1. (Facoltativo) Selezionare il repository creato e scegliere View push commands (Visualizza comandi push) per visualizzare i passaggi per effettuare il push di un'immagine al nuovo repository.
2. Eseguire il comando di accesso che consente di autenticare il client Docker sul registro utilizzando il comando dalla console a una finestra del terminale. Questo comando fornisce un token di autorizzazione valido per 12 ore.
3. (Facoltativo) Se possiedi un Dockerfile dell'immagine da inviare, sviluppa l'immagine e taggala per il nuovo archivio. Utilizzando il comando docker build dalla console in una finestra terminale. Assicurarsi di essere nella stessa directory del Dockerfile.
4. Amazon ECR publishes the following metrics in the namespace.Taggare l'immagine per il registro Amazon ECR e il nuovo archivio incollando il comando docker tag dalla console su una finestra del terminale. Il comando della console presume che l'immagine sia stata costruita da un Dockerfile in una fase precedente. Se l'immagine non è stata costruita in un Dockerfile, sostituire la prima istanza di `repository`:`latest` con l'ID dell'immagine o il nome dell'immagine locale da inviare.
5. Inviare l'immagine con il nuovo tag al repository utilizzando il comando docker push in una finestra del terminale.
6. Scegli Close (Chiudi).

Utilizzo di Amazon ECR con il AWS CLI

Le seguenti fasi illustrano i passaggi necessari per inviare un'immagine di container a un repository privato Amazon ECR per la prima volta utilizzando la CLI di Docker e AWS CLI.

Per ulteriori informazioni sugli altri strumenti disponibili per la gestione delle risorse AWS, tra cui i diversi SDK AWS, i kit di strumenti IDE e gli strumenti a riga di comando di Windows PowerShell, consulta http://aws.amazon.com/tools/.

Prerequisiti

Prima di iniziare, devi accertarti di aver completato le fasi in Configurazione con Amazon ECR.

Se non dispone già della versione più recente dell'AWS CLI e Docker installata e pronta per l'uso, attieniti alla seguente procedura per installare entrambi questi strumenti.

Installazione di AWS CLI

Puoi utilizzare gli strumenti a riga di comando AWS per inviare comandi alla riga di comando per eseguire Amazon ECR e altre attività AWS. Questa modalità può risultare più veloce e semplice rispetto all'uso della console. Gli strumenti a riga di comando sono inoltre utili per creare script che eseguono le attività di AWS.

Per utilizzare AWS CLI con Amazon ECR, installa la versione più recente di AWS CLI. Per informazioni, consulta Installazione dell'AWS Command Line Interface nella Guida per l'utente di AWS Command Line Interface.

Installa Docker

Docker è disponibile per diversi sistemi operativi, compresa la maggior parte delle distribuzioni Linux, ad esempio Ubuntu, e persino per macOS e Windows. Per ulteriori informazioni sull'installazione di Docker sul tuo specifico sistema operativo, consulta la guida all'installazione di Docker.

Per l'utilizzo di Docker non è necessario un sistema di sviluppo locale. Se già utilizzi Amazon EC2, puoi avviare un'istanza Amazon Linux 2023 e installare Docker per iniziare.

Se hai già installato Docker, passa a Fase 1: creazione di un'immagine Docker.

Installazione di Docker su un'istanza Amazon EC2 con un'AMI Amazon Linux 2023

1. Avvia un'istanza con l'ultima AMI Amazon Linux 2023. Per ulteriori informazioni, consulta Avvio di un'istanza nella Guida per l'utente di Amazon EC2 per istanze Linux.
2. Connettiti alla tua istanza. Per ulteriori informazioni, consulta Connessione a un'istanza Linux nella Guida per l'utente di Amazon EC2 per le istanze Linux.
3. Aggiorna i pacchetti installati e la cache dei pacchetti sulla tua istanza.

   ```
   sudo yum update -y
   ```

4. Installa il pacchetto Docker Community Edition più recente.

   ```
   sudo yum install docker
   ```

5. Avvia il servizio Docker.

   ```
   sudo service docker start
   ```

6. Aggiungi `ec2-user` al gruppo `docker` in modo da poter eseguire comandi Docker senza utilizzare `sudo`.

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

7. Esci e ripeti l'accesso per trovare il nuovo gruppo di autorizzazioni `docker`. A questo scopo, puoi chiudere la finestra del terminale SSH corrente e riconnetterti all'istanza in una nuova finestra. La nuova sessione SSH avrà le autorizzazioni del gruppo `docker` appropriate.
8. Verifica che `ec2-user` possa eseguire i comandi Docker senza `sudo`.

   ```
   docker info
   ```

   > **Note**
   >
   > In alcuni casi, l'assegnazione delle autorizzazioni necessarie a `ec2-user` per accedere al daemon Docker può richiedere il riavvio dell'istanza. Prova a riavviare l'istanza se visualizzi questo errore:

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

Fase 1: creazione di un'immagine Docker

In questa fase viene descritto come creare un'immagine Docker di una semplice applicazione Web e come testarla nel sistema locale o nell'istanza Amazon EC2.

Per creare un'immagine Docker di una semplice applicazione Web

1. Crea un file denominato `Dockerfile`. Un Dockerfile è un file manifest che descrive l'immagine di base da utilizzare per l'immagine Docker, nonché gli elementi da installare ed eseguire su di essa. Per ulteriori informazioni sui Dockerfile, consulta la documentazione di riferimento sui Dockerfile.

   ```
   touch Dockerfile
   ```

2. Modifica il `Dockerfile` appena creato e aggiungi i seguenti contenuti.

   ```
   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
   ```

Questo Dockerfile utilizza l'immagine pubblica di Amazon Linux 2 ospitata su Amazon ECR Public. Le istruzioni `RUN` aggiornano le cache dei pacchetti, installano alcuni pacchetti software per il server Web e infine scrivono il contenuto "Hello World!" nella root del documento del server Web. L'istruzione `EXPOSE` espone la porta 80 nel container, mentre l'istruzione `CMD` avvia il server Web.

3. Crea l'immagine Docker dal tuo Dockerfile.

> **Note**
>
> In alcune versioni di Docker, il seguente comando potrebbe richiedere il percorso completo al Dockerfile anziché il percorso relativo mostrato di seguito.

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

4. Elenca l'immagine del container.

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

Output:

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

5. Esegui l'immagine appena creata. L'opzione `-p 80:80` mappa la porta 80 esposta sul container alla porta 80 sul sistema host. Per ulteriori informazioni sul comando docker run, consulta la documentazione di riferimento di Docker run.

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

> **Note**
>
> L'output dal server Web Apache viene visualizzato nella finestra del terminale. Puoi ignorare il messaggio "`Could not reliably determine the fully qualified domain name`".

6. Apri un browser e accedi al server su cui è in esecuzione Docker e che ospita il tuo container.

   - Se utilizzi un'istanza EC2, si tratta del valore Public DNS (DNS pubblico) del server, che è lo stesso indirizzo utilizzato per la connessione all'istanza con SSH. Assicurati che il gruppo di sicurezza per l'istanza consenta il traffico in entrata sulla porta 80.
   - Se Docker è in esecuzione in locale, accedi con il browser a http://localhost/.
   - Se utilizzi docker-machine su un computer Windows o Mac, trova l'indirizzo IP della VM VirtualBox che ospita Docker tramite il comando docker-machine ip, sostituendo *nome-macchina* con il nome della macchina Docker che stai utilizzando.

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

   Visualizzerai una pagina Web con il tuo contenuto "Hello World!" dichiarazione.

7. Interrompi il container Docker digitando Ctrl+c.

Fase 2: autenticazione sul registro predefinito

Dopo aver installato e configurato l'AWS CLI, puoi autenticare la CLI Docker nel registro predefinito. In questo modo, il comando docker può inviare ed estrarre le immagini con Amazon ECR. L'AWS CLI fornisce un comando get-login-password per semplificare il processo di autenticazione.

Per autenticare Docker in un registro Amazon ECR con get-login-password, eseguire il comando aws ecr get-login-password. Quando si passa il token di autenticazione al comando docker login, usare il valore `AWS` per il nome utente e specificare l'URI di registro Amazon ECR a cui si desidera autenticare. Se si esegue l'autenticazione a più registri, è necessario ripetere il comando per ogni registro di sistema.

> **Important**
>
> Se viene visualizzato un errore, installare o eseguire l'upgrade alla versione più recente dell'AWS CLI. Per ulteriori informazioni, consulta Installazione dell'AWS Command Line Interface nella Guida per l'utente di 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
```

- Get-ECRLoginCommand (AWS Tools for Windows PowerShell)

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

Fase 3: creazione di un repository

Ora che hai un'immagine da inviare ad Amazon ECR, devi creare un repository in cui memorizzarla. In questo esempio, viene creato un archivio denominato `hello-repository` in cui successivamente inviare l'immagine `hello-world:latest`. Per creare un repository, eseguire il comando seguente:

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

Fase 4: invio di un'immagine ad Amazon ECR

Ora puoi inviare la tua immagine al repository Amazon ECR creato nella sezione precedente. Per inviare immagini, puoi utilizzare la CLI di docker, tuttavia vi sono alcuni prerequisiti che devono essere soddisfatti affinché questa operazione venga eseguita correttamente:

- È stata installata la versione minima di docker: 1.7
- Il token di autorizzazione Amazon ECR è stato configurato con docker login.

- Il repository Amazon ECR è stato creato e l'utente ha accesso per eseguire l'invio al repository stesso.

Dopo che tali prerequisiti sono stati soddisfatti, puoi inviare l'immagine al repository appena creato nel registro predefinito del tuo account.

Per assegnare un tag a un'immagine e inviarla ad Amazon ECR

1. Elencare le immagini memorizzate localmente per identificare l'immagine a cui aggiungere il tag e inviare.

   ```
   docker images
   ```

   Output:

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

2. Aggiungere un tag all'immagine da inviare al tuo repository.

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

3. Invia l'immagine.

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

   Output:

   ```
   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
   ```

Fase 5: estrazione di un'immagine da Amazon ECR

Dopo che l'immagine è stata inviata al repository di Amazon ECR, puoi estrarla da altre posizioni. Usa la CLI di docker per estrarre le immagini, tuttavia vi sono alcuni prerequisiti che devono essere soddisfatti affinché questa operazione venga eseguita correttamente:

- È stata installata la versione minima di docker: 1.7
- Il token di autorizzazione Amazon ECR è stato configurato con docker login.
- Il repository Amazon ECR è stato creato e l'utente ha accesso per eseguire l'estrazione dal repository stesso.

Dopo che tali prerequisiti sono stati soddisfatti, si può estrarre l'immagine. Per estrarre l'immagine di esempio da Amazon ECR, eseguire il comando seguente:

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

Output:

```
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
```

Fase 6: eliminazione di un'immagine

Se decidi che non hai più bisogno di un'immagine o non la vuoi in uno dei tuoi repository, puoi eliminarla con il comando batch-delete-image. Per eliminare un'immagine, devi specificare il repository in cui di trova e un valore `imageTag` o `imageDigest` per l'immagine. L'esempio di seguito elimina un'immagine dall'archivio `hello-repository` con il tag `latest` dell'immagine.

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

```
      --region region
```

Fase 7: eliminazione di un repository

Se decidi che non hai più bisogno o non vuoi un intero repository di immagini, puoi eliminarlo. Per impostazione predefinita, non puoi eliminare un repository che contiene immagini; tuttavia, il flag `--force` lo consente. Per eliminare un repository che contiene immagini (e tutte le immagini in esso contenute), esegui il comando seguente:

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

Registro privato Amazon ECR

Il registro privato Amazon ECR ospita le immagini di container in un'architettura altamente disponibile e scalabile. È possibile utilizzare il registro privato per gestire i repository di immagini privati costituiti da immagini e artefatti Docker e Open Container Initiative (OCI). Ciascun account AWS dispone di un registro Amazon ECR privato predefinito. Per ulteriori informazioni sui registri pubblici Amazon ECR, consulta Registri pubblici nella Guida per l'utente di Amazon Elastic Container Registry.

Concetti dei registri privati

- L'URL per il registro privato predefinito è `https://aws_account_id.dkr.ecr.us-west-2.amazonaws.com`.
- Per impostazione predefinita l'account ha accesso in lettura e in scrittura ai repository contenuti nel registro privato. Tuttavia, gli utenti richiedono le autorizzazioni per effettuare chiamate alle API di Amazon ECR e inviare o estrarre immagini da e verso i tuoi repository privati. Amazon ECR fornisce diverse policy gestite per controllare l'accesso degli utenti a diversi livelli. Per ulteriori informazioni, consulta Esempi di policy basate su Identità di Amazon Elastic Container Registry.
- Devi autenticare il tuo client Docker nel tuo registro privato in modo da poter utilizzare i comandi docker push e docker pull per inviare ed estrarre immagini dai repository in quel registro. Per ulteriori informazioni, consulta Autenticazione del registro privato.
- I repository privati possono essere controllati sia tramite le policy di accesso degli utenti sia con le policy relative ai repository stessi. Per ulteriori informazioni sulle policy dei repository, consulta Policy del repository privato.
- I repository nel registro privato possono essere replicati tra le regioni del proprio registro privato e tra account separati configurando la replica per il proprio registro privato. Per ulteriori informazioni, consulta Replica di immagini private.

Autenticazione del registro privato

Puoi utilizzare gli AWS Management Console, gli o gli AWS CLI AWS SDK per creare e gestire repository privati. Puoi utilizzare questi metodi anche per eseguire alcune operazioni sulle immagini, come elencarle o eliminarle. Questi client utilizzano metodi di AWS autenticazione standard. Anche se tecnicamente puoi utilizzare l'API Amazon ECR per inviare ed estrarre immagini, è più probabile che utilizzerai la CLI Docker o una libreria Docker specifica per la lingua.

La CLI Docker non supporta i metodi di autenticazione IAM nativi. È necessario eseguire ulteriori passaggi affinché Amazon ECR possa autenticare e autorizzare le richieste di invio ed estrazione di Docker.

Sono disponibili i metodi di autenticazione del registro illustrati nel dettaglio nelle sezioni seguenti.

Utilizzo dell'assistente delle credenziali Amazon ECR

Amazon ECR fornisce un supporto per le credenziali Docker che semplifica l'archiviazione e l'utilizzo delle credenziali Docker durante l'invio e l'estrazione delle immagini in Amazon ECR. Per i passaggi di installazione e configurazione, consulta Amazon ECR Docker Credential Helper.

> **Note**
>
> Al momento l'assistente credenziali Amazon ECR Docker non supporta l'autenticazione a più fattori (MFA) con più fattori.

Utilizzo di un token di autorizzazione

L'ambito di autorizzazione di un token di autorizzazione corrisponde a quello dell'entità principale IAM utilizzata per recuperare il token di autenticazione. Un token di autenticazione viene utilizzato per accedere a qualsiasi registro Amazon ECR a cui l'entità principale IAM ha accesso ed è valido per 12 ore. Per ottenere un token di autorizzazione, è necessario utilizzare l'operazione GetAuthorizationTokenAPI per recuperare un token di autorizzazione con codifica Base64 contenente il nome utente e una password codificata. `AWS` Il AWS CLI `get-login-password` comando semplifica questa operazione recuperando e decodificando il token di autorizzazione che è quindi possibile reindirizzare a un comando per l'autenticazione. docker login

Autenticazione di Docker su un registro privato Amazon ECR con la CLI

Per autenticare Docker in un registro Amazon ECR con get-login-password, esegui il comando. aws ecr get-login-password Quando si passa il token di autenticazione al comando docker login, usare il valore `AWS` per il nome utente e specificare l'URI di registro Amazon ECR a cui si desidera autenticare. Se si esegue l'autenticazione a più registri, è necessario ripetere il comando per ogni registro di sistema.

> **Important**
>
> Se viene visualizzato un errore, installare o eseguire l'upgrade alla versione più recente dell' AWS CLI. Per ulteriori informazioni, consulta Installazione dell' AWS Command Line Interface nella Guida per l'utente di 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
```

- Get-ECR () LoginCommandAWS Tools for Windows PowerShell

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

Utilizzo dell'autenticazione API HTTP

Amazon ECR supporta l'API HTTP del registro Docker. Tuttavia, poiché Amazon ECR è un registro privato, devi fornire un token di autorizzazione con ogni richiesta HTTP. È possibile aggiungere un'intestazione di autorizzazione HTTP utilizzando l'`-H`opzione for curl e passare il token di autorizzazione fornito dal comando. get-authorization-token AWS CLI

Per effettuare l'autenticazione con l'API HTTP di Amazon ECR

1. Recupera un token di autorizzazione con AWS CLI e impostalo su una variabile di ambiente.

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

2. Per effettuare l'autenticazione nell'API, passa la variabile `$TOKEN` all'opzione `-H` di curl. Ad esempio, il comando seguente elenca i tag immagine in un repository Amazon ECR. Per ulteriori informazioni, consulta API HTTP del registro Docker nella documentazione di riferimento.

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

L'output è il seguente:

```
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"]}
```

Impostazioni dei registri privati

Amazon ECR utilizza le impostazioni del registro privato per configurare le funzionalità a livello di registro. Le impostazioni del registro privato sono configurate separatamente per ogni regione. Puoi utilizzare le impostazioni del registro privato per configurare le seguenti funzionalità.

- Autorizzazioni del registro: una policy di autorizzazioni di registro consente il controllo sulla replica e sulle autorizzazioni di cache pull-through. Per ulteriori informazioni, consulta Autorizzazioni di registro privato.
- Regole di cache pull-through: una regola di cache pull-through viene utilizzata per memorizzare nella cache le immagini da un registro upstream nel registro privato di Amazon ECR. Per ulteriori informazioni, consulta Utilizzo delle regole della cache pull-through.
- Configurazione di replica: la configurazione di replica viene utilizzata per controllare se i repository vengono copiati tra regioni o account AWS . Per ulteriori informazioni, consultare Replica di immagini private
- Modelli di creazione di repository: un modello di creazione di repository viene utilizzato per definire le impostazioni standard da applicare quando Amazon ECR crea nuovi repository per tuo conto. Un esempio in tal senso è rappresentato dai repository creati mediante un'operazione di cache pull-through. Per ulteriori informazioni, consulta Gestione dei modelli di creazione repository.
- Scanning configuration (Configurazione della scansione): per impostazione predefinita, il registro è abilitato per la scansione base. Puoi abilitare la scansione avanzata che offre una modalità di scansione automatica e continua che esegue la scansione delle vulnerabilità del sistema operativo e dei pacchetti del linguaggio di programmazione. Per ulteriori informazioni, consulta Scansione delle immagini.

Autorizzazioni di registro privato

Amazon ECR utilizza una policy di registro per concedere le autorizzazioni a un principale AWS a livello di registro privato. Queste autorizzazioni vengono utilizzate per l'ambito dell'accesso alla replica e alle funzionalità della cache pull through.

Amazon ECR applica le seguenti autorizzazioni solo a livello di registro privato. Se vengono aggiunte altre operazioni alla policy di registro, si verificherà un errore.

- `ecr:ReplicateImage`: concede l'autorizzazione a un altro account, denominato registro di origine, per replicare le immagini nel proprio registro. Questa operazione viene utilizzata solo per la replica tra account.
- `ecr:BatchImportUpstreamImage`— Concede l'autorizzazione per recuperare l'immagine esterna e importarla nel registro privato.
- `ecr:CreateRepository` – Concede l'autorizzazione per creare un repository in un registro privato. Questa autorizzazione è necessaria se il repository che archivia le immagini replicate o memorizzate nella cache non esiste già.

> **Note**
>
> Mentre è possibile aggiungere l'operazione `ecr:*` a una policy delle autorizzazioni del registro privato, una best practice consiste nell'aggiungere solo le operazioni specifiche richieste in base alla funzionalità utilizzata e non utilizzare un carattere jolly.

Argomenti

Impostazione di un'istruzione di autorizzazione del registro privato

È possibile aggiungere o aggiornare le policy delle autorizzazioni per il registro utilizzando la procedura seguente. Puoi aggiungere più dichiarazioni di policy per ciascun registro. Per esempi di policy, consulta Esempi di policy dei registri privati.

Argomenti

Autorizzazioni del registro privato per la replica

Il tipo di policy tra più account viene usato per concedere le autorizzazioni a un'entità principale AWS , consentendo la replica dei repository da un registro di origine al tuo registro. Per impostazione predefinita, hai l'autorizzazione per configurare la replica tra regioni all'interno del tuo registro. È necessario configurare le policy di registro solo se si concede a un altro account l'autorizzazione per replicare il contenuto nel registro.

Una policy di registro deve concedere l'autorizzazione per il operazione API `ecr:ReplicateImage`. Questa API è un'API Amazon ECR interna in grado di replicare immagini tra regioni o account. È inoltre possibile concedere l'autorizzazione per il `ecr:CreateRepository`, che consente ad Amazon ECR di creare repository nel registro se non esistono già. Se l'autorizzazione `ecr:CreateRepository` non viene fornita, nel registro deve essere creato manualmente un repository con lo stesso nome del repository di origine. Se nessuno dei due viene creato, la replica ha esito negativo. Eventuali azioni non riuscite CreateRepository o relative all' ReplicateImage API vengono visualizzate in CloudTrail.

Per configurare una policy delle autorizzazioni per la replica (AWS Management Console)

Per configurare una policy delle autorizzazioni per la replica per un registro privato (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione, scegli la regione in cui configurare la policy del registro.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Registry permissions (Autorizzazioni di registro).
4. Alla pagina Registry permissions (Autorizzazioni di registro), scegli Generate statement (Genera istruzione).
5. Per definire la tua istruzione di policy usando il generatore di policy, completa i seguenti passaggi.

    a. Per Policy Type (Tipo di policy), scegli Cross-account policy (Policy tra account).

b. In Statement ID (ID istruzione), inserisci un ID istruzione univoco. Questo campo viene utilizzato come `Sid` sulle policy di registro.

c. Per Account (Account), immettere gli ID account per ogni account a cui si desidera concedere le autorizzazioni. Quando si specificano più ID account, separarli con una virgola.

6. Espandere la sezione Preview policy statement (Istruzione di policy di anteprima) per esaminare l'istruzione delle policy delle autorizzazioni del registro.
7. Una volta confermata la dichiarazione delle policy, scegliere Add to policy (Aggiungi alla policy) per salvare la policy nel registro.

Per configurare una policy delle autorizzazioni per la replica (AWS CLI)

Per configurare una policy delle autorizzazioni per un registro privato (AWS CLI)

1. Creare un file denominato `registry_policy.json` e popolarlo con una policy di registro.

```
{
    "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. Creare le policy di registro utilizzando il file delle policy.

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

3. Recuperare le policy di registro da confermare.

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

Autorizzazioni del registro privato per la cache pull-through

Le autorizzazioni del registro privato di Amazon ECR possono essere utilizzate per definire le autorizzazioni delle singole entità IAM per utilizzare la cache pull-through. Se un'entità IAM dispone di più autorizzazioni concesse da una policy IAM di quelle concesse dalla policy delle autorizzazioni del registro, la policy IAM ha la precedenza.

Per creare una policy delle autorizzazioni del registro privato (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione, scegli la regione in cui configurare l'istruzione delle autorizzazioni del registro privato.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Registry permissions (Autorizzazioni di registro).
4. Alla pagina Registry permissions (Autorizzazioni di registro), scegli Generate statement (Genera istruzione).
5. Per ogni istruzione delle policy di autorizzazione della cache pull-through che si desidera creare, procedi come segue.
   a. Per Policy type (Tipo di policy), scegli Pull through cache policy (Policy della cache pull-through).
   b. Per Statement id (ID istruzione), inserisci un nome per la policy dell'istruzione della cache pull-through.
   c. Per Entità IAM, specifica gli utenti, i gruppi o i ruoli da includere nella policy.
   d. Per Repository namespace (Spazio dei nomi del repository), seleziona la regola della cache pull-through a cui associare la policy.
   e. Per Repository names (Nomi dei repository), specifica il nome di base del repository per cui applicare la regola. Ad esempio, se si desidera specificare il repository Amazon Linux su Amazon ECR Public, il nome del repository sarà `amazonlinux`.

Eliminazione di un'istruzione di autorizzazione del registro privato

È possibile eliminare tutte le istruzioni delle policy delle autorizzazioni per il registro utilizzando la procedura seguente.

Per eliminare una policy delle autorizzazioni per un registro privato (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione, scegli la regione in cui configurare la policy delle autorizzazioni del registro.
3. Nel riquadro di spostamento, seleziona Registries (Registri).
4. Alla pagina Registries (Registri), seleziona il tuo registro Private (Privato) e scegli Permissions (Autorizzazioni).
5. Alla pagina Privacy registry permissions (Autorizzazioni di registro privato), scegli Delete (Elimina).
6. Nella schermata di conferma Delete registry policy (Elimina policy di registro), scegli Delete policy (Elimina policy).

Per eliminare una policy delle autorizzazioni per un registro privato (AWS CLI)

1. Eliminare la policy di registro.

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

2. Recuperare le policy di registro da confermare.

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

Esempi di policy dei registri privati

I seguenti esempi mostrano le dichiarazioni di policy di autorizzazione del registro che è possibile utilizzare per controllare le autorizzazioni degli utenti per il registro Amazon ECR.

> **Note**
>
> In ogni esempio, se l'operazione `ecr:CreateRepository` viene rimossa dall'istruzione di autorizzazione del registro, la replica può ancora verificarsi. Tuttavia, per la replica corretta, è necessario creare repository con lo stesso nome all'interno dell'account.

Esempio: consentire all'utente root di un account di origine di replicare tutti i repository

```
{
    "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/*"
            ]
        }
    ]
}
```

Esempio: abilitare più account

```
{
    "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/*"
            ]
        }
    ]
}
```

Esempio: consentire all'utente root di un account di origine di replicare tutti i repository con prefisso **`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-*"
            ]
```

```
        }
    ]
}
```

Repository Amazon ECR privati

Amazon Elastic Container Registry (Amazon ECR) fornisce operazioni API per creare, monitorare ed eliminare i repository di immagini e impostare le autorizzazioni che controllano l'accesso. È possibile eseguire le stesse operazioni nella sezione Repositories (Repository) della console Amazon ECR. Amazon ECR si integra anche con l'interfaccia CLI di Docker, in modo da inviare ed estrarre immagini dagli ambienti di sviluppo ai repository.

Argomenti

Concetti del repository privato

- Per impostazione predefinita il tuo account ha accesso in lettura e in scrittura ai repository contenuti nel registro predefinito (*aws_account_id*.dkr.ecr.*region*.amazonaws.com). Tuttavia, gli utenti devono chiedere le autorizzazioni per effettuare chiamate alle API Amazon ECR e per inviare ed estrarre immagini da e verso i tuoi repository. Amazon ECR fornisce diverse policy gestite per controllare l'accesso degli utenti a diversi livelli. Per ulteriori informazioni, consulta Esempi di policy basate su Identità di Amazon Elastic Container Registry.
- I repository possono essere controllati tramite le policy di accesso degli utenti oppure con le policy relative ai singoli repository. Per ulteriori informazioni, consulta Policy del repository privato.
- I nomi dei repository possono supportare i namespace, utili per raggruppare repository simili. Ad esempio, se vi sono diversi team che utilizzano lo stesso registro, il Team A potrebbe utilizzare il namespace `team-a` mentre il Team B potrebbe utilizzare il namespace `team-b`. In questo modo, ogni team ha la propria immagine chiamata `web-app` con ogni immagine anteposta dallo spazio dei nomi del team. Questa configurazione consente di utilizzare simultaneamente queste immagini su ogni team senza interferenze. L'immagine del team A è `team-a/web-app` e l'immagine del team B è `team-b/web-app`.

- Le immagini possono essere replicate in altri repository tra regioni del proprio registro e tra account. È possibile eseguire questa operazione specificando una configurazione di replica nelle impostazioni del registro. Per ulteriori informazioni, consulta Impostazioni dei registri privati.

Creazione di un repository privato

Le immagini del container sono memorizzate nei repository Amazon ECR. Per creare un repository privato usando la AWS Management Console, segui i seguenti passaggi. Per i passaggi per creare un repository utilizzando la AWS CLI, consulta Fase 3: creazione di un repository.

Per creare un repository (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegliere la regione in cui creare il repository.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository), selezionare la scheda Private (Privato), quindi selezionare Create repository (Crea repository).
5. Per Visibility settings (Impostazioni di visibilità), verificare che Private (Privato) sia selezionato.
6. Per Repository name (Nome repository), immettere un nome univoco per il repository. Il nome del repository può essere specificato autonomamente (ad esempio `nginx-web-app`). In alternativa, può esservi anteposto uno spazio dei nomi per raggruppare il repository in una categoria (ad esempio `project-a/nginx-web-app`).

   > **Note**
   >
   > Il nome del repository può contenere un massimo di 256 caratteri. Il nome deve iniziare con una lettera e può contenere solo lettere minuscole, numeri, trattini, trattini bassi, punti e barre. L'uso di un doppio trattino, un doppio trattino basso o una doppia barra non è supportato.

7. Per Tag immutability (Immutabilità dei tag), scegliere l'impostazione di mutabilità dei tag per il repository. I repository configurati con tag immutabili impediscono la sovrascrittura dei tag immagine. Per ulteriori informazioni, consulta Mutabilità dei tag immagine.
8. Per Scan on push (Scansione tramite push), mentre è possibile specificare le impostazioni di scansione a livello di repository per la scansione di base, la best practice è specificare la configurazione di scansione a livello di registro privato. Specificare le impostazioni di scansione

nel registro privato che consentono di abilitare la scansione avanzata o la scansione di base, nonché di definire i filtri per specificare quali repository vengono scansionati. Per ulteriori informazioni, consulta Scansione delle immagini.

9. Per Crittografia KMS, scegliere se abilitare la crittografia delle immagini contenute nel repository usando AWS Key Management Service. Per impostazione predefinita, quando la crittografia KMS è abilitata, Amazon ECR utilizza un Chiave gestita da AWS (chiave KMS) con l'alias `aws/ecr`. Questa chiave viene creata nel tuo account la prima volta che crei un repository con la crittografia KMS abilitata. Per ulteriori informazioni, consulta Crittografia dei dati a riposo.
10. Quando è attivata la crittografia KMS, selezionare Customer encryption settings (advanced) (Impostazioni di crittografia del cliente (avanzate)) per scegliere la propria chiave KMS. La chiave KMS deve trovarsi nella stessa regione del cluster. Scegliere Create an AWS KMS key (Crea una chiave KMS) per passare alla console AWS KMS per creare la tua chiave.
11. Scegliere Create repository (Crea repository).
12. (Facoltativo) Seleziona il repository creato e scegli View push commands (Visualizza comandi push) per visualizzare i passaggi per inviare un'immagine al nuovo repository. Per ulteriori informazioni su come inserire un'immagine nel repository, consulta Invio di un'immagine.

Visualizzazione dei dettagli di un repository privato

Dopo aver creato un repository, è possibile visualizzare i dettagli del repository nella AWS Management Console:

- Quali immagini sono archiviate in un repository
- I dettagli su ogni immagine memorizzata nel repository, incluse le dimensioni e il digest SHA per ciascuna immagine
- La frequenza di scansione specificata per il contenuto del repository
- Se al repository è associata una regola di cache pull-through attiva
- L'impostazione di crittografia per il repository

> **Note**
>
> A partire dalla versione Docker 1.9, il client Docker comprime i livelli delle immagini prima di inviarli a un registro Docker V2. L'output del comand docker images mostra la dimensione

dell'immagine non compressa. Pertanto, tieni presente che Docker potrebbe restituire un'immagine più grande dell'immagine visualizzata in AWS Management Console.

Per visualizzare le informazioni relative al repository (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegliere la regione in cui si trova il repository da visualizzare.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository), seleziona la scheda Private (Privato) e quindi il repository da visualizzare.
5. Nella pagina prodotto del repository, la console viene impostata di default sulla visualizzazione Images (Immagini). Utilizzare il menu di navigazione per visualizzare altre informazioni sul repository.
   - Selezionare Summary (Riepilogo) per visualizzare i dettagli del repository e i dati del pull count per il repository.
   - Selezionare la scheda Images (Immagini) per visualizzare le informazioni sui tag di immagine contenuti nel repository. Per visualizzare ulteriori informazioni sull'immagine, selezionare il tag dell'immagine. Per ulteriori informazioni, consulta Visualizzazione dei dettagli delle immagini.

     Se vi sono immagini senza tag che desideri eliminare, puoi selezionare la casella a sinistra dei repository da eliminare e scegliere Delete (Elimina). Per ulteriori informazioni, consulta Eliminazione di un'immagine.
   - Selezionare la scheda Permissions (Autorizzazioni) per visualizzare le policy dei repository applicate al repository stesso. Per ulteriori informazioni, consulta Policy del repository privato.
   - Scegliere Lifecycle Policy (Policy ciclo di vita) per visualizzare le regole delle policy del ciclo di vita applicate al repository. Qui viene anche visualizzata la cronologia degli eventi del ciclo di vita. Per ulteriori informazioni, consulta Policy del ciclo di vita.
   - Selezionare la scheda Tags (Tag) per visualizzare i tag dei metadati applicati al repository.

Modifica di un repository privato

I repository esistenti possono essere modificati per cambiare la mutabilità dei tag di immagine e le impostazioni di scansione delle immagini.

Per modificare un repository (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegliere la regione in cui si trova il repository da modificare.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository), selezionare la scheda Private (Privato), quindi selezionare il repository da modificare e scegliere Edit (Modifica).
5. Per Tag immutability (Immutabilità dei tag), scegliere l'impostazione di mutabilità dei tag per il repository. I repository configurati con tag immutabili impediscono la sovrascrittura dei tag immagine. Per ulteriori informazioni, consulta Mutabilità dei tag immagine.
6. Per Image scan settings (Impostazioni di scansione delle immagini), mentre è possibile specificare le impostazioni di scansione a livello di repository per la scansione di base, la best practice è specificare la configurazione di scansione a livello di registro privato. Specificare le impostazioni di scansione nel registro privato che consentono di abilitare la scansione avanzata o la scansione di base, nonché di definire i filtri per specificare quali repository vengono scansionati. Per ulteriori informazioni, consulta Scansione delle immagini.
7. Per Encryption settings (Impostazioni di crittografia), si tratta di un campo di sola visualizzazione in quanto le impostazioni di crittografia per un repository non possono essere modificate una volta creato il repository.
8. Scegliere Save (Salva) per aggiornare le impostazioni del repository.

Eliminazione di un repository privato

Al termine dell'utilizzo di un repository, puoi eliminarlo. Quando elimini un repository contenuto nella AWS Management Console, tutte le immagini in esso contenute vengono eliminate; quest'azione non può essere annullata.

Per eliminare un repository (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegliere la regione in cui si trova il repository da eliminare.

3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository), selezionare la scheda Private (Privato), quindi selezionare il repository da eliminare e scegliere Delete (Elimina).
5. Nella finestra Delete (Elimina) ***repository_name***, verificare che i repository selezionati debbano essere eliminati, quindi selezionare Delete (Elimina).

> **Important**
>
> Anche tutte le immagini contenute nei repository selezionati vengono eliminate.

Policy del repository privato

Amazon ECR utilizza autorizzazioni basate sulle risorse per controllare l'accesso ai repository. Le autorizzazioni basate sulle risorse ti consentono di specificare gli utenti o i ruoli che hanno accesso a un repository e quali operazioni possono eseguire. Per impostazione predefinita, solo l'account AWS che ha creato il repository ha accesso a un repository. Puoi applicare un documento di policy per consentire autorizzazioni aggiuntive al tuo repository.

Argomenti

Policy del repository e policy IAM

Le policy del repository Amazon ECR sono un sottoinsieme delle policy IAM che vengono definite e specificamente utilizzate per controllare l'accesso ai singoli repository Amazon ECR. Le policy IAM sono generalmente utilizzate per applicare le autorizzazioni per l'intero servizio Amazon ECR, ma possono anche essere utilizzate per controllare l'accesso alle risorse specifiche.

Le policy dei repository Amazon ECR e le policy IAM vengono entrambe utilizzate per determinare quali azioni possono essere eseguite da un utente o un ruolo specifico su un repository. Se a un utente o a un ruolo è consentito eseguire un'operazione tramite una policy del repository ma l'autorizzazione gli viene negata da una policy IAM (o viceversa), anche l'operazione viene negata.

A un utente o a un ruolo deve essere concessa l'autorizzazione per un'operazione tramite una policy del repository o una policy IAM, ma non entrambe le opzioni per consentire l'operazione.

> **Important**
>
> Amazon ECR richiede che gli utenti dispongano dell'autorizzazione per effettuare chiamate all'API `ecr:GetAuthorizationToken` tramite una policy IAM prima che possano autenticarsi in un registro ed eseguire l'invio o l'estrazione delle immagini da un repository Amazon ECR. Amazon ECR fornisce diverse policy IAM gestite per controllare l'accesso degli utenti a diversi livelli: per ulteriori informazioni consultare Esempi di policy basate su Identità di Amazon Elastic Container Registry.

È possibile utilizzare questi tipi di policy per controllare l'accesso ai repository, come illustrato negli esempi seguenti.

Questo esempio illustra una policy del repository Amazon ECR che consente a un utente specifico di descrivere il repository e le immagini all'interno del repository.

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

Questo esempio illustra una policy IAM che consente di raggiungere lo stesso obiettivo precedente, definendo l'ambito della policy per un repository (specificato dall'ARN completo del repository) utilizzando il parametro a livello di risorsa. Per maggiori informazioni sul formato Amazon Resource Name (ARN), consulta Risorse.

```
{
```

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

Impostazione di una dichiarazione di policy per i repository privati

Puoi aggiungere una dichiarazione di policy di accesso a un repository nella AWS Management Console seguendo la procedura indicata di seguito. Puoi aggiungere più dichiarazioni di policy per ciascun repository. Per esempi di policy, consulta Esempi di policy di repository privati.

> **Important**
>
> Amazon ECR richiede che gli utenti dispongano dell'autorizzazione per effettuare chiamate all'API `ecr:GetAuthorizationToken` tramite una policy IAM prima che possano autenticarsi in un registro ed eseguire l'invio o l'estrazione delle immagini da un repository Amazon ECR. Amazon ECR fornisce diverse policy IAM gestite per controllare l'accesso degli utenti a diversi livelli: per ulteriori informazioni consultare Esempi di policy basate su Identità di Amazon Elastic Container Registry.

Per impostare una dichiarazioni di policy per i repository

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Sulla barra di navigazione seleziona la regione che contiene il repository sul quale impostare una dichiarazione di policy.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Alla pagina Repositories (Repository), scegliere il repository sul quale impostare una dichiarazione di policy per visualizzare il contenuto del repository.

5. Dalla visualizzazione dell'elenco immagini del repository, nel pannello di navigazione, selezionare Permissions (Autorizzazioni), Edit (Modifica).

> **Note**
>
> Se non si visualizza l'opzione Permissions (Autorizzazioni) nel pannello di navigazione, assicurarsi di essere nella visualizzazione dell'elenco immagini del repository.

6. Nella pagina Edit permissions (Modifica autorizzazioni), scegli Add statement (Aggiungi istruzione).
7. Nel campo Statement name (Nome istruzione) inserisci un nome per l'istruzione.
8. Per Effect (Effetto), scegliere se la dichiarazione della policy restituisce un consenso o una negazione esplicita.
9. In Principal seleziona l'ambito a cui applicare la dichiarazione di policy. Per ulteriori informazioni, consulta Elementi delle policy JSON AWS: principale nella Guida per l'utente di IAM.

   - Puoi applicare la dichiarazione a tutti gli utenti AWS autenticati selezionando la casella di controllo Everyone (*) (Tutti).
   - Per Service principal (Principal del servizio), specificare il nome del principal del servizio (ad esempio, `ecs.amazonaws.com`) per applicare la dichiarazione a un determinato servizio.
   - Per AWS Account IDs (ID account AWS), specificare un numero di account AWS (ad esempio `111122223333`) per applicare la dichiarazione a tutti gli utenti in un determinato account AWS. È possibile specificare più account utilizzando un elenco delimitato da virgole.

   > **Important**
   >
   > L'account a cui si concedono le autorizzazioni deve avere abilitata la regione in cui si sta creando la policy del repository; in caso contrario si verificherà un errore.

   - Per IAM Entities (Entità IAM), selezionare i ruoli o gli utenti nell'account AWS a cui applicare la dichiarazione.

> **Note**
>
> Per le policy più complesse relative agli archivi che non sono attualmente supportate nella AWS Management Console, puoi applicare la policy con il comando set-repository-policy AWS CLI.

10. In Actions (Operazioni), scegli l'ambito delle operazioni API di Amazon ECR a cui applicare la dichiarazione di policy dall'elenco delle singole operazioni API.
11. Al termine, seleziona Save (Salva) per impostare la policy.
12. Ripeti i passaggi precedenti per ogni policy di repository da aggiungere.

Eliminazione di una dichiarazione di policy per i repository privati

Se non desideri più applicare una dichiarazione di policy per i repository esistente a un repository, puoi eliminarla.

Per eliminare una dichiarazione di policy per i repository

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Sulla barra di navigazione scegli la regione che contiene il repository dal quale eliminare una dichiarazione di policy.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository) seleziona il repository dal quale eliminare una dichiarazione di policy.
5. Nel riquadro di navigazione, seleziona Permissions (Autorizzazioni), Edit (Modifica).
6. Nella pagina Edit permissions (Modifica autorizzazioni), scegli Delete (Elimina).

Esempi di policy di repository privati

> **Important**
>
> Gli esempi di policy di repository riportati in questa pagina sono concepiti per essere applicati ai repository privati di Amazon ECR. Non funzioneranno correttamente se utilizzati direttamente con un principale IAM, a meno che non vengano modificati per specificare il repository di Amazon ECR come risorsa. Per ulteriori informazioni sull'impostazione delle

policy dei repository, consulta Impostazione di una dichiarazione di policy per i repository privati.

Le policy del repository Amazon ECR sono un sottoinsieme delle policy IAM che vengono definite e specificamente utilizzate per controllare l'accesso ai singoli repository Amazon ECR. Le policy IAM sono generalmente utilizzate per applicare le autorizzazioni per l'intero servizio Amazon ECR, ma possono anche essere utilizzate per controllare l'accesso alle risorse specifiche. Per ulteriori informazioni, consulta Policy del repository e policy IAM .

I seguenti esempi di policy dei repository mostrano le dichiarazioni di autorizzazione che puoi utilizzare per controllare l'accesso ai repository privati di Amazon ECR.

Important

Amazon ECR richiede che gli utenti dispongano dell'autorizzazione per effettuare chiamate all'API `ecr:GetAuthorizationToken` tramite una policy IAM prima che possano autenticarsi in un registro ed eseguire l'invio o l'estrazione delle immagini da un repository Amazon ECR. Amazon ECR fornisce diverse policy IAM gestite per controllare l'accesso degli utenti a diversi livelli: per ulteriori informazioni consultare Esempi di policy basate su Identità di Amazon Elastic Container Registry.

Esempio: consentire uno o più utenti

La policy del repository seguente consente a uno o più utenti di eseguire il push e il pull delle immagini da e verso un repository.

```
{
    "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"
            ]
        }
    ]
}
```

Esempio: abilita un altro account

La seguente policy di repository consente a un account specifico di inviare immagini.

> **Important**
>
> L'account a cui si concedono le autorizzazioni deve avere abilitata la regione in cui si sta creando la policy del repository; in caso contrario si verificherà un errore.

```
{
    "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 policy seguente del repository consente agli utenti di eseguire il pull di immagini (*pull-user-1* e *pull-user-2*) concedendo l'accesso completo un altro utente (*admin-user*).

> **Note**
>
> Per le policy più complesse relative agli archivi che non sono attualmente supportate nella AWS Management Console, puoi applicare la policy con il comando set-repository-policy AWS CLI.

```
{
    "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:*"
            ]
        }
    ]
}
```

Esempio: vieta a tutti

La seguente policy di repository nega a tutti gli utenti in tutti gli account la possibilità di estrarre immagini.

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

Esempio: limitazione dell'accesso a indirizzi IP specifici

Nell'esempio seguente vengono negate autorizzazioni a qualunque utente per eseguire qualsiasi operazione Amazon ECR quando applicata a un repository da uno specifico intervallo di indirizzi.

La condizione in questa istruzione identifica l'intervallo `54.240.143.*` di indirizzi IP Internet Protocol versione 4 (IPv4) consentiti.

Il blocco `Condition` utilizza le condizioni `NotIpAddress` e la chiave di condizione `aws:SourceIp`, che è una chiave di condizione valida per tutto AWS. Per ulteriori informazioni su queste chiavi di condizioni, consulta Chiavi di contesto delle condizioni globali AWS. I valori IPv4 `aws:sourceIp` utilizzano la notazione CIDR standard. Per ulteriori informazioni, consulta Operatori di condizione con indirizzo IP nella Guida per l'utente di IAM.

```
{
    "Version": "2012-10-17",
    "Id": "ECRPolicyId1",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Deny",
```

```
            "Principal": "*",
            "Action": "ecr:*",
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": "54.240.143.0/24"
                }
            }
        }
    ]
}
```

Esempio: consenti un servizio AWS

La seguente policy di repository consente l'accesso AWS CodeBuild alle operazioni API Amazon ECR necessarie per l'integrazione con il servizio. Quando utilizzi l'esempio seguente, è necessario utilizzare le chiavi di condizione `aws:SourceArn` e `aws:SourceAccount` per l'ambito delle risorse che possono assumere tali autorizzazioni. Per ulteriori informazioni, consulta Campione Amazon ECR per CodeBuild nella Guida per l'utente di AWS CodeBuild.

```
{
   "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"
            }
         }
      }
   ]
```

```
}
```

Tagging di un repository privato

Per semplificare la gestione dei repository Amazon ECR, puoi decidere di assegnare metadati personalizzati a ogni repository sotto forma di tag di risorse AWS. Questo argomento descrive i tag di risorse AWS e mostra come crearli.

Nozioni di base sui tag

Un tag è un'etichetta che assegni a una risorsa AWS. Ogni tag consiste di una chiave e di un valore, entrambi personalizzabili.

I tag consentono di categorizzare le tue risorse AWS in modi diversi, ad esempio, per scopo, proprietario o ambiente. Questa funzionalità è molto utile quando hai tante risorse dello stesso tipo: puoi rapidamente individuare una risorsa specifica in base ai tag assegnati. Ad esempio, puoi definire un set di tag per i repository Amazon ECR del tuo account che consentono di monitorare il proprietario di ciascun repository.

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti. Tramite un set di chiavi di tag coerente la gestione delle risorse risulta notevolmente semplificata. Puoi cercare e filtrare le risorse in base ai tag aggiunti.

I tag non hanno alcun significato semantico per Amazon ECR e vengono interpretati rigorosamente come una stringa di caratteri. Inoltre, i tag non vengono assegnati automaticamente alle risorse. Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

Puoi lavorare con i tag utilizzando la AWS Management Console, l'AWS CLI e l'API Amazon ECR.

Se utilizzi AWS Identity and Access Management (IAM), puoi controllare quali utenti nel tuo account AWS dispongono dell'autorizzazione per creare, modificare o eliminare i tag.

Tagging delle risorse

Puoi applicare ai repository tag Amazon ECR nuovi o esistenti.

Se utilizzi la console Amazon ECR, puoi applicare tag alle nuove risorse quando vengono create o alle risorse esistenti usando l'opzione Tags (Tag) nel riquadro di navigazione in qualsiasi momento.

Se utilizzi l'API Amazon ECR, l'AWS CLI o un SKD AWS, puoi applicare i tag ai nuovi repository con il parametro `tags` nell'operazione API `CreateRepository` oppure usare l'operazione API `TagResource` per applicare tag alle risorse esistenti. Per ulteriori informazioni, consultare TagResource.

Inoltre, se i tag non possono essere applicati durante la creazione del repository, eseguiamo il rollback del processo di creazione del repository. Ciò fa sì che i repository vengano creati con i tag oppure che non vengano creati affatto, nonché che nessuna risorsa sia mai sprovvista di tag. Il tagging dei repository in fase di creazione ti permette di evitare di eseguire script di tagging personalizzati dopo la creazione dei repository.

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per repository - 50.
- Per ciascun repository, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- La lunghezza massima della chiave è 128 caratteri Unicode in formato UTF-8
- La lunghezza massima del valore è 256 caratteri Unicode in formato UTF-8
- Se lo schema di tagging viene utilizzato in più servizi e risorse, è necessario tenere presente che in altri servizi possono essere presenti limiti sui caratteri consentiti. I caratteri generalmente consentiti sono: lettere, numeri e spazi rappresentabili in formato UTF-8 e i seguenti caratteri speciali + – = . _ : / @.
- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole.
- Non utilizzare il prefisso `aws:` per chiavi o valori; l'utilizzo di questo prefisso è esclusivo di AWS. Non è possibile modificare né eliminare le chiavi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per il limite del numero di tag per risorsa.

Tagging delle risorse per la fatturazione

I tag che aggiungi ai repository Amazon ECR sono utili quando rivedi l'allocazione dei costi dopo averli abilitati nel report su costi e utilizzo. Per ulteriori informazioni, consulta Report di utilizzo di Amazon ECR.

Per visualizzare il costo delle risorse combinate, puoi organizzare le informazioni di fatturazione in base alle risorse con gli stessi valori di chiave di tag. Puoi ad esempio applicare tag a numerose risorse con un nome di applicazione specifico, quindi organizzare le informazioni di fatturazione per visualizzare il costo totale dell'applicazione in più servizi. Per ulteriori informazioni sulla configurazione di un report di allocazione dei costi mediante i tag, consulta Report di allocazione dei costi mensili nella Guida per l'utente di AWS Billing.

> **Note**
>
> Se hai appena abilitato la reportistica, i dati relativi al mese corrente saranno disponibili per la visualizzazione dopo 24 ore.

Utilizzo di tag tramite la console

Con la console Amazon ECR puoi gestire i tag associati ai repository nuovi o esistenti.

Quando selezioni un repository specifico nella console Amazon ECR puoi visualizzare i tag selezionando Tags (Tag) nel pannello di navigazione.

Per aggiungere un tag a un repository (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Seleziona la regione da utilizzare nella barra di navigazione.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repository, seleziona la casella di controllo accanto al repository che desideri taggare.
5. Dal menu Azione, seleziona Tag del repository.
6. Nella pagina Tag del repository seleziona Aggiungi tag, Aggiungi tag.
7. Nella pagina Modifica tag specifica la chiave e il valore di ogni tag, quindi scegli Salva.

Per eliminare un tag da una singola risorsa (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Seleziona la regione da utilizzare nella barra di navigazione.
3. Nella pagina Repository, seleziona la casella di controllo accanto al repository da cui desideri rimuovere un tag.

4. Dal menu Azione, seleziona Tag del repository.
5. Nella pagina Tag del repository seleziona Modifica.
6. Nella pagina Modifica tag del repository, seleziona Rimuovi per ogni tag da eliminare, quindi scegli Salva.

Utilizzo di tag tramite l'AWS CLI o l'API

Utilizza le seguenti informazioni per aggiungere, aggiornare, elencare ed eliminare i tag per le risorse. Nella documentazione corrispondente vengono forniti alcuni esempi.

Supporto del tagging per le risorse Amazon ECR

Processo	AWS CLI	Operazione API
Aggiungere sovrascrivere uno o più tag.	tag-resource	TagResource
Eliminare uno o più tag.	untag-resource	UntagResource

Gli esempi seguenti mostrano come gestire i tag con l'AWS CLI.

Esempio 1: applicazione di un tag a un repository esistente

Il comando seguente applica dei tag a un repository esistente.

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

Esempio 2: applicazione di più tag a un repository esistente

Il comando seguente applica dei tag a un repository esistente.

```
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
```

Esempio 3: rimozione di tag da un repository esistente

Il comando seguente elimina un tag da un repository esistente.

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

Esempio 4: elenco dei tag per un repository

Il comando seguente elenca i tag associati a un repository esistente.

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

Esempio 5: creazione di un repository e applicazione di un tag

Il comando seguente crea un repository denominato `test-repo` e aggiunge un tag con chiave `team` e valore `devs`.

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

Immagini private

Amazon Elastic Container Registry (Amazon ECR) archivia le immagini Docker, le immagini OCI (Open Container Initiative) e gli artifact compatibili con OCI in repository privati. Puoi utilizzare la CLI di Docker, il tuo client preferito, per inviare ed estrarre immagini dai tuoi repository.

Argomenti

Invio di un'immagine

Puoi inviare immagini Docker, elenchi manifesto e immagini Open Container Initiative (OCI) e artefatti compatibili ai tuoi repository privati. Le pagine seguenti descrivono più dettagliatamente questi elementi.

Amazon ECR fornisce inoltre un modo per replicare le immagini in altri repository, nelle regioni nel tuo registro e in account diversi, specificando una configurazione di replica nelle impostazioni del registro privato. Per ulteriori informazioni, consulta Impostazioni dei registri privati.

Argomenti

- Autorizzazioni IAM richieste per l'invio di un'immagine
- Invio di un'immagine Docker
- Inviare un'immagine multi-architettura
- Invio di un grafico Helm

Autorizzazioni IAM richieste per l'invio di un'immagine

Amazon ECR richiede che gli utenti dispongano delle seguenti autorizzazioni per l'invio delle immagini. Seguendo la best practice che prevede la concessione di privilegi minimi, è possibile assegnare tali autorizzazioni a un repository specifico oppure concedere le autorizzazioni per tutti i repository. Un utente deve autenticarsi in ogni registro Amazon ECR a cui desidera inviare le immagini richiedendo un token di autorizzazione. Amazon ECR fornisce diverse policy IAM gestite per controllare l'accesso degli utenti a diversi livelli: per ulteriori informazioni consultare Esempi di policy basate su Identità di Amazon Elastic Container Registry.

La policy IAM seguente concede le autorizzazioni necessarie per l'invio di un'immagine senza ambito a un repository specifico.

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

La policy IAM seguente concede le autorizzazioni necessarie per l'invio di un'immagine con ambito a un repository specifico. Il repository deve essere specificato come Amazon Resource Name (ARN) completo.

```
{
    "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": "*"
        }
    ]
}
```

Invio di un'immagine Docker

Puoi inviare le immagini del container a un repository Amazon ECR con il comando docker push. Amazon ECR supporta anche la creazione e l'invio di elenchi di manifesto di Docker che vengono utilizzati per immagini multi-architettura. Ogni immagine a cui si fa riferimento in un elenco di manifesto è già stata inviata al repository. Per ulteriori informazioni, consulta Inviare un'immagine multi-architettura.

Per inviare un'immagine Docker a un repository Amazon ECR

Il repository Amazon ECR deve esistere prima di eseguire l'invio dell'immagine. Per ulteriori informazioni, consulta the section called “Creazione di un repository”.

1. Autentica il tuo client Docker nel registro Amazon ECR al quale desideri inviare l'immagine. Devi ottenere i token di autenticazione per ciascun registro utilizzato. I token hanno una validità di 12 ore. Per ulteriori informazioni, consulta Autenticazione del registro privato.

   Per autenticare Docker in un registro Amazon ECR, esegui il comando aws ecr get-login-password. Quando si passa il token di autenticazione al comando docker login, usare il valore

AWS per il nome utente e specificare l'URI di registro Amazon ECR a cui si desidera autenticare. Se si esegue l'autenticazione a più registri, è necessario ripetere il comando per ogni registro di sistema.

> **Important**
>
> Se viene visualizzato un errore, installare o eseguire l'upgrade alla versione più recente dell' AWS CLI. Per ulteriori informazioni, consulta Installazione dell' AWS Command Line Interface nella Guida per l'utente di 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. Se il tuo repository di immagini non esiste ancora nel registro al quale intendi effettuare l'invio, crealo. Per ulteriori informazioni, consulta Creazione di un repository privato.
3. Identifica l'immagine locale da inviare. Esegui il comando docker images per elencare le immagini container nel tuo sistema.

   ```
   docker images
   ```

   Puoi identificare un'immagine con il valore *repository:tag* o l'ID immagine nell'output del comando risultante.
4. Assegna un tag alla tua immagine con la combinazione di registro, repository, e nome tag immagine opzionale Amazon ECR da utilizzare. Il formato del registro è *aws_account_id*.dkr.ecr.*us-west-2*.amazonaws.com. Il nome del repository deve corrispondere a quello del repository che hai creato per la tua immagine. Se ometti il tag dell'immagine, presupponiamo che sia `latest`.

   Nell'esempio seguente vengono assegnati tag a un'immagine locale con l'ID *e9ae3c220b23* come *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. Invia l'immagine con il comando docker push:

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

6. (Opzionale) Assegna eventuali tag aggiuntivi alla tua immagine e invia questi tag ad Amazon ECR ripetendo Step 4 e Step 5.

Inviare un'immagine multi-architettura

Amazon ECR supporta la creazione e l'invio di elenchi di manifesto di Docker che vengono utilizzati per immagini multi-architettura. Un elenco manifesto è un elenco di immagini che viene creato specificando uno o più nomi di immagini. In genere l'elenco manifesto viene creato da immagini che assolvono la stessa funzione ma per sistemi operativi o architetture diversi. L'elenco manifesto non è obbligatorio. Per ulteriori informazioni, consulta Docker manifest.

> **Important**
>
> L'interfaccia a riga di comando (CLI) Docker deve avere le funzionalità sperimentali attive per utilizzare questa funzionalità. Per ulteriori informazioni, consulta Funzionalità sperimentali.

Un elenco manifesto può essere estratto o è possibile farvi riferimento in una definizione di attività Amazon ECS o specifiche del pod Amazon EKS come altre immagini Amazon ECR.

I passaggi seguenti possono essere utilizzati per creare e inviare un elenco manifesto Docker in un repository Amazon ECR. È necessario che le immagini siano già inserite nel repository a cui fare riferimento nel manifesto Docker. Per informazioni su come inviare un'immagine, consulta Invio di un'immagine Docker.

Per eseguire l'invio di un'immagine Docker multi-architettura in un repository Amazon ECR

Il repository Amazon ECR deve esistere prima di eseguire l'invio dell'immagine. Per ulteriori informazioni, consulta the section called “Creazione di un repository”.

1. Autentica il tuo client Docker nel registro Amazon ECR al quale desideri inviare l'immagine. Devi ottenere i token di autenticazione per ciascun registro utilizzato. I token hanno una validità di 12 ore. Per ulteriori informazioni, consulta Autenticazione del registro privato.

   Per autenticare Docker in un registro Amazon ECR, esegui il comando aws ecr get-login-password. Quando si passa il token di autenticazione al comando docker login, usare il valore

`AWS` per il nome utente e specificare l'URI di registro Amazon ECR a cui si desidera autenticare. Se si esegue l'autenticazione a più registri, è necessario ripetere il comando per ogni registro di sistema.

> **Important**
>
> Se viene visualizzato un errore, installare o eseguire l'upgrade alla versione più recente dell' AWS CLI. Per ulteriori informazioni, consulta Installazione dell' AWS Command Line Interface nella Guida per l'utente di 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. Elenca le immagini nel tuo repository, confermando i tag immagine.

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

3. Crea l'elenco manifesto Docker. Il comando `manifest create` verifica che le immagini di riferimento siano già presenti nel repository e crea il manifest localmente.

```
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. (Facoltativo) Ispezionare l'elenco dei manifest Docker. Ciò consente di confermare le dimensioni e il digest per ogni manifest immagine a cui si fa riferimento nell'elenco dei manifest.

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

5. Eseguire l'invio dell'elenco manifesto Docker nel repository Amazon ECR.

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

Invio di un grafico Helm

Amazon ECR supporta l'invio degli artefatti Open Container Initiative (OCI) nei tuoi repository. Per visualizzare questa funzionalità, segui i passaggi seguenti per inviare un grafico Helm ad Amazon ECR.

Per ulteriori informazioni sull'utilizzo dei grafici Helm con hosting di Amazon ECR con Amazon EKS, consulta Installazione di un grafico Helm con hosting su Amazon ECR con Amazon EKS.

Per inviare un grafico Helm a un repository Amazon ECR

1. Installa la versione più recente del client Helm. Questi passaggi sono stati scritti utilizzando la versione `3.8.2` di Helm. Per ulteriori informazioni, consulta l'argomento relativo all'installazione di Helm.
2. Utilizza i seguenti passaggi per creare un grafico Helm di prova. Per ulteriori informazioni, consulta Documenti Helm - Nozioni di base.

   a. Creare un grafico Helm denominato `helm-test-chart` e cancellare il contenuto della directory `templates`.

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

   b. Crea un `templates` file ConfigMap nella cartella.

   ```
   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. Creazione pacchetto del grafico. L'output conterrà il nome del file del grafico in pacchetto utilizzato quando si invia il grafico Helm.

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

Output

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

4. Creare un repository per archiviare il grafico Helm. Il nome del repository deve corrispondere al nome utilizzato nel grafico Helm al passaggio 2. Per ulteriori informazioni, consulta Creazione di un repository privato.

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

5. Autentica il tuo client Helm nel registro Amazon ECR al quale desideri inviare il grafico Helm. Devi ottenere i token di autenticazione per ciascun registro utilizzato. I token hanno una validità di 12 ore. Per ulteriori informazioni, consulta Autenticazione del registro privato.

```
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. Inviare il grafico Helm utilizzando il comando helm push. L'output deve includere l'URI del repository Amazon ECR e il digest SHA.

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

7. Descrivi il tuo grafico Helm.

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

Nell'output, verificare che il parametri `artifactMediaType` indichi il tipo di artefatto corretto.

```
{
    "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. (Facoltativo) Per ulteriori passaggi, installa la configmap di Helm e inizia a utilizzare Amazon EKS. Per ulteriori informazioni, consulta Installazione di un grafico Helm con hosting su Amazon ECR con Amazon EKS.

Firma di un'immagine

Amazon ECR si integra con AWS Signer per fornirti un modo per firmare le immagini dei contenitori. Puoi archiviare sia le immagini del container sia le firme nei tuoi repository privati.

Considerazioni

Quando usi la firma di immagini Amazon ECR, tieni in considerazione quanto riportato di seguito.

- Le firme archiviate nel repository vengono conteggiate nella quota di servizio relativa al numero massimo di immagini per repository. Per ulteriori informazioni, consulta Service Quotas di Amazon ECR..
- Quando si utilizzano le policy del ciclo di vita di Amazon ECR, qualsiasi azione effettuata da una regola per far scadere o eliminare un indice di immagini OCI comporterà l'eliminazione da parte di Amazon ECR di tutte le firme a cui si fa riferimento in quell'indice di immagini entro 24 ore.

Prerequisiti

Prima di iniziare, verifica che siano stati soddisfatti i seguenti requisiti preliminari.

- Installazione e configurazione della versione più recente di AWS CLI. Per ulteriori informazioni, consulta Installazione o aggiornamento della versione più recente della AWS CLI nella Guida per l'utente di AWS Command Line Interface .
- Installa la Notation CLI e AWS Signer il plugin per Notation. Per ulteriori informazioni, consulta Prerequisiti per la firma delle immagini di container nella Guida per gli sviluppatori di AWS Signer .
- Conserva un'immagine del container da firmare in un repository privato Amazon ECR. Per ulteriori informazioni, consulta Invio di un'immagine.

Configurazione dell'autenticazione per il client Notary

Prima di poter creare una firma utilizzando l'interfaccia a riga di comando di Notation, devi configurare il client in modo che possa autenticarsi su Amazon ECR. Se hai installato Docker sullo stesso host in cui installi il client Notation, Notation riutilizzerà lo stesso metodo di autenticazione utilizzato per il client Docker. Il comandi del Docker `login` e `logout` consentiranno ai comandi `sign` e `verify` di Notation di utilizzare le stesse credenziali e non sarà necessario autenticare Notation separatamente. Per ulteriori informazioni sulla configurazione del client Notation per l'autenticazione, consulta Autenticazione con registri conformi agli OCI nella documentazione di Notary Project

Se non utilizzi Docker o un altro strumento che utilizza le credenziali Docker, ti consigliamo di utilizzare l'assistente di gestione credenziali Docker di Amazon ECR come archivio di credenziali. Per ulteriori informazioni su come installare e configurare l'assistente credenziali di Amazon ECR, consulta Assistente di gestione credenziali Docker di Amazon ECR.

Firma di un'immagine

I passaggi seguenti possono essere utilizzati per creare le risorse necessarie per firmare un'immagine di container e archiviare la firma in un repository privato Amazon ECR. Notation firma le immagini utilizzando il digest.

Per firmare un'immagine

1. Crea un profilo di AWS Signer firma utilizzando la `Notation-OCI-SHA384-ECDSA` piattaforma di firma. Facoltativamente, puoi specificare un periodo di validità della firma utilizzando il parametro `--signature-validity-period`. Questo valore può essere specificato utilizzando `DAYS`, `MONTHS` o `YEARS`. Se non viene specificato alcun periodo di validità, sarà utilizzato il valore predefinito 135 mesi.

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

> **Note**
>
> Il nome del profilo di firma supporta solo caratteri alfanumerici e il trattino basso (_).

2. Autentica il client Notation nel tuo registro predefinito. L'esempio seguente utilizza AWS CLI per autenticare la CLI di Notation in un registro privato Amazon ECR.

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

3. Usa la CLI di Notation per firmare l'immagine, specificando l'immagine utilizzando il nome del repository e il digest SHA. Così la firma viene creata e inviata allo stesso repository privato Amazon ECR in cui si trova l'immagine da firmare.

   Nell'esempio seguente, stiamo firmando un'immagine nel repository `curl` con il digest 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"
```

Verifica un'immagine localmente dopo la firma

Dopo aver firmato l'immagine di un contenitore utilizzando AWS Signer and Notation, tu o un membro autorizzato del tuo team potete verificare l'origine e l'integrità dell'immagine con mezzi crittografici.

Completa la seguente procedura per verificare la validità di un'immagine con Notation.

Verifica di un'immagine

1. Per la verifica è necessario un trust store. Se hai usato il programma di installazione per il AWS Signer plugin e Notation, un trust store è stato configurato automaticamente e dotato di un certificato root.

2. Imposta una policy di attendibilità simile a quella riportata di seguito, modificando secondo necessità i nomi dei profili di firma utilizzati per verificare le immagini.

```
{
   "version":"1.0",
   "trustPolicies":[
      {
         "name":"aws-signer-tp",
         "registryScopes":[
            "*"
         ],
         "signatureVerification":{
            "level":"strict"
         },
         "trustStores":[
            "signingAuthority:aws-signer-ts"
         ],
         "trustedIdentities":[
            "arn:aws:signer:region:111122223333:/signing-
profiles/ecr_signing_profile",
            "arn:aws:signer:region:111122223333:/signing-
profiles/ecr_signing_profile2"
         ]
      }
   ]
}
```

3. Importa la policy in Notation.

```
$ notation policy import mypolicy.json
```

Output:

```
Existing trust policy configuration found, do you
want to overwrite it? [y/N] y

Trust policy configuration imported successfully.
```

4. Verifica la firma, specificandola utilizzando il nome del repository e il digest SHA.

```
$ notation verify 111122223333.dkr.ecr.region.amazonaws.com/curl@SHA256_digest
```

Output:

```
Successfully verified signature for 111122223333.dkr.ecr.us-
west-2.amazonaws.com/curl@SHA256_digest
```

Eliminazione di una firma

Quando crei e invii una firma utilizzando la CLI di Notation, viene creato anche un indice di immagine OCI nel repository Amazon ECR. L'API Amazon ECR non supporta l'eliminazione di artefatti o immagini referenziati da un indice di immagini OCI, quindi per la loro cancellazione sono disponibili le seguenti opzioni.

- (Consigliato) È possibile utilizzare la CLI di ORAS per eliminare l'artefatto e ORAS gestirà l'aggiornamento o l'eliminazione dell'indice dell'immagine.
- Puoi utilizzare l'API o la console Amazon ECR per eliminare prima l'indice delle immagini OCI e poi l'artefatto a cui esso fa riferimento, la firma per esempio.

Quando si utilizza il client ORAS per eliminare firme e altri artefatti di riferimento, ORAS gestisce l'indice delle immagini OCI. ORAS rimuoverà prima il riferimento all'artefatto dall'indice, quindi eliminerà il manifesto. È possibile utilizzare il comando `oras manifest delete`, facendo riferimento all'indice dell'artefatto firma. Per ulteriori informazioni sull'installazione e la configurazione del client ORAS, consulta Installazione nella documentazione di ORAS.

Il comando di esempio seguente può essere utilizzato per eliminare una firma.

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

Visualizzazione dei dettagli delle immagini

Dopo aver inviato un'immagine al repository, puoi visualizzarne le informazioni nella AWS Management Console. I dettagli inclusi sono i seguenti:

- URI immagine
- Tag di immagine

- Tipo di supporto di un artefatto
- Tipo di manifesto delle immagini
- Stato della scansione
- Le dimensioni dell'immagine in MB
- Data del push dell'immagine al repository
- Lo stato di replica

Per visualizzare i dettagli dell'immagine (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegliere la regione in cui si trova il repository che contiene la tua immagine.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository), selezionare il repository da visualizzare.
5. Nella pagina Repositories (Repository): ***repository_name*** seleziona l'immagine di cui visualizzare i dettagli.

Estrazione di un'immagine

Se desideri eseguire un'immagine Docker disponibile in Amazon ECR, puoi estrarla nel tuo ambiente locale con il comando docker pull. È possibile eseguire questa operazione dal registro predefinito o da un registro associato a un altro account. AWS Per utilizzare un'immagine Amazon ECR in una definizione di attività Amazon ECS, consulta Utilizzo delle immagini Amazon ECR con Amazon ECS.

> **Important**
>
> Amazon ECR richiede che gli utenti dispongano dell'autorizzazione per effettuare chiamate all'API `ecr:GetAuthorizationToken` tramite una policy IAM prima che possano autenticarsi in un registro ed eseguire l'invio o l'estrazione delle immagini da un repository Amazon ECR. Amazon ECR fornisce diverse policy IAM gestite per controllare l'accesso degli utenti a diversi livelli: per ulteriori informazioni consultare Esempi di policy basate su Identità di Amazon Elastic Container Registry.

Per estrarre un'immagine Docker da un repository Amazon ECR

1. Autentica il tuo client Docker nel registro Amazon ECR dal quale desideri estrarre la tua immagine. Devi ottenere i token di autenticazione per ciascun registro utilizzato. I token hanno una validità di 12 ore. Per ulteriori informazioni, consulta Autenticazione del registro privato.
2. (Opzionale) Identifica l'immagine da estrarre.
   - Puoi elencare i repository in un registro con il comando aws ecr describe-repositories:

     ```
     aws ecr describe-repositories
     ```

     Il precedente esempio di registro ha un repository denominato `amazonlinux`.
   - Puoi descrivere le immagini in un repository con il comando aws ecr describe-images:

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

     Il precedente repository di esempio ha un'immagine taggata come `latest` e `2016.09`, con il digest dell'immagine `sha256:f1d4ae3f7261a72e98c6ebefe9985cf10a0ea5bd762585a43e0700ed99863807`.
3. Estrai l'immagine con il comando docker pull. Il formato del nome dell'immagine deve essere *`registry`*`/`*`repository`*`[:`*`tag`*`]` per effettuare l'estrazione tramite tag o *`registry`*`/`*`repository`*`[@`*`digest`*`]` per effettuare l'estrazione tramite digest.

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

   > **Important**
   >
   > Se ricevi un errore *`repository-url`* `not found: does not exist or no pull access`, potrebbe essere necessario autenticare il tuo client Docker con Amazon ECR. Per ulteriori informazioni, consulta Autenticazione del registro privato.

Utilizzo delle regole della cache pull-through

Con le regole di cache pull-through, puoi sincronizzare il contenuto di un registro upstream con il tuo registro privato Amazon ECR. Amazon ECR attualmente supporta la creazione di regole di cache pull-through per i seguenti registri upstream.

- Docker Hub, Microsoft Azure Container Registry e GitHub Container Registry (richiede l'autenticazione)
- Amazon ECR Public, il registro di immagini di container Kubernetes e Quay (non richiede l'autenticazione)

Per i registri upstream che richiedono l'autenticazione, è necessario archiviare le credenziali in modo segreto. AWS Secrets Manager La console di Amazon ECR semplifica la creazione del segreto di Secrets Manager per ciascuno dei registri upstream autenticati. Per ulteriori informazioni sulla creazione di un segreto di Secrets Manager utilizzando la console di Secrets Manager, consulta Archiviazione segreta delle credenziali del repository originale AWS Secrets Manager.

Dopo aver creato una regola di cache pull-through per il registro upstream, è sufficiente estrarre un'immagine da quel registro upstream utilizzando l'URI del registro privato Amazon ECR. Amazon ECR, quindi, crea un repository e memorizza l'immagine nella cache nel tuo registro privato. Nelle richieste pull successive dell'immagine memorizzata nella cache con un determinato tag, Amazon ECR controlla il registro upstream per vedere se esiste una nuova versione dell'immagine con quel tag specifico e tenta di aggiornare l'immagine nel registro privato almeno una volta ogni 24 ore.

Amazon ECR ha aggiunto il supporto per i modelli di creazione di repository, attualmente in anteprima, che ti consente di specificare le configurazioni iniziali per i nuovi repository creati da Amazon ECR per tuo conto utilizzando le regole di cache pull-through. Ogni modello contiene un prefisso dello spazio dei nomi del repository che viene utilizzato per abbinare i nuovi repository a un modello specifico. I modelli possono specificare la configurazione per tutte le impostazioni del repository, comprese le policy di accesso basate sulle risorse, l'immutabilità dei tag, la crittografia e le policy del ciclo di vita. Le impostazioni in un modello di creazione di repository vengono applicate solo durante la creazione del repository e non hanno alcun effetto sui repository esistenti o sui repository creati con altri metodi. Per ulteriori informazioni, consulta Gestione dei modelli di creazione repository.

Considerazioni sull'utilizzo della cache pull-through

Quando utilizzi le regole di cache pull-through di Amazon ECR, tieni presente quanto segue.

- La creazione di regole di cache pull-through non è supportata nelle seguenti regioni.
  - Cina (Pechino) (`cn-north-1`)
  - Cina (Ningxia) (`cn-northwest-1`)
  - AWS GovCloud (Stati Uniti orientali) () `us-gov-east-1`

  - AWS GovCloud (Stati Uniti occidentali) () `us-gov-west-1`
- AWS Lambda non supporta l'estrazione di immagini di container da Amazon ECR utilizzando una regola pull through cache.
- Quando si estraggono immagini utilizzando la cache pull-through, gli endpoint del servizio FIPS di Amazon ECR non sono supportati la prima volta che viene estratta un'immagine. Tuttavia, l'utilizzo degli endpoint del servizio FIPS Amazon ECR funziona sui pull successivi.
- Quando un'immagine memorizzata nella cache viene estratta dall'URI del registro privato di Amazon ECR, i recuperi delle immagini vengono avviati dagli indirizzi IP. AWS Ciò garantisce che l'estrazione dell'immagine non tenga conto delle quote relative alla frequenza di estrazione implementate dal registro upstream.
- Quando un'immagine memorizzata nella cache viene estratta attraverso l'URI del registro privato di Amazon ECR, quest'ultimo controlla il repository upstream almeno una volta ogni 24 ore per verificare se la versione dell'immagine memorizzata nella cache è la più recente. Se è presente un'immagine più recente nel registro upstream, Amazon ECR tenta di aggiornare l'immagine memorizzata nella cache. Questo timer è basato sull'ultima estrazione dell'immagine memorizzata nella cache.
- Se per qualsiasi motivo Amazon ECR non è in grado di aggiornare l'immagine dal registro upstream e l'immagine viene estratta, l'ultima immagine memorizzata nella cache verrà comunque estratta.
- Quando crei il segreto di Secrets Manager contenente le credenziali del registro upstream, il nome del segreto deve utilizzare il prefisso `ecr-pullthroughcache/`. Il segreto, inoltre, deve trovarsi nello stesso account e nella stessa regione in cui è stata creata la regola di cache pull-through.
- Quando un'immagine multi-architettura viene estratta utilizzando una regola di cache pull-through, l'elenco manifesto e ogni immagine a cui fa riferimento nell'elenco manifesto vengono estratti nel repository Amazon ECR. Se si desidera estrarre solo un'architettura specifica, è possibile estrarre l'immagine utilizzando il digest dell'immagine o il tag associato all'architettura anziché il tag associato all'elenco manifesto.
- Amazon ECR utilizza un ruolo IAM collegato ai servizi che fornisce le autorizzazioni necessarie ad Amazon ECR per creare per tuo conto il repository, recuperare il valore segreto di Secrets Manager per l'autenticazione e inviare l'immagine memorizzata nella cache. Il ruolo IAM collegato ai servizi viene creato automaticamente quando viene creata una regola di cache pull-through. Per ulteriori informazioni, consulta Ruolo collegato ai servizi Amazon ECR per la cache pull-through.
- Per impostazione predefinita, il principale IAM che estrae l'immagine memorizzata nella cache dispone delle autorizzazioni concesse tramite la policy IAM. È possibile utilizzare la policy delle

autorizzazioni del registro privato di Amazon ECR per definire ulteriormente le autorizzazioni di un'entità IAM. Per ulteriori informazioni, consulta Utilizzo delle autorizzazioni di registro.

- I repository Amazon ECR creati utilizzando il flusso di lavoro della cache pull-through vengono trattati come qualsiasi altro repository Amazon ECR. Sono supportate tutte le funzionalità del repository, come la replica e la scansione delle immagini.
- Quando Amazon ECR crea un nuovo repository per tuo conto utilizzando un'azione di cache pull-through, al repository vengono applicate le impostazioni predefinite indicate di seguito, a meno che non esista un modello di creazione repository corrispondente. Puoi utilizzare un modello di creazione repository per definire le impostazioni applicate ai repository creati da Amazon ECR per tuo conto. Per ulteriori informazioni, consulta Gestione dei modelli di creazione repository.
  - Immutabilità dei tag: se disattivata, i tag sono mutabili e possono essere sovrascritti.
  - Crittografia: viene utilizzata la crittografia `AES256` predefinita.
  - Autorizzazioni del repository: se omesse, non vengono applicate policy relative alle autorizzazioni del repository.
  - Policy del ciclo di vita: se omesse, non vengono applicate policy del ciclo di vita.
  - Tag delle risorse: se omessi, non viene applicato alcun tag di risorsa.
- L'attivazione dell'immutabilità dei tag di immagine per i repository utilizzando una regola di cache pull-through impedirà ad Amazon ECR di aggiornare le immagini utilizzando lo stesso tag.
- Quando un'immagine viene recuperata utilizzando la regola pull-through cache per la prima volta, può essere necessario un percorso verso Internet. In alcune circostanze è necessario un percorso verso Internet, quindi è meglio impostare un percorso per evitare errori. Pertanto, se hai configurato Amazon ECR per utilizzare un'interfaccia che AWS PrivateLink utilizza un endpoint VPC, devi assicurarti che il primo pull abbia un percorso verso Internet. Un modo per farlo consiste nel creare una sottorete pubblica nello stesso VPC, con un gateway Internet, e quindi indirizzare tutto il traffico in uscita verso Internet dalla sottorete privata alla sottorete pubblica. I successivi recuperi di immagini che utilizzano la regola pull through cache non richiedono questa operazione. Per ulteriori informazioni, consulta Opzioni di routing di esempio nella Guida per l'utente di Amazon Virtual Private Cloud.

Autorizzazioni IAM richieste

Oltre alle autorizzazioni dell'API Amazon ECR necessarie per l'autenticazione in un registro privato e per l'invio e l'estrazione di immagini, sono necessarie le seguenti autorizzazioni aggiuntive per utilizzare efficacemente le regole di cache pull-through.

- `ecr:CreatePullThroughCacheRule` – Concede l'autorizzazione per creare una nuova regola di cache pull-through. Questa autorizzazione deve essere concessa tramite una policy IAM basata sull'identità.
- `ecr:BatchImportUpstreamImage`— Concede l'autorizzazione per recuperare l'immagine esterna e importarla nel registro privato. Questa autorizzazione può essere concessa utilizzando la policy delle autorizzazioni del registro privato, una policy IAM basata sull'identità o utilizzando la policy delle autorizzazioni del repository basate sulle risorse. Per ulteriori informazioni sull'uso delle autorizzazioni del repository, consulta Policy del repository privato.
- `ecr:CreateRepository` – Concede l'autorizzazione per creare un repository in un registro privato. Questa autorizzazione è necessaria se il repository che memorizza le immagini memorizzate nella cache non è già esistente. Questa autorizzazione può essere concessa da una policy IAM basata sull'identità o dalla policy delle autorizzazioni del registro privato.
- `ecr:TagResource`: concede l'autorizzazione all'aggiunta di tag di metadati a una risorsa di Amazon ECR. Questa autorizzazione è richiesta solo se stai estraendo un'immagine che utilizza una regola di cache pull-through associata a un modello di creazione repository configurato per l'aggiunta di tag di risorse al repository. Questa autorizzazione deve essere concessa tramite una policy IAM basata sull'identità.

Utilizzo delle autorizzazioni di registro

Le autorizzazioni del registro privato di Amazon ECR possono essere utilizzate per definire le autorizzazioni delle singole entità IAM per utilizzare la cache pull-through. Se un'entità IAM dispone di più autorizzazioni concesse da una policy IAM di quelle concesse dalla policy delle autorizzazioni del registro, la policy IAM ha la precedenza. Ad esempio, se a un utente sono state concesse autorizzazioni `ecr:*`, non occorrono altre autorizzazioni a livello di registro.

Per creare una policy delle autorizzazioni del registro privato (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione, scegli la regione in cui configurare l'istruzione delle autorizzazioni del registro privato.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Registry permissions (Autorizzazioni di registro).
4. Alla pagina Registry permissions (Autorizzazioni di registro), scegli Generate statement (Genera istruzione).

5. Per ogni istruzione delle policy di autorizzazione della cache pull-through che si desidera creare, procedi come segue.

   a. Per Policy type (Tipo di policy), scegli Pull through cache policy (Policy della cache pull-through).

   b. Per Statement id (ID istruzione), inserisci un nome per la policy dell'istruzione della cache pull-through.

   c. Per Entità IAM, specifica gli utenti, i gruppi o i ruoli da includere nella policy.

   d. Per Repository namespace (Spazio dei nomi del repository), seleziona la regola della cache pull-through a cui associare la policy.

   e. Per Repository names (Nomi dei repository), specifica il nome di base del repository per cui applicare la regola. Ad esempio, se si desidera specificare il repository Amazon Linux su Amazon ECR Public, il nome del repository sarà `amazonlinux`.

Per creare una policy delle autorizzazioni del registro privato (AWS CLI)

Utilizzare il AWS CLI comando seguente per specificare le autorizzazioni del registro privato utilizzando. AWS CLI

1. Crea un file locale denominato `ptc-registry-policy.json` con il contenuto della policy del registro. L'esempio seguente concede l'autorizzazione `ecr-pull-through-cache-user` per creare un repository ed eseguire il pull di un'immagine da Amazon ECR Public, che è l'origine upstream associata alla regola cache pull-through creata precedentemente.

```
{
  "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'autorizzazione `ecr-CreateRepository` è necessaria solo se il repository che memorizza le immagini memorizzate nella cache non è già esistente. Ad esempio, se l'operazione di creazione del repository e le operazioni di estrazione dell'immagine vengono eseguite da principali IAM separati come un amministratore e uno sviluppatore.

2. Utilizzare il put-registry-policycomando per impostare la politica del registro.

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

Passaggi successivi

Quando sei pronto a cominciare a utilizzare le regole di cache pull-through, attieniti ai passaggi seguenti.

- Crea una regola di cache pull-through. Per ulteriori informazioni, consulta Creazione di una regola di cache pull-through.
- Crea un modello di creazione repository. Un modello di creazione repository ti consente di gestire la definizione delle impostazioni da utilizzare per i nuovi repository creati da Amazon ECR per tuo conto nel corso di un'operazione di estrazione di cache pull-through. Per ulteriori informazioni, consulta Gestione dei modelli di creazione repository.
- Scopri come utilizzare le regole di cache pull-through. Per ulteriori informazioni, consulta Utilizzo delle regole di cache pull-through.

Creazione di una regola di cache pull-through

Devi creare una regola di cache pull-through per ogni registro upstream contenente le immagini da memorizzare nella cache del registro privato di Amazon ECR. Per i registri upstream che richiedono l'autenticazione, devi archiviare le credenziali in un segreto di Secrets Manager. Puoi creare il segreto di Secrets Manager nelle console di Amazon ECR o di Secrets Manager.

Prima di iniziare a creare le regole di cache pull-through, assicurati di disporre delle opportune autorizzazioni IAM. Per ulteriori informazioni, consulta Autorizzazioni IAM richieste.

Per creare una regola di cache pull-through (AWS Management Console)

Nei passaggi seguenti viene illustrato come creare una regola di cache pull-through e un segreto di Secrets Manager tramite la console di Amazon ECR. Per ulteriori informazioni sulla creazione di un segreto tramite la console di Secrets Manager, consulta Archiviazione segreta delle credenziali del repository originale AWS Secrets Manager.

Per Amazon ECR Public, il registro container Kubernetes o Quay

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione, scegli la regione in cui configurare le impostazioni del registro privato.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Pull through cache (Cache pull-through).
4. Nella pagina Pull through cache configuration (Configurazione della cache pull through), scegli Add rule (Aggiungi regola).
5. Nella pagina Passaggio 1: specifica un'origine, per Registro seleziona Amazon ECR Public, Kubernetes o Quay dall'elenco dei registri upstream, quindi seleziona Avanti.
6. Nella pagina Passaggio 2: specifica una destinazione, per Prefisso del repository Amazon ECR specifica il prefisso dello spazio dei nomi del repository da utilizzare per la memorizzazione nella cache delle immagini estratte dal registro pubblico di origine, quindi seleziona Avanti. Per impostazione predefinita, viene popolato uno spazio dei nomi ma è possibile specificare anche uno spazio dei nomi personalizzato.
7. Nella pagina Passaggio 3: rivedi e crea, esamina la configurazione della regola di cache pull-through, quindi seleziona Crea.
8. Ripeti il passaggio precedente per ogni cache pull-through da creare. Le regole della cache pull-through vengono create separatamente per ciascuna regione.

Per Docker Hub

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione, scegli la regione in cui configurare le impostazioni del registro privato.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Pull through cache (Cache pull-through).
4. Nella pagina Pull through cache configuration (Configurazione della cache pull through), scegli Add rule (Aggiungi regola).

5. Nel Passaggio 1: specifica un'origine, per Registro seleziona Docker Hub, Avanti.
6. Nella pagina Passaggio 2: configura l'autenticazione, per Credenziali Upstream devi archiviare le credenziali di autenticazione per Docker Hub in un segreto di AWS Secrets Manager . Puoi specificare un segreto esistente o utilizzare la console di Amazon ECR per crearne uno nuovo.

   a. Per utilizzare un segreto esistente, scegli Usa un AWS segreto esistente. Per Nome del segreto, utilizza il menu a discesa per selezionare il segreto esistente, quindi seleziona Avanti. Per ulteriori informazioni sulla creazione di un segreto di Secrets Manager utilizzando la console di Secrets Manager, consulta Archiviazione segreta delle credenziali del repository originale AWS Secrets Manager.

      > **Note**
      >
      > Visualizza AWS Management Console solo i segreti di Secrets Manager i cui nomi utilizzano il `ecr-pullthroughcache/` prefisso. Il segreto, inoltre, deve trovarsi nello stesso account e nella stessa regione in cui è stata creata la regola di cache pull-through.

   b. Per creare un nuovo segreto, seleziona Crea un segreto di AWS , effettua le seguenti operazioni e seleziona Avanti.

      i. Per Nome del segreto specifica un nome descrittivo per il segreto. I nomi dei segreti devono contenere un numero di caratteri Unicode compreso tra 1 e 512.

      ii. Per Nome utente di Docker Hub specifica il tuo nome utente di Docker Hub.

      iii. Per Token di accesso Docker Hub specifica il tuo token di accesso Docker Hub. Per ulteriori informazioni sulla creazione di un token di accesso Docker Hub, consulta Creazione e gestione di token di accesso nella documentazione di Docker.

7. Nella pagina Passaggio 3: specifica una destinazione, per Prefisso del repository Amazon ECR specifica lo spazio dei nomi del repository da utilizzare nel corso della memorizzazione nella cache delle immagini estratte dal registro pubblico di origine, quindi seleziona Avanti.

   Per impostazione predefinita, viene popolato uno spazio dei nomi ma è possibile specificare anche uno spazio dei nomi personalizzato.

8. Nella pagina Passaggio 4: rivedi e crea, esamina la configurazione della regola di cache pull-through, quindi seleziona Crea.
9. Ripeti il passaggio precedente per ogni cache pull-through da creare. Le regole della cache pull-through vengono create separatamente per ciascuna regione.

Per GitHub Container Registry

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione, scegli la regione in cui configurare le impostazioni del registro privato.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Pull through cache (Cache pull-through).
4. Nella pagina Pull through cache configuration (Configurazione della cache pull through), scegli Add rule (Aggiungi regola).
5. Nel Passaggio 1: Specificare una pagina di origine, per Registro, selezionare GitHub Container Registry, Next.
6. Nella pagina Passaggio 2: Configurazione dell'autenticazione, per le credenziali Upstream, è necessario archiviare le credenziali di autenticazione per GitHub Container Registry in un luogo segreto. AWS Secrets Manager Puoi specificare un segreto esistente o utilizzare la console di Amazon ECR per crearne uno nuovo.

    a. Per utilizzare un segreto esistente, scegli Usa un segreto esistente. AWS Per Nome del segreto, utilizza il menu a discesa per selezionare il segreto esistente, quindi seleziona Avanti. Per ulteriori informazioni sulla creazione di un segreto di Secrets Manager utilizzando la console di Secrets Manager, consulta Archiviazione segreta delle credenziali del repository originale AWS Secrets Manager.

    > **Note**
    >
    > Visualizza AWS Management Console solo i segreti di Secrets Manager i cui nomi utilizzano il `ecr-pullthroughcache/` prefisso. Il segreto, inoltre, deve trovarsi nello stesso account e nella stessa regione in cui è stata creata la regola di cache pull-through.

    b. Per creare un nuovo segreto, seleziona Crea un segreto di AWS , effettua le seguenti operazioni e seleziona Avanti.

        i. Per Nome del segreto specifica un nome descrittivo per il segreto. I nomi dei segreti devono contenere un numero di caratteri Unicode compreso tra 1 e 512.

        ii. Per il nome utente del GitHub Container Registry, specifica il tuo nome utente del GitHub Container Registry.

        iii. Per il token di accesso al GitHub Container Registry, specifica il token di accesso al GitHub Container Registry. Per ulteriori informazioni sulla creazione di un token

di GitHub accesso, consulta Gestire i token di accesso personali nella GitHub documentazione.

7. Nella pagina Passaggio 3: specifica una destinazione, per Prefisso del repository Amazon ECR specifica lo spazio dei nomi del repository da utilizzare nel corso della memorizzazione nella cache delle immagini estratte dal registro pubblico di origine, quindi seleziona Avanti.

   Per impostazione predefinita, viene popolato uno spazio dei nomi ma è possibile specificare anche uno spazio dei nomi personalizzato.

8. Nella pagina Passaggio 4: rivedi e crea, esamina la configurazione della regola di cache pull-through, quindi seleziona Crea.
9. Ripeti il passaggio precedente per ogni cache pull-through da creare. Le regole della cache pull-through vengono create separatamente per ciascuna regione.

Per Microsoft Azure Container Registry

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione, scegli la regione in cui configurare le impostazioni del registro privato.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Pull through cache (Cache pull-through).
4. Nella pagina Pull through cache configuration (Configurazione della cache pull through), scegli Add rule (Aggiungi regola).
5. Nella pagina Passaggio 1: specifica un'origine, procedi come segue.

   a. Per Registro seleziona Microsoft Azure Container Registry

   b. Per URL registro di origine, specifica il nome del registro dei container di Microsoft Azure, quindi seleziona Avanti.

   > **Important**
   >
   > Poiché il suffisso `.azurecr.io` viene compilato per tuo conto, devi specificare solo il prefisso.

6. Nella pagina Passaggio 2: configura l'autenticazione, per Credenziali Upstream devi archiviare le credenziali di autenticazione per Microsoft Azure Container Registry in un segreto di AWS Secrets Manager . Puoi specificare un segreto esistente o utilizzare la console di Amazon ECR per crearne uno nuovo.

a. Per utilizzare un segreto esistente, scegli Usa un AWS segreto esistente. Per Nome del segreto, utilizza il menu a discesa per selezionare il segreto esistente, quindi seleziona Avanti. Per ulteriori informazioni sulla creazione di un segreto di Secrets Manager utilizzando la console di Secrets Manager, consulta Archiviazione segreta delle credenziali del repository originale AWS Secrets Manager.

> **Note**
>
> Visualizza AWS Management Console solo i segreti di Secrets Manager i cui nomi utilizzano il `ecr-pullthroughcache/` prefisso. Il segreto, inoltre, deve trovarsi nello stesso account e nella stessa regione in cui è stata creata la regola di cache pull-through.

b. Per creare un nuovo segreto, seleziona Crea un segreto di AWS , effettua le seguenti operazioni e seleziona Avanti.

   i. Per Nome del segreto specifica un nome descrittivo per il segreto. I nomi dei segreti devono contenere un numero di caratteri Unicode compreso tra 1 e 512.

   ii. Per Nome utente di Microsoft Azure Container Registry, specifica il tuo nome utente per Microsoft Azure Container Registry.

   iii. Per Token di accesso di Microsoft Azure Container Registry, specifica il tuo token di accesso per Microsoft Azure Container Registry. Per ulteriori informazioni sulla creazione di un token di accesso per Microsoft Azure Container Registry, consulta Creazione token - portale nella documentazione di Microsoft Azure.

7. Nella pagina Passaggio 3: specifica una destinazione, per Prefisso del repository Amazon ECR specifica lo spazio dei nomi del repository da utilizzare nel corso della memorizzazione nella cache delle immagini estratte dal registro pubblico di origine, quindi seleziona Avanti.

   Per impostazione predefinita, viene popolato uno spazio dei nomi ma è possibile specificare anche uno spazio dei nomi personalizzato.

8. Nella pagina Passaggio 4: rivedi e crea, esamina la configurazione della regola di cache pull-through, quindi seleziona Crea.

9. Ripeti il passaggio precedente per ogni cache pull-through da creare. Le regole della cache pull-through vengono create separatamente per ciascuna regione.

Per creare una regola di cache pull-through (AWS CLI)

Usa il AWS CLI comando create-pull-through-cache-rule per creare una regola pull through cache per un registro privato Amazon ECR. Per i registri upstream che richiedono l'autenticazione, devi archiviare le credenziali in un segreto di Secrets Manager. Per ulteriori informazioni sulla creazione di un segreto tramite la console di Secrets Manager, consulta Archiviazione segreta delle credenziali del repository originale AWS Secrets Manager.

Gli esempi seguenti sono forniti per ogni registro upstream supportato.

Per Amazon ECR Public

L'esempio seguente crea una regola di cache pull-through per il registro pubblico di Amazon ECR. Specifica un prefisso di `ecr-public`, che fa sì che ciascun repository creato utilizzando la regola della cache pull-through abbia lo schema di denominazione di `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
```

Per il registro dei container Kubernetes

L'esempio seguente crea una regola di cache pull through per il registro pubblico Kubernetes. Specifica un prefisso di `kubernetes`, che fa sì che ciascun repository creato utilizzando la regola della cache pull-through abbia lo schema di denominazione di `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
```

Per Quay

L'esempio seguente crea una regola di cache pull-through per il registro pubblico Quay. Specifica un prefisso di `quay`, che fa sì che ciascun repository creato utilizzando la regola della cache pull-through abbia lo schema di denominazione di `quay/`*`upstream-repository-name`*.

```
aws ecr create-pull-through-cache-rule \
```

```
    --ecr-repository-prefix quay \
    --upstream-registry-url quay.io \
    --region us-east-2
```

Per Docker Hub

L'esempio seguente crea una regola di cache pull-through per il registro Docker Hub. Specifica un prefisso di `docker-hub`, che fa sì che ciascun repository creato utilizzando la regola della cache pull-through abbia lo schema di denominazione di `docker-hub/`*`upstream-repository-name`*. Devi specificare nella sua interezza il nome della risorsa Amazon (ARN) del segreto contenente le credenziali di 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
```

Per GitHub Container Registry

L'esempio seguente crea una regola pull through cache per il registro GitHub Container Registry. Specifica un prefisso di `docker-hub`, che fa sì che ciascun repository creato utilizzando la regola della cache pull-through abbia lo schema di denominazione di `github/`*`upstream-repository-name`*. È necessario specificare l'Amazon Resource Name (ARN) completo del segreto contenente le credenziali del GitHub Container Registry.

```
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
```

Per Microsoft Azure Container Registry

L'esempio seguente crea una regola di cache pull-through per il registro Microsoft Azure Container Registry. Specifica un prefisso di `azure`, che fa sì che ciascun repository creato utilizzando la regola della cache pull-through abbia lo schema di denominazione di `azure/`*`upstream-repository-name`*. Devi specificare nella sua interezza il nome della risorsa Amazon (ARN) del segreto contenente le credenziali di Microsoft 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
```

Passaggi successivi

Dopo aver creato le regole di cache pull-through, attieniti ai seguenti passaggi.

- Crea un modello di creazione repository. Un modello di creazione repository ti consente di gestire la definizione delle impostazioni da utilizzare per i nuovi repository creati da Amazon ECR per tuo conto nel corso di un'operazione di estrazione di cache pull-through. Per ulteriori informazioni, consulta Gestione dei modelli di creazione repository.
- Convalida le regole di cache pull-through. Durante la convalida di una regola cache di pull-through, Amazon ECR stabilisce una connessione di rete con il registro upstream, verifica di poter accedere al segreto di Secrets Manager contenente le credenziali del registro upstream e controlla che l'autenticazione sia avvenuta correttamente. Per ulteriori informazioni, consulta Convalida della regola di cache pull-through.
- Inizia a utilizzare le regole di cache pull-through. Per ulteriori informazioni, consulta Estrazione di un'immagine con una regola di cache pull-through.

Gestione dei modelli di creazione repository

Questa funzionalità è in versione di anteprima per Amazon ECR ed è soggetta a modifiche . Durante questa anteprima pubblica, può essere utilizzata solamente la AWS Management Console per gestire i modelli di creazione del repository.

I modelli di creazione di repository Amazon ECR ti consentono di gestire la definizione delle impostazioni da utilizzare per i nuovi repository creati da Amazon ECR per tuo conto nel corso di un'operazione di estrazione di cache pull-through. Le impostazioni in un modello di creazione di repository vengono applicate solo durante la creazione del repository e non hanno alcun effetto sui repository esistenti o sui repository creati con altri metodi.

I modelli di creazione di repository non sono supportati nelle seguenti regioni.

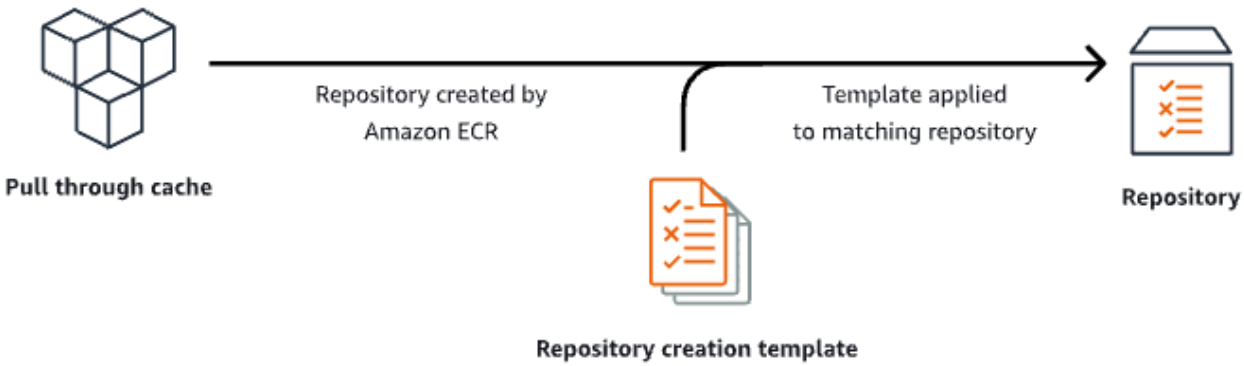
- Cina (Pechino) (`cn-north-1`)
- Cina (Ningxia) (`cn-northwest-1`)
- AWS GovCloud (Stati Uniti orientali) (`us-gov-east-1`)
- AWS GovCloud (Stati Uniti occidentali) (`us-gov-west-1`)

Funzionamento dei modelli di creazione di repository

A volte Amazon ECR deve creare un nuovo repository privato per tuo conto. Questo succede, ad esempio, la prima volta che utilizzi una regola di cache pull-through per recuperare il contenuto di un repository upstream e archiviarlo nel registro privato di Amazon ECR. Quando non è presente un modello di creazione di repository che corrisponda alla regola di cache pull-through, Amazon ECR utilizza le impostazioni predefinite per il nuovo repository. Queste impostazioni predefinite includono la disattivazione dell'immutabilità dei tag, l'utilizzo della crittografia `AES-256` e la mancata applicazione di policy di repository o del ciclo di vita.

L'utilizzo di un modello di creazione di repository con un prefisso che corrisponda a una regola di cache pull-through consente di definire le impostazioni che Amazon ECR applica ai nuovi repository creati tramite l'operazione di cache pull-through. Puoi definire l'immutabilità dei tag, la configurazione della crittografia, le autorizzazioni dei repository, la policy del ciclo di vita e i tag delle risorse per i nuovi repository.

Il diagramma seguente mostra il flusso di lavoro utilizzato da Amazon ECR quando viene utilizzato un modello di creazione repository.



Di seguito sono descritti in dettaglio i parametri di un modello di creazione repository.

Prefix

Il prefisso è il prefisso dello spazio dei nomi del repository da associare al modello. A tutti i repository creati utilizzando questo prefisso verranno applicate le impostazioni definite in questo modello. Ad esempio, il prefisso `prod` verrebbe applicato a tutti i repository che iniziano con `prod/`. Analogamente, il prefisso `prod/team` verrebbe applicato a tutti i repository che iniziano con `prod/team/`.

Per applicare un modello a tutti i repository del registro a cui non è associato un modello di creazione, puoi utilizzare `ROOT` come prefisso.

> **Important**
>
> Si presuppone che `/` venga sempre applicato alla fine del prefisso. Se specifichi `ecr-public` come prefisso, Amazon ECR lo considera come `ecr-public/`. Quando utilizzi una regola di cache pull-through, il prefisso del repository specificato durante la creazione della regola è quello da specificare anche come prefisso del modello di creazione di repository.

Descrizione

Questa descrizione del modello è facoltativa e viene utilizzata per illustrare lo scopo del modello di creazione repository.

Versione del modello

La versione del modello di creazione repository da utilizzare. Attualmente è supportata solo la versione del modello `TV1`.

Versione di configurazione

La versione di configurazione del repository utilizzata dal modello. Ogni modello deve includere una configurazione del repository. La versione di configurazione predefinita è `CV1` e comprende le impostazioni della mutabilità dei tag di immagine, della policy del repository e del ciclo di vita.

Mutabilità dei tag immagine

L'impostazione di mutabilità dei tag da utilizzare per i repository creati utilizzando il modello. Se questo parametro viene omesso, verrà utilizzata l'impostazione predefinita MUTABLE, che consentirà la sovrascrittura dei tag immagine. Questa è l'impostazione consigliata da utilizzare

per i modelli utilizzati per i repository creati dalle azioni di cache pull-through. Ciò garantisce che Amazon ECR possa aggiornare le immagini memorizzate nella cache quando i tag sono gli stessi.

Se è specificato IMMUTABLE, tutti i tag immagine all'interno del repository saranno immutabili, per cui non potranno essere sovrascritti.

Configurazione della crittografia

La configurazione della crittografia da utilizzare per i repository creati utilizzando il modello.

Se utilizzi il tipo di crittografia KMS, il contenuto del repository verrà crittografato utilizzando la crittografia lato server con la chiave AWS Key Management Service archiviata in AWS KMS. Quando utilizzi AWS KMS per crittografare i dati, puoi utilizzare la chiave gestita AWS AWS KMS per Amazon ECR o puoi specificare la tua chiave AWS KMS creata precedentemente. Per ulteriori informazioni, consulta Protezione dei dati tramite la crittografia lato server con una chiave AWS Key Management Service memorizzata in AWS Key Management Service (SSE-KMS) nella Guida per l'utente di Amazon Simple Storage Service.

Se utilizzi il tipo di crittografia AES256, Amazon ECR utilizza la crittografia lato server con chiavi di crittografia gestite da Amazon S3 che crittografano le immagini nel repository utilizzando un algoritmo di crittografia AES-256. Per ulteriori informazioni, consulta Protezione dei dati mediante la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3) nella Guida per l'utente di Amazon Simple Storage Service.

Autorizzazioni del repository

La policy di repository da applicare ai repository creati utilizzando il modello. Una policy di repository utilizza autorizzazioni basate sulle risorse per controllare l'accesso a un repository. Le autorizzazioni basate sulle risorse ti consentono di specificare gli utenti o i ruoli IAM che hanno accesso a un repository e quali operazioni possono eseguire. Per impostazione predefinita, solo l'account AWS che ha creato il repository ha accesso a un repository. Puoi applicare un documento di policy per concedere o negare autorizzazioni aggiuntive al tuo repository. Per ulteriori informazioni, consulta

Amazon ECR utilizza autorizzazioni basate sulle risorse per controllare l'accesso ai repository. Le autorizzazioni basate sulle risorse ti consentono di specificare gli utenti o i ruoli che hanno accesso a un repository e quali operazioni possono eseguire. Per impostazione predefinita, solo l'account AWS che ha creato il repository ha accesso a un repository. Puoi applicare un documento di policy per consentire autorizzazioni aggiuntive al tuo repository.

Argomenti

Policy del repository e policy IAM

Le policy del repository Amazon ECR sono un sottoinsieme delle policy IAM che vengono definite e specificamente utilizzate per controllare l'accesso ai singoli repository Amazon ECR. Le policy IAM sono generalmente utilizzate per applicare le autorizzazioni per l'intero servizio Amazon ECR, ma possono anche essere utilizzate per controllare l'accesso alle risorse specifiche.

Le policy dei repository Amazon ECR e le policy IAM vengono entrambe utilizzate per determinare quali azioni possono essere eseguite da un utente o un ruolo specifico su un repository. Se a un utente o a un ruolo è consentito eseguire un'operazione tramite una policy del repository ma l'autorizzazione gli viene negata da una policy IAM (o viceversa), anche l'operazione viene negata. A un utente o a un ruolo deve essere concessa l'autorizzazione per un'operazione tramite una policy del repository o una policy IAM, ma non entrambe le opzioni per consentire l'operazione.

> **Important**
>
> Amazon ECR richiede che gli utenti dispongano dell'autorizzazione per effettuare chiamate all'API `ecr:GetAuthorizationToken` tramite una policy IAM prima che possano autenticarsi in un registro ed eseguire l'invio o l'estrazione delle immagini da un repository Amazon ECR. Amazon ECR fornisce diverse policy IAM gestite per controllare l'accesso degli utenti a diversi livelli: per ulteriori informazioni consultare Esempi di policy basate su Identità di Amazon Elastic Container Registry.

È possibile utilizzare questi tipi di policy per controllare l'accesso ai repository, come illustrato negli esempi seguenti.

Questo esempio illustra una policy del repository Amazon ECR che consente a un utente specifico di descrivere il repository e le immagini all'interno del repository.

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

Questo esempio illustra una policy IAM che consente di raggiungere lo stesso obiettivo precedente, definendo l'ambito della policy per un repository (specificato dall'ARN completo del repository) utilizzando il parametro a livello di risorsa. Per maggiori informazioni sul formato Amazon Resource Name (ARN), consulta Risorse.

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

dichiarazioni di policy per ciascun repository. Per esempi di policy, consulta Esempi di policy di repository privati.

> **Important**
>
> Amazon ECR richiede che gli utenti dispongano dell'autorizzazione per effettuare chiamate all'API `ecr:GetAuthorizationToken` tramite una policy IAM prima che possano autenticarsi in un registro ed eseguire l'invio o l'estrazione delle immagini da un repository Amazon ECR. Amazon ECR fornisce diverse policy IAM gestite per controllare l'accesso degli utenti a diversi livelli: per ulteriori informazioni consultare Esempi di policy basate su Identità di Amazon Elastic Container Registry.

Per impostare una dichiarazioni di policy per i repository

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Sulla barra di navigazione seleziona la regione che contiene il repository sul quale impostare una dichiarazione di policy.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Alla pagina Repositories (Repository), scegliere il repository sul quale impostare una dichiarazione di policy per visualizzare il contenuto del repository.
5. Dalla visualizzazione dell'elenco immagini del repository, nel pannello di navigazione, selezionare Permissions (Autorizzazioni), Edit (Modifica).

   > **Note**
   >
   > Se non si visualizza l'opzione Permissions (Autorizzazioni) nel pannello di navigazione, assicurarsi di essere nella visualizzazione dell'elenco immagini del repository.

6. Nella pagina Edit permissions (Modifica autorizzazioni), scegli Add statement (Aggiungi istruzione).
7. Nel campo Statement name (Nome istruzione) inserisci un nome per l'istruzione.
8. Per Effect (Effetto), scegliere se la dichiarazione della policy restituisce un consenso o una negazione esplicita.

9. In Principal seleziona l'ambito a cui applicare la dichiarazione di policy. Per ulteriori informazioni, consulta Elementi delle policy JSON AWS: principale nella Guida per l'utente di IAM.
   - Puoi applicare la dichiarazione a tutti gli utenti AWS autenticati selezionando la casella di controllo Everyone (*) (Tutti).
   - Per Service principal (Principal del servizio), specificare il nome del principal del servizio (ad esempio, `ecs.amazonaws.com`) per applicare la dichiarazione a un determinato servizio.
   - Per AWS Account IDs (ID account AWS), specificare un numero di account AWS (ad esempio `111122223333`) per applicare la dichiarazione a tutti gli utenti in un determinato account AWS. È possibile specificare più account utilizzando un elenco delimitato da virgole.

     Important

     L'account a cui si concedono le autorizzazioni deve avere abilitata la regione in cui si sta creando la policy del repository; in caso contrario si verificherà un errore.
   - Per IAM Entities (Entità IAM), selezionare i ruoli o gli utenti nell'account AWS a cui applicare la dichiarazione.

     Note

     Per le policy più complesse relative agli archivi che non sono attualmente supportate nella AWS Management Console, puoi applicare la policy con il comando set-repository-policy AWS CLI.
10. In Actions (Operazioni), scegli l'ambito delle operazioni API di Amazon ECR a cui applicare la dichiarazione di policy dall'elenco delle singole operazioni API.
11. Al termine, seleziona Save (Salva) per impostare la policy.
12. Ripeti i passaggi precedenti per ogni policy di repository da aggiungere.

Eliminazione di una dichiarazione di policy per i repository privati

Se non desideri più applicare una dichiarazione di policy per i repository esistente a un repository, puoi eliminarla.

Per eliminare una dichiarazione di policy per i repository

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Sulla barra di navigazione scegli la regione che contiene il repository dal quale eliminare una dichiarazione di policy.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository) seleziona il repository dal quale eliminare una dichiarazione di policy.
5. Nel riquadro di navigazione, seleziona Permissions (Autorizzazioni), Edit (Modifica).
6. Nella pagina Edit permissions (Modifica autorizzazioni), scegli Delete (Elimina).

Esempi di policy di repository privati

> **Important**
>
> Gli esempi di policy di repository riportati in questa pagina sono concepiti per essere applicati ai repository privati di Amazon ECR. Non funzioneranno correttamente se utilizzati direttamente con un principale IAM, a meno che non vengano modificati per specificare il repository di Amazon ECR come risorsa. Per ulteriori informazioni sull'impostazione delle policy dei repository, consulta Impostazione di una dichiarazione di policy per i repository privati.

Le policy del repository Amazon ECR sono un sottoinsieme delle policy IAM che vengono definite e specificamente utilizzate per controllare l'accesso ai singoli repository Amazon ECR. Le policy IAM sono generalmente utilizzate per applicare le autorizzazioni per l'intero servizio Amazon ECR, ma possono anche essere utilizzate per controllare l'accesso alle risorse specifiche. Per ulteriori informazioni, consulta Policy del repository e policy IAM.

I seguenti esempi di policy dei repository mostrano le dichiarazioni di autorizzazione che puoi utilizzare per controllare l'accesso ai repository privati di Amazon ECR.

> **Important**
>
> Amazon ECR richiede che gli utenti dispongano dell'autorizzazione per effettuare chiamate all'API `ecr:GetAuthorizationToken` tramite una policy IAM prima che possano autenticarsi in un registro ed eseguire l'invio o l'estrazione delle immagini da un repository Amazon ECR. Amazon ECR fornisce diverse policy IAM gestite per controllare l'accesso degli utenti a diversi livelli: per ulteriori informazioni consultare Esempi di policy basate su Identità di Amazon Elastic Container Registry.

Esempio: consentire uno o più utenti

La policy del repository seguente consente a uno o più utenti di eseguire il push e il pull delle immagini da e verso un repository.

```
{
    "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": [
```

Esempio: abilita un altro account

La seguente policy di repository consente a un account specifico di inviare immagini.

> **Important**
>
> L'account a cui si concedono le autorizzazioni deve avere abilitata la regione in cui si sta creando la policy del repository; in caso contrario si verificherà un errore.

```
{
    "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"
            ]
        }
    ]
}
```

```
{
    "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:BatchGetImage",
                "ecr:GetDownloadUrlForLayer"
            ]
        }
    ]
}
```

Esempio: limitazione dell'accesso a indirizzi IP specifici

Nell'esempio seguente vengono negate autorizzazioni a qualunque utente per eseguire qualsiasi operazione Amazon ECR quando applicata a un repository da uno specifico intervallo di indirizzi.

La condizione in questa istruzione identifica l'intervallo `54.240.143.*` di indirizzi IP Internet Protocol versione 4 (IPv4) consentiti.

Il blocco `Condition` utilizza le condizioni `NotIpAddress` e la chiave di condizione `aws:SourceIp`, che è una chiave di condizione valida per tutto AWS. Per ulteriori informazioni su queste chiavi di condizioni, consulta Chiavi di contesto delle condizioni globali AWS. I valori IPv4 `aws:sourceIp` utilizzano la notazione CIDR standard. Per ulteriori informazioni, consulta Operatori di condizione con indirizzo IP nella Guida per l'utente di IAM.

```
{
    "Version": "2012-10-17",
    "Id": "ECRPolicyId1",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "ecr:*",
            "Condition": {
```

Esempio: consenti un servizio AWS

La seguente policy di repository consente l'accesso AWS CodeBuild alle operazioni API Amazon ECR necessarie per l'integrazione con il servizio. Quando utilizzi l'esempio seguente, è necessario utilizzare le chiavi di condizione `aws:SourceArn` e `aws:SourceAccount` per l'ambito delle risorse che possono assumere tali autorizzazioni. Per ulteriori informazioni, consulta Campione Amazon ECR per CodeBuild nella Guida per l'utente di AWS CodeBuild.

```
{
   "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":{
```

dei container, facendo scadere le immagini in base all'età o al conteggio. Per ulteriori informazioni, consulta Policy del ciclo di vita.

Tag delle risorse

I tag delle risorse sono metadati da applicare al repository per facilitarne la catalogazione e l'organizzazione. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

Autorizzazioni IAM necessarie per creare modelli di creazione repository

Le seguenti autorizzazioni sono necessarie per consentire a un principale IAM di gestire i modelli di creazione repository. Questa autorizzazione deve essere concessa utilizzando una policy IAM basata sull'identità.

- `ecr:CreateRepositoryCreationTemplate`: concede l'autorizzazione a creare un modello di creazione repository.
- `ecr:DeleteRepositoryCreationTemplate`: concede l'autorizzazione a eliminare un modello di creazione repository.
- `ecr:PutLifecyclePolicy`: concede l'autorizzazione a creare una policy del ciclo di vita e applicarla a un repository. Questa autorizzazione è necessaria solo se il modello di creazione repository include una policy del ciclo di vita.
- `ecr:SetRepositoryPolicy`: concede l'autorizzazione a creare una policy di autorizzazioni per un repository. Questa autorizzazione è necessaria solo se il modello di creazione repository include una policy del repository.
- `ecr:TagResource`: concede l'autorizzazione ad aggiungere tag metadati a una risorsa. Questa autorizzazione è necessaria solo se il modello di creazione repository include tag di risorse.

Creazione di un modello di creazione repository

Puoi creare un modello di creazione repository per definire le impostazione da utilizzare per i repository creati da Amazon ECR per tuo conto quando vengono eseguite operazioni di estrazione di cache pull-through. Una volta creato il modello di creazione repository, verranno applicate le impostazioni a tutti i nuovi repository creati. Ciò non ha alcun effetto sui repository creati in precedenza.

Creazione di un modello di creazione repository (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione seleziona la regione in cui creare il modello di creazione repository.
3. Nel riquadro di navigazione seleziona Registro privato, Modelli di creazione repository.
4. Nella pagina Modelli di creazione repository seleziona Crea modello.
5. Nella pagina Passaggio 1: definisci il modello, per Dettagli del modello seleziona Un prefisso specifico per applicare il modello a un prefisso dello spazio dei nomi di un repository specifico o seleziona Qualsiasi prefisso nel registro ECR per applicare il modello a tutti i repository che non corrispondono a nessun altro modello della Regione.

   a. Se selezioni Un prefisso specifico per Prefisso, specifica il prefisso dello spazio dei nomi del repository a cui applicare il modello. Si presuppone che `/` venga sempre applicato alla fine del prefisso. Ad esempio, il prefisso `prod` verrebbe applicato a tutti i repository che iniziano con `prod/`. Analogamente, il prefisso `prod/team` verrebbe applicato a tutti i repository che iniziano con `prod/team/`.

   b. Se selezioni Qualsiasi prefisso nel registro ECR, il Prefisso verrà impostato su. `ROOT`.

6. Per Descrizione del modello, specifica una descrizione facoltativa del modello, quindi seleziona Avanti.
7. Nella pagina Passaggio 2: aggiungi una configurazione di creazione del repository e specifica la configurazione delle impostazioni del repository da applicare ai repository creati utilizzando il modello.

   a. Per Mutabilità dei tag immagine, seleziona l'impostazione di mutabilità dei tag da utilizzare. Per ulteriori informazioni, consulta Mutabilità dei tag immagine.

      Quando è selezionato Mutable, i tag immagine possono essere sovrascritti. Questa è l'impostazione consigliata da utilizzare per i modelli utilizzati per i repository creati dalle azioni di cache pull-through. Ciò garantisce che Amazon ECR possa aggiornare le immagini memorizzate nella cache quando i tag sono gli stessi.

      Quando è selezionato Immutabile, i tag immagine non possono essere sovrascritti. Una volta configurato il repository per i tag immutabili, viene restituito un errore `ImageTagAlreadyExistsException` se si tenta di inviare un'immagine con un tag che esiste già nel repository. Quando l'immutabilità dei tag è attivata per un repository, tutti i tag saranno interessati e non sarà possibile rendere immutabili alcuni tag mentre altri no.

b. Per la configurazione della crittografia, scegli l'impostazione di crittografia da utilizzare. Per ulteriori informazioni, consulta Crittografia dei dati a riposo.

   Quando è selezionato AES-256, Amazon ECR utilizza la crittografia lato server con chiavi di crittografia gestite da Amazon Simple Storage Service che crittografa i dati a riposo utilizzando un algoritmo di crittografia AES-256 standard di settore. Questa funzionalità è disponibile senza costi aggiuntivi.

   Quando è selezionato AWS KMS, Amazon ECR utilizza la crittografia lato server con chiavi archiviate in AWS Key Management Service (AWS KMS). Quando utilizzi AWS KMS per crittografare i dati, puoi utilizzare la chiave predefinita gestita da AWS, che è gestita da Amazon ECR, oppure specificare la tua chiave AWS KMS, denominata chiave gestita dal cliente.

   > **Note**
   >
   > Le impostazioni di crittografia per un repository non possono essere modificate una volta che il repository è stato creato.

c. Per Autorizzazioni del repository specifica la policy di autorizzazione di repository da applicare ai repository creati utilizzando questo modello. Facoltativamente, puoi utilizzare il menu a discesa per selezionare uno degli esempi JSON per i casi d'uso più comuni. Per ulteriori informazioni, consulta Policy del repository privato.

d. Per Policy del ciclo di vita dei repository specifica la policy di ciclo di vita dei repository da applicare ai repository creati utilizzando questo modello. Facoltativamente, puoi utilizzare il menu a discesa per selezionare uno degli esempi JSON per i casi d'uso più comuni. Per ulteriori informazioni, consulta Policy del ciclo di vita.

e. Per Tag AWS dei repository specifica i metadati, sotto forma di coppie chiave-valore, da associare ai repository creati utilizzando questo modello, quindi seleziona Avanti. Per ulteriori informazioni, consulta Tagging di un repository privato.

8. Nella pagina Passaggio 3: rivedi e crea, rivedi le impostazioni specificate per il modello di creazione repository. Seleziona l'opzione Modifica per apportare le modifiche. Al termine, seleziona Crea.

Eliminazione di un modello di creazione repository

Puoi eliminare un modello di creazione repository se non è più utilizzato. Una volta eliminato il modello di creazione repository, a tutti i nuovi repository creati durante un'operazione di cache pull-through verranno applicate le impostazioni predefinite.

Eliminazione di un modello di creazione repository (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione seleziona la regione in cui si trova il modello di creazione repository da eliminare.
3. Nel riquadro di navigazione seleziona Registro privato, Modelli di creazione repository.
4. Nella pagina Modelli di creazione di repository, seleziona il modello di creazione repository da eliminare.
5. Dal menu a discesa Operazioni, seleziona Elimina.

Utilizzo delle regole di cache pull-through

Dopo aver creato una regola di cache pull-through per un registro upstream, puoi convalidare la regola per i registri upstream che richiedono l'autenticazione. A questo punto, puoi estrarre le immagini upstream utilizzando l'URI del repository Amazon ECR in modo che le immagini siano memorizzate nella cache nel registro privato di Amazon ECR.

Prima di iniziare a utilizzare le regole di cache pull-through, assicurati di disporre delle opportune autorizzazioni IAM. Per ulteriori informazioni, consulta Autorizzazioni IAM richieste.

Convalida della regola di cache pull-through

Dopo aver creato una regola di cache pull-through, puoi verificare che la regola funzioni correttamente. Durante la convalida di una regola cache di pull-through, Amazon ECR stabilisce una connessione di rete con il registro upstream, verifica di poter accedere al segreto di Secrets Manager contenente le credenziali del registro upstream e controlla che l'autenticazione sia avvenuta correttamente.

Creazione di una regola di cache pull-through (AWS Management Console)

Nei seguenti passaggi viene illustrato come convalidare una regola di cache pull-through tramite la console di Amazon ECR.

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione seleziona la regione in cui si trova la regola di cache pull-through da convalidare.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Pull through cache (Cache pull-through).
4. Nella pagina Configurazione di cache pull-through, seleziona la regola cache di pull-through da convalidare. Utilizza, quindi, il menu a discesa Azioni e seleziona Visualizza dettagli.
5. Nella pagina dei dettagli della regola cache di pull-through, utilizza il menu a discesa Azioni e seleziona Verifica l'autenticazione. Amazon ECR mostrerà un banner con il risultato.
6. Ripeti questi passaggi per ogni regola di cache pull-through da convalidare.

Creazione di una regola di cache pull-through (AWS CLI)

Il AWS CLI comando validate-pull-through-cache-rule viene utilizzato per convalidare una regola pull through cache per un registro privato Amazon ECR. Nell'esempio seguente viene utilizzato il prefisso dello spazio dei nomi `ecr-public`. Sostituisci tale valore con il valore del prefisso per la convalida della regola di cache pull-through.

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

Nella risposta, il parametro `isValid` indica se la convalida è riuscita. `true` indica che Amazon ECR è riuscito a raggiungere il registro upstream e che l'autenticazione è riuscita. `false` indica che si è verificato un problema e che la convalida non è riuscita. Il parametro `failure` indica la causa.

Estrazione di un'immagine con una regola di cache pull-through

Gli esempi seguenti mostrano la sintassi del comando da utilizzare quando estrai un'immagine utilizzando una regola di cache pull-through. In caso di errore durante l'estrazione di un'immagine upstream utilizzando una regola di cache pull-through, consulta Risoluzione dei problemi relativi alla cache pull-through per gli errori più comuni e come risolverli.

> **Note**
>
> I seguenti esempi utilizzano i valori di namespace del repository Amazon ECR predefiniti utilizzati. AWS Management Console Assicurati di utilizzare l'URI del repository privato di Amazon ECR configurato.

Per Amazon ECR Public

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

Registro dei container 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

Per le immagini ufficiali di Docker Hub:

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

> **Note**
>
> Per le immagini ufficiali di Docker Hub, il prefisso `/library` deve essere incluso. Per tutti gli altri repository di Docker Hub, è necessario omettere il prefisso `/library`.

Per tutte le altre immagini di Docker Hub:

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

GitHub Registro dei contenitori

```
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
```

Eliminazione di una regola di cache pull-through

È possibile eliminare una regola di cache pull-through per interrompere il comportamento della cache. L'eliminazione di una regola di cache pull-through non ha alcun effetto sui repository o sulle immagini memorizzate nella cache, ma blocca solo il futuro comportamento di memorizzazione nella cache.

Per eliminare una regola di cache pull-through (AWS Management Console)

Per eliminare una regola di cache pull-through (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Dalla barra di navigazione seleziona la regione in cui si trova la regola di cache pull-through da eliminare.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Pull through cache (Cache pull-through).
4. Nella pagina Configurazione di cache pull-through, eleziona le regole di cache pull-through da eliminare, quindi utilizza il menu a discesa Azioni e seleziona Elimina regola.
5. Nel riquadro di navigazione, seleziona Registro privato, Autorizzazioni.
6. (Facoltativo) Nella pagina Registry permissions (Autorizzazioni di registro), esamina le istruzioni delle policy di autorizzazione del registro esistenti. È possibile eliminare tutte le istruzioni delle policy di autorizzazione del registro associate allo spazio dei nomi del repository per la regola della cache pull-through eliminata.

Per eliminare una regola di cache pull-through (AWS CLI)

Usa il comando seguente per eliminare una regola di cache pull-through utilizzando la AWS CLI.

- delete-pull-through-cache-regola ()AWS CLI

Nell'esempio seguente viene eliminata una regola di cache pull-through che utilizza il prefisso del repository `ecr-public`.

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

Archiviazione segreta delle credenziali del repository originale AWS Secrets Manager

Quando crei una regola di cache pull-through per un repository upstream che richiede l'autenticazione, devi memorizzare le credenziali in un segreto di Secrets Manager. L'utilizzo di un segreto di Secrets Manager potrebbe essere soggetto a un costo. Per ulteriori informazioni, consultare Prezzi di AWS Secrets Manager.

Le procedure seguenti illustrano come creare un segreto di Secrets Manager per ogni repository upstream supportato. Anziché creare il segreto utilizzando la console di Secrets Manager, per creare il segreto puoi utilizzare anche il flusso di lavoro di creazione delle regole di cache pull-through nella console di Amazon ECR. Per ulteriori informazioni, consulta Creazione di una regola di cache pull-through.

Docker Hub

Creazione di un segreto di Secrets Manager per le credenziali di Docker Hub (AWS Management Console)

1. Apri la console di Secrets Manager all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Scegli Archivia un nuovo segreto.
3. Nella pagina Scegli tipo di segreto, procedi come segue.
    a. Per Secret type (Tipo di segreto), scegli Other type of secret (Altro tipo di segreto).
    b. In Coppie chiave/valore, crea due righe per le tue credenziali di Docker Hub. Puoi archiviare fino a 65536 byte nel segreto.
        i. Per la prima coppia chiave/valore, specifica `username` come chiave e il tuo nome utente Docker Hub come valore.

ii. Per la seconda coppia chiave/valore, specifica `accessToken` come chiave e il tuo token di accesso di Docker Hub come valore. Per ulteriori informazioni sulla creazione di un token di accesso di Docker Hub, consulta Creazione e gestione di token di accesso nella documentazione di Docker.

c. Per Chiave di crittografia, mantieni il valore predefinito AWS KMS key aws/secretsmanager, quindi seleziona Avanti. L'utilizzo di questa chiave non prevede costi aggiuntivi. Per ulteriori informazioni, consulta Crittografia e decrittografia del segreto in Secrets Manager nella Guida per l'utente di AWS Secrets Manager .

> **Important**
>
> Devi utilizzare la chiave di crittografia predefinita `aws/secretsmanager` per crittografare il tuo segreto. Per tale scopo, Amazon ECR non supporta l'utilizzo di una chiave gestita dal cliente (CMK).

4. Nella pagina Configura il segreto, procedi come segue.

a. Inserisci un Secret name (Nome del segreto) e una Description (Descrizione) descrittivi. I nomi dei segreti devono contenere un numero di caratteri Unicode compreso tra 1 e 512 e il prefisso `ecr-pullthroughcache/`.

> **Important**
>
> Amazon ECR visualizza AWS Management Console solo i segreti di Secrets Manager con nomi che utilizzano il `ecr-pullthroughcache/` prefisso.

b. (Facoltativo) Nella sezione Tags (Tag) aggiungere tag al segreto. Per le strategie di applicazione di tag, consulta Applicazione di tag ai segreti di Secrets Manager nella Guida per l'utente di AWS Secrets Manager . Non archiviare informazioni sensibili nei tag perché non sono crittografate.

c. (Facoltativo) In Permessi delle risorse, per aggiungere una policy delle risorse al tuo segreto, scegli Modifica delle autorizzazioni. Per ulteriori informazioni, consulta Collega una policy di autorizzazioni a un segreto di Secrets Manager nella Guida per l'utente di AWS Secrets Manager .

d. (Facoltativo) In Replica segreto, per replicare il tuo segreto su un altro Regione AWS, scegli Replica segreto. Puoi replicare il tuo segreto immediatamente o tornare e

replicarlo in un secondo momento. Per ulteriori informazioni, consulta Replica di un segreto per altre regioni nella Guida per l'utente di AWS Secrets Manager .

e. Seleziona Successivo.

5. (Facoltativo) Nella pagina Configure rotation (Configura la rotazione), puoi attivare la rotazione automatica. Puoi anche disattivare la rotazione e poi riattivarla in un secondo momento. Per ulteriori informazioni, consulta Rotazione di segreti su Secrets Manager nella Guida per l'utente di AWS Secrets Manager . Seleziona Successivo.
6. Nella pagina Review (Revisione), rivedi i dettagli dei segreti e quindi scegli Store (Archivia).

   Secrets Manager ritorna all'elenco dei segreti. Se il segreto nuovo non viene visualizzato, scegli il pulsante aggiorna.

GitHub Container Registry

Per creare un segreto di Secrets Manager per le credenziali del GitHub Container Registry ()AWS Management Console

1. Apri la console di Secrets Manager all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Scegli Archivia un nuovo segreto.
3. Nella pagina Scegli tipo di segreto, procedi come segue.

   a. Per Secret type (Tipo di segreto), scegli Other type of secret (Altro tipo di segreto).

   b. Nelle coppie chiave/valore, create due righe per le vostre credenziali. GitHub Puoi archiviare fino a 65536 byte nel segreto.

      i. Per la prima coppia chiave/valore, specificate `username` come chiave e il vostro GitHub nome utente come valore.

      ii. Per la seconda coppia chiave/valore, specificate `accessToken` come chiave e il token di GitHub accesso come valore. Per ulteriori informazioni sulla creazione di un token di GitHub accesso, consulta Gestire i token di accesso personali nella documentazione. GitHub

   c. Per Chiave di crittografia, mantieni il valore predefinito AWS KMS key aws/secretsmanager, quindi seleziona Avanti. L'utilizzo di questa chiave non prevede costi aggiuntivi. Per ulteriori informazioni, consulta Crittografia e decrittografia del segreto in Secrets Manager nella Guida per l'utente di AWS Secrets Manager .

> **Important**
>
> Devi utilizzare la chiave di crittografia predefinita `aws/secretsmanager` per crittografare il tuo segreto. Per tale scopo, Amazon ECR non supporta l'utilizzo di una chiave gestita dal cliente (CMK).

4. Nella pagina Configure secret (Configura il segreto), effettua le seguenti operazioni:

   a. Inserisci un Secret name (Nome del segreto) e una Description (Descrizione) descrittivi. I nomi dei segreti devono contenere un numero di caratteri Unicode compreso tra 1 e 512 e il prefisso `ecr-pullthroughcache/`.

   > **Important**
   >
   > Amazon ECR visualizza AWS Management Console solo i segreti di Secrets Manager con nomi che utilizzano il `ecr-pullthroughcache/` prefisso.

   b. (Facoltativo) Nella sezione Tags (Tag) aggiungere tag al segreto. Per le strategie di applicazione di tag, consulta Applicazione di tag ai segreti di Secrets Manager nella Guida per l'utente di AWS Secrets Manager . Non archiviare informazioni sensibili nei tag perché non sono crittografate.

   c. (Facoltativo) In Permessi delle risorse, per aggiungere una policy delle risorse al tuo segreto, scegli Modifica delle autorizzazioni. Per ulteriori informazioni, consulta Collega una policy di autorizzazioni a un segreto di Secrets Manager nella Guida per l'utente di AWS Secrets Manager .

   d. (Facoltativo) In Replica segreto, per replicare il tuo segreto su un altro Regione AWS, scegli Replica segreto. Puoi replicare il tuo segreto immediatamente o tornare e replicarlo in un secondo momento. Per ulteriori informazioni, consulta Replica di un segreto per altre regioni nella Guida per l'utente di AWS Secrets Manager .

   e. Seleziona Successivo.

5. (Facoltativo) Nella pagina Configure rotation (Configura la rotazione), puoi attivare la rotazione automatica. Puoi anche disattivare la rotazione e poi riattivarla in un secondo momento. Per ulteriori informazioni, consulta Rotazione di segreti su Secrets Manager nella Guida per l'utente di AWS Secrets Manager . Seleziona Successivo.

6. Nella pagina Review (Revisione), rivedi i dettagli dei segreti e quindi scegli Store (Archivia).

Secrets Manager ritorna all'elenco dei segreti. Se il segreto nuovo non viene visualizzato, scegli il pulsante aggiorna.

Microsoft Azure Container Registry

Creazione di un segreto di Secrets Manager per le credenziali di Microsoft Azure Container Registry (AWS Management Console)

1. Apri la console di Secrets Manager all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Scegli Archivia un nuovo segreto.
3. Nella pagina Scegli tipo di segreto, procedi come segue.
   a. Per Secret type (Tipo di segreto), scegli Other type of secret (Altro tipo di segreto).
   b. Per Coppie chiave/valore crea due righe per le tue credenziali di Microsoft Azure. Puoi archiviare fino a 65536 byte nel segreto.
      i. Per la prima coppia chiave/valore, come valore specifica `username` come chiave e il tuo nome utente di Microsoft Azure Container Registry.
      ii. Per la seconda coppia chiave/valore, come valore specifica `accessToken` come chiave e il tuo token di accesso di Microsoft Azure Container Registry. Per ulteriori informazioni sulla creazione di un token di accesso per Microsoft Azure, consulta Creazione token - portale nella documentazione di Microsoft Azure.
   c. Per Chiave di crittografia, mantieni il valore predefinito AWS KMS key aws/secretsmanager, quindi seleziona Avanti. L'utilizzo di questa chiave non prevede costi aggiuntivi. Per ulteriori informazioni, consulta Crittografia e decrittografia del segreto in Secrets Manager nella Guida per l'utente di AWS Secrets Manager .

   > **Important**
   >
   > Devi utilizzare la chiave di crittografia predefinita `aws/secretsmanager` per crittografare il tuo segreto. Per tale scopo, Amazon ECR non supporta l'utilizzo di una chiave gestita dal cliente (CMK).

4. Nella pagina Configure secret (Configura il segreto), effettua le seguenti operazioni:

a. Inserisci un Secret name (Nome del segreto) e una Description (Descrizione) descrittivi. I nomi dei segreti devono contenere un numero di caratteri Unicode compreso tra 1 e 512 e il prefisso `ecr-pullthroughcache/`.

> **Important**
>
> Amazon ECR visualizza AWS Management Console solo i segreti di Secrets Manager con nomi che utilizzano il `ecr-pullthroughcache/` prefisso.

b. (Facoltativo) Nella sezione Tags (Tag) aggiungere tag al segreto. Per le strategie di applicazione di tag, consulta Applicazione di tag ai segreti di Secrets Manager nella Guida per l'utente di AWS Secrets Manager . Non archiviare informazioni sensibili nei tag perché non sono crittografate.

c. (Facoltativo) In Permessi delle risorse, per aggiungere una policy delle risorse al tuo segreto, scegli Modifica delle autorizzazioni. Per ulteriori informazioni, consulta Collega una policy di autorizzazioni a un segreto di Secrets Manager nella Guida per l'utente di AWS Secrets Manager .

d. (Facoltativo) In Replica segreto, per replicare il tuo segreto su un altro Regione AWS, scegli Replica segreto. Puoi replicare il tuo segreto immediatamente o tornare e replicarlo in un secondo momento. Per ulteriori informazioni, consulta Replica di un segreto per altre regioni nella Guida per l'utente di AWS Secrets Manager .

e. Seleziona Successivo.

5. (Facoltativo) Nella pagina Configure rotation (Configura la rotazione), puoi attivare la rotazione automatica. Puoi anche disattivare la rotazione e poi riattivarla in un secondo momento. Per ulteriori informazioni, consulta Rotazione di segreti su Secrets Manager nella Guida per l'utente di AWS Secrets Manager . Seleziona Successivo.

6. Nella pagina Review (Revisione), rivedi i dettagli dei segreti e quindi scegli Store (Archivia).

   Secrets Manager ritorna all'elenco dei segreti. Se il segreto nuovo non viene visualizzato, scegli il pulsante aggiorna.

Risoluzione dei problemi relativi alla cache pull-through

Di seguito sono riportati gli errori più comuni che potresti ricevere durante l'estrazione di un'immagine upstream utilizzando una regola di cache pull-through.

Il repository non esiste

Un errore che indica che il repository non esiste è spesso causato dal repository non esistente nel registro privato Amazon ECR o dall'autorizzazione `ecr:CreateRepository` non concessa al principale IAM che estrae l'immagine a monte. Per risolvere questo errore, è necessario verificare che l'URI del repository nel comando pull sia corretto, che le autorizzazioni IAM richieste siano concesse al principale IAM che estrae l'immagine upstream o che il repository per l'immagine upstream da inviare venga creato nel registro privato di Amazon ECR prima di estrarre l'immagine upstream. Per ulteriori informazioni sulle autorizzazioni IAM richieste, consulta Autorizzazioni IAM richieste

Di seguito è illustrato un esempio di questo errore.

```
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'immagine richiesta non è stata trovata

Un errore che indica che l'immagine non può essere trovata è spesso causato dall'immagine non esistente nel registro upstream o dall'autorizzazione `ecr:BatchImportUpstreamImage` non concessa al principale IAM che estrae l'immagine upstream ma il repository è già stato creato nel registro privato di Amazon ECR. Per risolvere questo errore, è necessario verificare che l'immagine upstream e il nome del tag immagine siano corretti e che esistano e che le autorizzazioni IAM richieste siano concesse al principale IAM che estrea l'immagine upstream. Per ulteriori informazioni sulle autorizzazioni IAM richieste, consulta Autorizzazioni IAM richieste.

Di seguito è illustrato un esempio di questo errore.

```
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 Proibito quando si estrae da un repository Docker Hub

Quando estrai da un repository Docker Hub etichettato come Docker Official Image, devi includere `/library/` nell'URI utilizzato. Ad esempio, *`aws_account_id`*`.dkr.ecr.`*`region`*`.amazonaws.com/docker-hub/`

`library/`*`image_name:tag`*. Se ometti `/library/` per le immagini Docker Hub Offical, verrà restituito un errore `403 Forbidden` quando tenti di estrarre l'immagine utilizzando una regola di cache pull-through. Per ulteriori informazioni, consulta Estrazione di un'immagine con una regola di cache pull-through.

Di seguito è illustrato un esempio di questo errore.

```
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
```

Eliminazione di un'immagine

Quando hai finito di utilizzare un'immagine, puoi eliminarla dal tuo repository. Quando hai finito di utilizzare un repository, puoi eliminare l'intero repository e tutte le immagini al suo interno. Per ulteriori informazioni, consulta Eliminazione di un repository privato.

In alternativa all'eliminazione manuale delle immagini, puoi creare policy relative al ciclo di vita del repository che forniscono un maggiore controllo sulla gestione del ciclo di vita delle immagini nei tuoi repository. Le policy relative al ciclo di vita automatizzano questo processo per te. Per ulteriori informazioni, consulta Policy del ciclo di vita.

Per eliminare un'immagine (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Sulla barra di navigazione seleziona la regione in cui si trova l'immagine da eliminare.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository) seleziona il repository che contiene l'immagine da eliminare.
5. Nella pagina Repositories: ***`repository_name`*** (Repository: nome_repository) seleziona la casella a sinistra dell'immagine da eliminare e scegli Delete (Elimina).
6. Nella finestra di dialogo Delete image(s) (Elimina immagini) verifica che le immagini selezionate debbano essere realmente eliminate, quindi scegli Delete (Elimina).

Per eliminare un'immagine (AWS CLI)

1. Elenca le immagini nel tuo repository. Le immagini con tag assegnati avranno sia un digest di immagine che un elenco di tag associati. Le immagini senza tag assegnati avranno solo un digest delle immagini.

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

2. (Opzionale) Elimina i tag indesiderati per l'immagine specificando il tag associato all'immagine che desideri eliminare. Quando elimini l'ultimo tag da un'immagine, l'immagine viene anche eliminata.

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

3. Eliminare un'immagine con o senza tag assegnati specificando il digest dell'immagine. Quando elimini un'immagine facendo riferimento al suo digest, l'immagine e tutti i relativi tag vengono eliminati.

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

   Per eliminare più immagini, puoi specificare più tag immagine o digest immagine nella richiesta.

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

Ripetizione del nuovo tagging di un'immagine

Con le immagini Docker Image Manifest V2 Schema 2, puoi usare l'opzione `--image-tag` del comando put-image per inserire nuovamente un tag in un'immagine esistente. Puoi inserire nuovamente il tag senza estrarre o inviare l'immagine con Docker. Per le immagini più grandi, questo

processo consente di risparmiare una notevole quantità di larghezza di banda di rete e il tempo richiesto per reinserire un tag a un'immagine.

Per inserire nuovamente un tag in un'immagine (AWS CLI)

Per rietichettare un'immagine con AWS CLI

1. Utilizza il comando batch-get-image per ottenere il manifesto dell'immagine al fine di inserire nuovamente il tag nell'immagine e scriverla su un file. In questo esempio, il manifesto per un'immagine con il tag *latest* nel repository *amazonlinux* è scritto in una variabile di ambiente denominata *MANIFEST*.

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

2. Utilizza l'opzione `--image-tag` del comando put-image per inserire il manifesto dell'immagine in Amazon ECR con un nuovo tag. In questo esempio, il tag dell'immagine è *2017.03*.

> **Note**
>
> Se l'`--image-tag`opzione non è disponibile nella tua versione di AWS CLI, esegui l'upgrade alla versione più recente. Per ulteriori informazioni, consulta Installazione dell' AWS Command Line Interface nella Guida per l'utente di AWS Command Line Interface .

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

3. Verifica che il nuovo tag dell'immagine sia collegato all'immagine. Nell'output seguente, l'immagine presenta i tag `latest` e `2017.03`.

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

L'output è il seguente:

```
{
    "imageDetails": [
        {
            "imageSizeInBytes": 98755613,
```

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

Per inserire nuovamente un tag in un'immagine (AWS Tools for Windows PowerShell)

Per rietichettare un'immagine con AWS Tools for Windows PowerShell

1. Utilizzare il cmdlet Get-ECRImageBatch per ottenere la descrizione dell'immagine a cui assegnare nuovamente il tag e scriverla su una variabile di ambiente. In questo esempio, un'immagine con il tag, *latest*, nel repository, *amazonlinux*, è scritta nella variabile di ambiente, *$Image*.

   > **Note**
   >
   > Se il tuo sistema non dispone del cmdlet Get-ECRImageBatch, consulta Configurazione di AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Tools for Windows PowerShell .

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

2. Scrivere il manifest dell'immagine nella variabile di ambiente *$Manifest*.

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

3. Utilizza l'opzione `-ImageTag` del cmdlet Write-ECRImage per inserire il manifesto dell'immagine in Amazon ECR con un nuovo tag. In questo esempio, il tag dell'immagine è *2017.09*.

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

4. Verifica che il nuovo tag dell'immagine sia collegato all'immagine. Nell'output seguente, l'immagine presenta i tag `latest` e `2017.09`.

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

   L'output è il seguente:

   ```
   ImageDigest                                                             ImageTag
   -----------                                                             --------
   sha256:359b948ea8866817e94765822787cd482279eed0c17bc674a7707f4256d5d497 latest
   sha256:359b948ea8866817e94765822787cd482279eed0c17bc674a7707f4256d5d497 2017.09
   ```

Replica di immagini private

Puoi configurare il tuo registro privato Amazon ECR in modo da supportare la replica dei tuoi repository. Amazon ECR supporta sia la replica tra regioni che tra account. Affinché si verifichi la replica tra account, l'account di destinazione deve configurare una policy di autorizzazione del registro per consentire la replica dal registro. Per ulteriori informazioni, consulta Autorizzazioni di registro privato.

Argomenti

- Considerazioni per la replica di immagini private
- Configurazione della replica delle immagini private
- Visualizzazione dello stato della replica

Considerazioni per la replica di immagini private

Quando usi la replica di immagini private, tieni presenti le considerazioni seguenti:

- Vengono replicati solo i contenuti inviati in un repository dopo la configurazione della replica. Qualsiasi contenuto preesistente in un repository non sarà replicato. Una volta configurata la replica per un repository, Amazon ECR mantiene sincronizzate la destinazione e l'origine.

- Il nome del repository rimarrà lo stesso in tutte le regioni e gli account una volta che la replica sarà stata effettuata. Amazon ECR non supporta la modifica del nome del repository durante la replica.
- La prima volta che configuri il registro privato per la replica, Amazon ECR crea un ruolo IAM collegato ai servizi per tuo conto. Il ruolo IAM collegato ai servizi concede al servizio di replica Amazon ECR l'autorizzazione necessaria per creare repository e replicare immagini nel registro. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon ECR.
- Affinché si verifichi la replica tra account, la destinazione del registro privato deve concedere l'autorizzazione per consentire al registro di origine di replicare le immagini. Per questa operazione viene effettuato l'impostazione di una policy delle autorizzazioni del registro privato. Per ulteriori informazioni, consulta Autorizzazioni di registro privato.
- Se le policy di autorizzazione per un registro privato vengono modificate per rimuovere un'autorizzazione, le repliche in corso precedentemente concesse potrebbero essere completate.
- Affinché si verifichi la replica tra regioni, sia l'account di origine che quello di destinazione devono essere abilitati alla regione prima di eseguire qualsiasi azione di replica all'interno o verso quella regione. Per ulteriori informazioni, consulta Gestione delle regioni AWS nella Riferimenti generali di Amazon Web Services.
- La replica tra regioni non è supportata tra partizioni AWS. Ad esempio, un repository in `us-west-2` non può essere replicato in `cn-north-1`. Per ulteriori informazioni su partizioni AWS, consulta la sezione Formato ARN in Riferimenti generali AWS.
- La configurazione di replica per un registro privato può contenere fino a 25 destinazioni univoche per tutte le regole, con un massimo di 10 regole totali. Ogni regola può contenere fino a 100 filtri. Ciò consente di specificare regole separate per i repository contenenti immagini utilizzate per la produzione e il test, ad esempio.
- La configurazione di replica supporta il filtro dei repository di un registro privato che vengono replicati specificando un prefisso del repository. Per vedere un esempio, consulta Esempio: configurazione della replica tra regioni utilizzando un filtro repository.
- Un'operazione di replica si verifica una sola volta per invio di immagine. Ad esempio, se è stata configurata la replica tra regioni da `us-west-2` a `us-east-1` e da `us-east-1` a `us-east-2`, un'immagine inviata a `us-west-2` si replica solo in `us-east-1`, non si replica di nuovo in `us-east-2`. Questo comportamento si applica sia alla replica tra regioni e che tra account.
- La maggior parte delle immagini viene replicata in meno di 30 minuti, ma in rari casi la replica potrebbe richiedere più tempo.
- La replica del registro non esegue alcuna operazione di eliminazione. Le immagini e i repository replicati possono essere eliminati manualmente quando non sono più utilizzati.

- le policy del repository, tra cui le policy IAM e le policy del ciclo di vita, non vengono replicate e non hanno alcun effetto se non sul repository per cui sono definite.
- Le impostazioni del repository non vengono replicate. Le impostazioni di immutabilità dei tag, di scansione delle immagini e di crittografia del servizio di gestione delle chiavi sono disabilitate per impostazione predefinita in tutti i repository creati a causa di un'operazione di replica. L'impostazione di immutabilità dei tag e di scansione delle immagini può essere modificata dopo la creazione del repository. Tuttavia, l'impostazione si applica solo alle immagini inviate dopo che l'impostazione è stata modificata.
- Se l'immutabilità dei tag è abilitata in un repository e viene replicata un'immagine che utilizza lo stesso tag di un'immagine esistente, l'immagine viene replicata ma non conterrà il tag duplicato. In questo modo all'immagine potrebbero non essere assegnati tag.

Configurazione della replica delle immagini private

Le impostazioni di replica del registro privato sono configurate separatamente per ogni Regione. Utilizza la procedura seguente per configurare la replica per il registro privato utilizzando la AWS Management Console o la AWS CLI. Per esempi di uso comune della replica, consulta Esempi di replica di immagini private.

Per configurare le impostazioni di replica del registro (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegli la regione in cui configurare le impostazioni di replica del registro.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato).
4. Alla pagina Private registry (Registro privato) nella sezione Replication (Replica), scegliereEdit (Modifica).
5. Alla pagina Replication (Replica), scegliere Add replication rule (Aggiunta di regola di replica).
6. Alla pagina Destination types (Tipi di destinazione), scegliere se abilitare la replica tra regioni, la replica tra account o entrambe, quindi scegliere Next (Successivo).
7. Se la replica tra regioni è abilitata, per Configure destination regions (Configurare regioni di destinazione) scegliere una o più Destination regions (Regioni di destinazione) e quindi scegliere Next (Successivo).
8. Se la replica tra account è abilitata, per Cross-account replication (Replica tra account) scegliere l'impostazione di replica tra account per il registro. Per Destination account (Account

di destinazione), immettere l'ID account per l'account di destinazione e una o più Destination regions (Regioni di destinazione) a cui replicare. Scegliere Destination account + (Account di destinazione +) per configurare account aggiuntivi come destinazioni di replica.

> **Important**
>
> Affinché si verifichi la replica tra account, l'account di destinazione deve configurare una policy delle autorizzazioni del registro per consentire la replica dal registro. Per ulteriori informazioni, consulta Autorizzazioni di registro privato.

9. (Facoltativo) Alla pagina Add filters (Aggiungi filtri), specificare uno o più filtri per la regola di replica, quindi scegliere Add (Aggiungi). Ripetere questo passaggio per ogni filtro da associare all'operazione di replica. Un filtro deve essere specificato come prefisso del nome del repository. Se non viene aggiunto alcun filtro, il contenuto di tutti i repository viene replicato. Scegliere Next (Successivo) una volta aggiunti tutti i filtri.
10. Alla pagina Review and submit (Verifica e invia), verificare la configurazione della regola di replica e quindi scegliere Submit rule (Invia regola).

Per configurare le impostazioni di replica del registro (AWS CLI)

1. Creare un file JSON contenente le regole di replica da definire per il registro. Una configurazione di replica può contenere fino a 10 regole, con un massimo di 25 destinazioni specifiche in tutte le regole e 100 filtri per ciascuna regola. Per configurare la replica tra regioni all'interno del proprio account, è necessario specificare il proprio ID account. Per ulteriori esempi, consulta Esempi di replica di immagini private.

```
{
 "rules": [{
  "destinations": [{
   "region": "destination_region",
   "registryId": "destination_accountId"
  }],
  "repositoryFilters": [{
   "filter": "repository_prefix_name",
   "filterType": "PREFIX_MATCH"
  }]
 }]
}
```

2. Crea una configurazione di replica per il tuo registro.

```
aws ecr put-replication-configuration \
     --replication-configuration file://replication-settings.json \
     --region us-west-2
```

3. Confermare le impostazioni del registro.

```
aws ecr describe-registry \
     --region us-west-2
```

Esempi di replica di immagini private

Gli esempi seguenti riportano casi d'uso comuni per la replica di immagini private.

Esempio: configurazione della replica tra regioni in un'unica regione di destinazione

Di seguito viene illustrato un esempio per la configurazione della replica tra regioni all'interno di un unico registro. In questo esempio si presuppone che l'ID account sia `111122223333` e che si sta specificando questa configurazione di replica in una regione diversa da `us-west-2`.

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "us-west-2",
                    "registryId": "111122223333"
                }
            ]
        }
    ]
}
```

Esempio: configurazione della replica tra regioni utilizzando un filtro repository

Di seguito viene illustrato un esempio per la configurazione della replica tra regioni per repository che corrispondono a un valore del nome di prefisso. In questo esempio si presuppone che l'ID account sia `111122223333` e che si sta specificando questa configurazione di replica in una regione diversa da `us-west-1` e che ci siano repository con prefisso `prod`.

```
{
 "rules": [{
  "destinations": [{
   "region": "us-west-1",
   "registryId": "111122223333"
  }],
  "repositoryFilters": [{
   "filter": "prod",
   "filterType": "PREFIX_MATCH"
  }]
 }]
}
```

Esempio: configurazione della replica tra regioni più regioni di destinazione

Di seguito viene illustrato un esempio per la configurazione della replica tra regioni all'interno di un unico registro. In questo esempio si presuppone che l'ID account sia `111122223333` e che si sta specificando questa configurazione di replica in una regione diversa da `us-west-2` o da `us-west-1`.

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "us-west-1",
                    "registryId": "111122223333"
                },
                {
                    "region": "us-west-2",
                    "registryId": "111122223333"
                }
            ]
        }
    ]
}
```

Esempio: configurazione della replica tra account

Di seguito viene illustrato un esempio per la configurazione della replica tra account per il registro. In questo esempio viene configurata la replica per l'account `444455556666` e per la regione `us-west-2`.

> **Important**
>
> Affinché si verifichi la replica tra account, l'account di destinazione deve configurare una policy delle autorizzazioni del registro per consentire la replica dal registro. Per ulteriori informazioni, consulta Autorizzazioni di registro privato.

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "us-west-2",
                    "registryId": "444455556666"
                }
            ]
        }
    ]
}
```

Esempio: specifica di più regole in una configurazione

Di seguito viene illustrato un esempio per la configurazione di più regole di replica per il registro. In questo esempio viene configurata la replica per l'account *111122223333* con una regola che replica i repository con un prefisso `prod` alla regione `us-west-2` e i repository con un prefisso `test` alla regione `us-east-2`. Una configurazione di replica può contenere fino a 10 regole, ognuna delle quali specifica fino a 25 destinazioni.

```
{
 "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"
   }]
  }
 ]
}
```

Visualizzazione dello stato della replica

Dopo aver configurato il registro privato per la replica, sarà possibile visualizzare lo stato della replica per il contenuto dei repository. Lo stato di replica di una singola immagine container può essere visualizzato eseguendo query utilizzando il tag immagine o il digest dell'immagine.

Verifica dello stato della replica (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegliere la regione in cui si trova l'origine del registro replicato.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Alla pagina Repositories (Repository), scegliere il repository di cui verificare lo stato della replica.
5. Alla pagina dei dettagli dei repository, scegliere Image tag (Tag immagine) per verificare lo stato della replica.
6. Per Image replication status (Stato della replica delle immagini), verificare lo stato della replica. È possibile visualizzare lo stato della replica in base al tag immagine o al digest dell'immagine.

Verifica dello stato della replica (AWS CLI)

- Lo stato di replica del contenuto di un repository può essere visualizzato in base al tag immagine utilizzando il seguente comando.

```
aws ecr describe-image-replication-status \
     --repository-name repository_name \
     --image-id imageTag=image_tag \
     --region us-west-2
```

- Lo stato di replica del contenuto di un repository può essere visualizzato in base al digest dell'immagine utilizzando il seguente comando.

```
aws ecr describe-image-replication-status \
     --repository-name repository_name \
     --image-id imageDigest=image_digest \
     --region us-west-2
```

Policy del ciclo di vita

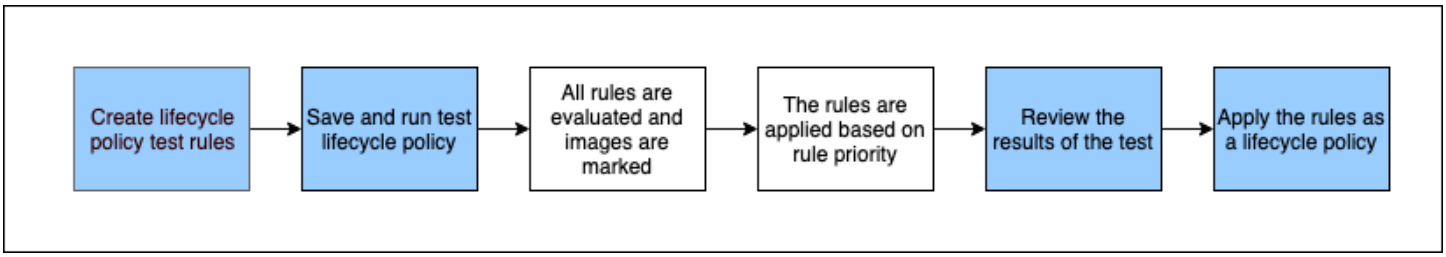
Le policy del ciclo di vita di Amazon ECR offrono un maggiore controllo sulla gestione del ciclo di vita delle immagini in un repository privato. Una policy del ciclo di vita contiene una o più regole, laddove ogni regola definisce un'operazione per Amazon ECR. Ciò consente di automatizzare la pulizia delle immagini dei container, facendo scadere le immagini in base all'età o al conteggio. Le immagini dovrebbero scadere entro 24 ore dal raggiungimento dei criteri di scadenza previsti dalla policy del ciclo di vita. Quando Amazon ECR esegue un'azione basata su una policy del ciclo di vita, questa viene acquisita come evento in AWS CloudTrail. Per ulteriori informazioni, consulta Registrazione delle azioni Amazon ECR con AWS CloudTrail.

Funzionamento delle policy del ciclo di vita

Una policy del ciclo di vita è costituita da una o più regole che determinano quali immagini in un repository devono scadere. Quando si considera l'utilizzo delle policy del ciclo di vita, è importante utilizzare la relativa anteprima per confermare quali immagini la policy del ciclo di vita fa scadere prima di applicarla a un repository. Una volta applicata una policy del ciclo di vita a un repository, le immagini interessate dovrebbero scadere entro 24 ore dal raggiungimento dei criteri di scadenza. Quando Amazon ECR esegue un'azione basata su una policy del ciclo di vita, questa viene acquisita come evento in AWS CloudTrail. Per ulteriori informazioni, consulta Registrazione delle azioni Amazon ECR con AWS CloudTrail.

> **Note**
>
> Se si utilizza la replica di Amazon ECR per creare copie di un repository in diverse Regioni o account, tieni presente che una policy del ciclo di vita può agire solo sui repository della Regione in cui è stata creata. Pertanto, se è stata attivata la replica, potrebbe essere necessario prendere in considerazione la creazione di una policy del ciclo di vita in ogni Regione e account su cui si stanno replicando i repository.

Il seguente diagramma mostra un flusso di lavoro di policy del il ciclo di vita.



1. Creare una o più regole di test.
2. Salvare le regole di test ed eseguire l'anteprima.
3. Il valutatore delle policy del ciclo di vita passa in rassegna tutte le regole e contrassegna le immagini interessate da ogni regola.
4. Il valutatore delle policy del ciclo di vita applica quindi le regole, in base alla priorità della regola, e visualizza quali immagini nel repository sono impostate per scadere.
5. Esaminare i risultati del test, assicurandosi che le immagini contrassegnate per scadere siano quelle previste.
6. Applicare le regole di test come policy del ciclo di vita per il repository.
7. Una volta creata la policy del ciclo di vita, le immagini dovrebbero scadere entro 24 ore dal raggiungimento dei criteri di scadenza.

Regole per la valutazione delle policy del ciclo di vita

Il valutatore della policy del ciclo di vita è responsabile dell'analisi del JSON di testo normale della policy del ciclo di vita, della valutazione di tutte le regole e quindi dell'applicazione di tali regole in base alla priorità della regola alle immagini nel repository. Di seguito viene illustrata la logica del valutatore delle policy del ciclo di vita in modo più dettagliato. Per alcuni esempi, consulta Esempi di policy del ciclo di vita.

- Tutte le regole vengono valutate contemporaneamente, a prescindere dalla priorità della regola. Dopo che tutte le regole sono state valutate, vengono applicate in base alla priorità della regola.
- Un'immagine è scaduta per esattamente una o zero regole.
- Un'immagine che corrisponde ai requisiti di tagging di una regola non può scadere per una regola con una priorità inferiore.
- Le regole non possono mai contrassegnare immagini contrassegnate da regole di priorità superiore, ma possono comunque identificarle come se non fossero scadute.

- Il set di regole deve contenere un set univoco di prefissi di tag.
- È consentita una sola regola per selezionare le immagini non taggate.
- Se a un'immagine fa riferimento un elenco di manifesti, non può scadere senza che l'elenco dei manifesti venga prima eliminato.
- La scadenza è sempre ordinata in base a `pushed_at_time` e scadono sempre prima le immagini meno recenti rispetto a quelle più recenti.
- Una regola della policy del ciclo di vita può specificare `tagPatternList` o `tagPrefixList`, ma non entrambi. Tuttavia, una policy del ciclo di vita può contenere più regole in cui regole diverse utilizzano sia elenchi di modelli che di prefissi.
- I parametri `tagPatternList` o `tagPrefixList` possono essere utilizzati solo se `tagStatus` è `tagged`.
- Quando si utilizza `tagPatternList`, un'immagine viene abbinata correttamente se corrisponde al filtro jolly. Ad esempio, se viene applicato un filtro `prod*`, questo corrisponderebbe ai repository il cui nome inizia con `prod`, `prod`, `prod1` o `production-team1`. Allo stesso modo, se viene applicato un filtro `*prod*`, corrisponderebbe ai repository il cui nome contiene, `prod` ad esempio `repo-production` o `prod-team`.

  > **Important**
  >
  > Esiste un limite massimo di quattro caratteri jolly (`*`) per stringa. Ad esempio, `["*test*1*2*3", "test*1*2*3*"]` è valido ma `["test*1*2*3*4*5*6"]` non è valido.

- Quando si utilizza `tagPrefixList`, un'immagine viene abbinata correttamente se tutti i tag nel valore `tagPrefixList` corrispondono a qualsiasi tag dell'immagine.
- Il parametro `countUnit` è utilizzato solo se `countType` è `sinceImagePushed`.
- Con `countType = imageCountMoreThan`, le immagini vengono ordinate dalla più recente alla meno recente sulla base del valore di `pushed_at_time`. Quindi tutte le immagini che superano il numero specificato sono scadute.
- Con `countType = sinceImagePushed`, tutte le immagini per cui il valore `pushed_at_time` è meno recente rispetto al numero di giorni specificato in `countNumber` sono scadute.

Modello di policy del ciclo di vita

Il contenuto della tua policy del ciclo di vita viene valutato prima di essere associato a un repository. Di seguito viene mostrato un modello di sintassi JSON per la policy del ciclo di vita. Per esempi di policy del ciclo di vita, consulta Esempi di policy del ciclo di vita.

```
{
    "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"
            }
        }
    ]
}
```

Parametri di una policy del ciclo di vita

Le policy del ciclo di vita si suddividono nelle seguenti parti:

Argomenti

- Priorità regola
- Descrizione
- Stato tag
- Elenco di modelli di tag
- Elenco prefissi tag
- Tipo di conteggio
- Unità conteggio

- Count number (Numero conteggio)
- Azione

Priorità regola

`rulePriority`

Tipo: Integer

Obbligatorio: sì

Imposta l'ordine in base al quale le regole vengono applicate, dal valore più basso a quello più alto. Una regola della policy del ciclo di vita con una priorità di 1 sarà applicata per prima, una regola con priorità di 2 sarà applicata successivamente, e così via. Quando aggiungi delle regole a una policy del ciclo di vita, queste devono avere un valore univoco per `rulePriority`. I valori delle diverse regole non devono necessariamente essere in sequenza in una policy. Una regola con valore `tagStatus` di `any` deve avere il valore più elevato per `rulePriority` ed essere valutata per ultima.

Descrizione

`description`

Tipo: string

Obbligatorio: no

(Opzionale) Descrive lo scopo di una regola nella policy del ciclo di vita.

Stato tag

`tagStatus`

Tipo: string

Obbligatorio: sì

Determina se la regola della policy del ciclo di vita che vuoi aggiungere specifica un tag per un'immagine. Le opzioni accettabili sono `tagged`, `untagged` o `any`. Se specifichi `any`, per tutte

le immagini la regola viene valutata rispetto ad esse. Se specifichi `tagged`, devi anche specificare un valore `tagPrefixList`. Se specifichi `untagged`, allora devi omettere `tagPrefixList`.

Elenco di modelli di tag

`tagPatternList`

Tipo: list[string]

Obbligatorio: sì, se `tagStatus` è impostato su Taggato e `tagPrefixList` non è specificato

Quando si crea una policy del ciclo di vita per le immagini con tag, è consigliabile utilizzare `tagPatternList` per specificare che i tag devono scadere. È necessario specificare un elenco separato da virgole di modelli per i tag di immagini che possono contenere caratteri jolly (*) sul quale lavorare con la policy del ciclo di vita. Ad esempio, se le immagini sono taggate come `prod`, `prod1`, `prod2` e così via, utilizzerai l'elenco di modelli di tag `prod*` per specificarle tutte. Se specifichi più tag, vengono selezionate solo le immagini che hanno tutti i tag specificati.

> **Important**
>
> Esiste un limite massimo di quattro caratteri jolly (*) per stringa. Ad esempio, `["*test*1*2*3", "test*1*2*3*"]` è valido ma `["test*1*2*3*4*5*6"]` non è valido.

Elenco prefissi tag

`tagPrefixList`

Tipo: list[string]

Obbligatorio: sì, se `tagStatus` è impostato su taggato e `tagPatternList` non è specificato

Utilizzato solo se è stato specificato `"tagStatus": "tagged"` e non si sta specificando un `tagPatternList`. Devi specificare un elenco separato da virgole di prefissi per i tag delle immagini sul quale operare con la tua policy del ciclo di vita. Ad esempio, se le tue immagini sono taggate come `prod`, `prod1`, `prod2` e così via, utilizzerai il prefisso di tag `prod` per specificarle tutte. Se specifichi più tag, vengono selezionate solo le immagini che hanno tutti i tag specificati.

Tipo di conteggio

`countType`

Tipo: string

Obbligatorio: sì

Specifica un tipo di conteggio da applicare alle immagini.

Se `countType` è impostato su `imageCountMoreThan`, devi specificare inoltre `countNumber` per creare una regola che impone un limite al numero di immagini presenti nel tuo repository. Se `countType` è impostato su `sinceImagePushed`, devi anche specificare `countUnit` e `countNumber` per specificare un limite di tempo sulle immagini presenti nel tuo repository.

Unità conteggio

`countUnit`

Tipo: string

Required: yes (Obbligatorio: sì) solo se il campo `countType` è impostato su `sinceImagePushed`

Specifica un unità di conteggio di `days` per definirla come unità di tempo, oltre a `countNumber`, che corrisponde al numero di giorni.

Questa specifica deve essere utilizzata solo quando `countType` è `sinceImagePushed`; se si specifica un'unità di conteggio quando `countType` è qualsiasi altro valore, si verificherà un errore.

Count number (Numero conteggio)

`countNumber`

Tipo: Integer

Obbligatorio: sì

Specifica un numero conteggio. I valori accettabili sono numeri interi positivi (`0` non è un valore accettato).

Se il `countType` utilizzato è `imageCountMoreThan`, allora il valore è il numero massimo di immagini che desideri conservare nel tuo repository. Se il `countType` utilizzato è `sinceImagePushed`, allora il valore è il limite di età massimo per le tue immagini.

Azione

`type`

Tipo: stringa

Obbligatorio: sì

Specifica un tipo di azione. Il valore supportato è `expire`.

Creazione di un'anteprima di una policy del ciclo di vita

L'anteprima di una policy del ciclo di vita ti consente di vedere l'impatto di questo tipo di policy su un repository di immagini prima di applicarla. Una best practice consiste nell'eseguire un'anteprima prima di applicare una policy del ciclo di vita a un repository. La procedura seguente illustra come creare un'anteprima di una policy del ciclo di vita.

Per creare un'anteprima di una policy del ciclo di vita (AWS Management Console)

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Sulla barra di navigazione seleziona la regione che contiene il repository sul quale eseguire un'anteprima della policy del ciclo di vita.
3. Nel riquadro di navigazione, in Registro privato, seleziona Repository.
4. Nella pagina Repository privati, seleziona un repository e utilizza il menu a discesa Operazioni per scegliere Policy del ciclo di vita.
5. Nella pagina delle regole della policy del ciclo di vita del repository, scegli Modifica regole di test, Crea regola.
6. Immetti i seguenti dettagli per ogni regola della policy del ciclo di vita di prova.
    a. In Rule priority (Priorità regola), digita un numero per la priorità della regola. La priorità delle regole determina l'ordine in cui vengono applicate le regole delle policy relative al ciclo di vita.

b. In Rule description (Descrizione regola), digita una descrizione della regola della policy del ciclo di vita.

c. Per Stato immagine, scegli Taggata (corrispondenza con caratteri jolly), Taggata (corrispondenza dei prefissi), Non taggata o Qualsiasi.

d. Se hai scelto Taggata (corrispondenza con caratteri jolly) per Stato immagine, allora per Specifica i tag per la corrispondenza con caratteri jolly, puoi specificare un elenco di tag di immagine con un carattere jolly (*) su cui intervenire con la tua policy del ciclo di vita. Ad esempio, se le immagini sono taggate come `prod`, `prod1`, `prod2` e così via, sarà necessario utilizzare `prod*` per specificarle tutte. Se specifichi più tag, vengono selezionate solo le immagini che hanno tutti i tag specificati.

> **Important**
>
> Esiste un limite massimo di quattro caratteri jolly (*) per stringa. Ad esempio, `["*test*1*2*3", "test*1*2*3*"]` è valido ma `["test*1*2*3*4*5*6"]` non è valido.

e. Se hai scelto Taggata (corrispondenza dei prefissi) per Stato immagine, allora per Specifica i tag per la corrispondenza dei prefissi, puoi specificare un elenco di tag di immagine su cui intervenire con la tua policy del ciclo di vita.

f. Per Criteri di corrispondenza, scegli Dall'invio dell'immagine o Conteggio immagini superiore a, quindi specifica un valore.

g. Selezionare Salva.

7. Per creare ulteriori regole per la policy del ciclo di vita di prova, ripeti le operazioni da 5 a 7.
8. Per eseguire l'anteprima della policy del ciclo di vita, seleziona Save and run test (Salva ed esegui test).
9. In Image matches for test lifecycle rules (Corrispondenze dell'immagine per le regole del ciclo di vita), verifica l'impatto dell'anteprima della tua policy del ciclo di vita.
10. Se i risultati ti soddisfano, seleziona Apply as lifecycle policy (Applica come policy del ciclo di vita) per creare una policy del ciclo di vita con le regole specificate. In genere, dopo aver applicato una policy del ciclo di vita, le immagini interessate scadono entro 24 ore.
11. Se non sei soddisfatto dei risultati dell'anteprima, puoi eliminare una o più regole del ciclo di vita del test e creare una o più regole per sostituirle e ripetere il test.

Creazione di una policy del ciclo di vita

Una policy del ciclo di vita ti consente di creare un gruppo di regole di scadenza per le immagini inutilizzate nei repository. La procedura seguente illustra come creare una policy del ciclo di vita. In genere, dopo aver creato una policy del ciclo di vita, le immagini interessate scadono entro 24 ore.

> **Important**
>
> Una best practice consiste nel creare un'anteprima delle policy del ciclo di vita per garantire che le immagini interessate dalle regole delle policy siano realmente quelle che si intende. Per ulteriori informazioni, consulta Creazione di un'anteprima di una policy del ciclo di vita.

Per creare una policy del ciclo di vita (AWS Management Console)

Per creare una policy del ciclo di vita tramite la console

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Sulla barra di navigazione seleziona la regione che contiene il repository per il quale creare una policy del ciclo di vita.
3. Nel riquadro di navigazione, in Registro privato, seleziona Repository.
4. Nella pagina Repository privati, seleziona un repository e utilizza il menu a discesa Operazioni per scegliere Policy del ciclo di vita.
5. Nella pagina della policy del ciclo di vita del repository, scegli Crea regola.
6. Immetti i seguenti dettagli per la regola della policy del ciclo di vita.

    a. In Rule priority (Priorità regola), digita un numero per la priorità della regola. La priorità delle regole determina l'ordine in cui vengono applicate le regole delle policy relative al ciclo di vita.

    b. In Rule description (Descrizione regola), digita una descrizione della regola della policy del ciclo di vita.

    c. Per Stato immagine, scegli Taggata (corrispondenza con caratteri jolly), Taggata (corrispondenza dei prefissi), Non taggata o Qualsiasi.

    d. Se hai scelto Taggata (corrispondenza con caratteri jolly) per Stato immagine, allora per Specifica i tag per la corrispondenza con caratteri jolly, puoi specificare un elenco di tag di immagine con un carattere jolly (*) su cui intervenire con la tua policy del ciclo di vita. Ad esempio, se le immagini sono taggate come `prod`, `prod1`, `prod2` e così via, sarà

necessario utilizzare `prod*` per specificarle tutte. Se specifichi più tag, vengono selezionate solo le immagini che hanno tutti i tag specificati.

> **Important**
>
> Esiste un limite massimo di quattro caratteri jolly (*) per stringa. Ad esempio, `["*test*1*2*3", "test*1*2*3*"]` è valido ma `["test*1*2*3*4*5*6"]` non è valido.

e. Se hai scelto Taggata (corrispondenza dei prefissi) per Stato immagine, allora per Specifica i tag per la corrispondenza dei prefissi, puoi specificare un elenco di tag di immagine su cui intervenire con la tua policy del ciclo di vita.

f. Per Criteri di corrispondenza, scegli Dall'invio dell'immagine o Conteggio immagini superiore a, quindi specifica un valore.

g. Selezionare Salva.

7. Per creare ulteriori regole per la policy del ciclo di vita, ripeti le operazioni da 5 a 7.

Per creare una policy del ciclo di vita (AWS CLI)

Per creare una politica del ciclo di vita utilizzando AWS CLI

1. Ottieni il nome del repository per il quale creare la policy del ciclo di vita.

```
aws ecr describe-repositories
```

2. Creare un file locale denominato `policy.json` con il contenuto della policy del ciclo di vita. Per esempi di policy del ciclo di vita, consulta Esempi di policy del ciclo di vita.
3. Creare una policy del ciclo di vita specificando il nome del repository e facendo riferimento al file JSON della policy del ciclo di vita creato.

```
aws ecr put-lifecycle-policy \
      --repository-name repository-name \
      --lifecycle-policy-text file://policy.json
```

Esempi di policy del ciclo di vita

Seguono degli esempi di policy del ciclo di vita che mostrano la sintassi.

Argomenti

Filtraggio per età delle immagini

L'esempio seguente mostra la sintassi della policy del ciclo di vita per una policy che prevede la scadenza delle immagini con un tag che inizia con `prod` utilizzando un `tagPatternList` di `prod*` anch'esso più vecchio di `14` giorni.

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Expire images older than 14 days",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["prod*"],
                "countType": "sinceImagePushed",
                "countUnit": "days",
                "countNumber": 14
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

Filtraggio per numero di immagini

L'esempio seguente mostra la sintassi della policy del ciclo di vita per una policy che mantiene una sola immagine non taggata e fa scadere tutte le altre.

```
{
    "rules": [
```

```
        {
            "rulePriority": 1,
            "description": "Keep only one untagged image, expire all others",
            "selection": {
                "tagStatus": "untagged",
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

Filtraggio per più regole

I seguenti esempi utilizzano più regole in una policy del ciclo di vita. Vengono forniti un repository e una policy del ciclo di vita di esempio insieme a una spiegazione del risultato.

Esempio A

Contenuto del repository:

- Immagine A, Elenco tag: ["beta-1", "prod-1"], Invio: 10 giorni fa
- Immagine B, Elenco tag: ["beta-2", "prod-2"], Invio: 9 giorni fa
- Immagine C, Elenco tag: ["beta-3"], Invio: 8 giorni fa

Testo della policy del ciclo di vita:

```
{
    "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 logica di questa policy del ciclo di vita è:

- La regola 1 identifica le immagini taggate con il prefisso `prod`. Dovrebbe contrassegnare le immagini, a iniziare da quella meno recente, fino a quando rimangono una o meno immagini corrispondenti. Contrassegna l'immagine A per la scadenza.
- La regola 2 identifica le immagini taggate con il prefisso `beta`. Dovrebbe contrassegnare le immagini, a iniziare da quella meno recente, fino a quando rimangono una o meno immagini corrispondenti. Contrassegna entrambe le immagini A e B per la scadenza. Tuttavia, l'immagine A è già stata vista dalla regola 1 e, se l'immagine B scadesse, violerebbe la regola 1, pertanto viene saltata.
- Risultato: l'immagine A scade.

Esempio B

Questo è lo stesso repository dell'esempio precedente, ma l'ordine di priorità delle regole è cambiato per mostrare questo altro esito.

Contenuto del repository:

- Immagine A, Elenco tag: ["beta-1", "prod-1"], Invio: 10 giorni fa
- Immagine B, Elenco tag: ["beta-2", "prod-2"], Invio: 9 giorni fa

- Immagine C, Elenco tag: ["beta-3"], Invio: 8 giorni fa

Testo della policy del ciclo di vita:

```
{
    "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 logica di questa policy del ciclo di vita è:

- La regola 1 identifica le immagini taggate con il prefisso `beta`. Dovrebbe contrassegnare le immagini, a iniziare da quella meno recente, fino a quando rimangono una o meno immagini corrispondenti. Vede tutte e tre le immagini e contrassegna l'immagine A e l'immagine B per la scadenza.

- La regola 2 identifica le immagini taggate con il prefisso `prod`. Dovrebbe contrassegnare le immagini, a iniziare da quella meno recente, fino a quando rimangono una o meno immagini corrispondenti. Non vede alcuna immagine, perché tutte le immagini disponibili sono già viste dalla regola 1, pertanto non vengono contrassegnate altre immagini.
- Risultato: l'immagine A e l'immagine B scadono.

Filtraggio per più tag in una stessa regola

I seguenti esempi specificano la sintassi della policy del ciclo di vita per più modelli di tag in una sola regola. Vengono forniti un repository e una policy del ciclo di vita di esempio insieme a una spiegazione del risultato.

Esempio A

Quando vengono specificati più modelli di tag in una sola regola, le immagini devono corrispondere a tutti i modelli di tag elencati.

Contenuto del repository:

- Immagine A, Elenco tag: ["alpha-1"], Invio: 12 giorni fa
- Immagine B, Elenco tag: ["beta-1"], Invio: 11 giorni fa
- Immagine C, Elenco tag: ["alpha-2", "beta-2"], Invio: 10 giorni fa
- Immagine D, Elenco tag: ["alpha-3"], Invio: 4 giorni fa
- Immagine E, Elenco tag: ["beta-3"], Invio: 3 giorni fa
- Immagine F, Elenco tag: ["alpha-4", "beta-4"], Invio: 2 giorni fa

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["alpha*", "beta*"],
                "countType": "sinceImagePushed",
                "countNumber": 5,
                "countUnit": "days"
```

```
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La logica di questa policy del ciclo di vita è:

- La regola 1 identifica le immagini taggate con il prefisso `alpha` e `beta`. Vede le immagini C ed F. Dovrebbe contrassegnare le immagini che hanno più di cinque giorni, in questo caso l'immagine C.
- Risultato: l'immagine C scade.

Esempio B

Il seguente esempio mostra che i tag non sono esclusivi.

Contenuto del repository:

- Immagine A, Elenco tag: ["alpha-1", "beta-1", "gamma-1"], Invio: 10 giorni fa
- Immagine B, Elenco tag: ["alpha-2", "beta-2"], Invio: 9 giorni fa
- Immagine C, Elenco tag: ["alpha-3", "beta-3", "gamma-2"], Invio: 8 giorni fa

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["alpha*", "beta*"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
```

```
}
```

La logica di questa policy del ciclo di vita è:

- La regola 1 identifica le immagini taggate con il prefisso `alpha` e `beta`. Vede tutte le immagini. Dovrebbe contrassegnare le immagini, a iniziare da quella meno recente, fino a quando rimangono una o meno immagini corrispondenti. Contrassegna le immagini A e B per la scadenza.
- Risultato: l'immagine A e l'immagine B scadono.

Filtro su tutte le immagini

I seguenti esempi di policy del ciclo di vita specificano tutte le immagini con diversi filtri. Vengono forniti un repository e una policy del ciclo di vita di esempio insieme a una spiegazione del risultato.

Esempio A

Quanto segue mostra la sintassi della policy del ciclo di vita per una policy che si applica a tutte le regole ma mantiene una sola immagine e fa scadere tutte le altre.

Contenuto del repository:

- Immagine A, Elenco tag: ["alpha-1"], Invio: 4 giorni fa
- Immagine B, Elenco tag: ["beta-1"], Invio: 3 giorni fa
- Immagine C, Elenco tag: [], Invio: 2 giorni fa
- Immagine D, Elenco tag: ["alpha-2"], Invio: 1 giorno fa

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "any",
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
```

```
            }
        }
    ]
}
```

La logica di questa policy del ciclo di vita è:

- La regola 1 identifica tutte le immagini. Vede le immagini A, B, C e D. Dovrebbe far scadere tutte le immagini tranne quelle più recenti. Contrassegna le immagini A, B e C per la scadenza.
- Risultato: le immagini A, B e C scadono.

Esempio B

Il seguente esempio mostra una policy del ciclo di vita che combina tutti i tipi di regole in un'unica policy.

Contenuto del repository:

- Immagine A, Elenco tag: ["alpha-1", "beta-1"], Invio: 4 giorni fa
- Immagine B, Elenco tag: [], Invio: 3 giorni fa
- Immagine C, Elenco tag: ["alpha-2"], Invio: 2 giorni fa
- Immagine D, Elenco tag: ["git hash"], Invio: 1 giorno fa
- Immagine E, Elenco tag: [], Invio: 1 giorno fa

```
{
    "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 logica di questa policy del ciclo di vita è:

- La regola 1 identifica le immagini taggate con il prefisso `alpha`. Identifica le immagini A e C. Mantiene l'immagine più recente e contrassegna il resto per la scadenza. Contrassegna l'immagine A per la scadenza.
- La regola 2 identifica le immagini non taggate. Identifica le immagini B ed E. Contrassegna tutte le immagini più vecchie di un giorno per la scadenza. Contrassegna l'immagine B per la scadenza.
- La regola 3 identifica tutte le immagini. Identifica le immagini A, B, C, D ed E. Mantiene l'immagine più recente e contrassegna il resto per la scadenza. Tuttavia, non può contrassegnare le immagini A, B, C o E perché sono identificate da regole di priorità superiore. Contrassegna l'immagine D per la scadenza.
- Risultato: le immagini A, B e D scadono.

Mutabilità dei tag immagine

Puoi configurare un repository in modo da attivare l'immutabilità dei tag e impedire che i tag immagine vengano sovrascritti. Una volta configurato il repository per i tag immutabili, viene restituito un errore `ImageTagAlreadyExistsException` se tenti di inviare un'immagine con un tag che esiste già nel repository. Quando l'immutabilità dei tag è attivata per un repository, tutti i tag saranno interessati e non sarà possibile rendere immutabili alcuni tag mentre altri no.

È possibile utilizzare gli AWS CLI strumenti AWS Management Console e per impostare la mutabilità dei tag di immagine per un nuovo repository durante la creazione o per un repository esistente in qualsiasi momento. Per le fasi della console, vedi Creazione di un repository privato e Modifica di un repository privato.

Per creare un repository con i tag immutabili configurati

Utilizza uno dei seguenti comandi per creare un nuovo repository di immagini con i tag immutabili configurati.

- 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
```

Per aggiornare le impostazioni di mutabilità dei tag immagine per un repository esistente

Utilizzare uno dei seguenti comandi per aggiornare le impostazioni di mutabilità dei tag immagine per un repository esistente.

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

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

- Write-ecr () ImageTagMutabilityAWS Tools for Windows PowerShell

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

Scansione delle immagini

La funzionalità di scansione di base migliorata è disponibile in anteprima per Amazon ECR ed è soggetta a modifiche. Durante questa anteprima pubblica, puoi utilizzare solo l'opzione AWS Management Console per attivare la versione di scansione di base migliorata.

La scansione immagini Amazon ECR aiuta a identificare le vulnerabilità del software nelle immagini del container. Sono disponibili i seguenti tipi di scansione.

> **Important**
>
> Il passaggio tra le versioni di scansione avanzata, scansione di base e scansione di base migliorata farà sì che le scansioni precedentemente stabilite non saranno più disponibili. Dovrai configurare nuovamente le scansioni. Tuttavia, se si torna alla versione di scansione precedente, le scansioni stabilite saranno disponibili.

- Scansione avanzata: Amazon ECR si integra con Amazon Inspector per offrire una scansione automatica e continua dei repository. Le immagini dei container vengono analizzate sia per i sistemi operativi che per le vulnerabilità dei pacchetti del linguaggio di programmazione. Quando compaiono nuove vulnerabilità, i risultati della scansione vengono aggiornati e Amazon Inspector emette un evento EventBridge per avvisarti. La scansione avanzata offre quanto segue:
  - Vulnerabilità dei pacchetti del sistema operativo e dei linguaggi di programmazione.
  - Due frequenze di scansione: scansione in modalità push e scansione continua.
- Scansione di base: Amazon ECR offre due versioni di scansione di base che utilizzano il database Common Vulnerabilities and Exposures (CVE); l'attuale versione GA che utilizza il progetto Clair open source e una versione recentemente migliorata della scansione di base (in anteprima) che utilizza la nostra tecnologia nativa. AWS Con la scansione di base, configuri i repository per la scansione tramite push o puoi eseguire scansioni manuali e Amazon ECR fornisce un elenco dei risultati della scansione. La scansione di base offre quanto segue:

- Scansioni del sistema operativo.
- Due frequenze di scansione: manuale e scansione a pressione.

> **Important**
>
> La nuova versione della scansione di base non supporta `imageScanFindingsSummary` e `imageScanStatus` nell'`DescribeImages`API. Per visualizzarli, usa l'`DescribeImageScanFindings`API.

Utilizzo dei filtri

Quando per il registro privato è configurata una scansione di immagini, puoi specificare che tutti i repository vengano scansionati o specificare filtri per l'ambito in cui i repository vengono scansionati.

Quando viene utilizzata la scansione di base, è possibile specificare la scansione sui filtri push per specificare quali repository sono impostati per eseguire una scansione delle immagini quando ne vengono inserite di nuove. Tutti i repository che non corrispondono a una scansione di base sul filtro push saranno impostati su una frequenza di scansione manuale, il che significa che per eseguire una scansione sarà necessario attivarla manualmente.

Quando viene utilizzata la scansione avanzata, è possibile specificare filtri separati per la scansione su push e la scansione continua. Tutti i repository che non corrispondono a un filtro di scansione avanzato avranno la scansione disattivata. Se si utilizza la scansione avanzata e si specificano filtri separati per la scansione su push e la scansione continua in cui più filtri corrispondono allo stesso repository, Amazon ECR applica il filtro di scansione continua sul filtro della scansione su push per quel repository.

Quando viene specificato un filtro, un filtro senza caratteri jolly corrisponderà a tutti i nomi del repository che contengono il filtro. Un filtro con caratteri jolly (*) corrisponde a qualsiasi nome del repository in cui il carattere jolly sostituisce zero o più caratteri nel nome del repository. La tabella seguente fornisce esempi in cui i nomi del repository sono espressi sull'asse orizzontale e i filtri di esempio sono specificati sull'asse verticale.

	prod	repo-prod	prod-repo	repo-prod-repo	prodrepo
prod	 S	 S	 S	 S	 Sì
*prod	 S	 S	 N	 N	 No
prod*	 S	 N	 S	 N	 Sì
prod	 S	 S	 S	 S	 Sì
prod*repo	 N	 N	 S	 N	 Sì

Argomenti

- Scansione avanzata
- Scansione di base
- Risoluzione dei problemi relativi alla scansione delle immagini

Scansione avanzata

La scansione avanzata di Amazon ECR è un'integrazione con Amazon Inspector che fornisce la scansione delle vulnerabilità delle immagini dei container. Le immagini di container vengono analizzate alla ricerca di vulnerabilità sia per i sistemi operativi che per i pacchetti del linguaggio di programmazione. Puoi visualizzare direttamente i risultati della scansione sia con Amazon ECR che

con Amazon Inspector. Per ulteriori informazioni su Amazon Inspector, consulta la sezione Scansione delle immagini dei container con Amazon Inspector nella Guida per l'utente di Amazon Inspector.

Con la scansione avanzata, è possibile scegliere quali repository sono configurati per la scansione automatica e continua e quali sono configurati per la scansione su push. Questo viene fatto impostando i filtri di scansione.

Considerazioni per le scansioni avanzate

Quando si abilita la scansione avanzata di Amazon ECR, è necessario considerare quanto segue.

- Amazon ECR non prevede costi aggiuntivi per l'utilizzo di questa funzione ma Amazon Inspector prevede un costo per la scansione delle immagini. Per ulteriori informazioni, consulta Prezzi di Amazon Inspector.
- La scansione avanzata non è supportata nelle seguenti regioni:
  - Medio Oriente (EAU) (`me-central-1`)
  - Asia Pacifico (Hyderabad) (`ap-south-2`)
  - Israele (Tel Aviv) (`il-central-1`)
  - Asia Pacifico (Melbourne) (`ap-southeast-4`)
  - Europa (Spagna) (`eu-south-2`)
- Amazon Inspector supporta la scansione per sistemi operativi specifici. Per un elenco completo, consulta la sezione Sistemi operativi supportati - Scansione Amazon ECR nella Guida per l'utente di Amazon Inspector.
- Amazon Inspector utilizza un ruolo IAM collegato al servizio, che fornisce le autorizzazioni necessarie per fornire una scansione avanzata dei repository. Il ruolo IAM collegato al servizio viene creato automaticamente da Amazon Inspector quando è attivata la scansione avanzata del registro privato. Per ulteriori informazioni, consulta la sezione Utilizzo di ruoli collegati ai servizi per Amazon Inspector nella Guida per l'utente di Amazon Inspector.
- Quando attivi inizialmente la scansione avanzata per il tuo registro privato, Amazon Inspector riconosce solo le immagini inviate ad Amazon ECR negli ultimi 30 giorni, in base al timestamp dell'immagine, o recuperate negli ultimi 90 giorni. Le immagini più vecchie avranno lo stato di scansione `SCAN_ELIGIBILITY_EXPIRED`. Se desideri che queste immagini vengano scansionate da Amazon Inspector, devi reinserirle nel tuo repository.
- Tutte le immagini inviate ad Amazon ECR dopo l'attivazione della scansione avanzata vengono scansionate continuamente per la durata configurata. Per impostazione predefinita, la durata è

Per sempre (Lifetime). Questa impostazione può essere configurata tramite la console di Amazon Inspector. Per ulteriori informazioni, consulta Modifica della durata della scansione avanzata.

- Quando per il registro privato Amazon ECR è abilitata la scansione avanzata, i repository corrispondenti ai filtri di scansione vengono scansionati solo utilizzando la scansione avanzata. I repository che non corrispondono a un filtro avranno una frequenza di scansione `Off`, ma non saranno sottoposti a scansione. Le scansioni manuali che utilizzano la scansione avanzata non sono supportate. Per ulteriori informazioni, consulta Utilizzo dei filtri.
- Se si specificano filtri separati per la scansione su push e la scansione continua in cui più filtri corrispondono allo stesso repository, Amazon ECR applica il filtro di scansione continua sul filtro della scansione su push per quel repository.
- Quando la scansione avanzata è attivata, Amazon ECR invia un evento a EventBridge quando viene modificata la frequenza di scansione di un repository. Amazon Inspector emette eventi EventBridge quando viene completata una scansione iniziale e quando viene creato, aggiornato o chiuso un risultato di scansione di immagini.

Autorizzazioni IAM richieste

La scansione avanzata di Amazon ECR richiede un ruolo IAM collegato al servizio Amazon Inspector e che il principale IAM che abilita e utilizza la scansione avanzata abbia le autorizzazioni per chiamare le API di Amazon Inspector necessarie per la scansione. Il ruolo IAM collegato al servizio Amazon Inspector viene creato automaticamente da Amazon Inspector quando è attivata la scansione avanzata del registro privato. Per ulteriori informazioni, consulta la sezione Utilizzo di ruoli collegati ai servizi per Amazon Inspector nella Guida per l'utente di Amazon Inspector.

La seguente policy IAM concede le autorizzazioni necessarie per l'attivazione e l'utilizzo della scansione avanzata. Include l'autorizzazione necessaria ad Amazon Inspector per creare il ruolo IAM collegato al servizio e le autorizzazioni API di Amazon Inspector necessarie per attivare e disattivare la scansione avanzata e recuperare i risultati della scansione.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Come utilizzare la scansione avanzata

AWS Management Console

Per attivare la scansione avanzata del registro privato (AWS Management Console)

La configurazione della scansione è definita a livello di registro privato in base alle regioni.

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegli la regione in cui impostare la configurazione della scansione.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Scanning (Scansione).
4. Nella pagina Scanning configuration (Configurazione della scansione), per Scan type (Tipo di scansione) scegli Enhanced scanning (Scansione avanzata).
5. (Facoltativo) Per impostazione predefinita, quando è selezionata l'opzione Enhanced scanning (Scansione avanzata), tutti i repository sono impostati su Continuous scanning (Scansione continua). È possibile modificare la configurazione di scansione predefinita deselezionando la casella Continuously scan all repositories (Scansione continua di tutti i repository). È quindi possibile configurare tutti i repository per la scansione su push oppure

specificare filtri di scansione separati per la scansione continua e la scansione su push. Quando sono impostati i filtri di scansione, è possibile scegliere Preview repository matches (Anteprima delle corrispondenze del repository) per verificare quali repository nel registro corrispondono ai filtri definiti.

> **Important**
>
> I filtri senza caratteri jolly corrisponderanno a tutti i nomi del repository che contengono il filtro. I filtri con caratteri jolly (*) corrispondono a qualsiasi nome di un repository in cui il carattere jolly sostituisce zero o più caratteri nel nome del repository.

6. Selezionare Salva.
7. Ripeti questi passaggi in ogni regione in cui desideri attivare la scansione avanzata.

AWS CLI

Usa il seguente AWS CLI comando per attivare la scansione avanzata per il tuo registro privato utilizzando il. AWS CLIÈ possibile specificare i filtri di scansione utilizzando l'oggetto `rules`.

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

  L'esempio seguente consente di attivare la scansione avanzata del registro privato. Per impostazione predefinita, quando non sono state specificate `rules`, Amazon ECR imposta la configurazione di scansione su una scansione continua per tutti i repository.

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

  L'esempio seguente consente di attivare la scansione avanzata del registro privato e specifica un filtro di scansione. Il filtro di scansione nell'esempio consente di attivare la scansione continua di tutti i repository con `prod` nel suo nome.

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

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

L'esempio seguente consente di attivare la scansione avanzata del registro privato e specifica più filtri di scansione. I filtri di scansione nell'esempio consentono di attivare la scansione continua di tutti i repository con `prod` nel nome e consentono di attivare la scansione su push solo per tutti gli altri repository.

```
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
```

Modifica della durata della scansione avanzata

Amazon Inspector supporta la configurazione della durata di monitoraggio continuo dei repository privati. Per impostazione predefinita, quando la scansione avanzata è attivata per il registro privato Amazon ECR, il servizio Amazon Inspector monitora continuamente i repository fino a quando l'immagine non viene eliminata o la scansione avanzata non viene disabilitata. La durata della scansione delle immagini da parte di Amazon Inspector può essere modificata utilizzando le impostazioni di Amazon Inspector. Le durate di scansione disponibili sono Ciclo di vita (impostazione predefinita), 180 giorni e 30 giorni. Al termine della durata della scansione di un repository, lo stato di scansione di `SCAN_ELIGIBILITY_EXPIRED` viene visualizzato quando si elencano le vulnerabilità di scansione. Per ulteriori informazioni, consulta Modifica della durata della nuova scansione automatica di Amazon ECR nella Guida per l'utente di Amazon Inspector.

Per modificare l'impostazione della durata di scansione avanzata

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Nel riquadro di navigazione di sinistra, espandi Impostazioni e quindi scegli General (Generali).
3. Nella pagina Impostazioni, in Durata della nuova scansione ECR scegli un'impostazione, quindi scegli Save (Salva).

EventBridge eventi

Quando la scansione avanzata è attivata, Amazon ECR invia un evento a EventBridge quando viene modificata la frequenza di scansione di un repository. Amazon Inspector emette eventi EventBridge quando viene completata una scansione iniziale e quando viene creato, aggiornato o chiuso un risultato di scansione di immagini.

Evento per una modifica della frequenza di scansione del repository

Quando la scansione avanzata è attivata per il registro, il seguente evento viene inviato da Amazon ECR quando si verifica una modifica con una risorsa che ha attivato la scansione avanzata. Ciò include la creazione di nuovi repository, la modifica della frequenza di scansione di un repository o la creazione o eliminazione di immagini nei repository con la scansione avanzata attivata. Per ulteriori informazioni, consulta Scansione delle immagini.

```
{
 "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"
 }
}
```

Evento per una scansione iniziale dell'immagine (scansione avanzata)

Quando la scansione avanzata è attivata per il registro, Amazon Inspector invia il seguente evento al termine della scansione iniziale dell'immagine. Il parametro `finding-severity-counts` restituirà un valore per un livello di gravità solo se ne esiste uno. Ad esempio, se l'immagine non contiene risultati a livello `CRITICAL`, non viene restituito alcun conteggio critico. Per ulteriori informazioni, consulta Scansione avanzata.

Modello di eventi:

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

Output di esempio:

```
{
    "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"
        ]
    }
}
```

Evento per un aggiornamento del risultato della scansione dell'immagine (scansione avanzata)

Quando la scansione avanzata è attivata per il registro, Amazon Inspector invia il seguente evento quando il rilevamento della scansione delle immagini viene creato, aggiornato o chiuso. Per ulteriori informazioni, consulta Scansione avanzata.

Modello di eventi:

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

Output di esempio:

```
{
    "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"
    }
}
```

Recupero dei risultati della scansione delle immagini

Puoi recuperare i risultati dell'ultima scansione delle immagini completata. I risultati elencano per gravità le vulnerabilità del software rilevate in base al database Common Vulnerabilities and Exposures (CVE).

Per la risoluzione dei problemi relativi ad alcuni problemi comuni durante la scansione delle immagini, consulta Risoluzione dei problemi relativi alla scansione delle immagini.

Per recuperare i risultati della scansione delle immagini (AWS Management Console)

AWS Management Console

Attieniti alla seguente procedura per recuperare i risultati della scansione delle immagini utilizzando la AWS Management Console.

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegli la regione in cui si trova il repository.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository), scegliere il repository che contiene l'immagine per cui recuperare i risultati della scansione.
5. Nella pagina Images (Immagini) selezionare nella colonna Vulnerabilities (Vulnerabilità) See findings (Vedi risultati) per l'immagine di cui si desidera recuperare i risultati della scansione.
6. Quando si visualizza la pagina Findings (Risultati), il nome della vulnerabilità nella colonna Name (Nome) è un collegamento alla console Amazon Inspector dove è possibile visualizzare ulteriori dettagli.

AWS CLI

Utilizza il seguente AWS CLI comando per recuperare i risultati della scansione delle immagini utilizzando. AWS CLI Puoi specificare un'immagine utilizzando `imageTag` o `imageDigest`, entrambe ottenibili utilizzando il comando CLI list-images.

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

  Nell'esempio seguente viene utilizzato un tag di immagine.

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

  Nell'esempio seguente viene utilizzato un digest di immagine.

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

Scansione di base

La funzionalità di scansione di base migliorata è disponibile in anteprima per Amazon ECR ed è soggetta a modifiche. Durante questa anteprima pubblica, puoi utilizzare solo l'opzione AWS Management Console per attivare la versione di scansione di base migliorata.

Amazon ECR offre due versioni di scansione di base che utilizzano il database Common Vulnerabilities and Exposures (CVeS); l'attuale versione GA che utilizza il progetto Clair open source e una versione recentemente migliorata della scansione di base (in anteprima) che utilizza la nostra tecnologia nativa. AWS Con entrambe le versioni di Amazon ECR basic scan abilitate sul tuo registro privato, puoi configurare i filtri del repository per specificare quali repository sono impostati per la scansione in modalità push oppure puoi eseguire scansioni manuali. Amazon ECR fornisce un elenco di risultati della scansione. Ogni immagine del container può essere analizzata una volta ogni 24 ore. Puoi esaminare i risultati della scansione per ottenere informazioni sulla sicurezza delle immagini dei

container che vengono distribuite utilizzando l'`DescribeImageScanFindings`API o all'interno della console. Per ulteriori informazioni su Clair, consulta Clair on. GitHub

Amazon ECR utilizza la gravità per un CVE dall'origine di distribuzione upstream, se disponibile, altrimenti si utilizza il punteggio CVSS (Common Vulnerability Scoring System). Il punteggio CVSS può essere utilizzato per ottenere il livello di gravità della vulnerabilità NVD. Per ulteriori informazioni, consulta NVD Vulnerability Severity Ratings.

Tutti i repository che non corrispondono a un filtro di scansione su push saranno impostati su una frequenza di scansione manuale, il che significa che per eseguire una scansione sarà necessario attivarla manualmente. I risultati delle ultime scansioni completate delle immagini possono essere recuperati per ogni immagine. Amazon ECR invia un evento ad Amazon EventBridge (precedentemente chiamato CloudWatch Events) quando viene completata una scansione dell'immagine. Per ulteriori informazioni, consulta Eventi Amazon ECR ed EventBridge.

> **Important**
>
> La nuova versione della scansione di base è supportata nelle seguenti regioni:

- Asia Pacifico (Hong Kong) (`ap-east-1`)
- Europa (Stoccolma) (`eu-north-1`)
- Medio Oriente (Bahrein) (`me-south-1`)
- Asia Pacifico (Mumbai) (`ap-south-1`)
- Europa (Parigi) (`eu-west-3`)
- AWS GovCloud (Stati Uniti orientali) (`us-gov-east-1`)
- Africa (Città del Capo) (`af-south-1`)
- Asia Pacifico (Giacarta) (`ap-southeast-3`)
- Europa (Francoforte) (`eu-central-1`)
- Europa (Irlanda) (`eu-west-1`)
- Sud America (San Paolo) (`sa-east-1`)
- Stati Uniti orientali (Ohio) (`us-east-2`)
- AWS GovCloud (Stati Uniti occidentali) () `us-gov-west-1`
- Asia Pacifico (Tokyo) (`ap-northeast-1`)
- Asia Pacifico (Seoul) (`ap-northeast-2`)

- Asia Pacifico (Osaka-Locale) (`ap-northeast-3`)
- Europa (Milano) (`eu-south-1`)
- Europa (Londra) (`eu-west-2`)
- Stati Uniti orientali (Virginia settentrionale) (`us-east-1`)
- Asia Pacifico (Singapore) (`ap-southeast-1`)
- Asia Pacifico (Sydney) (`ap-southeast-2`)
- Canada (Centrale) (`ca-central-1`)
- Stati Uniti occidentali (California settentrionale) (`us-west-1`)
- Stati Uniti occidentali (Oregon) (`us-west-2`)
- Europa (Zurigo) (`eu-central-2`)

Per la risoluzione dei problemi relativi ad alcuni problemi comuni durante la scansione delle immagini, consulta Risoluzione dei problemi relativi alla scansione delle immagini.

Come best practice di sicurezza e per una copertura continua, ti consigliamo di continuare a utilizzare le versioni supportate di un sistema operativo. In conformità alla politica dei fornitori, i sistemi operativi fuori produzione non vengono più aggiornati con patch e, in molti casi, non vengono più rilasciati nuovi avvisi di sicurezza relativi a tali sistemi. Inoltre, alcuni fornitori rimuovono gli avvisi e i rilevamenti di sicurezza esistenti dai propri feed quando un sistema operativo interessato raggiunge la fine del supporto standard. Una volta che una distribuzione perde il supporto del suo fornitore, Amazon ECR potrebbe non supportare più la scansione per individuare eventuali vulnerabilità. Qualsiasi risultato generato da Amazon ECR per un sistema operativo fuori produzione deve essere utilizzato solo a scopo informativo. Di seguito sono elencati i sistemi operativi e le versioni attualmente supportati.

Sistema operativo	Versione
Alpine Linux (Alpine)	3.19
Linux Alpine (Alpine)	3.18
Alpine Linux (Alpine)	3.17
Alpine Linux (Alpine)	3.16
Amazon Linux 2 (AL2)	AL2

Sistema operativo	Versione
Amazon Linux 2023 (AL2023)	AL2023
CentOS Linux (CentOS)	7
Server Debian (Bookworm)	12
Server Debian (Bullseye)	11
Server Debian (Buster)	10
Oracle Linux (Oracle)	9
Oracle Linux (Oracle)	8
Oracle Linux (Oracle)	7
Ubuntu (lunare)	23.04
Ubuntu (Jammy)	22.04 (LITRI)
Ubuntu (Focale)	20.024 (LITRI)
Ubuntu (Bionico)	18.04 (SECONDI)
Ubuntu (Xenial)	16.04 (SEM)
Ubuntu (affidabile)	14.04 (ESM)
Red Hat Enterprise Linux (RHEL)	7
Red Hat Enterprise Linux (RHEL)	8
Red Hat Enterprise Linux (RHEL)	9

Come utilizzare la scansione di base

Basic scanning with Clair

Per impostazione predefinita, Amazon ECR abilita la scansione di base su tutti i registri privati. Di conseguenza, a meno che non siano state modificate le impostazioni di scansione nel registro privato, non dovrebbe essere necessario abilitare la scansione di base. È possibile utilizzare la seguente procedura per verificare che la scansione di base sia abilitata e definire uno o più filtri di scansione su push.

Per attivare la scansione di base per il registro privato (AWS Management Console)

La configurazione della scansione è definita a livello di registro privato in base alle regioni.

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegli la regione in cui impostare la configurazione della scansione.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Scanning (Scansione).
4. Nella pagina Scanning configuration (Configurazione della scansione), per Scan type (Tipo di scansione) scegli Basic scanning (Scansione di base).
5. Per impostazione predefinita, tutti i repository sono impostati per la scansione Manual (Manuale). Puoi scegliere di configurare la scansione su push specificando Scan on push filters (Filtri di scansione su push). È possibile impostare la scansione su push per tutti i repository o i singoli repository. Per ulteriori informazioni, consulta Utilizzo dei filtri.

Improved basic scanning with AWS native technology (In preview)

Una nuova versione della scansione di base di Amazon ECR è ora disponibile in anteprima.

Per attivare la scansione di base migliorata per il registro privato ()AWS Management Console

La configurazione della scansione è definita a livello di registro privato in base alle regioni.

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegli la regione in cui impostare la configurazione della scansione.

3. Nel pannello di navigazione, seleziona Private registry (Registro privato), Scanning (Scansione).
4. Nella pagina di configurazione della scansione, per Tipo di scansione scegli Scansione di base migliorata (in anteprima) - nuova.
5. Per impostazione predefinita, tutti i repository sono impostati per la scansione Manual (Manuale). Puoi scegliere di configurare la scansione su push specificando Scan on push filters (Filtri di scansione su push). È possibile impostare la scansione su push per tutti i repository o i singoli repository. Per ulteriori informazioni, consulta Utilizzo dei filtri.

Scansione manuale di un'immagine

Puoi avviare manualmente le scansioni delle immagini quando vuoi eseguirla nei repository che non sono configurati per la scansione su push. Un'immagine può essere analizzata una sola volta al giorno. Questo limite include la scansione su push iniziale, se configurata e le eventuali scansioni manuali.

Per la risoluzione dei problemi relativi ad alcuni problemi comuni durante la scansione delle immagini, consulta Risoluzione dei problemi relativi alla scansione delle immagini.

AWS Management Console

Attieniti alla seguente procedura per avviare una scansione manuale dell'immagine utilizzando la AWS Management Console.

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegliere la regione in cui creare il repository.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).
4. Nella pagina Repositories (Repository) selezionare il repository contente l'immagine da scansionare.
5. Nella pagina Images (Immagini) selezionare l'immagine da scansionare, quindi scegliere Scan (Scansione).

AWS CLI

- start-image-scan (AWS CLI)

  Nell'esempio seguente viene utilizzato un tag di immagine.

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

Nell'esempio seguente viene utilizzato un digest di immagine.

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

AWS Tools for Windows PowerShell

- Get-ECR () ImageScanFindingAWS Tools for Windows PowerShell

  Nell'esempio seguente viene utilizzato un tag di immagine.

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

  Nell'esempio seguente viene utilizzato un digest di immagine.

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

Recupero dei risultati della scansione delle immagini

Puoi recuperare i risultati dell'ultima scansione delle immagini completata. I risultati elencano per gravità le vulnerabilità del software rilevate in base al database Common Vulnerabilities and Exposures (CVE).

Per la risoluzione dei problemi relativi ad alcuni problemi comuni durante la scansione delle immagini, consulta Risoluzione dei problemi relativi alla scansione delle immagini.

AWS Management Console

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/repositories.
2. Dalla barra di navigazione, scegliere la regione in cui creare il repository.
3. Nel riquadro di navigazione, selezionare Repositories (Repository).

4. Nella pagina Repositories (Repository), scegliere il repository che contiene l'immagine per cui recuperare i risultati della scansione.
5. Nella pagina Images (Immagini) selezionare nella colonna Vulnerabilities (Vulnerabilità) Details (Dettagli) per l'immagine di cui si desidera recuperare i risultati della scansione.

AWS CLI

Utilizzate il seguente AWS CLI comando per recuperare i risultati della scansione delle immagini utilizzando. AWS CLI Puoi specificare un'immagine utilizzando `imageTag` o `imageDigest`, entrambe ottenibili utilizzando il comando CLI list-images.

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

  Nell'esempio seguente viene utilizzato un tag di immagine.

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

  Nell'esempio seguente viene utilizzato un digest di immagine.

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

AWS Tools for Windows PowerShell

- get-ecr () ImageScanFindingAWS Tools for Windows PowerShell

  Nell'esempio seguente viene utilizzato un tag di immagine.

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

  Nell'esempio seguente viene utilizzato un digest di immagine.

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

Risoluzione dei problemi relativi alla scansione delle immagini

Di seguito sono riportati gli errori comuni relativi alla scansione delle immagini. Puoi visualizzare errori di questo tipo nella console Amazon ECR visualizzando i dettagli dell'immagine o tramite l'API o AWS CLI utilizzando l'`DescribeImageScanFindings`API.

UnsupportedImageError

È possibile ricevere un errore `UnsupportedImageError` nel tentativo di eseguire una scansione di base di un'immagine creata utilizzando un sistema operativo per il quale Amazon ECR non supporta la scansione di base delle immagini. Amazon ECR supporta la scansione delle vulnerabilità dei pacchetti per le versioni principali delle distribuzioni Amazon Linux, Amazon Linux 2, Debian, Ubuntu, CentOS, Oracle Linux, Alpine e RHEL Linux. Una volta che una distribuzione perde il supporto del suo fornitore, Amazon ECR potrebbe non supportare più la scansione per individuare eventuali vulnerabilità. Amazon ECR non supporta la scansione delle immagini create a partire dall'immagine scratch Docker.

> **Important**
>
> Quando si utilizza la scansione avanzata, Amazon Inspector supporta la scansione per tipi di supporto e sistemi operativi specifici. Per un elenco completo, consulta la sezione Tipi di supporto e sistemi operativi supportati nella Guida per l'utente di Amazon Inspector.

Viene restituito un livello di gravità `UNDEFINED`

È possibile che venga visualizzato un rilevamento di scansione con un livello di gravità `UNDEFINED`. Di seguito sono riportate le cause comuni per questo:

- Alla vulnerabilità non è stata assegnata una priorità dall'origine CVE.
- Alla vulnerabilità è stata assegnata una priorità che Amazon ECR non riconosce.

Per determinare la gravità e la descrizione di una vulnerabilità, è possibile visualizzare il CVE direttamente dall'origine.

Informazioni sullo stato della scansione **SCAN_ELIGIBILITY_EXPIRED**

Quando la scansione avanzata con Amazon Inspector è abilitata per il tuo registro privato e stai visualizzando le vulnerabilità della scansione, è possibile che venga visualizzato uno stato di scansione di `SCAN_ELIGIBILITY_EXPIRED`. Le cause più comuni sono le seguenti.

- Quando inizialmente attivi la scansione avanzata per il tuo registro privato, Amazon Inspector riconosce solo le immagini inviate ad Amazon ECR negli ultimi 30 giorni, in base al timestamp di invio delle immagini. Le immagini più vecchie avranno lo stato di scansione `SCAN_ELIGIBILITY_EXPIRED`. Se desideri che queste immagini vengano scansionate da Amazon Inspector, devi reinserirle nel tuo repository.
- Se la Durata della nuova scansione ECR viene modificata nella console di Amazon Inspector e questo tempo è trascorso, lo stato di scansione dell'immagine viene modificato in `inactive` con un codice motivo `expired` e tutti i resultati associati all'immagine sono programmati per essere chiusi. Il risultato è che la console Amazon ECR elenca lo stato di scansione come `SCAN_ELIGIBILITY_EXPIRED`.

Formati manifest per le immagini dei container

Amazon ECR supporta i seguenti formati manifesto per le immagini dei container:

- Docker Image Manifest V2 Schema 1 (utilizzato con Docker versione 1.9 e precedenti)
- Docker Image Manifest V2 Schema 2 (utilizzato con Docker versione 1.10 e successive)
- Open Container Initiative (OCI) Specifications (v1.0 e successive)

Il supporto di Docker Image Manifest V2 Schema 2 offre le seguenti funzionalità:

- La capacità di utilizzare più tag per un'unica immagine.
- Supporto dell'archiviazione delle immagini per i container Windows. Per ulteriori informazioni, consulta Invio di immagini di Windows ad Amazon ECR nella Guida per gli sviluppatori di Amazon Elastic Container Service.

Conversione del manifesto delle immagini Amazon ECR

Quando invii ed estrai immagini da Amazon ECR, il client del motore del container (ad esempio, Docker) comunica con il registro per concordare un formato manifesto che sia comprensibile dal client e dal registro per utilizzare l'immagine.

Quando invii un'immagine ad Amazon ECR con Docker versione 1.9 o precedente, il formato manifesto dell'immagine viene archiviato come Docker Image Manifest V2 Schema 1. Quando invii un'immagine ad Amazon ECR con Docker versione 1.10 o successiva, il formato manifesto dell'immagine viene archiviato come Docker Image Manifest V2 Schema 2.

Quando estrai un'immagine da Amazon ECR in base al tag, Amazon ECR restituisce il formato manifesto dell'immagine archiviato nel repository. Il formato viene restituito solo se è supportato dal client. Se il formato manifesto dell'immagine memorizzato non è supportato dal client, Amazon ECR converte il manifesto dell'immagine in un formato compreso. Ad esempio, se un client Docker 1.9 richiede un manifesto dell'immagine che è memorizzato come Docker Image Manifest V2 Schema 2, Amazon ECR restituisce il manifesto nel formato Docker Image Manifest V2 Schema 1. La tabella che segue descrive le conversioni disponibili supportate da Amazon ECR quando un'immagine viene estratta in base al tag:

Schema richiesto in base al client	Inviato a ECR come V2, schema 1	Inviato a ECR come V2, schema 2	Inviato a ECR come OCI
V2, schema 1	Nessuna conversione richiesta	Convertito in V2, schema 1	Convertito in V2, schema 1
V2, schema 2	Nessuna conversio ne disponibile, il client utilizza V2, schema 1	Nessuna conversione richiesta	Convertito in V2, schema 2
OCI	Nessuna conversione disponibile	Convertito in OCI	Nessuna conversione richiesta

Important

Se si estrae un'immagine in base al digest, non è disponibile alcuna traduzione. Il cliente deve comprendere il formato manifesto delle immagini archiviato in Amazon ECR. Se richiedi un'immagine Docker Image Manifest V2 Schema 2 per digest su un client Docker 1.9 o

precedente, l'estrazione dell'immagine non va a buon fine. Per ulteriori informazioni, consulta Compatibilità del registro nella documentazione Docker.
In questo esempio, se richiedi la stessa immagine in base al tag, Amazon ECR converte il formato manifesto dell'immagine in un formato che il client possa comprendere. L'immagine viene estratta con esito positivo.

Utilizzo delle immagini Amazon ECR con Amazon ECS

Puoi utilizzare i tuoi repository privati Amazon ECR per ospitare immagini di container e artefatti da cui le tue attività Amazon ECS possono eseguire il pull. A tal fine, l'agente del container, Amazon ECS o Fargate deve disporre delle autorizzazioni per creare le API `ecr:BatchGetImage`, `ecr:GetDownloadUrlForLayer` e `ecr:GetAuthorizationToken`.

Autorizzazioni IAM richieste

La tabella seguente mostra il ruolo IAM da utilizzare, per ogni tipo di avvio, che fornisce le autorizzazioni necessarie per il pull delle tue attività da un repository privato Amazon ECS. Amazon ECS fornisce policy IAM gestite che includono le autorizzazioni richieste.

Tipo di avvio	Ruolo IAM	Policy IAM gestita da AWS
Amazon ECS su istanze Amazon EC2	Usa il ruolo IAM dell'istanza di container associato all'istanza Amazon EC2 registrata nel tuo cluster Amazon ECS. Per maggiori informazioni, consulta Ruolo IAM dell'istanza di container nella Guida per lo sviluppatore di Amazon Elastic Container Service.	`AmazonEC2ContainerServiceforEC2Role` Per ulteriori informazioni, consulta AmazonEC2ContainerServiceforEC2Role nella Guida per lo sviluppatore di Amazon Elastic Container Service.
Amazon ECS su Fargate	Usa il ruolo IAM di esecuzione attività a cui fai riferimento nella definizione dell'attività Amazon ECS. Per ulteriori informazioni, consulta Ruolo	`AmazonECSTaskExecutionRolePolicy` Per ulteriori informazioni, consulta AmazonECSTaskExecutionRolePolicy nella

Tipo di avvio	Ruolo IAM	Policy IAM gestita da AWS
	IAM per l'esecuzione attività nella Guida per lo sviluppatore di Amazon Elastic Container Service.	Guida per lo sviluppatore di Amazon Elastic Container Service.
Amazon ECS su istanze esterne	Utilizza il ruolo IAM dell'istanza di container associato al server on-premise o alla macchina virtuale (VM) registrata nel tuo cluster Amazon ECS. Per ulteriori informazioni, consulta Ruolo Amazon ECS dell'istanza di container nella Guida per lo sviluppatore di Amazon Elastic Container Service.	`AmazonEC2ContainerServiceforEC2Role` Per ulteriori informazioni, consulta AmazonEC2ContainerServiceforEC2Role nella Guida per lo sviluppatore di Amazon Elastic Container Service.

Important

Le policy IAM gestite da AWS contengono autorizzazioni aggiuntive che potrebbe non essere necessario utilizzare. In questo caso, queste sono le autorizzazioni minime richieste per eseguire il pull da un repository privato Amazon ECR.

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

```
}
```

Specifica di un'immagine Amazon ECR in una definizione attività Amazon ECS

Quando crei una definizione attività Amazon ECS, puoi specificare un'immagine di container ospitata in un repository privato Amazon ECR. Nella definizione attività accertati di utilizzare la denominazione completa di `registry/repository:tag` per le immagini Amazon ECR. Ad esempio, *`aws_account_id`*`.dkr.ecr.`*`region`*`.amazonaws.com/`*`my-repository`*`:`*`latest`*.

Lo snippet di definizione dell'attività seguente mostra la sintassi da utilizzare per specificare un'immagine container ospitata in Amazon ECR nella definizione dell'attività Amazon ECS.

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

Utilizzo delle immagini Amazon ECR con Amazon EKS

L'utilizzo delle immagini Amazon ECR con Amazon EKS è possibile, purché siano soddisfatti i seguenti requisiti:

- Per i carichi di lavoro Amazon EKS ospitati su nodi gestiti o autogestiti, il ruolo IAM del nodo worker Amazon EKS (`NodeInstanceRole`) è obbligatorio. Il ruolo IAM del nodo worker Amazon EKS deve contenere le seguenti autorizzazioni delle policy IAM per Amazon ECR.

  ```
  {
  ```

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

> **Note**
>
> Se sono stati utilizzati `eksctl` o i modelli AWS CloudFormation delle Nozioni di base su Amazon EKS per creare i gruppi di nodi di lavoro e cluster, queste autorizzazioni IAM vengono applicate per impostazione predefinita al ruolo IAM del nodo di lavoro.

- Per carichi di lavoro Amazon EKS ospitati su AWS Fargate, devi utilizzare il ruolo di esecuzione del pod Fargate, che fornisce ai tuoi pod l'autorizzazione per estrarre immagini da repository Amazon ECR privati. Per ulteriori informazioni, consulta Creazione di un ruolo di esecuzione pod Fargate.
- Quando si fa riferimento a un'immagine da Amazon ECR, è necessario utilizzare la denominazione completa `registry/repository:tag` per l'immagine. Ad esempio, *`aws_account_id`*`.dkr.ecr.`*`region`*`.amazonaws.com/`*`my-repository`*`:`*`latest`*.

Installazione di un grafico Helm con hosting su Amazon ECR con Amazon EKS

I grafici Helm con hosting in Amazon ECR possono essere installati sui cluster Amazon EKS. I passaggi seguenti lo dimostrano.

Prerequisiti

Prima di iniziare, assicurati di aver completato i passaggi seguenti.

- Installa la versione più recente del client Helm. Questi passaggi sono stati scritti utilizzando la versione `3.9.0` di Helm. Per ulteriori informazioni, consulta l'argomento relativo all'installazione di Helm.
- Hai almeno la versione `1.23.9` o `2.6.3` del AWS CLI installata sul computer. Per ulteriori informazioni, consulta Installare o aggiornare la versione più recente della AWS CLI.
- Hai inviato un grafico Helm al tuo repository Amazon ECR. Per ulteriori informazioni, consulta Invio di un grafico Helm.
- Hai configurato `kubectl` affinché lavori con Amazon EKS. Per ulteriori informazioni, consulta Crea un `kubeconfig` per Amazon EKS nella Guida per l'utente di Amazon EKS. Se i comandi seguenti vanno a buon fine per il cluster, la configurazione è corretta.

```
kubectl get svc
```

Installa un grafico Helm con hosting su Amazon ECR in un cluster Amazon EKS

1. Autentica il tuo client Helm nel registro Amazon ECR che esegue l'hosting del tuo grafico Helm. Devi ottenere i token di autenticazione per ciascun registro utilizzato. I token hanno una validità di 12 ore. Per ulteriori informazioni, consulta Autenticazione del registro privato.

   ```
   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. Installare il grafico. Sostituisci *helm-test-chart* con il repository e *0.1.0* con il tag del grafico Helm.

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

   L'output dovrebbe avere questo aspetto:

   ```
   NAME: ecr-chart-demo
   LAST DEPLOYED: Tue May 31 17:38:56 2022
   NAMESPACE: default
   STATUS: deployed
   REVISION: 1
   ```

```
TEST SUITE: None
```

3. Verifica l'installazione del grafico.

```
helm list -n default
```

Output di esempio:

```
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. (Facoltativo) Vedi il grafico Helm installato `ConfigMap`.

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

5. Al termine dell'operazione, puoi rimuovere la versione del grafico dal cluster.

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

Immagine del container Amazon Linux

L'immagine di container Linux è costruita con gli stessi componenti software inclusi nell'Amazon Linux AMI. È disponibile per l'uso in qualsiasi ambiente come immagine di base per i carichi di lavoro di Docker. Se utilizzi già l'Amazon Linux AMI per le applicazioni in Amazon EC2, puoi containerizzare le tue applicazioni con l'immagine del container Amazon Linux.

Puoi utilizzare l'immagine del contenitore Amazon Linux nel tuo ambiente di sviluppo locale e quindi inviare l'applicazione all' AWS utilizzo di Amazon ECS. Per ulteriori informazioni, consulta Utilizzo delle immagini Amazon ECR con Amazon ECS.

L'immagine del container Amazon Linux è disponibile in Amazon ECR Public e in Docker Hub. Il supporto per l'immagine del container Amazon Linux è disponibile visitando i forum per gli sviluppatori AWS.

Per estrarre l'immagine del container Amazon Linux da Amazon ECR Public

1. Autentica il cliente Docker nel registro Amazon Linux Public. I token di autenticazione sono validi 12 ore. Per ulteriori informazioni, consulta Autenticazione del registro privato.

   > **Note**
   >
   > I ecr-public comandi sono disponibili in AWS CLI a partire dalla versione `1.18.1.187`, tuttavia consigliamo di utilizzare comunque la versione più recente di AWS CLI. Per ulteriori informazioni, consulta Installazione dell' AWS Command Line Interface nella Guida per l'utente di AWS Command Line Interface .

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

   L'output è il seguente:

   ```
   Login succeeded
   ```

2. Estrai l'immagine del container Amazon Linux con il comando docker pull. Per visualizzare l'immagine del container Amazon Linux nella galleria di Amazon ECR Public, consulta la galleria di Amazon ECR Public - amazonlinux.

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

3. (Opzionale) Esegui il container a livello locale.

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

Per estrarre l'immagine del container Amazon Linux da Docker Hub

1. Estrai l'immagine del container Amazon Linux con il comando docker pull.

   ```
   docker pull amazonlinux
   ```

2. (Opzionale) Esegui il container a livello locale.

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

Sicurezza in Amazon Elastic Container Registry

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon ECR, consulta Servizi AWS coperti dal programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si utilizza Amazon ECR. Gli argomenti seguenti descrivono come configurare Amazon ECR per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon ECR.

Argomenti

Identity and Access Management per Amazon Elastic Container Registry

AWS Identity and Access Management (IAM) è un servizio Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi è

autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) a utilizzare risorse Amazon ECR. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon ECR.

Utente del servizio: se utilizzi il servizio Amazon ECR per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di caratteristiche Amazon ECR utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in Amazon ECR, consulta Risoluzione dei problemi di Identity and Access Management per Amazon Elastic Container Registry.

Amministratore del servizio: se sei il responsabile delle risorse Amazon ECR presso la tua azienda, probabilmente disponi dell'accesso completo a Amazon ECR. Il compito dell'utente è determinare le funzionalità e le risorse di Amazon ECR a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon ECR, consulta Come funziona Amazon Elastic Container Registry con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti essere interessato a ottenere informazioni su come scrivere policy per gestire l'accesso a Amazon ECR. Per visualizzare policy basate su identità Amazon ECR di esempio che possono essere utilizzate in IAM, consulta Esempi di policy basate su Identità di Amazon Elastic Container Registry.

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane.

Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene

autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli

collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon Elastic Container Registry con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon ECR, è necessario comprendere quali funzioni IAM sono disponibili per l'uso con Amazon ECR. Per avere una visione di alto livello di come Amazon ECR e altri AWS servizi funzionano con IAM, consulta AWS Services That Work with IAM nella IAM User Guide.

Argomenti

- Policy basate su Identità Amazon ECR
- Policy basate sulle risorse Amazon ECR
- Autorizzazione basata sui tag Amazon ECR
- Ruoli IAM Amazon ECR

Policy basate su Identità Amazon ECR

Con le policy basate su identità di IAM, è possibile specificare quali azioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le azioni sono consentite o rifiutate. Amazon ECR supporta specifiche operazioni, risorse e chiavi di condizione. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le operazioni delle policy in Amazon ECR utilizzano il seguente prefisso prima dell'operazione: `ecr:`. Ad esempio, per concedere a qualcuno l'autorizzazione per creare un repository ECR mediante l'operazione API `CreateRepository` Amazon ECR, includi l'operazione `ecr:CreateRepository` nella policy. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Amazon ECR definisce un proprio set di operazioni che descrivono le attività che puoi eseguire con quel servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "ecr:action1",
      "ecr:action2"
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "ecr:Describe*"
```

Per visualizzare un elenco di operazioni Amazon ECR, consulta Operazioni, risorse e chiavi di condizione per Amazon Elastic Container Registry nella Guida per l'utente di IAM.

Risorse

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

La risorsa del repository Amazon ECR dispone del seguente ARN:

```
arn:${Partition}:ecr:${Region}:${Account}:repository/${Repository-name}
```

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Ad esempio, per specificare il repository `my-repo` nella regione `us-east-1` nell'istruzione, utilizza il seguente ARN:

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
```

Per specificare tutti i repository che appartengono a un account specifico, utilizza il carattere jolly (*):

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/*"
```

Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

```
"Resource": [
      "resource1",
```

```
        "resource2"
```

Per visualizzare un elenco dei tipi di risorse Amazon ECR e dei relativi ARN, consultare Risorse definite da Amazon Elastic Container Registry nella Guida per l'utente di IAM. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consultare Operazioni definite da Amazon Elastic Container Registry.

Chiavi di condizione

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Amazon ECR definisce il proprio set di chiavi di condizione e supporta anche l'uso di alcune chiavi di condizione globali. Per vedere tutte le chiavi di condizione AWS globali, consulta AWS Global Condition Context Keys nella Guida per l'utente IAM.

La maggior parte delle operazioni di Amazon ECR supporta le chiavi di condizione `aws:ResourceTag` e `ecr:ResourceTag`. Per ulteriori informazioni, consulta Uso del controllo degli accessi basato su tag.

Per visualizzare un elenco di chiavi di condizione Amazon ECR, consulta Chiave di condizione definita da Amazon Elastic Container Registry nella Guida per l'utente di IAM. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consultare Operazioni definite da Amazon Elastic Container Registry.

Esempi

Per visualizzare esempi di policy basate su identità Amazon ECR, consultare Esempi di policy basate su Identità di Amazon Elastic Container Registry.

Policy basate sulle risorse Amazon ECR

Le policy basate su risorse sono documenti di policy JSON che specificano le operazioni che possono essere eseguite da un'entità principale specificata su una risorsa Amazon ECR e in base a quali condizioni. Amazon ECR supporta policy di autorizzazione basate sulle risorse per i repository Amazon ECR. Le policy basate su risorse consentono di concedere l'autorizzazione all'utilizzo ad altri account per ogni risorsa. Puoi inoltre utilizzare una policy basata su risorse per consentire a un servizio AWS di accedere ai repository Amazon ECR.

Per consentire l'accesso a più account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata su risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa si trovano in AWS account diversi, è inoltre necessario concedere all'entità principale l'autorizzazione ad accedere alla risorsa. Concedi l'autorizzazione collegando una policy basata sull'identità all'entità. Tuttavia, se una policy basata su risorse concede l'accesso a un'entità principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Il servizio Amazon ECR supporta solo un tipo di policy basata su risorse detta policy di repository, che è collegata a un repository. Questa policy definisce quali entità principali (account, utenti, ruoli e utenti federati) possono eseguire operazioni sul repository. Per informazioni su come collegare una policy basata su risorse a un repository, consulta Policy del repository privato.

> **Note**
>
> In una politica di repository Amazon ECR, l'elemento della policy `Sid` supporta caratteri e spaziature aggiuntivi non supportati nelle policy IAM.

Esempi

Per visualizzare esempi di policy basate su risorse Amazon ECR, consulta Esempi di policy di repository privati.

Autorizzazione basata sui tag Amazon ECR

Puoi collegare i tag alle risorse Amazon ECR o inoltrarli in una richiesta ad Amazon ECR. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `ecr:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Per ulteriori informazioni sul tagging delle risorse di Amazon ECR, consultare Tagging di un repository privato.

Per visualizzare una policy basata sulle identità di esempio per limitare l'accesso a una risorsa basata su tag su tale risorsa, consulta Uso del controllo degli accessi basato su tag.

Ruoli IAM Amazon ECR

Un ruolo IAM è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Amazon ECR

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Ottieni credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo. GetFederationToken

Amazon ECR supporta l'uso di credenziali temporanee.

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Amazon ECR supporta i ruoli collegati ai servizi. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon ECR.

AWS politiche gestite per Amazon Elastic Container Registry

Amazon ECR fornisce diverse policy gestite che puoi collegare agli utenti IAM o alle istanze Amazon EC2. Queste policy consentono diversi livelli di controllo sull'accesso alle risorse Amazon ECR e alle

operazioni API. Puoi applicare queste policy direttamente oppure utilizzarle come punto di partenza per la creazione di tue policy. Per ulteriori informazioni su ciascuna operazione API citata in queste policy, consulta Actions (Operazioni) nella documentazione di riferimento alle API Amazon Elastic Container Registry.

Argomenti

- AmazonEC2ContainerRegistryFullAccess
- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryReadOnly
- AWSECRPullThroughCache_ServiceRolePolicy
- ECRReplicationServiceRolePolicy
- Aggiornamenti di Amazon ECR alle politiche AWS gestite

`AmazonEC2ContainerRegistryFullAccess`

È possibile allegare la policy `AmazonEC2ContainerRegistryFullAccess`alle identità IAM.

È possibile utilizzare questa policy gestita come punto di partenza per creare la propria policy IAM in base a requisiti specifici. Ad esempio, puoi creare una policy specifica per fornire un a utente o a un ruolo con l'accesso amministratore completo per gestire l'utilizzo di Amazon ECR. La caratteristica Policy del ciclo di vita Amazon ECR consente ai clienti di specificare la gestione del ciclo di vita di immagini in un repository. Gli eventi relativi alle politiche del ciclo di vita vengono segnalati come eventi. CloudTrail Amazon ECR è integrato AWS CloudTrail in modo da poter visualizzare gli eventi delle politiche del ciclo di vita direttamente nella console Amazon ECR. La policy IAM gestita `AmazonEC2ContainerRegistryFullAccess` include l'autorizzazione `cloudtrail:LookupEvents` per facilitare questo comportamento.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `ecr`: consente alle entità principali l'accesso completo a tutte le API di Amazon ECR.
- `cloudtrail`— Consente ai responsabili di cercare eventi di gestione o eventi AWS CloudTrail Insights acquisiti da. CloudTrail

La policy `AmazonEC2ContainerRegistryFullAccess` è la seguente.

```
{
    "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

È possibile allegare la policy `AmazonEC2ContainerRegistryPowerUser`alle identità IAM.

Questa policy concede le autorizzazioni amministrative che consentono agli utenti IAM di leggere e scrivere nei repository, ma non permette né di eliminare i repository né di modificare i documenti di policy ad essi applicati.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `ecr`: consente alle entità principali di leggere e scrivere nei repository, nonché di leggere le policy sul ciclo di vita. Alle entità principali non viene concessa l'autorizzazione per eliminare i repository o modificare le policy relative al ciclo di vita applicate ad essi.

La policy `AmazonEC2ContainerRegistryPowerUser` è la seguente.

```
{
    "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

È possibile allegare la policy `AmazonEC2ContainerRegistryReadOnly`alle identità IAM.

Questa policy concede le autorizzazioni che consentono l'accesso in sola lettura ad Amazon ECR. Ciò include la possibilità di elencare repository e immagini all'interno dei repository. Include anche la possibilità di estrarre immagini da Amazon ECR con la CLI di Docker.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `ecr`: consente alle entità principali di leggere i repository e le rispettive policy relative al ciclo di vita.

La policy `AmazonEC2ContainerRegistryReadOnly` è la seguente.

```
{
    "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

Non è possibile attribuire la policy IAM gestita `AWSECRPullThroughCache_ServiceRolePolicy` alle entità IAM. Questa policy è collegata a un ruolo collegato al servizio che consente ad Amazon ECR di inviare immagini nei repository attraverso il flusso di lavoro della cache pull-through. Per ulteriori informazioni, consulta Ruolo collegato ai servizi Amazon ECR per la cache pull-through.

ECRReplicationServiceRolePolicy

Non è possibile attribuire la policy IAM gestita `ECRReplicationServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente ad Amazon ECR di

eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon ECR.

Aggiornamenti di Amazon ECR alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon ECR dal momento in cui questo servizio ha iniziato a tracciare queste modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivere il feed RSS nella pagina di Cronologia dei documenti di Amazon ECR.

Modifica	Descrizione	Data
AWSECRPullThroughCache_ServiceRolePolicy: aggiornamento a una policy esistente	Amazon ECR ha aggiunto nuove autorizzazioni alla policy `AWSECRPullThroughCache_ServiceRolePolicy` . Queste autorizzazioni consentono ad Amazon ECR di recuperare i contenuti crittografati di un segreto di Secrets Manager. Ciò è necessario quando utilizzi una regola di cache pull-through per memorizzare nella cache le immagini da un registro upstream che richiede l'autenticazione.	15 novembre 2023
AWSECRPullThroughCache_ServiceRolePolicy: nuova policy	Amazon ECR ha aggiunto una nuova policy. Questa policy è associata al ruolo `AWSServiceRoleForECRPullThroughCache` collegato al servizio per la funzione di cache pull-through.	29 novembre 2021

Modifica	Descrizione	Data
ECRReplicationServiceRolePolicy: nuova politica	Amazon ECR ha aggiunto una nuova policy. Questa policy è associata al ruolo `AWSServiceRoleForECRReplication` collegato al servizio per la funzione di replica.	4 dicembre 2020
AmazonEC2 ContainerRegistryFullAccess — Aggiornamento a una politica esistente	Amazon ECR ha aggiunto nuove autorizzazioni alla policy `AmazonEC2ContainerRegistryFullAccess` . Queste autorizzazioni consentono alle entità principali di creare il ruolo collegato ai servizi Amazon ECR.	4 dicembre 2020
AmazonEC2 ContainerRegistryReadOnly — Aggiornamento a una politica esistente	Amazon ECR ha aggiunto nuove autorizzazioni alla policy `AmazonEC2ContainerRegistryReadOnly` che consentono alle entità principali di leggere le policy del ciclo di vita, elencare i tag e descrivere i risultati della scansione delle immagini.	10 dicembre 2019

Modifica	Descrizione	Data
AmazonEC2 Container RegistryPowerUser — Aggiornamento a una politica esistente	Amazon ECR ha aggiunto nuove autorizzazioni alla policy `AmazonEC2 ContainerRegistryP owerUser` . Consentono alle entità principali di leggere le policy del ciclo di vita, elencare i tag e descrivere i risultati della scansione delle immagini.	10 dicembre 2019
AmazonEC2 Container RegistryFullAccess — Aggiornamento a una politica esistente	Amazon ECR ha aggiunto nuove autorizzazioni alla policy `AmazonEC2 ContainerRegistryF ullAccess` . Consentono ai responsabili di cercare eventi di gestione o eventi AWS CloudTrail Insights acquisiti da. CloudTrail	10 Novembre 2017
AmazonEC2 Container RegistryReadOnly: aggiornam ento a una politica esistente	Amazon ECR ha aggiunto nuove autorizzazioni alla policy `AmazonEC2 ContainerRegistryR eadOnly` . Consentono alle entità principali di descrivere le immagini Amazon ECR.	11 ottobre 2016

Modifica	Descrizione	Data
AmazonEC2 Container RegistryPowerUser — Aggiornamento a una politica esistente	Amazon ECR ha aggiunto nuove autorizzazioni alla policy `AmazonEC2 ContainerRegistryP owerUser` . Consentono alle entità principali di descrivere le immagini Amazon ECR.	11 ottobre 2016
AmazonEC2 Container RegistryReadOnly — Nuova politica	Amazon ECR ha aggiunto una nuova policy che concede autorizzazioni di sola lettura ad Amazon ECR. Queste autorizzazioni prevedono la possibilità di elencare repository e immagini all'inter no dei repository. Prevedono anche la possibilità di estrarre immagini da Amazon ECR con la CLI di Docker.	21 dicembre 2015
AmazonEC2 Container RegistryPowerUser — Nuova politica	Amazon ECR ha aggiunto una nuova policy che concede autorizzazioni amministr ative che consentono agli utenti di leggere e scrivere nei repository, ma non consente né di eliminare i repository né di modificare i documenti di policy ad essi applicati.	21 dicembre 2015
AmazonEC2 Container RegistryFullAccess — Nuova politica	Amazon ECR ha aggiunto una nuova policy. Questa policy consente l'accesso completo ad Amazon ECR.	21 dicembre 2015

Modifica	Descrizione	Data
Amazon ECR ha iniziato a monitorare le modifiche	Amazon ECR ha iniziato a tracciare le modifiche per le policy AWS gestite.	24 giugno 2021

Utilizzo di ruoli collegati ai servizi per Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) AWS Identity and Access Management utilizza ruoli collegati ai servizi (IAM) per fornire le autorizzazioni necessarie per utilizzare le funzionalità di replica e pull through cache. Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente ad Amazon ECR. Il ruolo collegato ai servizi è predefinito da Amazon ECR. Include tutte le autorizzazioni richieste dal servizio per supportare le funzionalità di replica e cache pull-through per il registro privato. Dopo avere configurato la replica o la cache pull-through per il registro, viene creato automaticamente un ruolo collegato al servizio per conto dell'utente. Per ulteriori informazioni, consulta Impostazioni dei registri privati.

Un ruolo collegato ai servizi semplifica la configurazione della replica e della cace pull-trough con Amazon ECR. Ciò avviene perché, utilizzandolo, non sarà più necessario aggiungere manualmente tutte le autorizzazioni necessarie. Amazon ECR definisce le autorizzazioni del ruolo associato ai servizi e, salvo diversamente definito, solo Amazon ECR può assumere il ruolo. Le autorizzazioni definite includono policy di attendibilità e di autorizzazioni. Le policy di autorizzazioni non possono essere collegate a nessun'altra entità IAM.

Puoi eliminare il ruolo collegato ai servizi corrispondente solo dopo avere disabilitato la replica o la cache pull-trough nel registro. Ciò garantisce che l'utente non rimuova inavvertitamente le autorizzazioni richieste da Amazon ECR per queste funzionalità.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi consulta Servizi AWS che funzionano con IAM. In questa pagina collegata, cerca i servizi che hanno Yes (Sì) nella colonna Service-Linked Role (Ruolo collegato ai servizi). Scegli un link Yes (Sì) per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Argomenti

- Regioni supportate per i ruoli collegati ai servizi di Amazon ECR
- Ruolo collegato ai servizi Amazon ECR per la replica
- Ruolo collegato ai servizi Amazon ECR per la cache pull-through

Regioni supportate per i ruoli collegati ai servizi di Amazon ECR

Amazon ECR supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio Amazon ECR è disponibile. Per ulteriori informazioni sulla disponibilità delle regioni di Amazon ECR, consulta Regioni ed endpoint AWS.

Ruolo collegato ai servizi Amazon ECR per la replica

Autorizzazioni del ruolo collegato ai servizi per Amazon ECR

Amazon ECR utilizza ruoli collegati ai servizi denominati: AWSServiceRoleForECRReplicationconsente ad Amazon ECR di replicare le immagini su più account.

Il ruolo AWSServiceRoleForECRReplication collegato ai servizi si affida ai seguenti servizi per l'assunzione del ruolo:

- `replication.ecr.amazonaws.com`

La seguente policy delle autorizzazioni del ruolo `ECRReplicationServiceRolePolicy` consente ad Amazon ECR di eseguire le operazioni seguenti su tutte le risorse:

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

> **Note**
>
> La `ReplicateImage` è un'API interna utilizzata da Amazon ECR per la replica e non può essere chiamata direttamente.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Amazon ECR

Non devi creare manualmente il ruolo collegato al servizio Amazon ECR. Quando configuri le impostazioni di replica per il tuo registro nell'API AWS Management Console AWS CLI, nell'o nell' AWS API, Amazon ECR crea il ruolo collegato al servizio per te.

Se elimini questo ruolo collegato ai servizi e devi ricrearlo di nuovo, puoi utilizzare lo stesso processo per ricreare il ruolo nel tuo account. Quando si configurano le impostazioni di replica per il registro, Amazon ECR crea il ruolo collegato ai servizi per l'utente.

Modifica di un ruolo collegato ai servizi per Amazon ECR

Amazon ECR non consente la modifica manuale del ruolo collegato al AWSServiceRoleForECRReplication servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Amazon ECR

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, prima di poter eliminare manualmente il ruolo collegato ai servizi, è necessario rimuovere la configurazione della replica per il registro in ogni regione.

> **Note**
>
> Se provi a eliminare risorse mentre il servizio Amazon ECR utilizza ancora i ruoli, l'operazione di eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e riprova.

Per eliminare le risorse Amazon ECR utilizzate da AWSServiceRoleForECRReplication

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.

2. Dalla barra di navigazione, scegli la regione in cui configurare le impostazioni di replica.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato).
4. Nella pagina Private registry (Registro privato), nella sezione Replication configuration (Configurazione di replica) scegli Edit (Modifica).
5. Per eliminare tutte le regole di replica, scegli Delete all (Elimina tutto). Questo passaggio richiede una conferma.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForECRReplicationservizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Ruolo collegato ai servizi Amazon ECR per la cache pull-through

Amazon ECR utilizza un ruolo collegato al servizio denominato AWSServiceRoleForECRPullThroughCacheche autorizza Amazon ECR a eseguire azioni per tuo conto per completare le azioni pull through cache. Per ulteriori informazioni sulla cache pull-through, consulta Utilizzo delle regole della cache pull-through.

Autorizzazioni del ruolo collegato ai servizi per Amazon ECR

Il ruolo AWSServiceRoleForECRPullThroughCachecollegato al servizio si affida al seguente servizio per l'assunzione del ruolo.

- `pullthroughcache.ecr.amazonaws.com`

Dettagli dell'autorizzazione

La policy delle autorizzazioni `AWSECRPullThroughCache_ServiceRolePolicy` è attribuita al ruolo collegato ai servizi. Questa policy gestita concede ad Amazon ECR l'autorizzazione all'esecuzione delle operazioni seguenti. Per ulteriori informazioni, consulta `AWSECRPullThroughCache_ServiceRolePolicy`.

- `ecr`: consente al servizio Amazon ECR di inviare immagini a un repository privato.
- `secretsmanager:GetSecretValue`— Consente al servizio Amazon ECR di recuperare i contenuti crittografati di un AWS Secrets Manager segreto. Ciò è necessario quando utilizzi una

regola di cache pull-through per memorizzare nella cache le immagini da un registro upstream che richiede l'autenticazione nel tuo registro privato. Questa autorizzazione è valida solo per i segreti con il prefisso di nome `ecr-pullthroughcache/`.

La policy `AWSECRPullThroughCache_ServiceRolePolicy` contiene il JSON seguente.

```
{
    "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}"
                }
            }
        }
    ]
}
```

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Amazon ECR

Non devi creare manualmente il ruolo collegato al servizio Amazon ECR per la cache pull-trough. Quando crei una regola pull through cache per il tuo registro privato nell'API AWS Management Console, nell' AWS CLI o nell' AWS API, Amazon ECR crea il ruolo collegato al servizio per te.

Se elimini questo ruolo collegato ai servizi e devi ricrearlo di nuovo, puoi utilizzare lo stesso processo per ricreare il ruolo nel tuo account. Quando crei una regola di cache pull-through per il tuo registro privato, Amazon ECR crea il ruolo collegato ai servizi per te se non esiste già.

Modifica di un ruolo collegato ai servizi per Amazon ECR

Amazon ECR non consente la modifica manuale del ruolo collegato al AWSServiceRoleForECRPullThroughCacheservizio. Dopo aver creato un ruolo collegato ai servizi, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Tuttavia, utilizzando IAM è possibile modificarne la descrizione. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Amazon ECR

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, prima di poter eliminare manualmente il ruolo collegato ai servizi, è necessario eliminare le regole della cache pull-through per il registro in ogni regione.

> **Note**
>
> Se provi a eliminare risorse mentre il servizio Amazon ECR utilizza ancora il ruolo, l'operazione di eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e riprova.

Per eliminare le risorse Amazon ECR utilizzate dal ruolo collegato ai servizi AWSServiceRoleForECRPullThroughCache

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Nella barra di navigazione, seleziona la regione in cui vengono create le regole della cache pull-through.
3. Nel pannello di navigazione, seleziona Private registry (Registro privato).

4. Nella pagina Private registry (Registro privato), nella sezione Pull through cache configuration (Configurazione di cache pull through) scegli Edit (Modifica).
5. Per ogni regola di cache pull through che hai creato, seleziona la regola e quindi scegli Delete rule (Elimina regola).

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, l'o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForECRPullThroughCacheservizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel frattempo AWS, l'impersonificazione tra servizi può portare al confuso problema del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Ti consigliamo di utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` o `aws:SourceAccount` nelle policy delle risorse per limitare le autorizzazioni con cui Amazon ECR fornisce un altro servizio alla risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Se non conosci l'ARN completo della risorsa o scegli più risorse, utilizza la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (`*`) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:`*`servicename`*`:`*`region`*`:`*`123456789012`*`:*`.

Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un ARN di un bucket Amazon S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni.

Il valore di `aws:SourceArn` deve essere ResourceDescription.

L'esempio seguente mostra come utilizzare le chiavi di contesto della `aws:SourceArn` condizione `aws:SourceAccount` globale in una policy di repository Amazon ECR per consentire AWS CodeBuild l'accesso alle azioni dell'API Amazon ECR necessarie per l'integrazione con quel servizio, evitando al contempo il confuso problema del vice.

```
{
   "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"
            }
         }
      }
   ]
}
```

Esempi di policy basate su Identità di Amazon Elastic Container Registry

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Amazon ECR. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o API. AWS Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Amazon ECS, incluso il formato degli ARN per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon Elastic Container Service Registry nella Guida di riferimento per l'autorizzazione del servizio.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Argomenti

Best practice delle policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon ECR nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando

SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Amazon ECR

Per accedere alla console Amazon Elastic Container Registry, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon ECR nel tuo AWS account. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Per garantire che tali entità possano ancora utilizzare la console Amazon ECR, aggiungi la policy `AmazonEC2ContainerRegistryReadOnly` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di 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": "*"
        }
    ]
}
```

Non è necessario consentire autorizzazioni minime di console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, puoi accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consenti agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI 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": "*"
        }
    ]
}
```

Accesso a un repository Amazon ECR

In questo esempio, vuoi concedere a un utente del tuo AWS account l'accesso a uno dei tuoi repository Amazon ECR,. `my-repo` Si desidera anche consentire all'utente di inviare, estrarre ed elencare le immagini.

```
{
   "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"
      }
   ]
}
```

Uso del controllo degli accessi basato su tag

L'azione dell' CreateRepository API Amazon ECR consente di specificare i tag quando si crea il repository. Per ulteriori informazioni, consulta Tagging di un repository privato.

Per consentire agli utenti di applicare tag ai repository durante la creazione, essi devono disporre delle autorizzazioni per utilizzare l'operazione che crea la risorsa, ad esempio `ecr:CreateRepository`. Se i tag vengono specificati nell'azione di creazione delle risorse, Amazon esegue autorizzazioni aggiuntive per l'azione `ecr:CreateRepository` per verificare se gli utenti dispongono delle autorizzazioni per creare tag.

Puoi utilizzare il controllo degli accessi basato su tag tramite le policy IAM. Di seguito vengono mostrati gli esempi.

La policy seguente consente a un utente di creare o di applicare un tag a un repository come `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 policy seguente consente a un utente l'accesso a tutti i repository a meno che a tali repository non siano stati aggiunti tag come `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"
                }
            }
        }
    ]
}
```

Risoluzione dei problemi di Identity and Access Management per Amazon Elastic Container Registry

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Amazon ECR e IAM.

Argomenti

- Non sono autorizzato a eseguire un'operazione in Amazon ECR
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon ECR

Non sono autorizzato a eseguire un'operazione in Amazon ECR

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `ecr:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ecr:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `ecr:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, dovrai aggiornare le policy in modo da poter passare un ruolo ad Amazon ECR.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in Amazon ECR. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon ECR

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon ECR supporta queste caratteristiche, consultare Come funziona Amazon Elastic Container Registry con IAM.
- Per scoprire come fornire l'accesso alle tue risorse su Account AWS risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.

- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Protezione dei dati in Amazon ECR

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in Amazon Elastic Container Service. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Questi contenuti includono la configurazione della protezione e le attività di gestione per i servizi Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon ECS o altro Servizi AWS utilizzando la console, l'API o gli AWS SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Argomenti

Crittografia dei dati a riposo

Amazon ECR memorizza le immagini nei bucket Amazon S3 gestiti da Amazon ECR. Per impostazione predefinita, Amazon ECR utilizza la crittografia lato server con chiavi di crittografia gestite da Amazon S3 che crittografano i dati a riposo utilizzando un algoritmo di crittografia AES-256. Ciò non richiede alcuna operazione da parte tua e viene offerto senza costi aggiuntivi. Per ulteriori informazioni, consulta Protezione dei dati mediante la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3) nella Guida per l'utente di Amazon Simple Storage Service.

Per un maggiore controllo sulla crittografia per i tuoi repository Amazon ECR, puoi utilizzare la crittografia lato server con chiavi KMS archiviate in (). AWS Key Management Service AWS KMS Quando si utilizza AWS KMS per crittografare i dati, è possibile utilizzare l'impostazione predefinita Chiave gestita da AWS, gestita da Amazon ECR, o specificare la propria chiave KMS (denominata chiave gestita dal cliente). Per ulteriori informazioni, consulta Protezione dei dati utilizzando la crittografia lato server con chiavi KMS archiviate in AWS KMS (SSE-KMS) nella Guida per l'utente di Amazon Simple Storage Service.

Ogni repository Amazon ECR dispone di una configurazione di crittografia che viene impostata al momento della creazione del repository. È possibile utilizzare configurazioni di crittografia diverse su ciascun repository. Per ulteriori informazioni, consulta Creazione di un repository privato.

Quando viene creato un repository con la AWS KMS crittografia abilitata, viene utilizzata una chiave KMS per crittografare i contenuti del repository. Inoltre, Amazon ECR aggiunge una AWS KMS sovvenzione alla chiave KMS con l'archivio Amazon ECR come beneficiario principale.

Di seguito vengono fornite informazioni di alto livello su come Amazon ECR è integrato con AWS KMS per crittografare e decrittografare i repository:

1. Durante la creazione di un repository, Amazon ECR invia una DescribeKeychiamata a per AWS KMS convalidare e recuperare l'Amazon Resource Name (ARN) della chiave KMS specificata nella configurazione di crittografia.
2. Amazon ECR invia due CreateGrantrichieste per AWS KMS creare sovvenzioni sulla chiave KMS per consentire ad Amazon ECR di crittografare e decrittografare i dati utilizzando la chiave dati.
3. Quando si invia un'immagine, viene effettuata una GenerateDataKeyrichiesta AWS KMS che specifica la chiave KMS da utilizzare per crittografare il livello di immagine e il manifesto.
4. AWS KMS genera una nuova chiave dati, la cripta con la chiave KMS specificata e invia la chiave di dati crittografata da archiviare con i metadati del livello di immagine e il manifesto dell'immagine.
5. Quando si estrae un'immagine, viene effettuata una richiesta Decrypt a AWS KMS, specificando la chiave di dati crittografata.
6. AWS KMS decrittografa la chiave dati crittografata e invia la chiave dati decrittografata ad Amazon S3.
7. La chiave dati viene utilizzata per decrittografare il livello immagine prima che il livello immagine venga estratto.
8. Quando un repository viene eliminato, Amazon ECR invia due RetireGrantrichieste per AWS KMS ritirare le sovvenzioni create per il repository.

Considerazioni

Quando si utilizza la AWS KMS crittografia con Amazon ECR, è necessario considerare i seguenti punti.

- Se crei il tuo repository Amazon ECR con crittografia KMS e non specifichi una chiave KMS, Amazon ECR utilizza un alias Chiave gestita da AWS con l'alias per impostazione predefinita. `aws/ecr` Questa chiave KMS viene creata nel tuo account la prima volta che crei un repository con la crittografia KMS abilitata.
- Quando si utilizza la crittografia KMS con la propria chiave KMS, la chiave deve esistere nella stessa regione del repository.
- Le autorizzazioni che Amazon ECR crea per tuo conto non devono essere revocate. Se revochi la concessione che autorizza Amazon ECR a utilizzare AWS KMS le chiavi del tuo account, Amazon ECR non può accedere a questi dati, crittografare le nuove immagini inserite nel repository o

decrittografarle quando vengono estratte. Quando revochi una concessione per Amazon ECR, la modifica avviene immediatamente. Per revocare i diritti di accesso, eliminare il repository piuttosto che revocare la concessione. Quando un repository viene eliminato, Amazon ECR ritira le concessioni per tuo conto.

- L'utilizzo delle chiavi comporta AWS KMS un costo. Per ulteriori informazioni, consultare Prezzi di AWS Key Management Service.

Autorizzazioni IAM richieste

Quando crei o elimini un repository Amazon ECR con crittografia lato server utilizzando AWS KMS, le autorizzazioni richieste dipendono dalla chiave KMS specifica in uso.

Autorizzazioni IAM richieste Chiave gestita da AWS per l'utilizzo di Amazon ECR

Per impostazione predefinita, quando AWS KMS la crittografia è abilitata per un repository Amazon ECR ma non viene specificata alcuna chiave KMS, viene utilizzata la per Chiave gestita da AWS Amazon ECR. Quando la chiave KMS AWS gestita per Amazon ECR viene utilizzata per crittografare un repository, qualsiasi principale autorizzato a creare un repository può anche abilitare la crittografia sul repository. AWS KMS Tuttavia, l'entità principale IAM che elimina il repository deve disporre dell'autorizzazione `kms:RetireGrant`. Ciò consente il ritiro delle sovvenzioni che sono state aggiunte alla chiave al momento della creazione del repository. AWS KMS

La seguente policy IAM di esempio può essere aggiunta come policy inline a un utente per assicurarsi che questi disponga delle autorizzazioni minime necessarie per eliminare un repository per cui è attivata la crittografia. La chiave KMS utilizzata per crittografare il repository può essere specificata utilizzando il parametro della risorsa.

```
{
    "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"
```

```
        }
    ]
}
```

Autorizzazioni IAM richieste quando si utilizza una chiave gestita dal cliente

Quando si crea un repository con AWS KMS crittografia abilitata utilizzando una chiave gestita dal cliente, sono necessarie le autorizzazioni sia per la keypolicy KMS che per la policy IAM per l'utente o il ruolo che crea il repository.

Quando crei la tua chiave KMS, puoi utilizzare la chiave predefinita creata dalla policy AWS KMS o puoi specificare un'icona personalizzata. Per garantire che la chiave gestita dal cliente rimanga gestibile dal proprietario dell'account, la politica chiave per la chiave KMS dovrebbe consentire tutte le AWS KMS azioni all'utente root dell'account. Puoi aggiungere ulteriori autorizzazioni con ambito alle policy chiave, ma almeno all'utente root devono essere concesse autorizzazioni per gestire la chiave KMS. Per consentire l'utilizzo della chiave KMS solo per le richieste che provengono da Amazon ECR, puoi utilizzare la chiave kms: ViaService condition con il valore. `ecr.<region>.amazonaws.com`

L'esempio seguente di policy chiave fornisce all' AWS account (utente root) che possiede la chiave KMS l'accesso completo alla chiave KMS. Per ulteriori informazioni su questa policy chiave di esempio, consulta Consente l'accesso all' AWS account e abilita le politiche IAM nella AWS Key Management Service Developer Guide.

```
{
    "Version": "2012-10-17",
    "Id": "ecr-key-policy",
    "Statement": [
        {
            "Sid": "EnableIAMUserPermissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

L'utente IAM, il ruolo IAM o l' AWS account che crea i tuoi repository deve disporre dell'`kms:DescribeKey`autorizzazione e `kms:CreateGrant``kms:RetireGrant`, oltre alle autorizzazioni Amazon ECR necessarie.

> **Note**
>
> L'autorizzazione `kms:RetireGrant` deve essere aggiunta alla policy IAM dell'utente o del ruolo che crea il repository. Le autorizzazioni `kms:CreateGrant` e `kms:DescribeKey` possono essere aggiunte alla policy delle chiave per la chiave KMS o alla policy IAM dell'utente o del ruolo che creano il repository. Per ulteriori informazioni su come funzionano le AWS KMS autorizzazioni, consulta Autorizzazioni AWS KMS API: riferimento alle azioni e alle risorse nella Guida per gli sviluppatori.AWS Key Management Service

La seguente policy IAM di esempio può essere aggiunta come policy inline a un utente per assicurarsi che questi disponga delle autorizzazioni minime necessarie per creare un repository per cui è attivata la crittografia ed eliminare il repository al termine. La AWS KMS key utilizzata per crittografare il repository può essere specificata utilizzando il parametro delle risorse.

```
{
    "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"
        }
    ]
}
```

Consenti a un utente di elencare le chiavi KMS nella console durante la creazione di un repository

Quando si utilizza la console Amazon ECR per creare un repository, è possibile concedere le autorizzazioni per consentire a un utente di elencare le chiavi KMS gestite dal cliente nella regione quando si abilita la crittografia per il repository. L'esempio di policy IAM seguente illustra le autorizzazioni necessarie per elencare le chiavi e gli alias KMS quando si utilizza la console.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  }
}
```

Monitoraggio dell'interazione di Amazon ECR con AWS KMS

Puoi utilizzarlo AWS CloudTrail per tenere traccia delle richieste a cui Amazon ECR invia per tuo AWS KMS conto. Le voci di registro contenute nel CloudTrail registro contengono una chiave di contesto di crittografia per renderle più facilmente identificabili.

Contesto di crittografia di Amazon ECR

Un contesto di crittografia è un set di coppie chiave-valore che contiene dati arbitrari non segreti. Quando si include un contesto di crittografia in una richiesta di crittografia dei dati, associa AWS KMS crittograficamente il contesto di crittografia ai dati crittografati. lo stesso contesto di crittografia sia necessario per decrittografare i dati.

Nelle sue richieste GenerateDataKeye Decrypt a, AWS KMS Amazon ECR utilizza un contesto di crittografia con due coppie nome-valore che identificano il repository e il bucket Amazon S3 utilizzati. Questo viene mostrato nell'esempio seguente. I nomi non variano, ma i valori del contesto di crittografia combinati saranno diversi per ogni valore.

```
"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"
}
```

Puoi utilizzare il contesto di crittografia per identificare queste operazioni crittografiche nei record e nei log di controllo, come AWS CloudTrailAmazon CloudWatch Logs, e come condizione per l'autorizzazione nelle politiche e nelle concessioni.

Il contesto di crittografia di Amazon ECR è costituito da due coppie nome-valore.

- aws:s3:arn – La prima coppia nome-valore identifica il bucket. La chiave è `aws:s3:arn`. L'Amazon Resource Name (ARN) del bucket Amazon S3 è il valore.

  ```
  "aws:s3:arn": "ARN of an Amazon S3 bucket"
  ```

  Ad esempio, se l'ARN del bucket è `arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df`, il contesto di crittografia include la seguente coppia.

  ```
  "arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df"
  ```

- aws:ecr:arn – La seconda coppia nome-valore identifica l'Amazon Resource Name (ARN) del repository. La chiave è `aws:ecr:arn`. Il valore rappresenta l'ARN del repository.

  ```
  "aws:ecr:arn": "ARN of an Amazon ECR repository"
  ```

  Ad esempio, se l'ARN del repository è `arn:aws:ecr:us-west-2:111122223333:repository/repository-name`, il contesto di crittografia include la seguente coppia.

  ```
  "aws:ecr:arn": "arn:aws:ecr:us-west-2:111122223333:repository/repository-name"
  ```

Risoluzione dei problemi

Quando si elimina un repository Amazon ECR con la console, se il repository viene eliminato correttamente ma Amazon ECR non è in grado di ritirare le concessioni aggiunte alla chiave KMS per il repository, viene visualizzato il seguente errore.

```
The repository [{repository-name}] has been deleted successfully but the grants created
 by the kmsKey [{kms_key}] failed to be retired
```

Quando ciò si verifica, puoi ritirare tu stesso le AWS KMS sovvenzioni per il repository.

Ritirare manualmente le AWS KMS sovvenzioni per un deposito

1. Elenca le concessioni per la AWS KMS chiave utilizzata per il repository. Il valore `key-id` viene incluso nell'errore visualizzato dalla console. Puoi anche utilizzare il `list-keys` comando per elencare sia le chiavi KMS gestite dal Chiavi gestite da AWS cliente che quelle gestite dal cliente in una regione specifica del tuo account.

   ```
   aws kms list-grants \
        --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc
        --region us-west-2
   ```

   L'output include un `EncryptionContextSubset` con l'Amazon Resource Name (ARN) del repository. Questo può essere utilizzato per determinare quale concessione aggiunta alla chiave sia quella che si desidera ritirare. Il valore `GrantId` viene utilizzato quando si ritira la concessione nella fase successiva.

2. Ritira ogni concessione per la AWS KMS chiave aggiunta al repository. Sostituisci il valore per *`GrantId`*con l'ID della sovvenzione dall'output del passaggio precedente.

   ```
   aws kms retire-grant \
        --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc \
        --grant-id GrantId \
        --region us-west-2
   ```

Convalida della conformità per Amazon Elastic Container Registry

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

Sicurezza dell'infrastruttura in Amazon Elastic Container Registry

In quanto servizio gestito, Amazon Elastic Container Registry è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad Amazon ECR attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi richiamare queste operazioni API da qualsiasi posizione di rete, ma Amazon ECR non supporta le policy di accesso basate sulle risorse che possono includere limitazioni sull'indirizzo IP di origine. È inoltre possibile utilizzare le policy di Amazon ECR per controllare l'accesso da endpoint Amazon Virtual Private Cloud (Amazon VPC) o VPC specifici. In effetti, questo isola l'accesso alla rete a una determinata risorsa Amazon ECR solo dal VPC specifico all'interno della rete. AWS Per ulteriori informazioni, consulta Endpoint VPC con interfaccia Amazon ECR ()AWS PrivateLink.

Endpoint VPC con interfaccia Amazon ECR ()AWS PrivateLink

Puoi migliorare la posizione di sicurezza del VPC configurando Amazon ECR in modo che utilizzi un endpoint VPC di interfaccia. Gli endpoint VPC sono basati su una tecnologia che consente di AWS PrivateLink accedere in modo privato alle API di Amazon ECR tramite indirizzi IP privati. AWS PrivateLink limita tutto il traffico di rete tra il tuo VPC e Amazon ECR alla rete Amazon. Non è richiesto un gateway Internet, un dispositivo NAT o un gateway privato virtuale.

Per ulteriori informazioni sugli AWS PrivateLink endpoint VPC, consulta la sezione Endpoints VPC nella Amazon VPC User Guide.

Considerazioni sugli endpoint VPC di Amazon ECR

Prima di configurare gli endpoint VPC per Amazon ECR, tenere presente le considerazioni riportate di seguito:

- Per consentire alle tue attività Amazon ECS con hosting su istanze Amazon EC2 di estrarre le immagini private da Amazon ECR, assicurati di creare anche gli endpoint VPC per Amazon ECS. Per ulteriori informazioni, consulta Interface VPC Endpoints (AWS PrivateLink) nella Amazon Elastic Container Service Developer Guide.

  > **Important**
  >
  > Le attività Amazon ECS con hosting su Fargate non richiedono gli endpoint VPC dell'interfaccia Amazon ECS.

- Per sfruttare questa funzione, le attività Amazon ECS presenti su Fargate che utilizzano la versione della piattaforma Linux `1.3.0` o versioni precedenti richiedono solo l'endpoint VPC di Amazon ECR di com.amazonaws.***regione***.ecr.dkr e l'endpoint del gateway Amazon S3.
- Per sfruttare questa funzione, le attività Amazon ECS presenti su Fargate che utilizzano la versione della piattaforma Linux `1.4.0` o versioni successive richiedono sia gli endpoint VPC di Amazon ECR com.amazonaws.***regione***.ecr.dkr e com.amazonaws.***regione***.ecr.api che l'endpoint gateway Amazon S3.
- Per sfruttare questa funzione, le attività Amazon ECS presenti su Fargate che utilizzano la versione della piattaforma Windows `1.0.0` o versioni successive richiedono sia gli endpoint VPC di Amazon ECR com.amazonaws.***regione***.ecr.dkr e com.amazonaws.***regione***.ecr.api che l'endpoint gateway Amazon S3.
- Le attività Amazon ECS con hosting su Fargate che estraggono le immagini del container da Amazon ECR possono limitare l'accesso al VPC specifico utilizzato dalle attività e all'endpoint VPC utilizzato dal servizio aggiungendo le chiavi di condizione al ruolo IAM per l'attività. Per ulteriori informazioni, consulta Autorizzazioni IAM facoltative per attività Fargate che estraggono le immagini Amazon ECR su endpoint di interfaccia nella Guida per lo sviluppatore di Amazon Elastic Container.
- Le attività di Amazon ECS ospitate su Fargate che estraggono immagini di container da Amazon ECR e che utilizzano anche `awslogs` il driver di log per inviare informazioni di log a Logs richiedono l' CloudWatch CloudWatch endpoint VPC Logs. Per ulteriori informazioni, consulta Crea l'endpoint Logs CloudWatch .

- Il gruppo di sicurezza collegato all'endpoint VPC deve consentire le connessioni in entrata sulla porta 443 dalla sottorete privata del VPC.
- Gli endpoint VPC attualmente non supportano le richieste inter-Regionali. Assicurati di creare gli endpoint VPC nella stessa regione in cui prevedi di inviare le chiamate API ad Amazon ECR.
- Gli endpoint VPC al momento non supportano i repository pubblici di Amazon ECR. Prendi in considerazione l'utilizzo di una regola pull through della cache per ospitare l'immagine pubblica in un repository privato nella stessa regione dell'endpoint VPC. Per ulteriori informazioni, consulta Utilizzo delle regole della cache pull-through.
- Gli endpoint VPC supportano solo il DNS AWS fornito tramite Amazon Route 53. Se si desidera utilizzare il proprio DNS, è possibile usare l'inoltro condizionale sul DNS. Per ulteriori informazioni, consulta Set opzioni DHCP nella Guida per l'utente di Amazon VPC.
- Se i container dispongono di connessioni esistenti ad Amazon S3, le relative connessioni potrebbero essere interrotte per un breve periodo quando aggiungi l'endpoint gateway Amazon S3. Se si desidera evitare l'interruzione, creare un nuovo VPC che usi l'endpoint del gateway Amazon S3, quindi migrare il cluster Amazon ECS e i relativi container in un nuovo VPC.
- Quando un'immagine viene estratta utilizzando una regola di cache pull-through per la prima volta, se hai configurato Amazon ECR per l'utilizzo di un endpoint VPC di interfaccia tramite AWS PrivateLink , allora dovrai creare una sottorete pubblica nello stesso VPC, con un gateway NAT, quindi instradare tutto il traffico in uscita verso Internet dalla sottorete privata al gateway NAT per far funzionare il pull. Le operazioni successive di estrazione dell'immagine non richiedono questo passaggio. Per ulteriori informazioni, consulta Scenario: accesso a Internet da una sottorete privata nella Guida per l'utente di Amazon Virtual Private Cloud.

Considerazioni per le immagini Windows

Le immagini basate sul sistema operativo Windows includono artefatti con limitazioni di licenza che impediscono la distribuzione. Per impostazione predefinita, quando si inviano immagini Windows a un repository Amazon ECR, i livelli che includono questi artefatti non vengono inviati in quanto vengono considerati livelli estranei. Quando gli artefatti vengono forniti da Microsoft, i livelli estranei vengono recuperati dall'infrastruttura di Microsoft Azure. Per questo motivo, per consentire ai container di estrarre questi livelli estranei da Azure sono necessari passaggi aggiuntivi oltre alla creazione degli endpoint VPC.

È possibile sovrascrivere questo comportamento quando si inviano le immagini Windows ad Amazon ECR utilizzando il flag `--allow-nondistributable-artifacts` nel daemon Docker. Quando è

abilitato, questo flag invia i livelli concessi in licenza ad Amazon ECR, consentendo di estrarre queste immagini da Amazon ECR tramite l'endpoint VPC senza richiedere un ulteriore accesso ad Azure.

> **Important**
>
> L'utilizzo del flag `--allow-nondistributable-artifacts` non preclude l'obbligo dell'utente di rispettare i termini della licenza dell'immagine di base del container Windows; non è possibile pubblicare contenuti di Windows per la ridistribuzione pubblica o di terze parti. L'uso all'interno del proprio ambiente è consentito.

Per abilitare l'uso di questo flag per l'installazione Docker, è necessario modificare il file di configurazione del daemon Docker che, a seconda dell'installazione Docker, può in genere essere configurato nel menu delle impostazioni o delle preferenze nella sezione Docker Engine o modificando direttamente il file `C:\ProgramData\docker\config\daemon.json`.

Di seguito è illustrato un esempio della configurazione necessaria: Sostituisci il valore con l'URI del repository a cui stai inviando le immagini.

```
{
    "allow-nondistributable-artifacts": [
        "111122223333.dkr.ecr.us-west-2.amazonaws.com"
    ]
}
```

Dopo aver modificato il file di configurazione del daemon Docker, è necessario riavviare il daemon Docker prima di tentare di inviare l'immagine. Conferma che l'invio ha funzionato verificando che il livello base sia stato inviato nel repository.

> **Note**
>
> I livelli base per le immagini Windows sono grandi. Le dimensioni del livello si tradurranno in tempi più lunghi per l'invio e costi di archiviazione aggiuntivi in Amazon ECR per queste immagini. Per questi motivi, si consiglia di utilizzare questa opzione solo quando è strettamente necessaria per ridurre i tempi di costruzione e i costi di storage in corso. Ad esempio, l'immagine `mcr.microsoft.com/windows/servercore` è di circa 1,7 GiB di dimensioni quando viene compressa in Amazon ECR.

Creare gli endpoint VPC per Amazon ECR

Per creare gli endpoint VPC per Amazon ECR Service, utilizza la Creazione di un endpoint di interfaccia nella Amazon VPC User Guide.

Le attività Amazon ECS con hosting sulle istanze Amazon EC2 richiedono sia gli endpoint Amazon ECR che l'endpoint gateway Amazon S3.

Le attività Amazon ECS con hosting su Fargate che utilizzano la versione della piattaforma `1.4.0` o versioni successive richiedono sia gli endpoint VPC Amazon ECR sia gli endpoint gateway Amazon S3.

Le attività Amazon ECS con hosting su Fargate che utilizzano la versione della piattaforma `1.3.0` o versioni precedenti richiedono solo l'endpoint VPC di Amazon ECR di com.amazonaws.***regione***.ecr.dkr e gli endpoint del gateway Amazon S3.

> **Note**
>
> L'ordine in cui vengono creati gli endpoint non è rilevante.

com.amazonaws.***region***.ecr.dkr

Questo endpoint viene utilizzato per le API del registro Docker. I comandi del client Docker come `push` e `pull` utilizzano questo endpoint.

Quando si crea questo endpoint, è necessario abilitare un nome host DNS privato. Per eseguire questa operazione, accertarsi che l'opzione Enable Private DNS Name (Abilita nome DNS privato) sia selezionata nella console Amazon VPC quando si crea l'endpoint VPC.

com.amazonaws.***region***.ecr.api

> **Note**
>
> La *`regione`* specificata rappresenta l'identificatore della regione per una AWS regione supportata da Amazon ECR, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio).

Questo endpoint viene utilizzato per le chiamate all'API Amazon ECR. Operazioni API come `DescribeImages` e `CreateRepository` vanno su questo endpoint.

Quando viene creato questo endpoint, è possibile abilitare un nome host DNS privato. Abilita questo nome host selezionando Abilita nome DNS privato nella console VPC quando crei l'endpoint VPC. Se abiliti un nome host DNS privato per l'endpoint VPC, aggiorna l'SDK o AWS CLI alla versione più recente in modo che non sia necessario specificare un URL dell'endpoint quando si utilizza l'SDK o non sia necessario. AWS CLI

Se abiliti un nome host DNS privato e utilizzi un SDK o una AWS CLI versione rilasciata prima del 24 gennaio 2019, devi utilizzare il parametro per specificare gli endpoint dell'interfaccia. `--endpoint-url` Nell'esempio seguente viene illustrato il formato per l'URL dell'endpoint.

```
aws ecr create-repository --repository-name name --endpoint-url https://
api.ecr.region.amazonaws.com
```

Se non si abilita un nome host DNS privato per l'endpoint VPC, è necessario utilizzare il parametro `--endpoint-url` specificando l'ID dell'endpoint VPC per l'endpoint di interfaccia. Nell'esempio seguente viene illustrato il formato per l'URL dell'endpoint.

```
aws ecr create-repository --repository-name name --endpoint-url
 https://VPC_endpoint_ID.api.ecr.region.vpce.amazonaws.com
```

Creare l'endpoint gateway Amazon S3

Affinché le attività Amazon ECS possano estrarre immagini private da Amazon ECR, è necessario creare un endpoint gateway per Amazon S3. L'endpoint gateway è obbligatorio perché Amazon ECR utilizza Amazon S3 per archiviare i livelli di immagine. Quando i container scaricano immagini da Amazon ECR, devono accedere a Amazon ECR per ottenere il manifest dell'immagine e quindi ad Amazon S3 per scaricare i livelli effettivi dell'immagine. Di seguito è riportato l'Amazon Resource Name (ARN) del bucket Amazon S3 che contiene i livelli per ogni immagine Docker.

```
arn:aws:s3:::prod-region-starport-layer-bucket/*
```

Utilizzare la procedura Creazione di un endpoint gateway nella Amazon VPC User Guide per creare il seguente endpoint del gateway Amazon S3 per Amazon ECR. Quando crei l'endpoint, assicurati di selezionare le tabelle di routing per il VPC.

com.amazonaws.*region*.s3

L'endpoint del gateway Amazon S3 usa un documento di policy IAM per limitare l'accesso al servizio. La policy Full Access (Accesso completo) può essere utilizzata poiché qualsiasi limitazione relativa ai ruoli IAM dell'attività o ad altre policy utente IAM viene comunque applicata. Se si desidera limitare l'accesso del bucket Amazon S3 alle autorizzazioni minime richieste necessarie per utilizzare Amazon ECR, consulta Autorizzazioni minime del bucket Amazon S3 per Amazon ECR.

Autorizzazioni minime del bucket Amazon S3 per Amazon ECR

L'endpoint del gateway Amazon S3 usa un documento di policy IAM per limitare l'accesso al servizio. Per consentire solo le autorizzazioni minime del bucket Amazon S3 per Amazon ECR, limita l'accesso al bucket Amazon S3 utilizzato da Amazon ECR quando crei il documento di policy IAM per l'endpoint.

La tabella seguente descrive le autorizzazioni della policy del bucket Amazon S3 richieste da Amazon ECR.

Autorizzazione	Descrizione
`arn:aws:s3:::prod-` *`region`* `-starport-layer-bucket/*`	Fornisce l'accesso al bucket Amazon S3 contenente i livelli per ogni immagine Docker. Rappresenta l'identificatore di regione per una regione AWS supportata da Amazon ECR, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio).

Esempio

L'esempio seguente spiega come fornire l'accesso ai bucket Amazon S3 richiesti per le operazioni Amazon ECR.

```
{
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
```

```
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::prod-region-starport-layer-bucket/*"]
    }
  ]
}
```

Crea l'endpoint Logs CloudWatch

Le attività di Amazon ECS che utilizzano il tipo di avvio Fargate che utilizzano un VPC senza un gateway Internet e che utilizzano anche il driver di registro per inviare informazioni di registro CloudWatch a Logs richiedono **`awslogs`** la creazione del file com.amazonaws. endpoint VPC dell'interfaccia ***`region`*** .logs per i registri. CloudWatch Per ulteriori informazioni, consulta Using CloudWatch Logs with interface VPC endpoint nella CloudWatch Amazon Logs User Guide.

Creazione di una policy di endpoint per l'endpoint VPC di Amazon ECR

Una policy endpoint VPC è una policy della risorsa IAM che viene collegata a un endpoint durante la creazione o la modifica dell'endpoint. Se non alleghi una policy quando crei un endpoint, ti AWS allega una policy predefinita che consente l'accesso completo al servizio. Una policy endpoint non esclude né sostituisce policy dell'utente o policy specifiche del servizio. Si tratta di una policy separata per controllare l'accesso dall'endpoint al servizio specificato. Le policy endpoint devono essere scritte in formato JSON. Per ulteriori informazioni, consultare Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Ti consigliamo di creare un'unica policy di risorse IAM e di collegarla a entrambi gli endpoint VPC di Amazon ECR.

Di seguito è riportato un esempio di una policy endpoint per l'API di Amazon ECR. Questa policy consente a un ruolo IAM specifico di estrarre immagini da Amazon ECR.

```
{
 "Statement": [{
  "Sid": "AllowPull",
  "Principal": {
   "AWS": "arn:aws:iam::1234567890:role/role_name"
  },
  "Action": [
   "ecr:BatchGetImage",
```

```
    "ecr:GetDownloadUrlForLayer",
                    "ecr:GetAuthorizationToken"
   ],
   "Effect": "Allow",
   "Resource": "*"
  }]
}
```

La seguente policy endpoint di esempio impedisce l'eliminazione di un repository specificato.

```
{
 "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'esempio di policy endpoint seguente combina i due esempi precedenti in un'unica policy.

```
{
 "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": "*"
   }
  ]
}
```

Per modificare la policy endpoint VPC per Amazon ECR

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Se non hai già creato gli endpoint VPC per Amazon ECR, consulta Creare gli endpoint VPC per Amazon ECR.
4. Selezionare l'endpoint VPC di Amazon ECR a cui aggiungere una policy e scegliere la scheda Policy (Policy) nella metà inferiore della schermata.
5. Scegli Edit Policy (Modifica policy) e apporta le modifiche alla policy.
6. Selezionare Save (Salva) per salvare la policy.

Sottoreti condivise

Non puoi creare, descrivere, modificare o eliminare gli endpoint VPC nelle sottoreti condivise con te. Tuttavia, puoi utilizzare gli endpoint VPC in sottoreti condivise con te.

Monitoraggio Amazon ECR

Puoi monitorare l'uso delle API Amazon ECR con Amazon CloudWatch, che raccoglie ed elabora i dati non elaborati da Amazon ECR e li trasforma in parametri leggibili quasi in tempo reale. Queste statistiche vengono registrate per un periodo di due settimane, per permettere l'accesso a informazioni storiche e acquisire una prospettiva migliore sull'uso delle API. I dati dei parametri di Amazon ECR vengono automaticamente inviati a CloudWatch in periodi di 1 minuto. Per ulteriori informazioni su CloudWatch, consulta la Guida per l'utente di Amazon CloudWatch.

Amazon ECR fornisce i parametri basati sull'utilizzo dell'API per le azioni di autorizzazione, invio ed estrazione di immagini.

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di Amazon ECR e delle soluzioni AWS. Si consiglia di raccogliere i dati di monitoraggio dalle risorse che compongono la soluzione AWS in modo da poter eseguire più facilmente il debug di eventuali guasti in più punti. Prima di iniziare il monitoraggio di Amazon ECR è tuttavia opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

La fase successiva consiste nello stabilire una baseline per le prestazioni normali di Amazon ECR nell'ambiente, misurando le prestazioni in diversi momenti e con condizioni di carico differenti. Quando monitori Amazon ECR, archivia i dati di monitoraggio cronologici per poterli confrontare con i nuovi dati sulle prestazioni e per poter identificare i normali modelli di prestazioni e le anomalie e ideare metodi per risolvere i problemi.

Argomenti

- Parametri del repository Amazon ECR
- Eventi Amazon ECR ed EventBridge
- Registrazione delle azioni Amazon ECR con AWS CloudTrail

Visualizzazione delle quote di servizio e impostazione degli allarmi

Puoi utilizzare la console CloudWatch per visualizzare le quote di servizio e vedere un confronto dell'utilizzo corrente rispetto alle quote di servizio. Puoi anche impostare gli allarmi per ricevere una notifica quando ti avvicini a una quota.

Per visualizzare una quota di servizio e impostare facoltativamente un allarme

1. Aprire la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, selezionare Parametri.
3. Nella scheda All metrics (Tutti i parametri), scegli Usage (Utilizzo), quindi seleziona By AWS Resource (Per risorsa).

   Viene visualizzato l'elenco dei parametri di utilizzo delle quote di servizio.
4. Seleziona la casella di controllo accanto a uno dei parametri.

   Il grafico visualizza l'uso corrente di tale risorsa AWS.
5. Per aggiungere la quota di servizio al grafico, procedere come indicato di seguito:

   a. Seleziona la scheda Graphed metrics (Parametri nel grafico).

   b. Scegli Math expression (Espressione matematica), Start with an empty expression (Inizia con un'espressione vuota). Quindi nella nuova riga, in Details (Dettagli), immettere **`SERVICE_QUOTA(m1)`**.

      Una nuova riga viene aggiunta al grafico, visualizzando la quota di servizio per la risorsa rappresentata nel parametro.
6. Per visualizzare l'utilizzo corrente come una percentuale della quota, aggiungere una nuova espressione o modificare l'espressione SERVICE_QUOTA corrente. Per la nuova espressione, utilizzare **`m1/60/SERVICE_QUOTA(m1)*100`**
7. (Facoltativo) Per impostare un allarme che avvisa se ci si avvicina alla quota di servizio, procedere nel modo seguente:

a. Nella riga **`m1/60/SERVICE_QUOTA(m1)*100`**, in Actions (Operazioni), scegliere l'icona di allarme. L'aspetto è simile quello di una campana.

   Viene visualizzata la pagina di creazione dell'allarme.

b. In Conditions (Condizioni), assicurarti che Threshold type (Tipo di soglia) sia Static (Statico) e Whenever Expression1 is (Ogni volta che Expression1 è) sia impostato su Greater (Maggiore). In than (di), immetti **`80`**. Viene creato un allarme che passo nello stato ALARM quando l'utilizzo supera l'80% della quota.

c. Seleziona Successivo.

d. Nella pagina successiva, selezionare un argomento Amazon SNS o crearne uno nuovo. Questo argomento riceve una notifica quando l'allarme passa nello stato ALLARME. Quindi scegli Next (Successivo).

e. Nella pagina successiva, immetti un nome e una descrizione per l'allarme, quindi scegli Next (Avanti).

f. Scegli Crea allarme.

Parametri di utilizzo Amazon ECR

Puoi utilizzare i parametri di utilizzo di CloudWatch per fornire visibilità sull'utilizzo delle risorse del tuo account. Utilizza questi parametri per visualizzare l'uso del servizio corrente su grafici e pannelli di controllo di CloudWatch.

I parametri di utilizzo di Amazon ECR corrispondono alle Service Quotas AWS. È possibile configurare gli allarmi che avvisano quando l'uso si avvicina a una quota di servizio. Per ulteriori informazioni sulle quote di servizio per Amazon ECR, consulta Service Quotas di Amazon ECR..

Amazon ECR pubblica i seguenti parametri nello spazio dei nomi `AWS/Usage`.

Parametro	Descrizione
`CallCount`	Il numero di chiamate di operazione API dal tuo account. Le risorse sono definite dalle dimensioni associate al parametro. La statistica più utile per questo parametro è `SUM`, che rappresenta la somma dei valori di tutti i collaboratori durante il periodo definito.

Le seguenti dimensioni vengono utilizzate per perfezionare i parametri di utilizzo pubblicati da Amazon ECR.

Dimensione	Descrizione
`Service`	Il nome del servizio AWS contenente la risorsa. Per i parametri di utilizzo di Amazon ECR, il valore per questa dimensione è `ECR`.
`Type`	Il tipo di entità che viene segnalato. Attualmente, l'unico valore valido per i parametri di utilizzo Amazon ECR è `API`.
`Resource`	Il tipo di risorsa in esecuzione. Attualmente, Amazon ECR restituisce informazioni sull'utilizzo dell'API per le seguenti operazioni API. • GetAuthorizationToken • BatchCheckLayerAvailability • InitiateLayerUpload • UploadLayerPart • CompleteLayerUpload • PutImage • BatchGetImage • GetDownloadUrlForLayer
`Class`	La classe della risorsa monitorata. Attualmente, Amazon ECR non utilizza la dimensione della classe.

Report di utilizzo di Amazon ECR

AWS fornisce uno strumento gratuito per il reporting chiamato Cost Explorer, che consente di analizzare i costi e l'utilizzo delle risorse Amazon ECR.

Utilizza Cost Explorer per visualizzare i grafici relativi all'utilizzo e ai costi. Puoi visualizzare i dati degli ultimi 13 mesi e prevedere le spese per i successivi tre mesi. Puoi utilizzare Cost Explorer per vedere l'andamento della spesa sulle risorse AWS nel tempo, identificare le aree che necessitano di

maggiore attenzione e vedere le tendenze che puoi utilizzare per comprendere i costi. Puoi anche specificare intervalli di tempo per i dati e visualizzare i dati temporali per mese o per giorno.

I dati di misurazione nel report su costi e utilizzo mostrano l'utilizzo in tutti i repository Amazon ECR. Per ulteriori informazioni, consulta Tagging delle risorse per la fatturazione.

Per ulteriori informazioni sulla creazione di un report su costi e utilizzo di AWS, consulta l'argomento relativo al report su costi e utilizzo di AWS nella Guida per l'utente di AWS Billing .

Parametri del repository Amazon ECR

Amazon ECR invia i parametri del pull count del repository ad Amazon CloudWatch. I dati dei parametri di Amazon ECR vengono automaticamente inviati a CloudWatch in periodi di 1 minuto. Per ulteriori informazioni su CloudWatch, consulta la Guida per l'utente di Amazon CloudWatch.

Argomenti

Abilitazione dei parametri CloudWatch

Amazon ECR invia automaticamente i parametri del repository per tutti i repository. Non è necessario intraprendere alcuna procedura manuale.

Parametri e dimensioni disponibili

Di seguito sono elencati i parametri e le dimensioni inviati da Amazon ECR ad Amazon CloudWatch.

Parametri Amazon ECR

Amazon ECR fornisce dei parametri per monitorare i repository. È possibile misurare il numero di pull.

Il namespace `AWS/ECR` include i parametri descritti di seguito.

`RepositoryPullCount`

Il numero totale di pull per le immagini nel repository.

Dimensioni valide: `RepositoryName`.

Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma), Sample Count (Conteggio campione). La statistica più utile è somma.

Unità: numero intero

Dimensioni per i parametri Amazon ECR

I parametri di Amazon ECR utilizzano lo spazio dei nomi `AWS/ECR` e forniscono i parametri per le seguenti dimensioni.

`RepositoryName`

Questa dimensione filtra i dati richiesti per tutte le immagini del container in un repository specificato.

Visualizzazione dei parametri Amazon ECR

Puoi visualizzare i parametri di replica di Amazon ECR nella console CloudWatch. La console CloudWatch fornisce una visualizzazione dettagliata e personalizzabile delle risorse.

Visualizzazione dei parametri Amazon ECR tramite la console CloudWatch

Puoi visualizzare i parametri del repository Amazon ECR nella console CloudWatch. La console fornisce la vista più dettagliata dei parametri Amazon ECR e puoi personalizzare le visualizzazioni in base alle esigenze. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon CloudWatch.

Per visualizzare i parametri nella console di CloudWatch

1. Aprire la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, seleziona Metrics (Parametri), All metrics (Tutti i parametri).
3. Nella scheda Browse (Sfoglia), sottoAWSNamespaces, scegliECR.
4. Scegli i parametri da visualizzare. I parametri del repository vengono presi in considerazione comeECR > Parametri del repository.

Eventi Amazon ECR ed EventBridge

Amazon EventBridge ti consente di automatizzare i servizi AWS e rispondere automaticamente a eventi di sistema, come i problemi relativi alla disponibilità delle applicazioni o le modifiche delle

risorse. Gli eventi dei servizi AWS vengono recapitati a EventBridge quasi in tempo reale. Puoi scrivere regole semplici che indichino quali eventi sono considerati di interesse per te e includere le azioni automatizzate da intraprendere quando un evento corrisponde a una regola. Le azioni che possono essere attivate automaticamente includono le seguenti:

- Aggiunta di eventi ai gruppi di log in CloudWatch Logs
- Richiamo di una funzione AWS Lambda
- Richiamo del comando di esecuzione di Amazon EC2
- Inoltro dell'evento a Amazon Kinesis Data Streams
- Attivazione di una macchina a stati AWS Step Functions
- Notifica di un argomento Amazon SNS o di una coda Amazon SQS

Per ulteriori informazioni, consulta Nozioni di base di Amazon EventBridge nella Guida per l'utente di Amazon EventBridge.

Esempi di eventi da Amazon ECR

Di seguito sono riportati eventi di esempio di Amazon ECR. Gli eventi vengono emessi nel miglior modo possibile.

Evento per il push di un'immagine completata

Il seguente evento viene inviato al termine di ogni push dell'immagine. Per ulteriori informazioni, consulta Invio di un'immagine Docker.

```
{
    "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"
    }
}
```

Evento per un'azione di cache pull-through

Il seguente evento viene inviato quando viene tentata un'azione di cache pull-through. Per ulteriori informazioni, consulta Utilizzo delle regole della cache pull-through.

```
{
    "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",
    }
}
```

Evento per la scansione completa di un'immagine (scansione di base)

Quando la scansione di base è abilitata per il registro, viene inviato il seguente evento al termine di ogni scansione dell'immagine. Il parametro `finding-severity-counts` restituirà un valore per un livello di gravità solo se ne esiste uno. Ad esempio, se l'immagine non contiene risultati a livello `CRITICAL`, non viene restituito alcun conteggio critico. Per ulteriori informazioni, consulta Scansione di base.

> **Note**
>
> Per informazioni dettagliate sugli eventi emessi da Amazon Inspector quando è abilitata la scansione avanzata, consulta EventBridge eventi.

```
{
    "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": []
    }
}
```

Evento per una notifica di modifica su una risorsa con scansione avanzata abilitata (scansione avanzata)

Quando la scansione avanzata è abilitata per il registro, il seguente evento viene inviato da Amazon ECR quando si verifica una modifica con una risorsa che ha abilitato la scansione avanzata. Ciò include la creazione di nuovi repository, la modifica della frequenza di scansione di un repository o la creazione o eliminazione di immagini nei repository con la scansione avanzata abilitata. Per ulteriori informazioni, consulta Scansione delle immagini.

```
{
 "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"
 }
}
```

Evento per l'eliminazione di un'immagine

Il seguente evento viene inviato quando un'immagine viene eliminata. Per ulteriori informazioni, consulta Eliminazione di un'immagine.

```
{
    "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"
    }
}
```

Registrazione delle azioni Amazon ECR con AWS CloudTrail

Amazon ECR è integrato con AWS CloudTrail, un servizio che offre un registro delle operazioni eseguite da un utente, un ruolo o un servizio AWS in Amazon ECR. CloudTrail acquisisce le seguenti operazioni Amazon ECR come eventi:

- Tutte le chiamate API, incluse le chiamate dalla console Amazon ECR
- Tutte le operazioni intraprese a causa delle impostazioni di crittografia nei repository
- Tutte le operazioni eseguite a causa delle regole delle policy relative al ciclo di vita, incluse le operazioni riuscite e non riuscite

> **Important**
>
> A causa delle limitazioni di dimensioni dei singoli eventi CloudTrail, per le azioni delle policy del ciclo di vita in cui sono scadute 10 o più immagini, Amazon ECR invia più eventi a CloudTrail. Inoltre, Amazon ECR include un massimo di 100 tag per immagine.

Quando viene creato un percorso, è possibile abilitare la distribuzione continua di eventi CloudTrail a un bucket Amazon S3, inclusi gli eventi per Amazon ECR. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella console di CloudTrail in Cronologia eventi. Utilizzando queste informazioni, puoi determinare la richiesta effettuata ad Amazon ECR, l'indirizzo IP da cui è stata effettuata la richiesta, l'autore della richiesta, il momento in cui è stata effettuata e altri dettagli.

Per ulteriori informazioni, consulta la Guida per l'utente di AWS CloudTrail.

Informazioni su Amazon ECR in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in Amazon ECR, questa viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella Event History (Cronologia degli eventi). È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi nella cronologia degli eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account AWS, inclusi gli eventi per Amazon ECR, crea un percorso. Un percorso abilita la distribuzione da parte di CloudTrail dei file di log in un bucket Amazon S3. Quando si crea un percorso nella console, è possibile applicarlo a una singola regione o a tutte le regioni geografiche. Il trail registra gli eventi nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare e utilizzare i dati evento raccolti nei registri CloudTrail. Per ulteriori informazioni, consulta:

- Creazione di un percorso per il tuo account AWS
- Integrazioni dei servizi AWS con i registri CloudTrail
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più Regioni e Ricezione di file di log CloudTrail da più account

Tutte le operazioni API di Amazon ECR vengono registrate da CloudTrail e sono documentate nella Documentazione di riferimento delle API di Amazon Elastic Container Registry. Quando si eseguono le attività comuni, vengono generate le sezioni nei file di log CloudTrail per ogni operazione API che fa parte dell'attività. Ad esempio, quando crei un repository, vengono generate le sezioni `GetAuthorizationToken`, `CreateRepository` e `SetRepositoryPolicy` nei file di log CloudTrail. Quando esegui il push di un'immagine in un repository, vengono generate le sezioni `InitiateLayerUpload`, `UploadLayerPart`, `CompleteLayerUpload` e `PutImage`. Quando esegui il pull di un'immagine, vengono generate le sezioni `GetDownloadUrlForLayer` e `BatchGetImage`. Per esempi di attività comuni, consulta Esempi di voci di log di CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.

- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta l'elemento CloudTrail `userIdentity`.

Informazioni sulle voci del file di log Amazon ECR

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da qualsiasi origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. I file di log di CloudTrail non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

Esempi di voci di log di CloudTrail

I seguenti esempi mostrano le voci di log CloudTrail per alcune attività comuni Amazon ECR.

> **Note**
>
> Questi esempi sono stati formattati per migliorare la leggibilità. In un file di log CloudTrail, tutte le voci e gli eventi sono concatenati in una singola riga. Inoltre, questo esempio è limitato a una singola voce Amazon ECR. In un file di log CloudTrail reale sono visualizzate le voci e gli eventi provenienti da più servizi AWS.

Argomenti

- Esempio: crea operazione del repository
- Esempio: azione API CreateGrant AWS KMS durante la creazione di un repository Amazon ECR
- Esempio: operazione di invio immagine
- Esempio: operazione di estrazione immagine
- Esempio: operazione delle policy relative al ciclo di vita delle immagini

Esempio: crea operazione del repository

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione `CreateRepository`.

```
{
    "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"
}
```

Esempio: azione API CreateGrant AWS KMS durante la creazione di un repository Amazon ECR

L'esempio seguente mostra una voce di log CloudTrail che illustra l'operazione CreateGrant AWS KMS durante la creazione di un repository Amazon ECR con crittografia KMS abilitata. Per ogni repository creato con la crittografia KMS attivata, è necessario visualizzare due voci di log CreateGrant in 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"
}
```

Esempio: operazione di invio immagine

L'esempio seguente mostra una voce di log CloudTrail che descrive l'invio di un'immagine che utilizza l'operazione `PutImage`.

> **Note**
>
> Quando esegui l'invio di un'immagine, vedrai anche i riferimenti `InitiateLayerUpload`, `UploadLayerPart` e `CompleteLayerUpload` nei log CloudTrail.


```
{
    "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"
}
```

Esempio: operazione di estrazione immagine

L'esempio seguente mostra una voce di log CloudTrail che descrive l'invio di un'immagine che utilizza l'operazione `BatchGetImage`.

> **Note**
>
> Quando esegui il pull di un'immagine, se non hai ancora l'immagine localmente, vedrai anche i riferimenti `GetDownloadUrlForLayer` nei log CloudTrail.

```
{
    "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"
}
```


Esempio: operazione delle policy relative al ciclo di vita delle immagini

Nell'esempio seguente viene illustrata una voce di log CloudTrail che mostra quando un'immagine è scaduta a causa di una regola delle policy del ciclo di vita. Questo tipo di evento può essere individuato applicando un filtro `PolicyExecutionEvent` per il campo del nome dell'evento.

> **Important**
>
> A causa delle limitazioni di dimensioni dei singoli eventi CloudTrail, per le azioni delle policy del ciclo di vita in cui sono scadute 10 o più immagini, Amazon ECR invia più eventi a CloudTrail. Inoltre, Amazon ECR include un massimo di 100 tag per immagine.

```
{
    "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
            }
        ]
    }
}
```

Service Quotas di Amazon ECR.

Nella tabella seguente sono indicate le Service Quotas per Amazon Elastic Container Registry (Amazon ECR).

Nome	Predefinita	Adattabile	Description
Filtri per regola in una configurazione di replica	Ogni regione supportata: 100	No	Il numero massimo di filtri per regola in una configurazione di replica.
Immagine per repository	Ogni regione supportata: 10.000	Sì	Numero massimo di immagini per repository.
Parti di livello	Ogni regione supportata: 4.200	No	Il numero massimo di parti del livello. Questo è applicabile solo se utilizzi direttamente le operazioni API Amazon ECR per avviare caricamenti in più parti per le operazioni di invio delle immagini.
Lunghezza della policy del ciclo di vita	Ogni regione supportata: 30.720	No	Numero massimo di caratteri in una policy del ciclo di vita.
Dimensione massima della parte del livello	Ogni regione supportata: 10	No	La dimensione massima (MiB) di una parte del livello. Questo è applicabile solo se utilizzi direttamente le operazioni API Amazon ECR per avviare caricamenti in più parti per le operazioni di invio delle immagini.

Nome	Predefinita	Adatta e	Description
Dimensione massima del livello	Ogni regione supportata: 52.000	No	La dimensione massima (MiB) di un livello.
Dimensione minima della parte del livello	Ogni Regione supportata: 5	No	La dimensione minima (MiB) di una parte del livello. Questo è applicabile solo se utilizzi direttamente le operazioni API Amazon ECR per avviare caricamenti in più parti per le operazioni di invio delle immagini.
Regole di cache pull-through per registro	Ogni regione supportata: 50	No	Il numero massimo di regole di cache pull-through.
Frequenza di richieste BatchCheckLayerAvailability	Ogni regione supportata: 1.000 al secondo	Sì	Il numero massimo di richieste BatchCheckLayerAvailability che puoi effettuare al secondo nella regione corrente. Quando si esegue il push di un'immagine in un repository, ogni livello dell'immagine viene controllato per verificare se è stato già caricato. Se è stato caricato, il livello dell'immagine viene ignorato.

Nome	Predefinita	Adatta e	Description
Frequenza di richieste BatchGetImage	Ogni regione supportata: 2.000 al secondo	Sì	Il numero massimo di richieste BatchGetImage che puoi effettuare al secondo nella regione corrente. Quando si esegue il pull di un'immagine, l'API BatchGetImage viene chiamata una volta per recuperare il manifesto dell'immagine. Se richiedi un aumento della quota per questa API, consulta anche l'utilizzo di GetDownloadUrlForLayer.
Frequenza di richieste CompleteLayerUpload	Ogni regione supportata: 100 al secondo	Sì	Il numero massimo di richieste CompleteLayerUpload che puoi effettuare al secondo nella regione corrente. Quando si esegue il push di un'immagine, l'API CompleteLayerUpload viene chiamata una volta per ogni nuovo livello dell'immagine per verificare che il caricamento sia stato completato.

Nome	Predefinita	Adatta e	Description
Frequenza di richieste GetAuthorizationToken	Ogni regione supportata: 500 al secondo	Sì	Il numero massimo di richieste GetAuthorizationToken che puoi effettuare al secondo nella regione corrente.
Frequenza di richieste GetDownloadUrlForLayer	Ogni regione supportata: 3.000 al secondo	Sì	Il numero massimo di richieste GetDownloadUrlForLayer che puoi effettuare al secondo nella regione corrente. Quando si esegue il pull di un'immagine, l'API GetDownloadUrlForLayer viene chiamata una volta per ogni livello dell'immagine che non è già stato memorizzato nella cache. Se richiedi un aumento della quota per questa API, controlla anche l'utilizzo di BatchGetImage.

Nome	Predefinita	Adatta e	Description
Frequenza di richieste InitiateLayerUpload	Ogni regione supportata: 100 al secondo	Sì	Il numero massimo di richieste InitiateLayerUpload che puoi effettuare al secondo nella regione corrente. Quando si esegue il push di un'immagine, l'API InitiateLayerUpload viene chiamata una volta per ogni livello dell'immagine che non è già stato caricato. Se un livello dell'immagine è già stato caricato o meno viene determinato dall'operazione API BatchCheckLayerAvailability.
Frequenza di richieste PutImage	Ogni regione supportata: 10 al secondo	Sì	Il numero massimo di richieste PutImage che puoi effettuare al secondo nella regione corrente. Quando si esegue il push di un'immagine e sono stati caricati tutti i nuovi livelli dell'immagine, l'API PutImage viene chiamata una volta per creare o aggiornare il manifesto e i tag associati all'immagine.

Nome	Predefinita	Adattabile	Description
Frequenza di richieste UploadLayerPart	Ogni regione supportata: 500 al secondo	Sì	Il numero massimo di richieste UploadLayerPart che puoi effettuare al secondo nella regione corrente. Quando esegui il push di un'immagine, ogni nuovo livello dell'immagine viene caricato in parti e l'API UploadLayerPart viene chiamata una volta per ogni nuova parte del livello dell'immagine.
Frequenza delle scansioni delle immagini	Ogni regione supportata: 1	No	Il numero massimo di scansioni di immagini per immagine, al giorno.
Repository registrati	Ogni regione supportata: 10.000	Sì	Il numero massimo di repository che è possibile creare in questo account nella regione corrente.
Regole per la policy del ciclo di vita	Ogni regione supportata: 50	No	Numero massimo di regole in una policy del ciclo di vita
Regole per la configurazione di repliche	Ogni regione supportata: 10	No	Il numero massimo di regole in una configurazione di replica.
Tag per immagine	Ogni regione supportata: 1.000	No	Il numero massimo di tag per immagine.

Nome	Predefinita	Adatta e	Description
Destinazioni univoche per tutte le regole in una configurazione di replica	Ogni regione supportata: 25	No	Il numero massimo di destinazioni univoche in tutte le regole di una configurazione di replica.

Gestione delle Service Quotas Amazon ECR in AWS Management Console

Amazon ECR è integrato con Service Quotas, un servizio AWS che ti consente di visualizzare e gestire le quote da una posizione centrale. Per ulteriori informazioni, consulta Cos'è Service Quotas? nella Guida per l'utente di Service Quotas.

Service Quotas semplifica la ricerca del valore di tutte le quote di servizio Amazon ECR.

Per visualizzare le Service Quotas di Amazon ECR (AWS Management Console)

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/
2. Nel pannello di navigazione, scegli Servizi AWS.
3. Nell'elenco servizi AWS, cerca e seleziona Amazon Elastic Container Registry (Amazon ECR).

   Nell'elenco Service Quotas, è possibile visualizzare il nome della quota di servizio, il valore applicato (se è disponibile), la quota predefinita AWS e se il valore della quota è adattabile.
4. Per visualizzare ulteriori informazioni su una quota di servizio, ad esempio la descrizione, scegli il nome della quota.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas.

Creazione di un allarme CloudWatch per monitorare i parametri di utilizzo delle API

Amazon ECR fornisce i parametri di utilizzo CloudWatch che corrispondono alle Service Quotas AWS per ciascuna delle API coinvolte nelle operazioni di autenticazione del registro, push immagine e

pull immagine. Nella console Service Quotas puoi visualizzare l'utilizzo in un grafico e configurare gli allarmi che ti avvisano quando l'utilizzo si avvicina a una quota di servizio. Per ulteriori informazioni, consulta Parametri di utilizzo Amazon ECR.

Attieniti alla seguente procedura per creare un allarme CloudWatch basato su uno dei parametri di utilizzo dell'API Amazon ECR.

Per creare un allarme basato sulle quote di utilizzo Amazon ECR (AWS Management Console)

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/
2. Nel pannello di navigazione, scegli Servizi AWS.
3. Nell'elenco servizi AWS, cerca e seleziona Amazon Elastic Container Registry (Amazon ECR).
4. Nell'elenco Service quotas (Quote di servizio) selezionare la quota di utilizzo Amazon ECR per cui si desidera creare un allarme.
5. Nella sezione allarmi di Eventi Amazon CloudWatch, seleziona Crea.
6. Per Alarm threshold (Soglia di allarme), scegli la percentuale del valore della quota applicata che si desidera impostare come valore per l'allarme.
7. Per Nome allarme, immetti un nome per l'allarme e quindi scegli Crea.

Risoluzione dei problemi di Amazon ECR

Questo capitolo ti aiuta a trovare informazioni diagnostiche per Amazon Elastic Container Registry (Amazon ECR) e ti illustra la procedura per risolvere problemi comuni e messaggi di errore.

Argomenti

Abilitazione dell'output di debug di Docker

Per iniziare il debug di problemi relativi a Docker, inizia abilitando l'output di debug di Docker nel daemon Docker in esecuzione sulle tue istanze in hosting. Per maggiori informazioni su come abilitare il debug di Docker se utilizzi immagini estratte da Amazon ECR su istanze di container Amazon ECS, consulta Enabling Docker Debug Output (Abilitazione dell'output di debug di Docker) nella Guida per sviluppatori di Amazon Elastic Container Service.

Abilitazione AWS CloudTrail

Ulteriori informazioni sugli errori restituiti da Amazon ECR possono essere scoperte abilitando AWS CloudTrail, un servizio che registra AWS le chiamate per il tuo AWS account. CloudTrailconsegna file di log a un bucket Amazon S3. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare quali richieste sono state inoltrate correttamente ai AWS servizi, chi ha effettuato la richiesta, quando è stata effettuata e così via. Per ulteriori informazioni CloudTrail, incluso come attivarlo e trovare i file di registro, consulta la Guida per l'AWS CloudTrail utente. Per ulteriori informazioni sull'utilizzo CloudTrail con Amazon ECR, consultaRegistrazione delle azioni Amazon ECR con AWS CloudTrail.

Ottimizzazione delle prestazioni per Amazon ECR

La sezione che segue contiene raccomandazioni su impostazioni e strategie che puoi utilizzare per ottimizzare le prestazioni quando utilizzi Amazon ECR.

Scegli Docker 1.10 e versioni successive per cogliere i vantaggi degli upload di livelli simultanei

Le immagini Docker sono composte da livelli, ovvero fasi intermedie di compilazione dell'immagine. Ciascuna riga in un Dockerfile porta alla creazione di un nuovo livello. Quando utilizzi Docker 1.10 e versioni successive, per impostazione predefinita Docker invia il maggior numero possibile di livelli come upload simultanei a Amazon ECR, pertanto gli upload risultano più veloci.

Utilizza un'immagine base più piccola

Le immagini predefinite disponibili tramite Docker Hub possono contenere molte dipendenze di cui la tua applicazione non ha bisogno. Potresti pertanto utilizzare un'immagine più piccola creata e gestita da altri nella community Docker oppure creare la tua immagine base utilizzando l'immagine scratch minima di Docker. Per ulteriori informazioni, consulta Creare un'immagine base nella documentazione Docker.

Posiziona le dipendenze che sono meno soggette a variazione all'inizio nel tuo Dockerfile

Docker memorizza i livelli nella cache velocizzando i tempi di compilazione. Se nulla è cambiato in un livello dall'ultima compilazione, Docker utilizza la versione nella cache invece di ricompilare il livello. Tuttavia, ciascun livello dipende dai livelli che lo hanno preceduto. Se un livello cambia, Docker ricompila non solo quel livello, ma anche tutti i livelli che vengono dopo.

Per ridurre al minimo il tempo necessario per ricompilare un file Docker e per ricaricare i livelli, è utile posizionare le dipendenze che cambiano con minore frequenza all'inizio nel Dockerfile. Posiziona quelle che cambiano rapidamente (come il codice sorgente dell'applicazione) più avanti nello stack.

Concatena i comandi per evitare lo storage di file non necessari

I file intermedi creati su un livello rimangono parte di quel livello anche se vengono eliminati in un livello successivo. Considera il seguente esempio:

```
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
```

In questo esempio i livelli creati dal primo e dal secondo comando RUN contengono il file .tar.gz originale e tutti i suoi componenti non compressi anche se il file .tar.gz viene eliminato dal quarto

comando RUN. Questi comandi possono essere concatenati in un unico comando RUN affinché i file non necessari non facciano parte dell'immagine 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
```

Utilizza l'endpoint regionale più vicino

Puoi ridurre la latenza nell'estrazione delle immagini da Amazon ECR assicurandoti di utilizzare l'endpoint regionale più vicino al luogo in cui la tua applicazione è in esecuzione. Se la tua applicazione è in esecuzione su un'istanza Amazon EC2, puoi utilizzare il seguente codice shell per ottenere la regione dalla zona di disponibilità dell'istanza:

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

La regione può essere passata ai AWS CLI comandi utilizzando il --region parametro o impostata come regione predefinita per un profilo utilizzando il aws configure comando. È inoltre possibile impostare la regione quando si effettuano chiamate utilizzando l' AWS SDK. Per ulteriori informazioni, consulta la documentazione sugli SDK per il tuo linguaggio di programmazione specifico.

Risoluzione degli errori con i comandi Docker quando si utilizza Amazon ECR

A volte eseguire un comando Docker su Amazon ECR può portare a un messaggio di errore. Alcuni messaggi di errore comuni e possibili soluzioni sono spiegati di seguito.

Argomenti

- Errore: "Filesystem Verification Failed" (Verifica del file system non riuscita) oppure "404: Image Not Found" (404: Immagine non trovata) durante l'estrazione di un'immagine da un repository Amazon ECR
- Errore: "Filesystem Layer Verification Failed" (Verifica dei livelli del file system non riuscita) durante l'estrazione di immagini da Amazon ECR

- Errore HTTP 403 o errore "no basic auth credentials" (Nessuna credenziale di autenticazione di base) quando effettui l'invio al repository

Errore: "Filesystem Verification Failed" (Verifica del file system non riuscita) oppure "404: Image Not Found" (404: Immagine non trovata) durante l'estrazione di un'immagine da un repository Amazon ECR

Potresti ricevere l'errore `Filesystem verification failed` quando utilizzi il comando docker pull per estrarre un'immagine da un repository Amazon ECR con Docker 1.9 o versione successiva. Puoi visualizzare l'errore `404: Image not found` quando usi le versioni di Docker precedenti a 1.9.

Di seguito sono elencate alcune possibili cause e le relative spiegazioni.

Il disco locale è pieno

Se il disco locale sul quale esegui docker pull è pieno, il valore hash SHA-1 calcolato sul file locale può essere diverso dal valore calcolato da Amazon ECR. Controlla che sul tuo disco locale vi sia spazio libero sufficiente per conservare l'immagine Docker che stai estraendo. Puoi anche eliminare le immagini meno recenti per fare spazio a nuove immagini. Usa il comando docker images per vedere un elenco di tutte le immagini Docker scaricate in locale con le relative dimensioni.

Il client non è in grado di connettersi al repository remoto a causa di un errore di rete

Le chiamate a un repository Amazon ECR richiedono una connessione valida a Internet. Verifica le impostazioni di rete e che altri strumenti e applicazioni possano accedere alle risorse su Internet. Se esegui docker pull su un'istanza Amazon EC2 in una sottorete privata, verifica che la sottorete abbia una route a Internet. Utilizzare un server NAT (Network Address Translation) o un gateway NAT gestito.

Al momento, le chiamate a un repository Amazon ECR richiedono anche accesso di rete tramite il firewall aziendale a Amazon Simple Storage Service (Amazon S3). Se la tua organizzazione utilizza un firewall o un dispositivo NAT che consente gli endpoint del servizio, verifica che gli endpoint del servizio Amazon S3 per la regione corrente siano autorizzati.

Se utilizzi Docker dietro un proxy HTTP, puoi configurare Docker con le impostazioni proxy appropriate. Per ulteriori informazioni, consulta Proxy HTTP nella documentazione Docker.

Errore: "Filesystem Layer Verification Failed" (Verifica dei livelli del file system non riuscita) durante l'estrazione di immagini da Amazon ECR

Puoi visualizzare l'errore `image image-name not found` quando estrai le immagini utilizzando il comando docker pull. Se ispezioni i log di Docker, potresti trovare un errore simile al seguente:

```
filesystem layer verification failed for digest sha256:2b96f...
```

Questo errore indica che non è stato possibile scaricare uno o più livelli per la tua immagine. Di seguito sono elencate alcune possibili cause e le relative spiegazioni.

Stai utilizzando una versione di Docker meno recente

Questo errore può verificarsi in una piccola percentuale di casi quando utilizzi una versione di Docker precedente alla 1.10. Aggiorna il tuo client Docker alla versione 1.10 o versione successiva.

Il client ha riscontrato un errore di rete o del disco

Un problema di disco pieno o di rete può impedire a uno o più livelli di essere scaricati, come descritto precedentemente in merito al messaggio `Filesystem verification failed`. Segui le raccomandazioni suddette per assicurarti che il tuo file system non sia pieno e che tu abbia abilitato l'accesso ad Amazon S3 dalla tua rete.

Errore HTTP 403 o errore "no basic auth credentials" (Nessuna credenziale di autenticazione di base) quando effettui l'invio al repository

Ci sono volte in cui puoi visualizzare un errore `HTTP 403 (Forbidden)` oppure il messaggio di errore `no basic auth credentials` dal comando docker push o docker pull, anche sei ti sei autenticato correttamente in Docker utilizzando il comando aws ecr get-login-password. Di seguito sono elencate alcune cause note di questo problema:

Hai effettuato l'autenticazione per una regione diversa

Le richieste di autenticazione sono legate a regioni specifiche e non possono essere utilizzate in regioni diverse. Ad esempio, se ottieni un token di autorizzazione dagli Stati Uniti occidentali (Oregon), non puoi utilizzarlo per l'autenticazione dei tuoi repository negli Stati Uniti orientali (Virginia settentrionale). Per risolvere il problema, assicurati di aver recuperato un token di

autenticazione dalla stessa regione in cui esiste il repository. Per ulteriori informazioni, consulta the section called “Autenticazione del registro”.

Hai autenticato il push in un repository per cui non disponi delle autorizzazioni

Non disponi delle autorizzazioni necessarie per eseguire il push al repository. Per ulteriori informazioni, consulta Policy del repository privato.

Il tuo token è scaduto

Il periodo di scadenza del token di autorizzazione predefinito per i token ottenuti tramite l'operazione `GetAuthorizationToken` è 12 ore.

Bug nella gestione credenziali `wincred`

Alcune versioni di Docker per Windows utilizzano una gestione credenziali denominata `wincred`, he non è in grado di gestire correttamente il comando di login di Docker generato da aws ecr get-login-password (per ulteriori informazioni, consulta https://github.com/docker/docker/issues/22910). Puoi eseguire il comando di login di Docker ottenuto, ma quando tenti di inviare o estrarre immagini, questi comandi non vanno a buon fine. Per risolvere questo bug, rimuovi lo schema `https://` dall'argomento del registro nel comando di login di Docker che risulta da aws ecr get-login-password. Di seguito viene mostrato un esempio di comando di login di Docker senza lo schema HTTPS.

```
docker login -u AWS -p <password> <aws_account_id>.dkr.ecr.<region>.amazonaws.com
```

Risoluzione dei problemi relativi ai messaggi di errore Amazon ECR

In alcuni casi, una chiamata API attivata tramite la console Amazon ECS o AWS CLI si chiude con un messaggio di errore. Alcuni messaggi di errore comuni e possibili soluzioni sono spiegati di seguito.

HTTP 429: Troppe richieste o ThrottleException

Potresti ricevere un `429: Too Many Requests` errore o un `ThrottleException` errore da una o più azioni o chiamate API di Amazon ECR. Ciò indica che stai chiamando un singolo endpoint in Amazon ECR più volte in un breve intervallo di tempo e che le tue richieste vengono limitate. Il throttling si verifica quando le chiamate a un singolo endpoint da uno stesso utente superano una certa soglia in un periodo di tempo.

A ogni operazione API in Amazon ECR è associata una limitazione di velocità. Ad esempio, la limitazione per l'operazione `GetAuthorizationToken` è di 20 transazioni al secondo (TPS),

con un aumento consentito fino a 200 TPS. In ogni regione, ogni account riceve un bucket che può ospitare fino a 200 crediti `GetAuthorizationToken`. Questi crediti vengono riforniti a una velocità di 20 al secondo. Se il bucket ospita 200 crediti, puoi ottenere 200 transazioni API `GetAuthorizationToken` al secondo per un secondo, quindi mantenere 20 transazioni al secondo a tempo indeterminato. Per ulteriori informazioni sui limiti di velocità per le API di Amazon ECR, consulta. Service Quotas di Amazon ECR.

Per gestire gli errori di throttling, implementa una funzione di nuovo tentativo con backoff incrementale nel tuo codice. Per ulteriori informazioni, consulta Retry behavior nella Guida di riferimento agli AWS SDK and Tools. Un'altra opzione è richiedere un aumento del limite di velocità, cosa che puoi fare utilizzando la console Service Quotas. Per ulteriori informazioni, consulta Gestione delle Service Quotas Amazon ECR in AWS Management Console.

HTTP 403: "User [arn] is not authorized to perform [operation]" (HTTP 403: l'utente [arn] non è autorizzato a eseguire [operazione])

Puoi visualizzare il seguente errore quando tenti di eseguire un'operazione con 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: *
```

Ciò indica che il tuo utente non ha ricevuto le autorizzazioni per utilizzare Amazon ECR oppure che quelle autorizzazioni non sono configurare correttamente. In particolare, se esegui delle operazioni su un repository Amazon ECR, verifica che l'utente abbia ricevuto le autorizzazioni per accedere a quel repository. Per ulteriori informazioni sulla creazione e le verifica delle autorizzazioni per Amazon ECR, consulta Identity and Access Management per Amazon Elastic Container Registry.

Errore HTTP 404: "Repository Does Not Exist" (HTTP 404: il repository non esiste)

Se specifichi un repository del Docker Hub che non esiste, Docker Hub lo crea automaticamente. Con Amazon ECR, i nuovi repository devono essere creati esplicitamente prima di poter essere utilizzati. Ciò impedisce la creazione accidentale di nuovi repository (ad esempio, per errori di digitazione) e assicura inoltre che venga assegnata una policy d'accesso adeguata ai nuovi repository. Per ulteriori informazioni sulla creazione dei repository, consulta Repository Amazon ECR privati.

Errore: impossibile eseguire un accesso interattivo da un dispositivo non TTY

Se ricevi l'errore `Cannot perform an interactive login from a non TTY device`, i seguenti passaggi per la risoluzione dei problemi dovrebbero aiutarti.

- Verifica di utilizzare la AWS CLI versione 2 e di non avere una versione in conflitto della AWS CLI versione 1 sul tuo sistema. Per ulteriori informazioni, consulta Installare o aggiornare la versione più recente della AWS CLI.
- Verifica di aver configurato il tuo AWS CLI con credenziali valide. Per ulteriori informazioni, consulta Installare o aggiornare la versione più recente della AWS CLI.
- Verifica che la sintassi del AWS CLI comando sia corretta.

Cronologia dei documenti

Nella tabella seguente vengono descritte le modifiche importanti apportate alla documentazione dall'ultima versione di Amazon ECR. Inoltre, aggiorniamo frequentemente la documentazione per tener conto del feedback inviatoci.

Modifica	Descrizione	Data
Aggiornamento della policy del ciclo di vita di Amazon ECR per aggiungere il supporto per l'uso di caratteri jolly	Amazon ECR ha aggiunto il supporto per i caratteri jolly in una policy del ciclo di vita mediante l'uso del parametro `tagPatternList` in una regola della policy del ciclo di vita. Per ulteriori informazioni, consulta Policy del ciclo di vita.	18 dicembre 2023
Modelli di creazione dei repository di Amazon ECR	Amazon ECR ha aggiunto il supporto per i modelli di creazione del repository. Per ulteriori informazioni, consulta Gestione dei modelli di creazione repository.	15 novembre 2023
Aggiunta la cache pull-through di Amazon ECR, supportata per registri upstream autenticati	Amazon ECR ha aggiunto il supporto per l'utilizzo di registri upstream che richiedono l'autenticazione per le regole di cache pull-through. Per ulteriori informazioni, consulta Utilizzo delle regole della cache pull-through.	15 novembre 2023
AWSECRPullThroughCache_ServiceRolePolicy: aggiornamento a una policy esistente	Amazon ECR ha aggiunto nuove autorizzazioni alla policy `AWSECRPullThroughCache_ServiceRolePolicy`. Queste autorizzazioni consentono ad Amazon ECR di recuperare i contenuti crittografati di un segreto di Secrets Manager. Ciò è necessario quando utilizzi una regola di cache pull-through per memorizzare nella cache le immagini da un registro upstream che richiede l'autenticazione.	15 novembre 2023
Firma delle immagini Amazon ECR	Amazon ECR e AWS Signer hanno aggiunto il supporto per la creazione e l'invio delle firme delle immagini dei container utilizzando il client Notary. Per ulteriori informazioni, consulta Firma di un'immagine.	6 giugno 2023

Modifica	Descrizione	Data
Registro del container Kubernetes aggiunto alle regole della cache pull-through	Amazon ECR ha aggiunto il supporto per la creazione di regole della cache pull-through per il registro dei container Kubernetes. Per ulteriori informazioni, consulta Utilizzo delle regole della cache pull-through.	1 giugno 2023
Supporto della durata della scansione avanzata di Amazon ECR	Amazon Inspector ha aggiunto il supporto per l'impostazione della durata di monitoraggio dei repository quando è abilitata la scansione avanzata. Per ulteriori informazioni, consulta Modifica della durata della scansione avanzata.	28 giugno 2022
Amazon ECR invia i parametri del pull count del repository ad Amazon CloudWatch	Amazon ECR invia i parametri del pull count del repository ad Amazon CloudWatch. Per ulteriori informazioni, consulta Parametri del repository Amazon ECR.	6 gennaio 2022
Supporto di replica espanso	Amazon ECR ha aggiunto il supporto per filtrare i repository replicati. Per ulteriori informazioni, consulta Replica di immagini private.	21 settembre 2021
Policy gestite da AWS per Amazon ECR	Amazon ECR ha aggiunto la documentazione delle policy gestite da AWS. Per ulteriori informazioni, consulta AWS politiche gestite per Amazon Elastic Container Registry.	24 giugno 2021
Replica tra regioni e tra account	Amazon ECR ha aggiunto il supporto per la configurazione delle impostazioni di replica per il tuo registro privato. Per ulteriori informazioni, consulta Impostazioni dei registri privati.	8 dicembre 2020

Modifica	Descrizione	Data
Supporto artefatti OCI	Amazon ECR ha aggiunto il supporto per inviare ed estrarre gli artefatti Open Container Initiative (OCI). Un nuovo parametro `artifactMediaType` è stato aggiunto alla riposta API `DescribeImages` per indicare il tipo di artefatto. Per ulteriori informazioni, consulta Invio di un grafico Helm.	24 agosto 2020
Crittografia dei dati a riposo	Amazon ECR ha aggiunto il supporto per la configurazione della crittografia per i tuoi repository utilizzando la crittografia lato server con le chiavi gestite dal cliente archiviate in AWS Key Management Service (AWS KMS). Per ulteriori informazioni, consulta Crittografia dei dati a riposo.	29 luglio 2020
Immagini multi-architettura	Amazon ECR ha aggiunto il supporto per la creazione e l'invio di elenchi di manifesti di Docker che vengono utilizzati per le immagini multi-architettura. Per ulteriori informazioni, consulta Inviare un'immagine multi-architettura.	28 aprile 2020
Parametri di utilizzo Amazon ECR	Amazon ECR ha aggiunto i parametri di utilizzo CloudWatch che forniscono la visibilità dell'utilizzo delle risorse del tuo account. Inoltre, hai la possibilità di creare allarmi CloudWatch dalle console CloudWatch e Service Quotas per ricevere avvisi quando l'utilizzo si avvicina alla tua quota di servizio applicata. Per ulteriori informazioni, consulta Parametri di utilizzo Amazon ECR.	28 febbraio 2020

Modifica	Descrizione	Data
Aggiornate Service Quotas di Amazon ECR.	Aggiornate le Service Quotas di Amazon ECR per includere le quote per le API. Per ulteriori informazioni, consulta Service Quotas di Amazon ECR..	19 febbraio 2020
Aggiunto il comando `get-login-password`	Aggiunto il supporto per get-login-password, che fornisce un metodo semplice e sicuro per recuperare un token di autorizzazione. Per ulteriori informazioni, consulta Utilizzo di un token di autorizzazione.	4 febbraio 2020
Scansione delle immagini	Aggiunto il supporto per la scansione delle immagini, che aiuta a identificare le vulnerabilità del software nelle immagini di container. Amazon ECR utilizza il database CVE (Common Vulnerabilities and Exposures) del progetto open source CoreOS Clair e fornisce l'elenco dei risultati della scansione. Per ulteriori informazioni, consulta Scansione delle immagini.	24 ottobre 2019
Policy degli endpoint VPC	Aggiunto il supporto per l'impostazione di una policy IAM sugli endpoint VPC dell'interfaccia Amazon ECR. Per ulteriori informazioni, consulta Creazione di una policy di endpoint per l'endpoint VPC di Amazon ECR.	26 settembre 2019
Mutabilità dei tag immagine	È stato aggiunto il supporto per la configurazione di un repository in modo che sia immutabile, per impedire che i tag immagine vengano sovrascritti. Per ulteriori informazioni, consulta Mutabilità dei tag immagine.	25 luglio 2019

Modifica	Descrizione	Data
Endpoint VPC dell'interfaccia (AWS PrivateLink)	Aggiunto il supporto per la configurazione degli endpoint VPC dell'interfaccia con tecnologia AWS PrivateLink. Ciò consente di creare una connessione privata tra il VPC e Amazon ECR senza richiedere l'accesso tramite Internet, un'istanza NAT, una connessione VPN o AWS Direct Connect. Per ulteriori informazioni, consulta Endpoint VPC con interfaccia Amazon ECR ()AWS PrivateLink.	25 gennaio 2019
Aggiunta di tag alle risorse	In Amazon ECR è stato implementato il supporto per aggiungere i tag di metadati ai repository. Per ulteriori informazioni, consulta Tagging di un repository privato.	18 dicembre 2018
Modifica del nome Amazon ECR	Amazon Elastic Container Registry viene stato rinominato (in precedenza Amazon EC2 Container Registry).	21 novembre 2017
Policy del ciclo di vita	Le policy del ciclo di vita di Amazon ECR consentono di specificare la gestione del ciclo di vita delle immagini in un repository. Per ulteriori informazioni, consulta Policy del ciclo di vita.	11 ottobre 2017
Supporto Amazon ECR per manifesto immagine Docker 2, schema 2	Amazon ECR supporta ora Docker Image Manifest V2 Schema 2 (utilizzato con la versione Docker 1.10 e più recente). Per ulteriori informazioni, consulta Formati manifest per le immagini dei container.	27 gennaio 2017
Disponibilità generale di Amazon ECR	Amazon Elastic Container Registry (Amazon ECR) è un servizio di registro Docker AWS gestito che offre sicurezza, scalabilità e affidabilità.	21 dicembre 2015

Glossario per AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.