aws

使用者指南

# Amazon ECR

API 版本 2015-09-21

# Amazon ECR: 使用者指南

# Table of Contents

# 什麼是 Amazon Elastic Container Registry？

Amazon Elastic Container Registry (Amazon ECR) 是安全、可擴展且可靠的 AWS 受管容器映像登錄服務。Amazon ECR 使 AWS 用 IAM 支援具有以資源為基礎的許可的私有存放庫。如此可讓指定的使用者或 Amazon EC2 執行個體存取您的容器儲存庫及映像。您可以使用偏好的 CLI 來推送、提取和管理 Docker 映像、Open Container Iniative (OCI) 映像以及與 OCI 相容的成品。

> **Note**
>
> Amazon ECR 也支援公有容器映像存放庫。如需詳細資訊，請參閱《Amazon ECR Public 使用者指南》中的什麼是 Amazon ECR Public。

AWS 容器服務團隊會維護上的公開藍圖 GitHub。它包含有關團隊正在努力的信息，並允許所有 AWS 客戶提供直接反饋的能力。如需詳細資訊，請參閱 AWS 容器藍圖。

## Amazon ECR 的元件

Amazon ECR 包含以下元件：

登錄檔

每個 AWS 帳戶都提供 Amazon ECR 私有登錄；您可以在登錄中建立一或多個儲存庫，並在其中存放 Docker 映像、開放容器倡議 (OCI) 映像以及與 OCI 相容的成品。如需詳細資訊，請參閱 Amazon ECR 私有登錄檔。

驗證字符

您的用戶端在能夠推送與提取映像前，需要驗證至 Amazon ECR 私有登錄檔以做為 AWS 使用者。如需詳細資訊，請參閱 Amazon ECR 中的私有登錄身份驗證。

儲存庫

Amazon ECR 儲存庫包含您的 Docker 映像、開放容器計畫 (OCI) 映像以及與 OCI 相容的成品。如需詳細資訊，請參閱 Amazon ECR 私有儲存庫。

儲存庫政策

您可透過儲存庫政策來控制您儲存庫的存取以及其中的內容。如需詳細資訊，請參閱 Amazon ECR 中的私有儲存庫政策。

映像

您可以推送與提取容器映像至您的儲存庫。您可在開發系統上以本機使用這些映像，或者您也可以在 Amazon ECS 任務定義和 Amazon EKS Pod 規格。如需更多詳細資訊，請參閱 將 Amazon ECR 映像與 Amazon ECS 搭配使用 及 將 Amazon ECR 映像與 Amazon EKS 搭配使用。

# Amazon ECR 的功能

Amazon ECR 提供以下功能：

- 生命週期政策有助於管理儲存庫中映像的生命週期。您定義會導致清理未使用映像的規則。您可以在將規則套用至儲存庫前先進行測試。如需詳細資訊，請參閱 在 Amazon ECR 中使用生命週期政策自動清理映像檔。
- 映像掃描有助於識別容器映像中的軟體漏洞。每個儲存庫都可以設定為在推送時掃描。這可確保會對每個推送到儲存庫的新映像進行掃描。之後，您可以擷取映像掃描的結果。如需詳細資訊，請參閱 掃描影像以查看 Amazon ECR 中的軟體漏洞。
- 跨區域和跨帳戶複寫可讓您更輕鬆地將映像放置在所需的地方。這會設定為登錄設定，並且以每一區域為基礎。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表設置。
- 提取快取規則提供了一個方式，可在私有 Amazon ECR 登錄檔中快取上游登錄檔中的儲存庫。使用提取快取規則，Amazon ECR 將定期聯繫上游登錄檔，以確保 Amazon ECR 私有登錄檔中的快取映像是最新的。如需詳細資訊，請參閱 將上游註冊表與 Amazon ECR 私有註冊表同步。

# 如何開始使用 Amazon ECR

如果您使用的是 Amazon 彈性容器服務（Amazon ECS）或 Amazon 彈性 Kubernetes 服務（Amazon EKS），請注意，這兩個服務的設置類似於亞馬遜 ECR 的設置，因為亞馬遜 ECR 是兩種服務的擴展。

AWS Command Line Interface 與 Amazon ECR 搭配使用時，請使用支援最新 Amazon ECR 功 AWS CLI 能的版本。如果您在中看不到對 Amazon ECR 功能的支援 AWS CLI，請升級到最新版本的 AWS CLI. 若要取得有關安裝最新版本的資訊 AWS CLI，請參閱《使用指南》 AWS CLI中的〈安裝或更新至最新版本的AWS Command Line Interface〉。

若要了解如何使用 AWS CLI 和 Docker 將容器映像推送到私有 Amazon ECR 儲存庫，請參閱。在 Amazon ECR 中在其生命週期中移動圖像

# Amazon ECR 定價

使用 Amazon ECR，您只需支付儲存庫中儲存的資料量，以及從映像推送和提取的資料傳輸費用。如需詳細資訊，請參閱 Amazon ECR 定價。

# 在 Amazon ECR 中在其生命週期中移動圖像

如果您是第一次使用 Amazon ECR，請使用 Docker CLI 和以下步驟建立範例映像、對預設登錄進行驗證，然後建立私有存放庫。 AWS CLI 然後將映像推送到私有存儲庫並從中提取圖像。當您完成範例影像時，請刪除範例影像和存放庫。

若要使用 AWS Management Console 而不是 AWS CLI，請參閱the section called “建立儲存庫以儲存影像”。

如需有關可用於管理 AWS 資源的其他工具的詳細資訊，包括不同的 AWS 軟體開發套件、IDE 工具組和 Windows PowerShell 命令列工具，請參閱 http://aws.amazon.com/tools/。

## 必要條件

如果您尚未安裝最新版 AWS CLI 和 Docker，並且可以使用，請使用下列步驟來安裝這兩個工具。

### 安裝 AWS CLI

若要 AWS CLI 搭配 Amazon ECR 使用，請安裝最新 AWS CLI 版本。如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》中的安裝 AWS Command Line Interface。

### 安裝 Docker

Docker 可在多個不同的作業系統上使用，包括大部分的現代 Linux 發行版本，例如 Ubuntu，甚至是 macOS 和 Windows。如需如何在特定作業系統上安裝 Docker 的詳細資訊，請前往「Docker 安裝指南」。

您不需要本機開發系統，就能使用 Docker。如果您已在使用 Amazon EC2，則可以啟動 Amazon Linux 2023 執行個體，並安裝 Docker 以開始使用。

如果您已經安裝 Docker，請跳到「步驟 1：建立 Docker 映像」。

使用 Amazon Linux 2023 AMI 在 Amazon EC2 執行個體上 安裝 Docker

1. 使用最新版 Amazon Linux 2023 AMI 啟動執行個體。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的啟動執行個體。
2. 連線到您的執行個體。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 Connect 到 Linux 執行個體。

3. 更新已安裝的套裝服務，並在執行個體上封裝快取。

```
sudo yum update -y
```

4. 安裝最新的 Docker Community Edition 套裝服務。

```
sudo yum install docker
```

5. 啟動 Docker 服務。

```
sudo service docker start
```

6. 將 ec2-user 新增至 docker 群組，讓您可以在不使用 sudo 的情況下執行 Docker 命令。

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

7. 登出並重新登入，以取得新的 docker 群組許可。關閉目前的 SSH 終端機視窗，即可完成此操作，並在新的 SSH 終端機視窗中重新連接至執行個體。新的 SSH 工作階段將會有適當的 docker 群組許可。
8. 驗證 ec2-user 可以在不使用 sudo 的情況下執行 Docker 命令。

```
docker info
```

> **Note**
>
> 在某些情況下，您可能需要重新啟動執行個體，才能提供 ec2-user 存取 Docker 常駐程式的許可。如果您看到下列錯誤，請嘗試重新啟動執行個體：
>
> ```
> Cannot connect to the Docker daemon. Is the docker daemon running on this
>  host?
> ```

# 步驟 1：建立 Docker 映像

在此步驟中，您將建立簡易 Web 應用程式的 Docker 映像檔，並在本機系統或 Amazon EC2 執行個體上進行測試。

建立簡單 Web 應用程式的 Docker 映像

1. 建立稱為 `Dockerfile` 的檔案。Dockerfile 是一種資訊清單，說明用於您 Docker 映像的基本映像，以及您要安裝並在其上執行的項目。如需 Dockerfile 的詳細資訊，請前往「Dockerfile 參考」。

   ```
   touch Dockerfile
   ```

2. 編輯您剛建立的 `Dockerfile`，並新增下列內容。

   ```
   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
   ```

   該 Dockerfile 使用在 Amazon ECR 公共上託管的 Amazon Linux 2 映像。`RUN` 指令會更新套件快取，並安裝 Web 伺服器的一些軟體套件服務，然後寫入 "Hello World!" 內容至 Web 伺服器文件根目錄。`EXPOSE` 指令會公開容器上的連接埠 80，而 `CMD` 指令會啟動 Web 伺服器。

3. 從 Dockerfile 建置 Docker 映像。

   > **Note**
   >
   > 在下列命令中，有些 Docker 版本可能需要 Dockerfile 的完整路徑，而不是下面所示的相對路徑。

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

4. 列出您的容器映像。

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

輸出：

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

5. 執行新建置的映像。-p 80:80 選項會將容器上的公開連接埠 80 映射至主機系統上的連接埠 80。如需 docker run 的詳細資訊，請前往「Docker run 參考」。

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

> **Note**
>
> Apache Web 伺服器中的輸出會顯示在終端機視窗中。您可以忽略 "Could not reliably determine the fully qualified domain name" 訊息。

6. 開啟瀏覽器，然後指向執行 Docker 並託管容器的伺服器。

   - 如果您使用的是 EC2 執行個體，則這是伺服器的「公有 DNS」值，這是您使用 SSH 來連線至執行個體的同個地址。請確定您執行個體的安全群組允許連接埠 80 上的入站流量。
   - 如果您在本機執行 Docker，請將瀏覽器指向 http://localhost/。
   - *#### Windows # Mac ##**docker-machine**#######**docker-machine ip**###### docker # VirtualBox ##### IP ############################*

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

   您應該會看到網頁，內含您的 "Hello World!" 陳述式。

7. 輸入 Ctrl + c，以停止 Docker 容器。

## 步驟 2：驗證至您的預設登錄檔

安裝並設定完成之後 AWS CLI，請向您的預設登錄驗證 Docker CLI。docker 命令可以透過該方法使用 Amazon ECR 來推送和提取映像。提 AWS CLI 供簡化驗證程序的get-login-password命令。

若要使用向 Amazon ECR 登錄驗證碼頭視窗 get-login-password，請執行命令。aws ecr get-login-password將身分驗證字符傳遞給 docker login 命令時，使用 AWS 的值作為使用者名稱並指定您要驗證的 Amazon ECR 登錄檔 URI。如果是向多個登錄進行驗證，您必須針對每個登錄重複此命令。

> **Important**
>
> 若您收到錯誤，請安裝或升級至最新版本的 AWS CLI。如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》中的安裝 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
```

- 取得 ECR () LoginCommandAWS Tools for Windows PowerShell

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

## 步驟 3：建立一個儲存庫

現在您已擁有可推送至 Amazon ECR 的映像，您必須建立儲存庫以存放它。在此範例中，您建立一個稱為 `hello-repository` 的儲存庫，以在稍後推送 `hello-world:latest` 映像。若要建立一個儲存庫，請執行下列命令：

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

# 步驟 4：將映像推送至 Amazon ECR

現在您可推送映像至您在前一節建立的 Amazon ECR 儲存庫。符合下列必要條件後，使用 docker CLI 推送映像：

- 已安裝的docker最低版本：1.7。
- Amazon ECR 授權令牌設定為. docker login
- Amazon ECR 儲存庫存在，且使用者可存取並推送至儲存庫。

在那些必要條件滿足後，您可推送映像至您帳戶預設登錄檔中新建立的儲存庫。

標記映像並推送映像至 Amazon ECR

1. 列出您在本機儲存的映像以識別欲標記與推送的映像。

   ```
   docker images
   ```

   輸出：

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

2. 標記映像以推送至您的儲存庫。

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

3. 推送映像。

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

   輸出：

   ```
   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
```

## 步驟 5：從 Amazon ECR 提取映像

將映像推送到 Amazon ECR 儲存庫之後，您可以從其他位置提取映像。符合下列必要條件之後，使用 docker CLI 提取映像：

- 已安裝的docker最低版本：1.7。
- Amazon ECR 授權令牌設定為. docker login
- Amazon ECR 儲存庫存在，且使用者擁有從儲存庫提取的存取權。

在滿足那些必要條件後，您可提取您的映像。若要從 Amazon ECR 提取您的範例映像，請執行下列命令：

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

輸出：

```
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
```

## 步驟 6：刪除映像

如果您在其中一個儲存庫中不再需要映像檔，可以刪除該映像檔。若要刪除影像，請指定影像所在的儲存庫，以及影像的`imageDigest`值`imageTag`或值。下列範例會刪除`hello-repository`儲存庫中含有 image 標籤的影像`latest`。若要從儲存庫中刪除範例影像，請執行下列命令：

```
aws ecr batch-delete-image \
```

```
      --repository-name hello-repository \
      --image-ids imageTag=latest \
      --region region
```

## 步驟 7：刪除儲存庫

如果您不再需要整個影像儲存庫，您可以刪除儲存庫。下列範例會使用`--force`旗標來刪除包含影像的儲存庫。若要刪除包含映像的儲存庫 (以及其中所有的映像)，您可執行以下命令：

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

# 最佳化 Amazon ECR 的效能

您可以使用下列有關設定和策略的建議來優化使用 Amazon ECR 時的效能。

使用 Docker 1.10 與以上版本以取得同時分層上傳優勢

Docker 映像是由各層組成，亦是映像的中介建立階段。Dockerfile 中的每一行都會導致新層的建立。當您使用 Docker 1.10 或以上版本，Docker 預設會在同時上傳 Amazon ECR 時盡量推送越多的層，因此上傳時間會更快。

使用較小的基礎映像

整個 Docker Hub 可用的預設映像可能會包括許多您的應用程式不需要的依存項目。請考慮使用 Docker 社群中由其他人所建立並維護的較小映象，或者使用 Docker 的最小 Scratch 映像建立您自己的基礎映像。如需詳細資訊，請參閱 Docker 文件中的建立基礎映像。

先前在 Dockerfile 中放置最少更改的依存項目

Docker 快取層可加速建立時間。如果最後一次建立後分層便沒有任何變更，Docker 會使用快取的版本，而不會重新建立該分層。然而，每一分層會以之前的分層作為依據。如果分層變更了，Docker 不僅會重新編譯該分層，也會重新編譯任何之後的分層。

若要將重建 Docker 檔案與重新上傳分層的時間縮至最短，請考慮在您的 Docker 檔案中先置放變更頻率最少的依存項目。並稍後在堆疊中置放快速變更的依存項目 (例如您的應用程式原始碼)。

鏈結命令以避免不必要的檔案儲存

分層上建立的中介檔案即使在後續分層中被刪除了，仍將保持為該分層的一部分。請思考下列範例：

```
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
```

在此範例中，由第一、二個 RUN 命令所建立的分層仍將包括原始的 .tar.gz 檔案以及其所有解壓縮的內容。即使第四個 RUN 命令已將 .tar.gz 檔案刪除，這些命令可鏈結在一起成為單一的 RUN 陳述式，以確保這些不必要的檔案不會成為最終 Docker 映像的一部分：

```
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
```

### 使用最接近的區域端點

您可透過使用最接近您執行中的應用程式的區域端點，以減少從 Amazon ECR 提取映像的延遲。如果您的應用程式正在 Amazon EC2 執行個體上執行，您可使用下列 shell 程式碼以從該執行個體的可用區域取得區域：

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

可以使用--region參數將區域傳遞至 AWS CLI 指令，或使用指aws configure令設定為輪廓的預設區域。您也可以在使用 AWS SDK 撥打電話時設定區域。如需詳細資訊，請參閱您特定程式設計語言的開發套件文件。

# Amazon ECR 私有登錄檔

Amazon ECR 私有登錄檔採用可用度高且可擴展的架構來託管您的容器映像。您可以使用自己的私有登錄檔來管理由 Docker 和開放容器計畫 (OCI) 映像和成品組成的私有映像儲存庫。每個 AWS 帳戶都提供預設的私有 Amazon ECR 登錄檔。如需 Amazon ECR 公有登錄檔的詳細資訊，請參閱《Amazon Elastic Container Registry Public 使用者指南》中的公有登錄檔。

## 私有登錄檔概念

- 預設私有登錄檔的 URL 是 `https://aws_account_id.dkr.ecr.us-west-2.amazonaws.com`。
- 根據預設，您的帳戶在私有登錄檔中擁有讀取與寫入存取權。不過，使用者需要許可才能呼叫 Amazon ECR API，以及將映像推送或從您的私有儲存庫提取影像。Amazon ECR 提供數個受管政策，以控制不同層級的使用者存取。如需詳細資訊，請參閱 Amazon Elastic Container Registry 身分型政策的範例。
- 必須授權您的 Docker 用戶端到私有登錄檔，才可使用 docker push 與 docker pull 命令來推送映像至該登錄檔中的儲存庫及自該儲存庫中提取映像。如需詳細資訊，請參閱 Amazon ECR 中的私有登錄身份驗證。
- 私有儲存庫可透過 使用者存取政策及儲存庫政策加以控制。如需有關儲存庫政策的詳細資訊，請參閱 Amazon ECR 中的私有儲存庫政策。
- 透過為您的私有登錄檔配置複寫，您的私有登錄檔中的儲存庫可以橫越您自己的私有登錄檔中的區域複寫，也可以橫越單獨的帳戶複寫。如需詳細資訊，請參閱 Amazon ECR 中的私有映像複寫。

# Amazon ECR 中的私有登錄身份驗證

您可以使用 AWS Management Console AWS CLI、或 AWS SDK 來建立和管理私有存放庫。您可以使用這些方法來在映像上執行部分動作，例如列清單或刪除。這些用戶端使用標準 AWS 驗證方法。即使您可以使用 Amazon ECR API 推送並提取映像，您仍較有可能使用 Docker CLI 或依語言而定的 Docker 資料庫。

Docker CLI 不支援原生的 IAM 驗證方法。必須採取額外的步驟，Amazon ECR 才能驗證及授權 Docker 推送與提取請求。

下列各節詳述的登錄檔驗證方法可用。

# 使用 Amazon ECR 憑證協助程式

Amazon ECR 提供 Docker 憑證協助程式，可在推送和提取映像至 Amazon ECR 時更容易儲存和使用 Docker 憑證。如要了解安裝和設定步驟，請參閱 Amazon ECR Docker 憑證協助程式。

> **Note**
>
> Amazon ECR Docker 憑證協助程式目前不支援多重要素驗證 (MFA)。

## 使用授權字符

授權字符的許可權範圍與用來擷取身分驗證字符之 IAM 委託人的許可範圍相符。身分驗證字符是用來存取 IAM 委託人有權存取且有效期為 12 小時的任何 Amazon ECR 登錄檔。若要取得授權權杖，您必須使用 GetAuthorizationTokenAPI 作業擷取包含使用者名稱AWS和編碼密碼的 base64 編碼授權權杖。該 AWS CLI `get-login-password`命令通過檢索並解碼授權令牌來簡化此操作，然後您可以將其傳輸到docker login命令中進行身份驗證。

若要使用 get-login 向 Amazon ECR 私有登錄檔驗證 Docker

- 若要使用向 Amazon ECR 登錄驗證碼頭視窗 get-login-password，請執行命令。aws ecr get-login-password將身分驗證字符傳遞給 docker login 命令時，使用 AWS 的值作為使用者名稱並指定您要驗證的 Amazon ECR 登錄檔 URI。如果是向多個登錄進行驗證，您必須針對每個登錄重複此命令。

  > **Important**
  >
  > 若您收到錯誤，請安裝或升級至最新版本的 AWS CLI。如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》中的安裝 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
    ```

  - 取得 ECR () LoginCommandAWS Tools for Windows PowerShell

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

## 使用 HTTP API 身分驗證

Amazon ECR 支援 Docker 登錄檔 HTTP API。但是，因 Amazon ECR 為私有登錄檔，您必須使用每個 HTTP 請求來提供驗證字符。您可以使用 for -H 選項新增 HTTP 授權標頭，curl並傳遞命get-authorization-token AWS CLI 令提供的授權權杖。

使用 Amazon ECR HTTP API 進行身分驗證

1. 使用擷取授權權杖， AWS CLI 並將其設定為環境變數。

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

2. 將 $TOKEN 變數傳遞到 curl 的 -H 選項來向 API 驗證身分。例如，下列命令會列出在 Amazon ECR 儲存庫中的映像標籤。如需詳細資訊，請參閱 Docker 登錄檔 HTTP API 參考文件。

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

   其輸出如下：

   ```
   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"]}
   ```

# Amazon ECR 中的私有註冊表設置

Amazon ECR 使用私有登錄檔設定在登錄檔層級設定功能。私有登錄檔設定會針對每個區域分別設定。您可以使用私有登錄檔設定來設定下列功能。

- 登錄檔許可：登錄檔許可政策可控制複寫並提取快取許可。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表許可。
- 提取快取規則：使用提取快取規則，從 Amazon ECR 私有登錄檔的上游登錄檔快取映像。如需詳細資訊，請參閱 將上游註冊表與 Amazon ECR 私有註冊表同步。
- 複寫組態：複寫組態可用來控制是否要跨 AWS 區域或帳戶複製儲存庫。如需更多資訊，請參閱Amazon ECR 中的私有映像複寫
- 儲存庫建立範本：儲存庫建立範本用於定義 Amazon ECR 代表您建立新儲存庫時要套用的標準設定。例如，透過提取快取動作建立的儲存庫。如需詳細資訊，請參閱 用於控制在提取快取動作期間建立的儲存庫的範本。
- 掃描組態：預設情況下，登錄檔已啟用基本型掃描。您可以啟用提供自動化連續掃描模式的增強型掃描，來掃描作業系統和程式設計語言套件的弱點。如需詳細資訊，請參閱 掃描影像以查看 Amazon ECR 中的軟體漏洞。

# Amazon ECR 中的私有註冊表許可

Amazon ECR 使用登錄檔政策，將許可授予在私有登錄檔層級的 AWS 主體。這些許可用於設定對複寫以及「透過快取提取」功能的存取權限範圍。

Amazon ECR 僅在私有登錄檔層級強制執行以下許可。如果將任何其他動作新增至登錄檔政策中，則會發生錯誤。

- `ecr:ReplicateImage` – 授予許可給另一個帳戶 (稱為來源登錄檔)，以將其映像複製到登錄檔。這僅用於跨帳戶複寫。
- `ecr:BatchImportUpstreamImage` – 授予檢索外部映像並將其匯入到您的私有登錄檔的許可。
- `ecr:CreateRepository` – 授予在私有登錄檔中建立儲存庫的許可。如果存放複製或快取映像的儲存庫在私有登錄檔中尚不存在，則需要此許可。

> **Note**
>
> 雖然可以將 `ecr:*` 動作新增到私有登錄檔許可政策中，但最佳實務是僅根據您使用的功能新增所需的特定動作，而不是使用萬用字元。

主題

- Amazon ECR 的私有註冊表政策示例

- 授與 Amazon ECR 中跨帳戶複寫的登錄許可
- 授予登錄許可以在 Amazon ECR 中提取快取

## Amazon ECR 的私有註冊表政策示例

以下範例顯示您可以用來控制使用者具有之 Amazon ECR 登錄檔許可的登錄檔許可政策陳述式。

> **Note**
>
> 在每個範例中，如果 `ecr:CreateRepository` 動作會從您的登錄檔許可陳述式中移除，複寫仍然可能發生。但是，為了成功複寫，您需要在帳戶中建立具有相同名稱的儲存庫。

### 範例：允許來源帳戶的根使用者複寫所有儲存庫

下列登錄權限原則可讓來源帳戶的 root 使用者複寫所有儲存庫。

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

### 範例：允許來自多個帳戶的 root 使用者

下列登錄權限原則有兩個陳述式。每個陳述式都允許來源帳戶的 root 使用者複寫所有儲存庫。

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

### 範例：允許來源帳戶的根使用者複寫具有字首 **prod-** 的所有儲存庫。

下列登錄權限原則可讓來源帳戶的 root 使用者複寫以開頭的所有儲存庫`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-*"
            ]
        }
    ]
}
```

## 授與 Amazon ECR 中跨帳戶複寫的登錄許可

跨帳戶政策類型會用來授予 AWS 委託人許可，允許將儲存庫從來源登錄檔複寫到登錄檔。根據預設，您可以在自己的登錄檔中設定跨區域複寫的許可。您只需要設定登錄檔政策，如果您授予另一個帳戶將內容複寫到登錄檔的許可。

登錄檔政策必須授予 `ecr:ReplicateImage` API 動作的許可。這個 API 為內部的 Amazon ECR API，可以在區域或帳戶之間複寫映像。您也可以授予 `ecr:CreateRepository` 許可，這允許 Amazon ECR 在您的登錄檔中建立儲存庫 (如果它們尚不存在)。如果未提供 `ecr:CreateRepository` 許可，則必須在登錄檔中手動建立具有與來源儲存庫相同名稱的儲存庫。如果兩者都未完成，複寫則會失敗。任何失敗 CreateRepository 或 ReplicateImage API 動作都會顯示在中 CloudTrail。

設定複寫許可政策 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列，選擇要在其中設定登錄檔政策的區域。
3. 在導覽窗格中，選擇 Private registry (私有登錄檔)、Registry permissions (登錄檔許可)。
4. 在 Registry permissions (登錄檔許可) 頁面上，選擇 Generate statement (產生陳述式)。
5. 使用政策產生器完成下列步驟以定義您的政策陳述式。
    a. 對於 Policy Type (政策類型)，選擇 Cross-account policy (跨帳戶政策)。
    b. 對於 Statement ID (陳述式 ID)，輸入唯一陳述式 ID。此欄位用作 `Sid` 在登錄檔政策上。

c. 對於 Accounts (帳戶)，輸入您要授予許可的每個帳戶的帳戶 ID。指定多個帳戶 ID 時，以逗號分隔。

6. 展開 Preview policy statement (預覽政策陳述式) 章節，以檢閱登錄檔許可政策陳述式。
7. 確認政策陳述式後，選擇 Add to policy (新增至政策) 以將政策儲存至您的登錄檔。

### 設定複寫許可政策 (AWS CLI)

1. 建立名為 `registry_policy.json` 的檔案，並將其填入登錄檔政策。

```
{
    "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. 使用政策檔案建立登錄檔政策。

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

3. 擷取登錄檔的政策以確認。

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

# 授予登錄許可以在 Amazon ECR 中提取快取

Amazon ECR 私有登錄檔許可可用來設定個別 IAM 實體使用提取快取的許可範圍。如果 IAM 實體擁有的由 IAM 政策授予的許可多過登錄檔許可政策授予的許可，則 IAM 政策優先。

建立私有登錄檔的許可政策 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列選擇要在其中設定私有登錄檔許可陳述式的區域。
3. 在導覽窗格中，選擇 Private registry (私有登錄檔)、Registry permissions (登錄檔許可)。
4. 在 Registry permissions (登錄檔許可) 頁面上，選擇 Generate statement (產生陳述式)。
5. 針對您要建立的每個提取快取許可政策陳述式，執行下列動作。

    a. 針對 Policy type (政策類型)，選擇 Pull through cache policy (提取快取政策)。

    b. 針對 Statement id (陳述式 ID)，提供提取快取陳述式政策的名稱。

    c. 針對 IAM entities (IAM 實體)，指定要包含在政策中的使用者、群組或角色。

    d. 針對 Repository namespace (儲存庫命名空間)，選取要與政策建立關聯的提取快取規則。

    e. 針對 Repository names (儲存庫名稱)，指定要套用規則的儲存庫基本名稱。例如，如果您想要在 Amazon ECR Public 上指定 Amazon Linux 儲存庫，則儲存庫名稱會是 `amazonlinux`。

# Amazon ECR 私有儲存庫

Amazon ECR 私有儲存庫包含您的碼頭映像、開放容器倡議 (OCI) 映像，以及 OCI 相容成品。您可以使用 Amazon ECR API 操作或 Amazon ECR 主控台的儲存庫區段來建立、監控和刪除映像儲存庫，以及設定可以存取這些影像儲存庫的權限。Amazon ECR 也與 Docker CLI 整合，因此您可以將開發環境中的映像推送和提取到儲存庫。

主題



## 私有儲存庫概念

- 根據預設，您的帳戶在預設登錄檔中擁有讀取與寫入存取權 (*aws_account_id*.dkr.ecr.*region*.amazonaws.com)。然而，使用者需要許可來對 Amazon ECR API 進行呼叫，並從您的儲存庫推送或提取映像。Amazon ECR 提供數個受管政策，以控制不同層級的使用者存取。如需詳細資訊，請參閱 Amazon Elastic Container Registry 身分型政策的範例。
- 儲存庫可透過 使用者存取政策及個別儲存庫政策加以控制。如需詳細資訊，請參閱 Amazon ECR 中的私有儲存庫政策。
- 儲存庫名稱可支援命名空間，您也可用該命名空間為相似的儲存庫分組。例如，如果有數個團隊使用相同的登錄檔，團隊 A 可使用 `team-a` 命名空間，而團隊 B 可使用 `team-b` 命名空間。如果這麼做，每個團隊都有自己的名為 `web-app` 的映像，每個映像都以團隊命名空間開頭。此組態允許在不干擾的情況下同時使用每個團隊上的這些映像。A 團隊的映像為 `team-a/web-app`，B 團隊的映像為 `team-b/web-app`。
- 您的映像可以在您自己的登錄檔和帳戶之間複寫到其他儲存庫。您可以藉由在登錄檔設定中指定複寫組態來執行這項操作。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表設置。

# 建立 Amazon ECR 私有儲存庫來存放映像檔

建立 Amazon ECR 私有儲存庫，然後使用儲存庫存放您的容器映像。遵循以下步驟，使用 AWS Management Console建立私有儲存庫。如需使用建立存放庫的步驟 AWS CLI，請參閱步驟 3：建立一個儲存庫。

建立儲存庫 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列選擇您儲存庫所建立的區域。
3. 在「儲存庫」頁面上，選擇「專用儲存區域」，然後選擇「建立儲存區
4. 對於 Visibility settings (可見度設定)，確認已選取 Private (私有)。
5. 在 Repository name (儲存庫名稱), 中，為您的儲存庫輸入獨一無二的名稱。儲存庫名稱可以自行指定 (例如 `nginx-web-app`)。或者，可以在其前面加上命名空間，以將儲存庫分組到類別中 (例如 `project-a/nginx-web-app`)。

   > **Note**
   >
   > 儲存庫名稱可以是最多 256 個字元的容器。名稱必須以字母開頭，且只能包含小寫字母、數字、連字號、底線、句號和斜線。不支援使用雙連字號、雙底線或雙斜線。

6. 對於 Tag mutability (標籤不變性)，選擇儲存庫的標籤可變性設定。設定不可變標籤的儲存庫會防止映像被覆寫。如需詳細資訊，請參閱 防止 Amazon ECR 中的圖像標籤被覆蓋。
7. 對於 Scan on push (推送時掃描)，雖然您可以在儲存庫層級指定基本掃描的掃描設定，但最佳實務是在私有登錄檔層級指定掃描組態。在私有登錄檔層級指定掃描設定讓您能啟用增強型掃描或基本掃描，還能定義篩選條件來指定要掃描哪些儲存庫。如需詳細資訊，請參閱 掃描影像以查看 Amazon ECR 中的軟體漏洞。
8. 對於 KMS 加密，請選擇是否使用啟用存放庫中映像的加密 AWS Key Management Service。根據預設，啟用 KMS 加密時，Amazon ECR 會使用別名 AWS 受管金鑰 `aws/ecr` (KMS 金鑰)。首次建立啟用 KMS 加密的儲存庫時，會在您的帳戶中建立此金鑰。如需詳細資訊，請參閱 靜態加密。
9. 啟用 KMS 加密時，請選取 Customer encryption settings (advanced) (客戶加密設定 (進階)) 來選擇您自己的 KMS 金鑰。KMS 金鑰必須位於與叢集相同的區域。選擇 [建立 AWS KMS 金鑰] 以瀏覽至主 AWS KMS 控台以建立您自己的金鑰。
10. 選擇建立儲存庫。

## 後續步驟

若要檢視將影像推送至儲存庫的步驟，請選取儲存區域，然後選擇檢視推送命令。如需將映像推送到您的儲存庫的詳細資訊，請參閱 將映像推送到 Amazon ECR 私有存儲庫。

# 檢視 Amazon ECR 中私有儲存庫的內容和詳細資訊

建立私人存放庫之後，您可以在以下位置檢視有關儲存庫的詳細資訊 AWS Management Console：

- 在儲存庫中存放的是哪些映像
- 有關存放在儲存庫中每個映像的詳細資訊，包括每個映像的大小和 SHA 摘要
- 指定的儲存庫內容掃描頻率
- 儲存庫是否具有與其相關聯的作用中提取快取規則
- 儲存庫的加密設定

> **Note**
>
> 若以 Docker 1.9 版本開始，Docker 用戶端在將映像推送至 V2 Docker 登錄檔前，會先壓縮映像層。docker images 命令的輸出會顯示未壓縮的映像大小。因此，請記住，Docker 可能會傳回比 AWS Management Console中顯示的映像更大的映像。

檢視儲存庫資訊 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列上，選擇包含要檢視的儲存庫區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在 Repositories (儲存庫) 頁面上，選擇 Private (私有) 分頁，然後選擇要檢視的儲存庫。
5. 在儲存庫詳細資訊頁面上，主控台預設為顯示 Images (映像) 檢視。使用導覽選單檢視與儲存庫有關的其他資訊。
   - 選擇 Summary (摘要) 檢視儲存庫詳細資訊和儲存庫的提取計數資料。
   - 選擇 Images (映像) 檢視關於儲存庫中映像標籤的資訊。若要檢視關於映像的詳細資訊，請選取映像標籤。如需詳細資訊，請參閱 在 Amazon ECR 中查看圖像詳細信息。

     如果有您想刪除的未標記映像，您可以選擇儲存庫左方的方塊以刪除並選擇 Delete(刪除)。如需詳細資訊，請參閱 刪除 Amazon ECR 中的圖像。

- 選擇 Permissions (許可) 以檢視套用到儲存庫的儲存庫政策。如需詳細資訊，請參閱 Amazon ECR 中的私有儲存庫政策。
- 選擇 Lifecycle Policy (生命週期政策) 以檢視套用到儲存庫的生命週期政策。您也可在此檢視生命週期事件歷史。如需詳細資訊，請參閱 在 Amazon ECR 中使用生命週期政策自動清理映像檔。
- 選擇 Tags (標籤) 以檢視套用到儲存庫的中繼資料標籤。

# 刪除 Amazon ECR 中的私有存儲庫

如果儲存庫已使用完畢，即可將其刪除。當您刪除中的存放庫時 AWS Management Console，儲存庫中包含的所有影像也會一併刪除；這無法復原。

> **Important**
>
> 刪除的儲存庫中的影像也會被刪除。您無法復原此操作。

若要刪除儲存庫 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列上，選擇包含要刪除的儲存庫區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在 Repositories (儲存庫) 頁面上，選擇 Private (私有) 分頁，然後選擇要刪除的儲存庫並選擇 Delete (刪除)。
5. 在 Delete ***repository_name*** (刪除 repository_name) 視窗中，確認應刪除的儲存庫已被選擇，再選擇 Delete (刪除)。

# Amazon ECR 中的私有儲存庫政策

Amazon ECR 使用資源型許可來控制儲存庫的存取。以資源為基礎的權限可讓您指定哪些使用者或角色可以存取存放庫，以及他們可以在存放庫上執行哪些動作。依預設，只有建立儲存庫的 AWS 帳戶才能存取存放庫。您可以套用儲存庫原則，以允許其他存取存放庫。

主題

- 儲存庫政策與 IAM 政策的比較

- Amazon ECR 中的私有儲存庫政策範例
- 在 Amazon ECR 中設定私有儲存庫政策聲明

## 儲存庫政策與 IAM 政策的比較

Amazon ECR 儲存庫政策是 IAM 政策的子集，其範圍和專門用於控制對單個 Amazon ECR 儲存庫的存取。IAM 政策通常用於套用整個 Amazon ECR 服務的許可，但也可用於控制對特定資源的存取。

在決定特定使用者或角色可以對儲存庫執行哪些動作時，Amazon ECR 儲存庫政策和 IAM 政策都會用到。如果使用者或角色透過儲存庫政策獲准執行某個動作，但是透過 IAM 政策被拒絕許可 (反之亦然)，則該動作將被拒絕。透過儲存庫政策或 IAM 政策任何一個即可允許使用者或角色的動作許可，但不需要兩者都允許。

> **Important**
>
> Amazon ECR 要求使用者擁有透過 IAM 政策呼叫 `ecr:GetAuthorizationToken` API 的許可，然後才能對登錄檔進行身分驗證，並從任何 Amazon ECR 儲存庫推送或提取任何映像。Amazon ECR 提供數個受管 IAM 政策來控制各種層級的使用者存取；如需詳細資訊，請參閱 Amazon Elastic Container Registry 身分型政策的範例。

您可以使用這些政策類型的任何一個，來控制對您儲存庫的存取，如下列範例所示。

此範例顯示一個 Amazon ECR 儲存庫政策，允許特定使用者描述儲存庫和儲存庫中的映像。

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

此範例顯示一個 IAM 政策，透過使用資源參數將政策的範圍限定在儲存庫 (以儲存庫的完整 ARN 指定)，可達成上述相同的目標。如需有關 Amazon 資源名稱 (ARN) 格式的詳細資訊，請參閱 資源。

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

## Amazon ECR 中的私有儲存庫政策範例

> **Important**
>
> 此頁面上的儲存庫政策範例旨在套用至 Amazon ECR 私有儲存庫。如果直接與 IAM 主體搭配使用，除非為了將 Amazon ECR 儲存庫指定為資源而進行修改，否則它們將無法正常運作。如需有關設定儲存庫政策的詳細資訊，請參閱 在 Amazon ECR 中設定私有儲存庫政策聲明。

Amazon ECR 儲存庫政策是 IAM 政策的子集，其範圍和專門用於控制對單個 Amazon ECR 儲存庫的存取。IAM 政策通常用於套用整個 Amazon ECR 服務的許可，但也可用於控制對特定資源的存取。如需詳細資訊，請參閱 儲存庫政策與 IAM 政策的比較。

以下儲存庫政策範例顯示您可以用來控制 Amazon ECR 私有儲存庫存取的許可陳述式。

> **Important**
>
> Amazon ECR 要求使用者擁有透過 IAM 政策呼叫 `ecr:GetAuthorizationToken` API 的許可，然後才能對登錄檔進行身分驗證，並從任何 Amazon ECR 儲存庫推送或提取任何映像。Amazon ECR 提供數個受管 IAM 政策來控制各種層級的使用者存取；如需詳細資訊，請參閱 Amazon Elastic Container Registry 身分型政策的範例。

## 範例：允許一或多個 使用者

以下儲存庫政策允許一個或多個 使用者向儲存庫推送和從儲存庫提取映像。

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

## 範例：允許其他帳戶

下列儲存庫政策允許特定帳戶推入映像。

> **Important**
>
> 您授予許可的帳戶必須啟用您正在建立儲存庫政策的區域，否則會發生錯誤。

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

下列儲存庫政策允許部分使用者提取映像 (*pull-user-1* 與 *pull-user-2*)，同時提供其他使用者 (*admin-user*) 完整存取權限。

> **Note**
>
> 對於目前不支援的更複雜的儲存庫原則 AWS Management Console，您可以使用set-repository-policy AWS CLI 命令套用原則。

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

## 範例：拒絕全部

下列儲存庫政策拒絕所有使用者擁有抽出映像的能力。

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

## 範例：限制特定 IP 地址的存取

在套用來自特定地址範圍的儲存庫時，下列範例拒絕任何使用者執行任何 Amazon ECR 操作的許可。

此陳述式中的條件會識別允許之網際網路通訊協定第 4 版 (IPv4) IP 地址的 `54.240.143.*` 範圍。

該Condition塊使用NotIpAddress條件和條aws:SourceIp件鍵，這是一個 AWS寬的條件鍵。如需有關這些條件索引鍵的詳細資訊，請參閱 AWS 全域條件內容索引鍵。aws:sourceIp IPv4 值會使用標準 CIDR 表示法。如需詳細資訊，請參閱《IAM 使用者指南》中的 IP 地址條件運算子。

```
{
```

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

## 範例：允許 AWS 服務

下列儲存庫政策允許 AWS CodeBuild 存取與該服務整合所需的 Amazon ECR API 動作。使用以下範例時，您應該使用 `aws:SourceArn` 和 `aws:SourceAccount` 條件索引鍵來調查可以承擔這些許可的資源。如需詳細資訊，請參閱AWS CodeBuild 使用者指南 CodeBuild中的 Amazon ECR 範例。

```
{
   "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"
```

```
            }
         }
      }
   ]
}
```

## 在 Amazon ECR 中設定私有儲存庫政策聲明

您可以 AWS Management Console 依照下列步驟將存取原則陳述式新增至中的存放庫。您可以為每個儲存庫新增多個政策陳述式。如需範例政策，請參閱 Amazon ECR 中的私有儲存庫政策範例。

> **Important**
>
> Amazon ECR 要求使用者擁有透過 IAM 政策呼叫 `ecr:GetAuthorizationToken` API 的許可，然後才能對登錄檔進行身分驗證，並從任何 Amazon ECR 儲存庫推送或提取任何映像。Amazon ECR 提供數個受管 IAM 政策來控制各種層級的使用者存取；如需詳細資訊，請參閱 Amazon Elastic Container Registry 身分型政策的範例。

設定儲存庫政策陳述式

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列上，選擇其中包含要設定政策陳述式的儲存庫之區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在 Repositories (儲存庫)頁面上，選擇要設定政策陳述式的儲存庫來檢視儲存庫內容。
5. 從儲存庫映像清單檢視的導覽窗格中，選擇 Permissions (許可)、Edit (編輯)。

   > **Note**
   >
   > 如果您在導覽窗格中看不到 Permissions (許可) 選項，請確保您位於儲存庫映像清單檢視中。

6. 在 Edit permissions (編輯許可) 頁面上，選擇 Add statement (新增陳述式)。
7. 對於 Statement name (陳述式名稱)，輸入陳述式的名稱。
8. 對於 Effect (效果)，選擇會產生允許或明確拒絕的政策陳述式。
9. 對於 Principal (代理人)，請選擇要套用政策陳述式的使用者範圍。如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS IAM JSON 政策元素：條件。

- 您可以選取 [每個人 (*)] 核取方塊，將陳述式套 AWS 用至所有已驗證的使用者。
- 對於 Service principal (服務委託人)，指定服務委託人名稱 (例如 `ecs.amazonaws.com`) 以套用陳述式到特定的服務。
- 對於AWS 帳戶 ID，請指定 AWS 帳戶號碼 (例如，111122223333)，將對帳單套用至特定 AWS 帳戶下的所有使用者。您可以使用逗號分隔清單來指定多個帳戶。

> **Important**
>
> 您授予許可的帳戶必須啟用您正在建立儲存庫政策的區域，否則會發生錯誤。

- 對於 IAM 實體，請選取您 AWS 帳戶下要套用陳述式的角色或使用者。

> **Note**
>
> 對於目前不支援的更複雜的儲存庫原則 AWS Management Console，您可以使用set-repository-policy AWS CLI 命令套用原則。

10. 對於 Actions (動作)，請選擇政策陳述式應從個別 API 操作清單中套用的 Amazon ECR API 操作範圍。
11. 當您完成時，請選擇 Save (儲存) 來設定政策。
12. 為要新增之每個儲存庫政策的重複之前的步驟。

# 在 Amazon ECR 中標記私有存儲庫

為了協助您管理 Amazon ECR 儲存庫，您可以使用 AWS 資源標籤，將自己的中繼資料指派給新的或現有的 Amazon ECR 儲存庫。例如，您可以為帳戶的 Amazon ECR 儲存庫定義一組標籤，協助您追蹤各個儲存庫的擁有者。

## 標籤基本概念

標籤對 Amazon ECR 來說不具有任何語意意義，並會嚴格解譯為字元字串。標籤不會自動指派給您的資源。您可以編輯標籤金鑰和值，並且可以隨時從資源移除標籤。您可以將標籤的值設為空白字串，但您無法將標籤的值設為 Null。若您將與現有標籤具有相同鍵的標籤新增到該資源，則新值會覆寫舊值。如果您刪除資源，也會刪除任何該資源的標籤。

您可以使用 Amazon ECR 主控台 AWS CLI、和 Amazon ECR API 使用標籤。

您可以使用 AWS Identity and Access Management (IAM) 控制 AWS 帳戶中哪些使用者有權建立、編輯或刪除標籤。如需 IAM 政策中標籤的相關資訊，請參閱the section called “使用標籤型存取控制”。

## 標記您的資源以便計費

您新增至 Amazon ECR 儲存庫的標籤在成本與用量報告中啟用後，有助於檢視成本分配。如需詳細資訊，請參閱 Amazon ECR 用量報告。

若想要查看合併資源的成本，您可根據具有相同標籤金鑰值的資源來整理您的帳單資訊。例如，您可以使用特定應用程式名稱來標記數個資源，然後整理帳單資訊以查看該應用程式跨數項服務的總成本。如需有關使用標籤設定成本分配報告的詳細資訊，請參閱《AWS Billing 使用者指南》中的每月成本分配報告。

> **Note**
>
> 若您才剛啟用報告，目前月份的資料會在 24 小時之後提供檢視。

## 在 Amazon ECR 中將標籤添加到私有存儲庫

您可以將標籤新增至私人存放庫。

如需有關標籤名稱和最佳做法的資訊，請參閱《標記 AWS 資源使用指南》中的標籤命名限制和要求和最佳做法。

將標籤新增至儲存庫 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列中選取要使用的區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在儲存庫頁面上，選取要標記之儲存庫旁邊的核取方塊。
5. 從動作選單中選取儲存庫標籤。
6. 在儲存庫標籤頁面上，選取新增標籤、新增標籤。
7. 在編輯儲存庫標籤頁面上，指定每個標籤的索引鍵和值，然後選擇儲存。

將標籤添加到存儲庫（AWS CLI 或 API）

您可以使用或 API 來新增或覆寫一 AWS CLI 或多個標籤。

- AWS CLI -標籤資源
- API 動作-TagResource

下列範例顯示如何使用新增標籤 AWS CLI。

範例 1：標記儲存庫

下面的命令標記一個存儲庫。

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

範例 2：使用多個標籤標記儲存庫

下面的命令添加三個標籤到一個存儲庫。

```
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
```

範例 3：列出儲存庫的標籤

下面的命令列出了與存儲庫關聯的標籤。

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

範例 4：建立儲存庫並新增標籤

以下命令建立名為 `test-repo` 的儲存庫，並新增索引鍵為 `team` 和值為 `devs` 的標籤。

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

## 從 Amazon ECR 中的私有存儲庫中刪除標籤

您可以從私人存放庫刪除標籤。

若要從私人存放庫刪除標籤 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列中選取要使用的區域。
3. 在儲存庫頁面上，選取要移除標籤之儲存庫旁邊的核取方塊。
4. 從動作選單中選取儲存庫標籤。
5. 在儲存庫標籤頁面上，選取編輯。
6. 在編輯儲存庫標籤頁面上，針對您要刪除的每個標籤，選取移除圖示，然後選擇儲存。

若要從私人存放庫刪除標籤 (AWS CLI)

您可以使用或 API 刪除一 AWS CLI 或多個標籤。

- AWS CLI -無標記資源
- API 動作-UntagResource

下列範例顯示如何使用刪除儲存庫中的標籤 AWS CLI。

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

# Amazon ECR 中的私人映像

Amazon ECR 會將 Docker 映像、開放容器倡議 (OCI) 映像以及與 OCI 相容的成品儲存在私有儲存庫中。您可以使用 Docker CLI 或您偏好的用戶端來向您的儲存庫推送和提取映像。

主題



## 將映像推送到 Amazon ECR 私有存儲庫

您可以將 Docker 映像、資訊清單清單和開放容器計畫 (OCI) 映像和相容的成品推送至您的私有儲存庫。

Amazon ECR 也提供一種將映像複寫到其他儲存庫的方法。透過在私人登錄設定中指定複寫組態，您可以跨區域在自己的登錄和不同帳戶之間進行複寫。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表設置。

主題

# 將映像推送到 Amazon ECR 私有儲存庫的 IAM 許可

使用者需要 IAM 許可才能將映像推送到 Amazon ECR 私有儲存庫。遵循授與最少權限的最佳作法，您可以授與特定存放庫的存取權。您也可以授予所有存放庫的存取權。

使用者必須透過請求授權字符，向他們想要推送映像的每個 Amazon ECR 登錄檔進行身分驗證。Amazon ECR 提供多種 AWS 受管政策，以控制不同層級的使用者存取。如需詳細資訊，請參閱 AWS Amazon 彈性容器註冊表的受管政策。

您也可以建立自己的 IAM 政策。以下 IAM 政策授予將映像推送到特定存放庫的必要許可。儲存庫必須指定為完整的 Amazon Resource Name (ARN)。

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

以下 IAM 政策授予將映像推送到所有存放庫的必要許可。

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

```
                "ecr:CompleteLayerUpload",
                "ecr:GetAuthorizationToken",
                "ecr:UploadLayerPart",
                "ecr:InitiateLayerUpload",
                "ecr:BatchCheckLayerAvailability",
                "ecr:PutImage"
            ],
            "Resource": "*"
        }
    ]
}
```

## 將碼頭映像推送到 Amazon ECR 私有存儲庫

您可以使用 docker push 命令將容器映像推送到 Amazon ECR 儲存庫。

Amazon ECR 也支援建立和推送用於多架構映像的 Docker 資訊清單清單。如需相關資訊，請參閱將多架構映像推送到 Amazon ECR 私有儲存庫。

將 Docker 映像推送至 Amazon ECR 儲存庫

在您推送映像之前，Amazon ECR 儲存庫必須存在。如需詳細資訊，請參閱 the section called “建立儲存庫以儲存影像”。

1. 向打算推送映像的 Amazon ECR 登錄檔驗證您的 Docker 用戶端。所用的每個登錄檔皆必須取得身分驗證字符，字符有效期間為 12 個小時。如需詳細資訊，請參閱 Amazon ECR 中的私有登錄身份驗證。

   若要向 Amazon ECR 登錄檔驗證 Docker，請執行 aws ecr get-login-password 命令。將身分驗證字符傳遞給 docker login 命令時，使用 AWS 的值作為使用者名稱並指定您要驗證的 Amazon ECR 登錄檔 URI。如果是向多個登錄進行驗證，您必須針對每個登錄重複此命令。

   > **Important**
   >
   > 若您收到錯誤，請安裝或升級至最新版本的 AWS CLI。如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》中的安裝 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. 如果打算推送映像的登錄檔內沒有您的映像儲存庫，請自行建立。如需詳細資訊，請參閱 建立 Amazon ECR 私有儲存庫來存放映像檔。
3. 找出要推送的本機映像。執行 docker images 命令，列出系統上的容器映像。

   ```
   docker images
   ```

   可用 *repository:tag* 值或映像 ID 從產生的命令輸出中找出映像。
4. 在映像上標記要使用的 Amazon ECR 登錄檔、儲存庫和可選用的映像標籤名稱組合。登錄檔格式為 *aws_account_id*.dkr.ecr.*us-west-2*.amazonaws.com。儲存庫名稱應與您為映像建立的儲存庫名稱相符。如果省略映像標籤，系統將假設標籤為 latest。

   以下範例將 ID *e9ae3c220b23* 的本機映像標記為 *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. 使用 docker push 命令推送映像：

   ```
   docker push aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository:tag
   ```
6. (選用) 重覆執行 Step 4 和 Step 5，套用任何其他標籤至映像，並將標籤推送至 Amazon ECR。

## 將多架構映像推送到 Amazon ECR 私有儲存庫

您可以建立和推送 Docker 資訊清單清單，將多架構映像推送至 Amazon ECR 儲存庫。資訊清單列表是藉由指定一或多個映像名稱而建立的映像清單。在大多數情況下，資訊清單清單是從提供相同功能但適用於不同作業系統或架構的映像檔建立的。資訊清單不是必要選項。如需詳細資訊，請參閱 Docker 資訊清單。

資訊清單列表可以像其他 Amazon ECR 映像一樣，在 Amazon ECS 任務定義或 Amazon EKS Pod 規格中提取或參考。

先決條件

- 在 Docker CLI 中，開啟實驗性功能。如需實驗性功能的相關資訊，請參閱 Docker 文件中的實驗性功能。

- 在您推送映像之前，Amazon ECR 儲存庫必須存在。如需詳細資訊，請參閱 the section called “建立儲存庫以儲存影像”。
- 在創建 Docker 清單之前，必須將映像推送到您的存儲庫。如需如何推送映像的資訊，請參閱 將碼頭映像推送到 Amazon ECR 私有存儲庫。

將多架構 Docker 映像推送到 Amazon ECR 儲存庫

1. 向打算推送映像的 Amazon ECR 登錄檔驗證您的 Docker 用戶端。所用的每個登錄檔皆必須取得身分驗證字符，字符有效期間為 12 個小時。如需詳細資訊，請參閱 Amazon ECR 中的私有登錄身份驗證。

   若要向 Amazon ECR 登錄檔驗證 Docker，請執行 aws ecr get-login-password 命令。將身分驗證字符傳遞給 docker login 命令時，使用 AWS 的值作為使用者名稱並指定您要驗證的 Amazon ECR 登錄檔 URI。如果是向多個登錄進行驗證，您必須針對每個登錄重複此命令。

   > **Important**
   >
   > 若您收到錯誤，請安裝或升級至最新版本的 AWS CLI。如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》中的安裝 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. 列出儲存庫中的映像，請確認映像標籤。

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

3. 建立 Docker 資訊清單列表。`manifest create` 命令會驗證參考的映像是否已在您的儲存庫中，並在本機建立資訊清單。

   ```
   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. (選用) 檢查 Docker 資訊清單列表。這可讓您確認資訊清單列表中參照的每個映像資訊清單的大小和摘要。

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

5. 將 Docker 資訊清單列表推送至您的 Amazon ECR 儲存庫。

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

## 將頭盔圖推送到 Amazon ECR 私有存儲庫

您可以將開放容器倡議 (OCI) 成品推送至 Amazon ECR 儲存庫。若要查看此功能的範例，請使用下列步驟將頭盔圖推送至 Amazon ECR。

如需將您的 Amazon ECR 託管頭盔圖與 Amazon EKS 搭配使用的相關資訊，請參閱。在 Amazon EKS 集群上安裝頭盔圖

將 Helm Chart 推送到 Amazon ECR 儲存庫

1. 安裝 Helm 用戶端的最新版本。這些步驟是使用 Helm 版本 `3.8.2` 進行編寫。如需詳細資訊，請參閱安裝 Helm。
2. 使用下列步驟來建立測試 Helm Chart。如需詳細資訊，請參閱 Helm Docs - 開始使用。

   a. 建立一個名為 `helm-test-chart` 的 Helm Chart 並清除 `templates` 目錄的內容。

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

   b. 在`templates`文件夾 ConfigMap 中創建一個。

   ```
   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. 封裝圖表。輸出將包含您在推送 Helm Chart 時使用的封裝圖表的檔案名稱。

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

輸出

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

4. 建立儲存庫以存放 Helm Chart。儲存庫的名稱應與您在步驟 2 中建立 Helm Chart 時使用的名稱相符。如需詳細資訊，請參閱 建立 Amazon ECR 私有儲存庫來存放映像檔。

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

5. 將您的 Helm 用戶端驗證到您打算將 Helm Chart 推送到的 Amazon ECR 登錄檔。所用的每個登錄檔皆必須取得身分驗證字符，字符有效期間為 12 個小時。如需詳細資訊，請參閱 Amazon ECR 中的私有登錄身份驗證。

```
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. 使用 helm push 命令推送 Helm Chart。輸出應該包括 Amazon ECR 儲存庫 URI 和 SHA 摘要。

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

7. 描述您的 Helm Chart。

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

在輸出中，確認 `artifactMediaType` 參數指出適當的成品類型。

```
{
    "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. (選用) 如需其他步驟，請安裝 Helm ConfigMap 並開始使用 Amazon EKS。如需詳細資訊，請參閱 在 Amazon EKS 集群上安裝頭盔圖。

# 簽署儲存在 Amazon ECR 私有儲存庫中的映像

Amazon ECR 與 AWS Signer 整合，為您提供簽署容器映像的方式。您可以將容器映像和簽署同時儲存在私有儲存庫中。

## 考量事項

使用 Amazon ECR 映像檔簽署時應考慮以下事項。

- 儲存在儲存庫中的簽署會計入每個儲存庫映像數目上限的服務配額。如需詳細資訊，請參閱 Amazon ECR 服務配額。
- 使用 Amazon ECR 生命週期政策時，任何藉由規則到期或刪除 OCI 映像索引的動作都將導致 Amazon ECR 在 24 小時內刪除該映像索引所參照的所有簽署。

## 必要條件

開始之前，請先達成以下先決條件。

- 安裝和設定最新版 AWS CLI。如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》中的「安裝或更新最新版 AWS CLI」。

- 安裝符號 CLI 和符號的 AWS Signer 插件。如需詳細資訊，請參閱《AWS Signer 開發人員指南》中的「簽署容器映像的先決條件」。
- 在 Amazon ECR 私有儲存庫中，儲存了需要簽署的容器映像。如需詳細資訊，請參閱 將映像推送到 Amazon ECR 私有存儲庫。

## 設定 Notary 用戶端的身分驗證

您必須先設定用戶端，才能使用 Notation CLI 建立簽署，以便能向 Amazon ECR 進行身分驗證。如果您在安裝 Notation 用戶端的同一台主機上安裝了 Docker，則 Notation 將重複使用您用於 Docker 用戶端的相同身分驗證方法。Docker `login` 和 `logout` 命令將允許 Notation `sign` 和 `verify` 命令使用這些相同的憑證，而且您不必單獨對 Notation 進行身分驗證。有關設定 Notation 用戶端以進行身分驗證的詳細資訊，請參閱 Notary 專案文件中的《使用符合 OCI 的登錄檔進行身分驗證》

如果您沒有使用 Docker 或其他使用 Docker 憑證的工具，則建議您使用 Amazon ECR Docker 憑證助手做為您的憑證存放區。如需有關如何安裝和設定 Amazon ECR 憑證助手的詳細資訊，請參閱《Amazon ECR Docker 憑證助手》。

## 簽署映像

下列步驟可用於建立簽署容器映像並將簽章儲存在 Amazon ECR 私有儲存庫中的所需資源。Notation 使用摘要簽署映像。

簽署映像

1. 使用 AWS Signer 簽署平台建立`Notation-OCI-SHA384-ECDSA`簽署設定檔。您可以選擇使用 `--signature-validity-period` 參數來指定簽章有效期。此值可以使用`DAYS`、`MONTHS` 或 `YEARS` 來指定。如果未指定任何驗證期間，則會使用預設值 135 個月。

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

   > **Note**
   >
   > 簽署設定檔名稱僅支援英數字元和底線 (_)。

2. 驗證 Notation 客戶端到您的預設登錄檔。下列範例使用 AWS CLI 向 Amazon ECR 私有登錄驗證符號 CLI。

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

3. 使用 Notation CLI 來簽署映像檔，並使用儲存庫名稱和 SHA 摘要來指定映像檔。如此可建立簽章，並將其推播到正在簽署的該映像所在之相同 Amazon ECR 私有儲存庫。

   在下列範例中，我們會使用 SHA 摘要 `sha256:ca78e5f730f9a789ef8c63bb55275ac12dfb9e8099e6EXAMPLE` 來簽署 `curl` 儲存庫中的映像檔。

```
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"
```

## 後續步驟

簽署容器映像後，您可以在本機驗證簽名。有關驗證映像的說明，請參閱AWS Signer 開發人員指南中的登錄後在本地驗證映像

# 從 Amazon ECR 私有存儲庫刪除簽名

您可以從 Amazon ECR 私有儲存庫刪除簽章。當您使用 Notation CLI 建立和推播簽章時，系統也會在 Amazon ECR 儲存庫中建立 OCI 映像索引。Amazon ECR API 不支援刪除 OCI 映像索引參照的成品或映像；以下是清理這些成品的可用選項。

- (建議) 您可以使用 ORAS CLI 來刪除成品，ORAS 將處理更新或刪除映像索引。
- 您可以使用 Amazon ECR API 或主控台先刪除 OCI 映像索引，然後再刪除參考的成品 (例如簽章)。

使用 ORAS 用戶端刪除簽章和其他參考類型成品時，ORAS 會管理 OCI 映像索引。ORAS 會先從索引刪除對成品的參照，然後再刪除清單檔案。您可以使用 `oras manifest delete` 命令，參照簽章成品的索引。

若要使用 ORAS CLI 刪除簽章

1. 安裝和配置 ORAS 客戶端。

如需有關安裝和設定 ORAS 用戶端的資訊，請參閱 ORAS 說明文件中的安裝。

2. 若要使用 ORAS CLI 刪除簽章，請執行下列命令：

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

# 在 Amazon ECR 中查看圖像詳細信息

將映像推送到儲存庫之後，您可以檢視該映像檔的相關資訊。包含的詳細資訊如下：

- 映像 URI
- 映像標籤
- 成品媒體類型
- 映像資訊清單類型
- 掃描狀態
- 映像大小 (以 MB 為單位)
- 將映像推送至儲存庫的時間
- 複寫狀態

檢視映像詳細資訊 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列上，選擇包含映像的儲存庫的區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在 Repositories (儲存庫) 頁面上，選擇儲存庫以檢視。
5. 在 Repositories : ***repository_name*** (儲存庫：repository_name) 頁面上，選擇要檢視的詳細資訊的映像。

# 從 Amazon ECR 私有儲存庫將映像檔提取到您的本機環境

如果您要執行在 Amazon ECR 中可用的 Docker 映像，您可以使用 docker pull 命令來將其提取至本機環境。您可以從預設登錄或與其他 AWS 帳戶相關聯的登錄中執行此操作。

若要在 Amazon ECS 任務定義中使用 Amazon ECR 映像，請參閱 將 Amazon ECR 映像與 Amazon ECS 搭配使用。

> **Important**
>
> Amazon ECR 要求使用者擁有透過 IAM 政策呼叫 `ecr:GetAuthorizationToken` API 的許可，然後才能對登錄檔進行身分驗證，並從任何 Amazon ECR 儲存庫推送或提取任何映像。Amazon ECR 提供多種 AWS 受管政策，以控制不同層級的使用者存取。如需 Amazon ECR 受 AWS 管政策的相關資訊，請參閱AWS Amazon 彈性容器註冊表的受管政策。

從 Amazon ECR 儲存庫提取 Docker 映像

1. 向打算提取映像的 Amazon ECR 登錄檔驗證您的 Docker 用戶端。所用的每個登錄檔皆必須取得身分驗證字符，字符有效期間為 12 個小時。如需詳細資訊，請參閱 Amazon ECR 中的私有登錄身份驗證。
2. (選用) 找出要提取的映像。
   - 可用 aws ecr describe-repositories 命令列出登錄檔內的儲存庫：

     ```
     aws ecr describe-repositories
     ```

     上述的登錄檔範例有一個名為 `amazonlinux` 的儲存庫。
   - 可用 aws ecr describe-images 命令描述儲存庫內的映像：

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

     上述的儲存庫範例有標記為 `latest` 和 `2016.09`，映像摘要為 `sha256:f1d4ae3f7261a72e98c6ebefe9985cf10a0ea5bd762585a43e0700ed99863807` 的映像。
3. 使用 docker pull 命令提取映像。映像名稱格式應為 *`registry`*`/`*`repository`*`[:`*`tag`*`]` 才可依標籤提取，或為 *`registry`*`/`*`repository`*`[@`*`digest`*`]` 才可依摘要提取。

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

> **Important**
>
> 如果出現 *repository-url* not found: does not exist or no pull access 錯誤，則需向 Amazon ECR 驗證您的 Docker 用戶端。如需詳細資訊，請參閱 Amazon ECR 中的私有登錄身份驗證。

# 拉動 Amazon Linux 容器映像

Amazon Linux 容器映像是透過在 Amazon Linux AMI 中包含的相同軟體元件所建置。Amazon Linux 容器映像檔可用於任何環境，做為 Docker 工作負載的基本映像檔。如果您將 Amazon Linux AMI 用於亞 Amazon EC2 中的應用程序，則可以使用 Amazon Linux 容器映像對應用程序進行容器化。

您可以在本機開發環境中使用 Amazon Linux 容器映像檔，然後將應用程式推送至 AWS 使用 Amazon ECS。如需詳細資訊，請參閱 將 Amazon ECR 映像與 Amazon ECS 搭配使用。

Amazon Linux 容器映像可在 Amazon ECR Public 及 Docker Hub 使用。如需 Amazon Linux 容器映像檔的支援，請前往AWS 開發人員論壇。

從 Amazon ECR Public 中提取 Amazon Linux 容器映像

1. 向 Amazon Linux Public 登錄檔驗證您的 Docker 用戶端。驗證字符有效時間為 12 小時。如需詳細資訊，請參閱 Amazon ECR 中的私有登錄身份驗證。

   > **Note**
   >
   > 從版本 1.18.1.187 開始，可以在 AWS CLI 中使用 ecr-public 命令，但我們建議使用最新版的 AWS CLI。如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》中的安裝 AWS Command Line Interface。

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

   其輸出如下：

   ```
   Login succeeded
   ```

2. 使用 docker pull 命令提取 Amazon Linux 容器映像。若要在 Amazon ECR Public Gallery 上查看 Amazon Linux 容器映像，請參閱 Amazon ECR Public Gallery - amazonlinux。

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

3. (選用) 在本機執行容器。

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

從 Docker Hub 提取 Amazon Linux 容器映像

1. 使用 docker pull 命令提取 Amazon Linux 容器映像。

```
docker pull amazonlinux
```

2. (選用) 在本機執行容器。

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

# 刪除 Amazon ECR 中的圖像

如果您已完成使用映像，即可將其從儲存庫中刪除。如果您完成使用儲存庫，您可以刪除整個儲存庫及其中的所有映像。如需詳細資訊，請參閱 刪除 Amazon ECR 中的私有存儲庫。

作為手動刪除映像的替代方法，您可以建立儲存庫生命週期政策，以更好地控制儲存庫中映像的生命週期管理。生命週期政策會為您自動執行此程序。如需詳細資訊，請參閱 在 Amazon ECR 中使用生命週期政策自動清理映像檔。

刪除映像 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列上，選擇包含要刪除之映像的區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在 Repositories (儲存庫) 頁面上，選擇包含要刪除之映像的儲存庫。
5. 在 Repositories: ***repository_name*** (儲存庫：repository_name) 頁面，選擇要刪除之映像左側的方塊，再選擇 Delete (刪除)。

6. 在 Delete image(s) (刪除映像) 對話方塊中，確認應刪除的映像已被選擇，再選擇 Delete (刪除)。

刪除映像 (AWS CLI)

1. 在儲存庫中列出映像。標籤映像會同時具有映像摘要以及相關標籤的清單。未標籤的映像只會有映像摘要。

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

2. (選用) 透過指定與要刪除的映像關聯的標籤來刪除映像的任何不需要的標籤。當從映像中刪除最後一個標籤時，映像也會遭到刪除。

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

3. 指定映像摘要以刪除標籤或未標籤的映像。透過參照摘要的方式刪除映像時，該映像及其所有標籤將遭刪除。

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

若要刪除多個映像，您可以在請求中指定多個映像標籤或映像摘要。

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

# 在 Amazon ECR 中重新標記圖像

透過 Docker 映像資訊清單 V2 結構描述 2 映像，您可以使用 `--image-tag` 命令的 put-image 選項以重新標記現有映像。您可以使用 Docker 來重新標記，而不需提取和推送映像。針對較大的映像，此程序節省了重新標記映像所需的大量網路頻寬與時間。

## 重新標記映像 (AWS CLI)

使用重新標記影像 AWS CLI

1. 使用 batch-get-image 命令以取得映像的映像資訊清單，來重新標記並將其寫入檔案。在此範例中，儲存庫 *amazonlinux* 中擁有 *latest* 標籤的映像資訊清單，被寫入名為 *MANIFEST* 的環境變數。

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

2. 使用 put-image 命令的 `--image-tag` 選項，以新標籤將映像工作資訊清單檔案放至 Amazon ECR。在此範例中，該映像被標記為 *2017.03*。

> **Note**
>
> 如果該`--image-tag`選項在您的版本中不可用 AWS CLI，請升級至最新版本。如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》中的安裝 AWS Command Line Interface。

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

3. 確認您的新映像標籤已連接至您的映像。在下方的輸出中，該映像有標籤 `latest` 與 `2017.03`。

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

其輸出如下：

```
{
    "imageDetails": [
        {
            "imageSizeInBytes": 98755613,
            "imageDigest":
 "sha256:8d00af8f076eb15a33019c2a3e7f1f655375681c4e5be157a26EXAMPLE",
            "imageTags": [
                "latest",
                "2017.03"
            ],
```

```
            "registryId": "aws_account_id",
            "repositoryName": "amazonlinux",
            "imagePushedAt": 1499287667.0
        }
    ]
}
```

## 重新標記映像 (AWS Tools for Windows PowerShell)

使用重新標記影像 AWS Tools for Windows PowerShell

1. 使用 Get-ECRImageBatch cmdlet 以取得映像的描述，來重新標記並將其寫入環境變數。在此範例中，儲存庫 *amazonlinux* 中擁有 *latest* 標籤的映像，被寫入環境變數 *$Image*。

   > **Note**
   >
   > 如果系統上沒有可用的 Get-ECRImageBatch cmdlet，請參閱《AWS Tools for Windows PowerShell 使用者指南》中的設定 AWS Tools for Windows PowerShell。

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

2. 將映像的資訊清單寫入 *$Manifest* 環境變數。

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

3. 使用 Write-ECRImage cmdlet 的 `-ImageTag` 選項，以新標籤將映像工作資訊清單檔案放至 Amazon ECR。在此範例中，該映像被標記為 *2017.09*。

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

4. 確認您的新映像標籤已連接至您的映像。在下方的輸出中，該映像有標籤 `latest` 與 `2017.09`。

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

   其輸出如下：

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

# 防止 Amazon ECR 中的圖像標籤被覆蓋

您可以透過在儲存庫中開啟標籤不變性來防止影像標籤遭到覆寫。開啟標籤不變性之後，如果您推送含有已存在於儲存庫中的標籤的映像，則會傳回`ImageTagAlreadyExistsException`錯誤。標籤不變性會影響所有標籤。您不能使某些標籤不可變，而其他標籤則不可變。

您可以使用 AWS Management Console 和 AWS CLI 工具來設定新儲存庫或現有儲存庫的影像標籤可變性。若要使用主控台步驟建立存放庫，請參閱建立 Amazon ECR 私有儲存庫來存放映像檔。

## 設置圖像標籤可變性（ ）AWS Management Console

若要設定影像標籤可變性

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列上，選擇包含要編輯之儲存庫的區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在 Repositories (儲存庫) 頁面上，選擇 Private (私有) 分頁，然後選擇要編輯的儲存庫並選擇 Edit (編輯)。
5. 對於 Tag mutability (標籤不變性)，選擇儲存庫的標籤可變性設定。設定不可變標籤的儲存庫會防止映像被覆寫。如需詳細資訊，請參閱 防止 Amazon ECR 中的圖像標籤被覆蓋。
6. 對於 Image scan settings (映像掃描設定)，雖然您可以在儲存庫層級指定基本掃描的掃描設定，但最佳實務是在私有登錄檔層級指定掃描組態。在私有登錄檔層級指定掃描設定讓您能啟用增強型掃描或基本掃描，還能定義篩選條件來指定要掃描哪些儲存庫。如需詳細資訊，請參閱 掃描影像以查看 Amazon ECR 中的軟體漏洞。
7. 對於 Encryption settings (加密設定)，這是一個僅能檢視的欄位，因為儲存庫建立後，就無法變更儲存庫的加密設定。
8. 選擇 Save (儲存) 更新儲存庫設定。

## 設置圖像標籤可變性（ ）AWS CLI

建立儲存庫並設定不可變標籤

使用以下其中一個命令來建立新的映像儲存庫，並設定不可變標籤。

- 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
```

若要更新儲存庫的影像標籤可變性設定

使用以下其中一個命令來更新現有儲存庫的映像標籤可變性設定。

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

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

- 寫入 ECR ImageTag 可變性 ()AWS Tools for Windows PowerShell

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

# Amazon ECR 中的容器映像資訊清單格式支援

Amazon ECR 支援以下的容器映像資訊清單格式：

- Docker 映像資訊清單 V2 結構描述 1 (需搭配 1.9 或更舊版本的 Docker 使用)
- Docker 映像資訊清單 V2 結構描述 2 (需搭配 1.10 或更新版本的 Docker 使用)
- 開放容器計畫 (OCI) 規格 (v1.0 以上版本)

Docker 映像資訊清單 V2 結構描述 2 支援提供下列功能：

- 可在單數映像上使用多重標籤。
- 支援儲存 Windows 容器映像。

## Amazon ECR 映像資訊清單轉換

推送映像至 Amazon ECR 及提取映像時，容器引擎用戶端 (例如 Docker) 會與登錄檔通訊，以取得一致同意用戶端支援且供登錄檔用於映像的資訊清單格式。

使用 Docker 1.9 或更早版本推送映像至 Amazon ECR 時，映像的資訊清單格式將存放為 Docker 映像資訊清單 V2 結構描述 1。使用 Docker 1.10 或更新版本推送映像至 Amazon ECR 時，映像的資訊清單格式將存放為 Docker 映像資訊清單 V2 結構描述 2。

當您依標籤從 Amazon ECR 提取映像時，Amazon ECR 會傳回存放在儲存庫中的映像資訊清單格式。只有在用戶端支援該格式，才會傳回該格式。如果客戶端不理解存放的映像資訊清單格式，Amazon ECR 會將映像資訊清單轉換為可以理解的格式。例如，如果 Docker 1.9 用戶端請求以 Docker 映像資訊清單 V2 結構描述 2 形式存放的映像資訊清單，Amazon ECR 會傳回在 Docker 映像資訊清單 V2 結構描述 1 格式中的資訊清單。下表描述透過依標籤提取映像時，Amazon ECR 支援的可用轉換：

| 用戶端要求的結構描述 | 以 V2 結構描述 1 推送至 ECR | 以 V2 結構描述 2 推送至 ECR | 以 OCI 推送至 ECR |
|---|---|---|---|
| V2 結構描述 1 | 不需翻譯 | 翻譯為 V2 結構描述 1 | 翻譯為 V2 結構描述 1 |
| V2 結構描述 2 | 不需翻譯，用戶端回退至 V2 結構描述 1 | 不需翻譯 | 翻譯為 V2 結構描述 2 |
| OCI | 沒有可用的翻譯 | 翻譯為 OCI | 不需翻譯 |

**Important**

如果您依摘要提取映像，則沒有可用的翻譯。用戶端必須瞭解存放在 Amazon ECR 中的映像資訊清單格式。如果在 Docker 1.9 或更舊版本用戶端上依摘要要求 Docker 映像資訊清單 V2 結構描述 2 映像，映像提取將失敗。如需詳細資訊，請參閱 Docker 文件中的「登錄檔相容性」。

在此範例中，如果您依標籤要求相同的映像，Amazon ECR 則會將映像資訊清單翻譯為用戶端支援的格式。映像會提取成功。

# 將 Amazon ECR 映像與 Amazon ECS 搭配使用

您可以使用 Amazon ECR 私有儲存庫，來託管 Amazon ECS 任務可能從中提取的容器映像和成品。若要使用此功能，Amazon ECS 或 Fargate、容器代理程式必須具有進行 `ecr:BatchGetImage`、`ecr:GetDownloadUrlForLayer` 和 `ecr:GetAuthorizationToken` API 的許可。

## 所需的 IAM 許可

下表顯示了要針對每個啟動類型使用的 IAM 角色，這些角色為您的任務提供從 Amazon ECR 私有儲存庫提取所需的許可。Amazon ECS 提供受管 IAM 政策，其中包含必要許可。

| 啟動類型 | IAM 角色 | AWS 受管理的 IAM 政策 |
| --- | --- | --- |
| Amazon EC2 執行個體上的 Amazon ECS | 使用容器執行個體 IAM 角色，此角色與 Amazon ECS 叢集中註冊的 Amazon EC2 執行個體相關聯。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的容器執行個體 IAM 角色。 | `AmazonEC2ContainerServiceforEC2Role`<br><br>如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的 AmazonEC2ContainerServiceforEC2Role。 |
| Fargate 上的 Amazon ECS | 使用您在 Amazon ECS 任務定義中參照的任務執行 IAM 角色。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的任務執行 IAM 角色。 | `AmazonECSTaskExecutionRolePolicy`<br><br>如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的 AmazonECSTaskExecutionRolePolicy。 |
| 外部執行個體上的 Amazon ECS | 使用容器執行個體 IAM 角色，此角色與 Amazon ECS 叢集中註冊的內部部署伺服器或 | `AmazonEC2ContainerServiceforEC2Role` |

| 啟動類型 | IAM 角色 | AWS 受管理的 IAM 政策 |
| --- | --- | --- |
| | 虛擬機器 (VM) 相關聯。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的容器執行個體 Amazon ECS 角色。 | 如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的 AmazonEC2ContainerServiceforEC2Role。 |

**Important**

受 AWS 管 IAM 政策包含您可能不需要的其他許可。在此情況下，這些是從 Amazon ECR 私有儲存庫提取的最低必要許可。

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

## 在 Amazon ECS 任務定義中指定 Amazon ECR 映像

建立 Amazon ECS 任務定義時，您可以指定託管在 Amazon ECR 私有儲存庫中的容器映像。在任務定義中，確保您的 Amazon ECR 映像使用完整的 `registry/repository:tag` 名稱。例如，*`aws_account_id`*`.dkr.ecr.`*`region`*`.amazonaws.com/`*`my-repository`*`:`*`latest`*。

下列任務定義片段會顯示您在 Amazon ECS 任務定義中，會用於指定 Amazon ECR 中託管的容器映像。

```
{
```

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

# 將 Amazon ECR 映像與 Amazon EKS 搭配使用

您可以將 Amazon ECR 圖像與 Amazon EKS 一起使用。

從 Amazon ECR 參考映像時，您必須為映像使用完整的 `registry/repository:tag` 命名。例如：*aws_account_id*.dkr.ecr.*region*.amazonaws.com/*my-repository*:*latest*。

## 所需的 IAM 許可

如果您在受管節點、自我管理節點上託管 Amazon EKS 工作負載，或者 AWS Fargate，請檢閱以下內容：

- 託管在受管或自我管理節點上的 Amazon EKS 工作負載：需要 Amazon EKS 工作者節點 IAM 角色 (NodeInstanceRole)。Amazon EKS 工作節點 IAM 角色必須包含適用於 Amazon ECR 的下列 IAM 政策許可。

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

```
        }
    ]
}
```

> **Note**
>
> 如果您使用 Amazon EKS 入門中的 AWS CloudFormation範本`eksctl`或範本來建立叢集和工作者節點群組，這些 IAM 許可預設會套用至您的工作者節點 IAM 角色。

- 託管於其上的 Amazon EKS 工作負載 AWS Fargate：使用 Fargate 網繭執行角色，該角色可提供網繭從私有 Amazon ECR 儲存庫提取映像的權限。如需詳細資訊，請參閱建立 Fargate Pod 執行角色。

## 在 Amazon EKS 集群上安裝頭盔圖

Amazon ECR 託管的頭盔圖可以安裝在您的 Amazon EKS 集群上。

先決條件

- 安裝 Helm 用戶端的最新版本。這些步驟是使用 Helm 版本 `3.9.0` 進行編寫。如需詳細資訊，請參閱安裝 Helm。
- 您至少已將 AWS CLI 的版本 `1.23.9` 或 `2.6.3` 安裝在自己的電腦上。如需詳細資訊，請參閱安裝或更新最新版本的 AWS CLI。
- 您已經將 Helm Chart 推送到您的 Amazon ECR 儲存庫。如需詳細資訊，請參閱 將頭盔圖推送到 Amazon ECR 私有存儲庫。
- 您已設定 `kubectl` 與 Amazon EKS 合作。如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的為 Amazon EKS 建立 `kubeconfig`。若下列命令在您的叢集上成功執行，就表示您的設定正確。

```
kubectl get svc
```

在 Amazon EKS 叢集上安裝頭盔圖

1. 對您的 Helm 用戶端驗證您的 Helm Chart 託管的 Amazon ECR 登錄檔。所用的每個登錄檔皆必須取得身分驗證字符，字符有效期間為 12 個小時。如需詳細資訊，請參閱 Amazon ECR 中的私有登錄身份驗證。

   ```
   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. 安裝圖表。替換為您*helm-test-chart*的存儲庫，*0.1.0* 替換為您的頭盔圖表的標籤。

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

輸出看起來會與此類似：

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

3. 驗證圖表安裝。

```
helm list -n default
```

輸出範例：

```
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. (選擇性) 請參閱已安裝的 Helm Chart ConfigMap。

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

5. 完成後，您可以從叢集中移除圖表版本。

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

# 掃描影像以查看 Amazon ECR 中的軟體漏洞

改進的基本掃描功能在 Amazon ECR 的預覽版中，可能會有所變更。在此公開預覽期間，您只能使用選擇 AWS Management Console 加入改進的基本掃描版本。

Amazon ECR 影像掃描有助於識別容器映像中的軟體弱點。提供下列掃描類型。

> **Important**
>
> 在增強型掃描、基本掃描和改進的基本掃描版本之間切換，將導致先前建立的掃描無法再使用。您將不得不再次設置掃描。但是，如果切換回以前的掃描版本，則可以使用已建立的掃描。

- 增強型掃描：Amazon ECR 與 Amazon Inspector 整合，為儲存庫提供自動連續掃描。系統會掃描容器映像，檢查是否有作業系統和程式設計語言套件漏洞。隨著新漏洞出現，掃描結果也會更新，Amazon Inspector 會發出事件 EventBridge 通知您。增強型掃描提供下列功能：
  - 作業系統和程式設計語言封裝漏洞
  - 兩種掃描頻率：在推送和連續掃描時進行掃描。
- 基本掃描 — Amazon ECR 提供兩種使用常見弱點和暴露 (CVE) 資料庫的基本掃描版本：使用開放原始碼 Clair 專案的目前 GA 版本，以及使用我們原生技術的新改良版基本掃描 (預覽版)。 AWS 若使用基本型掃描，您可以將儲存庫設定為在推送時掃描，也可以執行手動掃描；Amazon ECR 會提供掃描問題清單。基本掃描提供下列功能：
  - 作業系統掃描。
  - 兩種掃描頻率：手動和推送掃描。

> **Important**
>
> 新版本的基本掃描不支持，`imageScanFindingsSummary`並且`imageScanStatus`在 `DescribeImages` API 中。若要檢視這些內容，請使用 `DescribeImageScanFindings` API。

# 用於選擇要在 Amazon ECR 中掃描哪些儲存庫的篩選器

當您為私人登錄設定映像掃描時，可以使用篩選器來選擇要掃描的儲存庫。

如果使用基本掃描，您可以指定「依據推送篩選條件進行掃描」，這樣便可以指定有新映像推送時要對哪些儲存庫執行映像掃描。任何不符合「依據推送篩選條件進行掃描」基本掃描的儲存庫都將設為手動掃描頻率，這意味著若要執行掃描，您必須手動觸發掃描。

如果使用增強掃描，您可以為「依據推送進行掃描」和「連續掃描」分別指定篩選條件。任何不符合增強掃描篩選條件的儲存庫都將停止掃描。如果您正在使用增強掃描並為「依據推送進行掃描」和「連續掃描」分別指定了篩選條件，發生同一儲存庫符合多個篩選條件的情況，則 Amazon ECR 會對該儲存庫強制優先執行「連續掃描」，而非「依據推送篩選條件進行掃描」。

## 篩選萬用字元

指定篩選條件時，沒有萬用字元的篩選條件會比對內含篩選條件的所有儲存庫名稱。具有萬用字元 (*) 的篩選條件會比對任何儲存庫名稱，其中萬用字元會取代儲存庫名稱中零個以上的字元。

下表提供範例，其中儲存庫名稱在水平軸上表示，而範例篩選條件在垂直軸上指定。

| | prod | repo-prod | Prod-repo | repo-prod-repo | prodrepo |
|---|---|---|---|---|---|
| prod | 是 | 是 | 是 | 是 | 是 |
| *prod | 是 | 是 | 否 | 否 | 否 |
| prod* | 是 | 否 | 是 | 否 | 是 |
| *prod* | 是 | 是 | 是 | 是 | 是 |
| prod*repo | 否 | 否 | 是 | 否 | 是 |

# 掃描映像以查看 Amazon ECR 中的作業系統和程式設計語言套件漏洞

Amazon ECR 增強型掃描已與 Amazon Inspector 整合，可為容器映像提供漏洞掃描。系統會掃描容器映像，檢查是否有作業系統和程式設計語言套件漏洞。您可以使用 Amazon ECR 和 Amazon Inspector

直接檢視掃描問題清單。如需有關 Amazon Inspector 的詳細資訊，請參閱《Amazon Inspector 使用者指南》中的使用 Amazon Inspector 掃描容器映像。

透過增強型掃描，您可以選擇要將哪些儲存庫設定為自動連續掃描，以及將哪些儲存庫設定為推送時掃描。設定掃描篩選條件可完成此操作。

## 增強型掃描的注意事項

啟用 Amazon ECR 增強型掃描之前，請考慮下列事項。

- 使用此功能不會從 Amazon ECR 產生任何額外成本，但是，掃描映像檔則會從 Amazon Inspector 產生成本。如需詳細資訊，請參閱 Amazon Inspector 定價。
- 下列區域不支援增強型掃描：
  - 中東 (阿拉伯聯合大公國) (`me-central-1`)
  - 亞太區域 (海德拉巴) (`ap-south-2`)
  - 以色列 (特拉維夫) (`il-central-1`)
  - 亞太區域 (墨爾本) (`ap-southeast-4`)
  - 歐洲 (西班牙) (`eu-south-2`)
- Amazon Inspector 支援掃描特定作業系統。如需完整清單，請參閱《Amazon Inspector 使用者指南》中的支援的作業系統：Amazon ECR 掃描。
- Amazon Inspector 使用服務連結 IAM 角色，該角色提供為儲存庫提供增強型掃描所需的許可。為私有登錄檔開啟增強型掃描時，Amazon Inspector 會自動建立服務連結 IAM 角色。如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的使用 Amazon Inspector 的服務連結角色。
- 當您一開始為私有登錄開啟增強型掃描時，Amazon Inspector 只會根據映像推送時間戳記或過去 90 天內擷取的影像，辨識過去 30 天內推送至 Amazon ECR 的影像。較舊的映像會具有 `SCAN_ELIGIBILITY_EXPIRED` 掃描狀態。如果您希望 Amazon Inspector 掃描這些映像，則必須將這些映像再次推送到儲存庫中。
- 開啟增強型掃描後，推送至 Amazon ECR 的所有映像都會在設定的持續時間內不斷掃描。根據預設，持續時間為生命週期。可使用 Amazon Inspector 主控台以完成設定。如需詳細資訊，請參閱 在 Amazon Inspector 中更改圖像的增強掃描持續時間。
- 為 Amazon ECR 私有登錄檔開啟增強型掃描時，系統只會使用增強型掃描來掃描符合掃描篩選條件的所有儲存庫。不符合篩選條件的儲存庫都會具備 `Off` 掃描頻率，且不會被掃描。不支援使用增強掃描的手動掃描。如需詳細資訊，請參閱 用於選擇要在 Amazon ECR 中掃描哪些儲存庫的篩選器。

- 如果您為「依據推送進行掃描」和「連續掃描」分別指定了篩選條件，發生同一儲存庫符合多個篩選條件的情況，則 Amazon ECR 會對該儲存庫強制優先執行「連續掃描」，而非「依據推送篩選條件進行掃描」。
- 開啟增強型掃描時，Amazon ECR 會在儲存庫的掃描頻率變更 EventBridge 時傳送事件。Amazon Inspector 會在初始掃描完成 EventBridge 時以及建立、更新或關閉影像掃描發現項目時發出事件。

## 在 Amazon ECR 中進行增強掃描所需的 IAM 許可

Amazon ECR 增強型掃描需要 Amazon Inspector 服務連結 IAM 角色，且啟用和使用增強型掃描的 IAM 委託人有權呼叫掃描所需的 Amazon Inspector API。為私有登錄檔開啟增強型掃描時，Amazon Inspector 會自動建立 Amazon Inspector 服務連結 IAM 角色。如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的使用 Amazon Inspector 的服務連結角色。

下列 IAM 政策授予啟用及使用增強型掃描的必要許可。其中包含 Amazon Inspector 建立服務連結 IAM 角色所需的許可，以及開啟和關閉增強型掃描和擷取掃描問題清單所需的 Amazon Inspector API 許可。

```
{
    "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"
                    ]
                }
```

```
            }
        }
    ]
}
```

# 在 Amazon ECR 中設定影像的增強型掃描

針對您的私人登錄設定每個區域的增強型掃描。

確認您擁有適當的 IAM 許可來設定增強型掃描。如需相關資訊，請參閱在 Amazon ECR 中進行增強掃描所需的 IAM 許可。

AWS Management Console

開啟私人登錄的增強型掃描

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列選擇要為其設定掃描組態的區域。
3. 在功能窗格中，選擇 [私人登錄]、[設定]、[掃描]。
4. 在 Scanning configuration (掃描組態) 頁面，針對 Scan type (掃描類型) 選擇 Enhanced scanning (增強型掃描)。

   依預設，選取「增強型掃描」時，會持續掃描所有儲存庫。
5. 若要選擇要持續掃描的特定存放庫，請清除 [持續掃描所有存放庫] 方塊，然後定義篩選器：

   > **Important**
   >
   > 沒有萬用字元的篩選條件會比對內含篩選條件的所有儲存庫名稱。具有萬用字元 (*) 的篩選條件會比對儲存庫名稱，其中萬用字元會取代儲存庫名稱中零個以上的字元。若要查看篩選器運作方式的範例，請參閱the section called “篩選萬用字元”。

   a. 根據存放庫名稱輸入篩選器，然後選擇 [新增篩選器]。

   b. 決定推送影像時要掃描的儲存庫：

      - 若要在推送時掃描所有儲存庫，請選取推送所有儲存庫時掃描。
      - 若要選擇要在推送時掃描的特定儲存庫，請根據儲存庫名稱輸入篩選器，然後選擇 [新增篩選器]。

6. 選擇儲存。
7. 在要開啟增強型掃描的各個區域重複這些步驟。

### AWS CLI

使用下列 AWS CLI 命令，使用開啟私人登錄的增強型掃描 AWS CLI。您可以使用 `rules` 物件指定掃描篩選條件。

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

  下列範例會為私有登錄檔開啟增強型掃描。在預設情況下，當未指定 `rules` 時，Amazon ECR 會將掃描組態設定為替所有儲存庫連續掃描。

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

  下列範例會為私有登錄檔開啟增強型掃描，並指定掃描篩選條件。範例中的掃描篩選條件可針對在其名稱具有 `prod` 的所有儲存庫開啟連續掃描。

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

  下列範例會為私有登錄檔開啟增強型掃描，並指定多個掃描篩選條件。範例中的掃描篩選條件可針對在其名稱中具有 `prod` 的所有儲存庫開啟連續掃描，並且僅針對所有其他儲存庫開啟推送時掃描。

  ```
  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
  ```

## 在 Amazon Inspector 中更改圖像的增強掃描持續時間

您可以變更 Amazon Inspector 持續掃描 Amazon ECR 私有儲存庫中影像的天數。根據預設，當開啟您 Amazon ECR 私有登錄檔的增強型掃描時，Amazon Inspector 服務會持續監控您的儲存庫，直到映像遭到刪除或停用增強型掃描為止。可以使用 Amazon Inspector 設定變更 Amazon Inspector 掃描映像的持續時間。可用的掃描持續時間為 Lifetime (default) (生命週期 (預設))、180 days (180 天)，以及30 days (30 天)。儲存庫的掃描持續時間過後，在列示您的掃描弱點時會顯示掃描狀態為 SCAN_ELIGIBILITY_EXPIRED。如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的變更 Amazon ECR 自動重新掃描持續時間。

若要變更增強型掃描持續時間設定

1. 打開 Amazon Inspector 控制台 https://console.aws.amazon.com/inspector/v2/home.
2. 在左側導覽中，展開 Settings (設定)，然後選擇General (一般)。
3. 在 Settings (設定) 頁面的 ECR re-scan duration (ECR 重新掃描持續時間) 之下，選擇設定，然後選擇 Save (儲存)。

## EventBridge 在 Amazon ECR 中為增強掃描而傳送的事件

開啟增強型掃描時，Amazon ECR 會在儲存庫的掃描頻率變更 EventBridge 時傳送事件。Amazon Inspector 會在初始掃描完成 EventBridge 時以及建立、更新或關閉影像掃描發現項目時傳送事件。

儲存庫掃描頻率變更事件

為登錄檔開啟增強型掃描時，Amazon ECR 會在開啟了增強型掃描的資源發生變更時傳送下列事件。這包含正在建立的新儲存庫、正在變更的儲存庫掃描頻率，或是在開啟了增強型掃描的儲存庫中建立或刪除映像時。如需詳細資訊，請參閱 掃描影像以查看 Amazon ECR 中的軟體漏洞。

```
{
 "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"
 }
}
```

初始映像掃描事件 (增強型掃描)

為登錄檔開啟增強型掃描時，Amazon Inspector 會在初始映像掃描完成時傳送下列事件。`finding-severity-counts` 參數只會在出現嚴重性等級時才傳回嚴重性等級的值。例如，如果映像在 CRITICAL 等級沒有問題清單，則不會傳回任何重要等級數值。如需詳細資訊，請參閱 [掃描映像以查看 Amazon ECR 中的作業系統和程式設計語言套件漏洞](#)。

事件模式：

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

輸出範例：

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

映像掃描問題清單更新事件 (增強型掃描)

為登錄檔開啟增強型掃描時，Amazon Inspector 會在建立、更新或關閉映像掃描問題清單時傳送下列事件。如需詳細資訊，請參閱 掃描映像以查看 Amazon ECR 中的作業系統和程式設計語言套件漏洞。

事件模式：

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

輸出範例：

```
{
    "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"
    }
}
```

## 在 Amazon ECR 中擷取發現項目以進行增強型掃描

您可以擷取上次完成的增強型影像掃描的掃描發現項目，然後在 Amazon Inspector 中開啟發現項目以查看更多詳細資訊。發現的軟體弱點會根據「常見弱點與暴露」(CVE) 資料庫，依嚴重性列出。

如需在掃描映像時某些常見問題的故障診斷詳細資訊，請參閱 疑難排解 Amazon ECR 中的影像掃描。

AWS Management Console

使用下列步驟以利用 AWS Management Console擷取映像掃描結果。

擷取影像掃描發現項目

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列選擇儲存庫所在的區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在 Repositories (儲存庫) 頁面上，選擇包含要擷取掃描結果之映像的儲存庫。
5. 在 Images (映像) 頁面的 Vulnerabilities (漏洞) 欄下方，選取映像的 See findings (查看問題清單) 來擷取掃描問題清單。
6. 若要在 Amazon Inspector 主控台中檢視更多詳細資訊，請在「名稱」欄中選擇弱點名稱。

AWS CLI

使用下列 AWS CLI 命令可使用擷取影像掃描發現項目 AWS CLI。您可以使用 `imageTag` 或 `imageDigest` 指定映像，兩者皆可利用 list-images CLI 命令取得。

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

  下列範例使用映像標籤。

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

  下列範例使用映像摘要。

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

# 掃描影像以查看 Amazon ECR 中的作業系統漏洞

改進的基本掃描功能在 Amazon ECR 的預覽版中，可能會有所變更。在此公開預覽期間，您只能使用選擇 AWS Management Console 加入改進的基本掃描版本。

Amazon ECR 提供兩種版本的基本掃描，這些掃描使用「常見弱點和暴露」(CVE) 資料庫：

- 使用開放原始碼 Claire 專案的目前 GA 版本。如需有關 Clair 的詳細資訊，請參閱 Claire 上的。GitHub
- 使用 AWS 原生技術的基本掃描（在預覽中）的新改進版本。

Amazon ECR 會使用來自上游分發來源之 CVE 的嚴重性 (如果有的話)。否則，會使用常見弱點評分系統 (CVSS) 分數。CVSS 分數可用於取得 NVD 漏洞嚴重性等級。如需詳細資訊，請參閱 NVD 漏洞嚴重性等級。

兩個版本的 Amazon ECR 基本掃描都支援篩選器，以指定要在推送時掃描的儲存庫。任何與推送過濾器掃描不匹配的存儲庫都會設置為手動掃描頻率，這意味著您必須手動啟動掃描。每 24 小時可掃描一次影像。24 小時包括推送時的初始掃描 (若已設定)，以及任何手動掃瞄。

可以為每個映像擷取上次完成的映像掃描結果。影像掃描完成後，Amazon ECR 會將事件傳送至 Amazon EventBridge。如需詳細資訊，請參閱 Amazon ECR 活動和 EventBridge。

## 區域支援改善基本掃描

下列區域支援基本掃描的改良版本：

- 亞太區域 (香港)ap-east-1
- 歐洲 (斯德哥爾摩) (eu-north-1)
- 中東 (巴林) (me-south-1)
- 亞太區域 (孟買)ap-south-1
- 歐洲 (巴黎) (eu-west-3)
- AWS GovCloud (美國東部) (us-gov-east-1)
- 非洲 (開普敦)af-south-1
- 亞太區域 (雅加達) (ap-southeast-3)
- 歐洲 (法蘭克福) (eu-central-1)
- 歐洲 (愛爾蘭) (eu-west-1)
- 南美洲 (聖保羅) (sa-east-1)
- 美國東部 (俄亥俄) (us-east-2)
- AWS GovCloud (美國西部) (us-gov-west-1)
- 亞太區域 (東京) (ap-northeast-1)
- 亞太區域 (首爾) (ap-northeast-2)
- 亞太區域 (大阪) (ap-northeast-3)
- 歐洲 (米蘭) (eu-south-1)
- 歐洲 (倫敦) (eu-west-2)
- 美國東部 (維吉尼亞北部) (us-east-1)
- 亞太區域 (新加坡) (ap-southeast-1)
- 亞太區域 (雪梨) (ap-southeast-2)
- 加拿大 (中部) (ca-central-1)

- 美國西部 (加利佛尼亞北部) (us-west-1)
- 美國西部 (奧勒岡) (us-west-2)
- 歐洲 (蘇黎世) (eu-central-2)

## 操作系統支持基本掃描和改進的基本掃描

我們建議您繼續使用受支援的作業系統版本，作為安全性最佳實務和持續涵蓋範圍。根據供應商政策，已停止使用的作業系統不再使用修補程式更新，而且在許多情況下，不再為其發佈新的安全建議。此外，某些廠商會在受影響的作業系統達到標準支援結束時，從其摘要中移除現有的安全性建議和偵測。分發失去其廠商的支援後，Amazon ECR 可能不再支援掃描其漏洞。Amazon ECR 確實針對停止的作業系統產生的任何發現項目，應僅用於參考目的。下面列出了當前支持的操作系統和版本。

| 作業系統 | 版本 |
| --- | --- |
| 高山 Linux（高山） | 3.19 |
| 高山 Linux（高山） | 3.18 |
| 高山 Linux（高山） | 3.17 |
| 高山 Linux（高山） | 3.16 |
| Amazon Linux 2 (AL2) | AL2 |
| Amazon AL2023 | AL2023 |
| CentOS CentOS 版 | 7 |
| Debian 伺服器 (書蟲) | 12 |
| 伺服器 (靶心) | 11 |
| 巴斯特伺服器 | 10 |
| 甲骨文 Linux (甲骨文) | 9 |
| 甲骨文 Linux (甲骨文) | 8 |
| 甲骨文 Linux (甲骨文) | 7 |

| 作業系統 | 版本 |
| --- | --- |
| 月球 | 23.04 |
| 阿布图 | 22 月 4 日（英文） |
| Ubuntu (焦點) | 20.04（英文） |
| 仿生 | 18.04 (埃斯姆) |
| 超級戰鬥機 | 16.04 (埃斯姆) |
| Ubuntu 的（值得信賴） | 14.04 (埃斯姆) |
| Red Hat Enterprise Linux (RHEL) | 7 |
| Red Hat Enterprise Linux (RHEL) | 8 |
| Red Hat Enterprise Linux (RHEL) | 9 |

## 在 Amazon ECR 中為映像配置改進的基本掃描

Amazon ECR 基本掃描的改良版現已提供預覽版。改進的基本掃描使用 AWS 原生技術。

針對您的私人存放庫設定每個區域的改進基本掃描。如需支援改善基本掃描的區域清單，請參閱區域支援改善基本掃描。

為私人登錄開啟改善的基本掃描

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列選擇要為其設定掃描組態的區域。
3. 在導覽窗格中，依序選擇 Private registry (私有登錄檔)、Scanning (掃描)。
4. 在 [掃描配置] 頁面上，針對 [掃描類型] 選擇 [改進的基本掃描 (預覽中)-新增]。
5. 在預設情況下，系統將所有儲存庫設定為 Manual (手動) 掃描。您可選擇設定推送時掃描，方法是指定推送時掃描篩選條件。您可以為所有儲存庫或個別儲存庫設定推送時掃描。如需詳細資訊，請參閱 用於選擇要在 Amazon ECR 中掃描哪些儲存庫的篩選器。

# 在 Amazon ECR 中設定映像的基本掃描

根據預設，Amazon ECR 會開啟所有私有登錄的基本掃描。因此，除非您已變更私人登錄上的掃描設定，否則無需開啟基本掃描。基本掃描使用開放原始碼 Claire 專案。

您可以使用下列步驟定義推送篩選器上的一或多個掃描。

開啟私人登錄的基本掃描

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列選擇要為其設定掃描組態的區域。
3. 在導覽窗格中，依序選擇 Private registry (私有登錄檔)、Scanning (掃描)。
4. 在 Scanning configuration (掃描組態) 頁面，針對 Scan type (掃描類型) 選擇 Basic scanning (基本型掃描)。
5. 在預設情況下，系統將所有儲存庫設定為 Manual (手動) 掃描。您可選擇設定推送時掃描，方法是指定推送時掃描篩選條件。您可以為所有儲存庫或個別儲存庫設定推送時掃描。如需詳細資訊，請參閱 用於選擇要在 Amazon ECR 中掃描哪些儲存庫的篩選器。

# 手動掃描影像以查找 Amazon ECR 中的作業系統漏洞

如果您的儲存庫未設定為在推送時掃描，您可以手動啟動映像掃描。每 24 小時可掃描一次影像。24 小時包括推送時的初始掃描 (若已設定)，以及任何手動掃瞄。

如需在掃描映像時某些常見問題的故障診斷詳細資訊，請參閱 疑難排解 Amazon ECR 中的影像掃描。

AWS Management Console

使用下列步驟，利用 AWS Management Console以啟動手動映像掃描。

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列選擇您儲存庫所建立的區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在 Repositories (儲存庫) 頁面上，選擇包含要掃描之映像的儲存庫。
5. 在 Images (映像) 頁面上，選取要掃描的映像，然後選擇 Scan (掃描)。

AWS CLI

- start-image-scan (AWS CLI)

下列範例使用映像標籤。

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

下列範例使用映像摘要。

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

AWS Tools for Windows PowerShell

- 取得 ECR 搜ImageScan尋結果 ()AWS Tools for Windows PowerShell

  下列範例使用映像標籤。

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

  下列範例使用映像摘要。

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

## 擷取 Amazon ECR 中基本掃描的發現項目

您可以擷取上次完成的基本影像掃描的掃描發現項目。發現的軟體弱點會根據「常見弱點與暴露」(CVE) 資料庫，依嚴重性列出。

如需在掃描映像時某些常見問題的故障診斷詳細資訊，請參閱 疑難排解 Amazon ECR 中的影像掃描。

AWS Management Console

使用下列步驟以利用 AWS Management Console擷取映像掃描結果。

擷取影像掃描發現項目

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。

2. 從導覽列選擇您儲存庫所建立的區域。
3. 在導覽窗格中，選擇 Repositories (儲存庫)。
4. 在 Repositories (儲存庫) 頁面上，選擇包含要擷取掃描結果之映像的儲存庫。
5. 在 Images (映像) 頁面的 Vulnerabilities (漏洞) 欄下方，選取映像的 Details (詳細資訊)，以擷取掃描結果。

AWS CLI

使用下列 AWS CLI 命令可使用擷取影像掃描發現項目 AWS CLI。您可以使用 `imageTag` 或 `imageDigest` 指定映像，兩者皆可利用 list-images CLI 命令取得。

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

  下列範例使用映像標籤。

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

  下列範例使用映像摘要。

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

AWS Tools for Windows PowerShell

- 取得 ECR 搜ImageScan尋結果 ()AWS Tools for Windows PowerShell

  下列範例使用映像標籤。

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

  下列範例使用映像摘要。

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

# 疑難排解 Amazon ECR 中的影像掃描

以下是常見的映像掃描失敗。您可以透過顯示影像詳細資料、透過 API 或使用 API，在 Amazon ECR 主控台中檢視類似 AWS CLI 的錯誤。`DescribeImageScanFindings`

UnsupportedImage錯誤

嘗試對使用 Amazon ECR 不支援基本映像掃描的作業系統建置的映像執行基本型掃描時，您可能會收到 `UnsupportedImageError` 錯誤訊息。Amazon ECR 支援對 Amazon Linux、Amazon Linux 2、Debian、Ubuntu、CentOS、Oracle Linux、Alpine 和 RHEL Linux 發行版本的主要版本進行包漏洞掃描。一旦發行版本失去廠商的支援，Amazon ECR 可能不再支援掃描它是否有漏洞。Amazon ECR 不支援掃描從 Docker scratch 映像建置的映像。

> **Important**
>
> 使用增強型掃描時，Amazon Inspector 支援掃描特定類型的作業系統和媒體。如需完整清單，請參閱《Amazon Inspector 使用者指南》中的支援的作業系統和媒體類型。

傳回 `UNDEFINED` 嚴重性等級。

您可能會收到具有 `UNDEFINED` 嚴重性等級的掃描結果。下列是造成此問題的常見原因：

- CVE 來源未指派漏洞的優先順序。
- Amazon ECR 無法辨識指派給漏洞的優先順序。

若要判定漏洞的嚴重性和描述，您可以直接從來源檢視 CVE。

## 了解掃描狀態 SCAN_ELIGIBILITY_EXPIRED

當為您的私有登錄檔啟用使用 Amazon Inspector 的增強型掃描而且您正在檢視掃描弱點時，您可能會看到掃描狀態為 `SCAN_ELIGIBILITY_EXPIRED`。以下是造成此問題的最常見原因。

- 當您一開始為私有登錄檔開啟增強型掃描時，Amazon Inspector 只會根據映像推送時間戳記，辨識過去 30 天內推送至 Amazon ECR 的映像。較舊的映像會具有 `SCAN_ELIGIBILITY_EXPIRED` 掃描狀態。如果您希望 Amazon Inspector 掃描這些映像，則必須將這些映像再次推送到儲存庫中。
- 如果在 Amazon Inspector 主控台中變更 ECR re-scan duration (ECR 重新掃描持續時間)，且經過這段時間後，映像的掃描狀態變更為 `inactive` 並出現原因代碼 `expired`，且該

映像的所有相關發現結果都排定為關閉。這會導致 Amazon ECR 主控台將掃描狀態列示為 SCAN_ELIGIBILITY_EXPIRED。

# 將上游註冊表與 Amazon ECR 私有註冊表同步

使用提取快取規則，您可以將上游登錄的內容與 Amazon ECR 私有登錄同步。

Amazon ECR 目前支援為下列上游登錄檔建立提取快取規則。

- 碼頭集線器，Microsoft Azure 容器註冊表，容器註冊表和 GitHub GitLab 容器註冊表（需要身份驗證）
- Amazon ECR Public、Kubernetes 容器映像登錄檔和 Quay (不需要身分驗證)

對於 GitLab 容器登錄，Amazon ECR 僅支援透過提供項目 GitLab .com GitLab software-as-a-service 提取快取。

對於需要驗證的上游登錄，您必須將認證儲存在 AWS Secrets Manager 密碼中。Amazon ECR 主控台可讓您輕鬆為每個經過身分驗證的上游登錄檔建立 Secrets Manager 秘密。如需有關使用 Secret 管理員主控台建立密碼管理 Secrets Manager 碼的詳細資訊，請參閱將您的上游存儲庫憑據存儲在 AWS Secrets Manager 密鑰中。

為上游登錄檔建立提取快取規則之後，只要使用 Amazon ECR 私有登錄檔 URI，從該上游登錄檔提取映像即可。接著 Amazon ECR 會建立儲存庫，並在您的私有登錄中快取該映像。在具有指定標籤的快取映像後續提取請求中，Amazon ECR 會檢查上游登錄，查看是否有具有該特定標記的映像檔的新版本，並嘗試至少每 24 小時更新私有登錄中的映像一次。

## 存放庫建立範本

Amazon ECR 已新增對儲存庫建立範本的支援 (目前處於預覽版中)，讓您可以控制使用提取快取規則為 Amazon ECR 代表您建立的新儲存庫指定初始組態。每個範本都包含一個儲存庫命名空間字首，用於將新儲存庫與特定範本匹配。範本可以指定所有儲存庫設定的組態，包括資源型存取政策、標籤不變性、加密和生命週期政策。儲存庫建立範本中的設定只會在建立儲存庫期間套用，對使用任何其他方法建立的現有儲存庫或儲存庫沒有任何影響。如需詳細資訊，請參閱 用於控制在提取快取動作期間建立的儲存庫的範本。

## 使用提取快取規則的考量

使用 Amazon ECR 提取快取規則時，請考慮下列事項。

- 下列區域不支援提取快取規則的建立。

  - 中國 (北京) (cn-north-1)
  - 中國 (寧夏) (cn-northwest-1)
  - AWS GovCloud (美國東部) (us-gov-east-1)
  - AWS GovCloud (美國西部) (us-gov-west-1)
- AWS Lambda 不支援使用提取快取規則從 Amazon ECR 提取容器映像。
- 使用提取快取提取映像時，第一次提取映像時不支援 Amazon ECR FIPS 服務端點。不過，使用 Amazon ECR FIPS 服務端點可以處理後續的提取。
- 透過 Amazon ECR 私有登錄 URI 提取快取映像時，映像提取會由 AWS IP 地址啟動。這可確保映像提取不會計入上游登錄檔實作的任何提取速率配額。
- 當快取映像透過 Amazon ECR 私有登錄檔 URI 提取時，Amazon ECR 至少每 24 小時檢查一次上游儲存庫，以便驗證快取映像是否為最新版本。如果上游登錄檔中有較新的映像，Amazon ECR 會嘗試更新快取映像。這個計時器是基於快取映像的最後一次提取。
- 如果 Amazon ECR 因任何原因無法從上游登錄檔更新映像，並且已提取映像，則仍會提取最後一個快取映像。
- 建立包含上游登錄檔憑證的 Secrets Manager 秘密時，秘密名稱必須使用 ecr-pullthroughcache/ 字首。秘密也必須位於在其中建立提取快取規則的相同帳戶和區域中。
- 使用提取快取規則提取多架構映像時，資訊清單和資訊清單中參照的每個映像都會提取至 Amazon ECR 儲存庫。如果只想提取特定架構，您可以使用與架構相關聯的映像摘要或標籤 (而不是與資訊清單相關聯的標籤) 來提取映像。
- Amazon ECR 使用服務連結 IAM 角色，該角色提供 Amazon ECR 建立儲存庫、擷取用於身分驗證的 Secrets Manager 秘密值，和代表您推送快取映像所需的許可。建立提取快取規則時，會自動建立服務連結 IAM 角色。如需詳細資訊，請參閱 用於提取快取的 Amazon ECR 服務連結角色。
- 依預設，提取快取映像的 IAM 主體具有透過其 IAM 政策授予他們的許可。您可以使用 Amazon ECR 私有登錄檔許可政策，進一步設定 IAM 實體的許可範圍。如需詳細資訊，請參閱 使用登錄檔許可。
- 使用提取快取工作流程建立的 Amazon ECR 儲存庫，會被視作與其他 Amazon ECR 儲存庫一樣。支援所有儲存庫功能，例如複寫和映像掃描。
- Amazon ECR 代表您使用提取快取動作建立新儲存庫時，下列預設設定會套用至儲存庫，除非有相符的儲存庫建立範本。您可以使用儲存庫建立範本，定義套用至 Amazon ECR 代表您建立的儲存庫的設定。如需詳細資訊，請參閱 用於控制在提取快取動作期間建立的儲存庫的範本。
  - 標籤不變性 — 關閉，標籤為可變並且可覆寫的。
  - 加密 — 使用預設 AES256 加密。
  - 儲存庫許可 — 已省略，不套用儲存庫許可政策。
  - 生命週期政策 — 已省略，不套用生命週期政策。

  - 資源標籤 — 已省略，不套用任何資源標籤。
- 使用提取快取規則為儲存庫開啟映像標籤不變性，可防止 Amazon ECR 使用相同標籤更新映像。
- 當第一次使用提取快取規則提取影像時，可能需要通往網際網路的路由。在某些情況下，需要通往 Internet 的路由，因此最好設置路由以避免任何故障。因此，如果您已將 Amazon ECR 設定為使用介面 VPC 端點， AWS PrivateLink 則需要確保第一次提取具有通往網際網路的路由。其中一種方法是使用網際網路閘道在同一個 VPC 中建立公用子網路，然後將所有輸出流量從其私有子網路路由到公有子網路。使用提取快取規則的後續影像擷取不需要此動作。如需詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的路由選項範例。

# 將上游登錄與 Amazon ECR 私有登錄同步所需的 IAM 許可

除了向私有登錄檔進行身分驗證以及推送和提取映像所需的 Amazon ECR API 許可之外，還需要以下額外許可才能有效使用提取快取規則。

- `ecr:CreatePullThroughCacheRule` – 授予建立提取快取規則的許可。必須透過身分型 IAM 政策授予此許可。
- `ecr:BatchImportUpstreamImage` – 授予檢索外部映像並將其匯入到您的私有登錄檔的許可。可以藉由使用身分型 IAM 政策的私有登錄檔許可政策或藉由使用資源型儲存庫許可政策來授予此許可。如需使用儲存庫許可的詳細資訊，請參閱 Amazon ECR 中的私有儲存庫政策。
- `ecr:CreateRepository` – 授予在私有登錄檔中建立儲存庫的許可。如果存放快取映像的儲存庫尚不存在，則需要此許可。可以由身分型 IAM 政策或私有登錄檔許可政策授予此許可。
- `ecr:TagResource`：准許將中繼資料標籤新增至 Amazon ECR 資源。唯有當您提取使用提取快取規則的映像，該映像具有關聯的儲存庫建立範本 (設定為將資源標籤新增至儲存庫) 時，才需要此許可。必須透過身分型 IAM 政策授予此許可。

## 使用登錄檔許可

Amazon ECR 私有登錄檔許可可用來設定個別 IAM 實體使用提取快取的許可範圍。如果 IAM 實體擁有的由 IAM 政策授予的許可多過登錄檔許可政策授予的許可，則 IAM 政策優先。例如，如果使用者已具有 `ecr:*` 許可，則在登錄檔層級不需要額外的許可。

建立私有登錄檔的許可政策 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列選擇要在其中設定私有登錄檔許可陳述式的區域。

3. 在導覽窗格中，選擇 Private registry (私有登錄檔)、Registry permissions (登錄檔許可)。
4. 在 Registry permissions (登錄檔許可) 頁面上，選擇 Generate statement (產生陳述式)。
5. 針對您要建立的每個提取快取許可政策陳述式，執行下列動作。
   a. 針對 Policy type (政策類型)，選擇 Pull through cache policy (提取快取政策)。
   b. 針對 Statement id (陳述式 ID)，提供提取快取陳述式政策的名稱。
   c. 針對 IAM entities (IAM 實體)，指定要包含在政策中的使用者、群組或角色。
   d. 針對 Repository namespace (儲存庫命名空間)，選取要與政策建立關聯的提取快取規則。
   e. 針對 Repository names (儲存庫名稱)，指定要套用規則的儲存庫基本名稱。例如，如果您想要在 Amazon ECR Public 上指定 Amazon Linux 儲存庫，則儲存庫名稱會是 `amazonlinux`。

### 建立私有登錄檔的許可政策 (AWS CLI)

使用下列 AWS CLI 命令指定使用的私人登錄權限 AWS CLI。

1. 建立具有您登錄檔政策內容的名為 `ptc-registry-policy.json` 的本機檔案。下列範例會授予 `ecr-pull-through-cache-user` 許可，以建立儲存庫並從 Amazon ECR Public 中提取映像，其為與之前建立的提取快取規則相關聯的上游來源。

```
{
  "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**
>
> 僅當存放快取映像的儲存庫尚不存在時，才需要 `ecr-CreateRepository` 許可。例如，如果儲存庫建立動作和映像提取動作是由不同的 IAM 主體 (例如管理員和開發人員) 所執行。

2. 使用 put-registry-policy 命令設定登錄檔政策。

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

## 後續步驟

準備好開始使用提取快取規則時，以下為接下來的步驟。

- 建立提取快取規則。如需詳細資訊，請參閱 在 Amazon ECR 中創建提取緩存規則。
- 建立儲存庫建立範本。儲存庫建立範本賦予您控制權，於提取快取動作期間，定義用於 Amazon ECR 代表您建立的新儲存庫的設定。如需詳細資訊，請參閱 用於控制在提取快取動作期間建立的儲存庫的範本。

# 在 Amazon ECR 中創建提取緩存規則

對於包含您想要在 Amazon ECR 私有登錄中快取之映像的每個上游登錄，您必須建立提取快取規則。

對於需要驗證的上游登錄，您必須將認證儲存在 Secret Manager 密碼中。您可以使用現有密碼或建立新密碼。您可以在 Amazon ECR 主控台或秘 Secrets Manager 主控台中建立 Secrets Manager 碼。若要使用 Secrets Manager 主控台而非 Amazon ECR 主控台建立 Secrets Manager 理員，請參閱將您的上游存儲庫憑據存儲在 AWS Secrets Manager 密鑰中。

## 必要條件

- 確認您具有適當的 IAM 許可來建立提取快取規則。如需相關資訊，請參閱將上游登錄與 Amazon ECR 私有登錄同步所需的 IAM 許可。
- 對於需要驗證的上游登錄：如果您想要使用現有密碼，請確認 Secrets Manager 密碼是否符合下列需求：

- 密碼的名稱開頭為`ecr-pullthroughcache/`。 AWS Management Console 僅顯示帶有前綴的密碼 Secrets Manager 密`ecr-pullthroughcache/`碼。
- 密碼所在的帳戶和區域必須與提取快取規則所在的帳戶和區域相符。

## 建立提取快取規則 (AWS Management Console)

下列步驟說明如何使用 Amazon ECR 主控台建立提取快取規則和 Secrets Manager 秘密。若要使用 Secret 管理員主控台建立密碼，請參閱將您的上游存儲庫憑據存儲在 AWS Secrets Manager 密鑰中。

針對 Amazon ECR 公共，Kubernetes 容器登錄檔或 Quay

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列選擇要在其中進行私有登錄檔設定的區域。
3. 在導覽窗格中，選擇 Private registry (私有登錄檔)、Pull through cache (提取快取)。
4. 在 Pull through cache configuration (提取快取組態) 頁面上，選擇 Add rule (新增規則)。
5. 在步驟 1：指定來源頁面上，針對登錄檔，從上游登錄檔清單中選擇 Amazon ECR 公共、Kubernetes 或 Quay，接著選擇下一步。
6. 在步驟 2：指定目的地頁面上，針對 Amazon ECR 儲存庫字首，指定快取從來源公有登錄檔提取的映像時要使用的儲存庫命名空間字首，接著選擇下一步。預設會填入命名空間，但也可以指定自訂命名空間。
7. 在步驟 3：檢閱並建立頁面上，檢閱提取快取規則組態，接著選擇建立。
8. 為要建立的每個提取快取重複前面的步驟。系統會針對每個區域分別建立提取快取規則。

對於 Docker Hub

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列選擇要在其中進行私有登錄檔設定的區域。
3. 在導覽窗格中，選擇 Private registry (私有登錄檔)、Pull through cache (提取快取)。
4. 在 Pull through cache configuration (提取快取組態) 頁面上，選擇 Add rule (新增規則)。
5. 在步驟 1：指定來源頁面上，針對登錄檔選擇 Docker Hub、下一步。
6. 在步驟 2：設定身分驗證頁面上，針對上游憑證，您必須將 Docker Hub 的身分驗證憑證儲存在 AWS Secrets Manager 秘密中。您可以指定現有秘密，或使用 Amazon ECR 主控台建立新秘密。

a. 若要使用現有的密碼，請選擇 [使用現有 AWS 密碼]。針對秘密名稱，使用下拉式選單選取您現有的秘密，接著選擇下一步。

> **Note**
>
> AWS Management Console 只會顯示名稱使用前綴的密碼 Secrets Manager 密`ecr-pullthroughcache/`碼。秘密也必須位於在其中建立提取快取規則的相同帳戶和區域中。

b. 若要建立新秘密，請選擇建立 AWS 秘密，執行下列動作，接著選擇下一步。

i. 針對秘密名稱，指定秘密的描述性名稱。秘密名稱必須含有 1 至 512 個 Unicode 字元。

ii. 針對 Docker Hub 使用者名稱，請指定您的 Docker Hub 使用者名稱。

iii. 針對 Docker Hub 存取字符，請指定您的 Docker Hub 存取字符。如需建立 Docker Hub 存取字符的詳細資訊，請參閱 Docker 文件中的建立和管理存取字符。

7. 在步驟 3：指定目的地頁面上，針對 Amazon ECR 儲存庫字首，指定快取從來源公有登錄檔提取的映像時要使用的儲存庫命名空間，接著選擇下一步。

   預設會填入命名空間，但也可以指定自訂命名空間。

8. 在步驟 4：檢閱並建立頁面上，檢閱提取快取規則組態，接著選擇建立。

9. 為要建立的每個提取快取重複前面的步驟。系統會針對每個區域分別建立提取快取規則。

對於 GitHub 容器註冊表

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。

2. 從導覽列選擇要在其中進行私有登錄檔設定的區域。

3. 在導覽窗格中，選擇 Private registry (私有登錄檔)、Pull through cache (提取快取)。

4. 在 Pull through cache configuration (提取快取組態) 頁面上，選擇 Add rule (新增規則)。

5. 在 [步驟 1：指定來源] 頁面上，針對 [登錄] 選擇 [GitHub 容器登錄]，[下一步]。

6. 在 [步驟 2：設定驗證] 頁面上，對於上游認證，您必須將 GitHub 容器登錄的驗證認證儲存在 AWS Secrets Manager 密碼中。您可以指定現有秘密，或使用 Amazon ECR 主控台建立新秘密。

   a. 若要使用現有的密碼，請選擇 [使用現有 AWS 密碼]。針對秘密名稱，使用下拉式選單選取您現有的秘密，接著選擇下一步。

> **Note**
>
> AWS Management Console 只會顯示名稱使用前綴的密碼 Secrets Manager 密`ecr-pullthroughcache/`碼。秘密也必須位於在其中建立提取快取規則的相同帳戶和區域中。

b. 若要建立新秘密，請選擇建立 AWS 秘密，執行下列動作，接著選擇下一步。

   i. 針對秘密名稱，指定秘密的描述性名稱。秘密名稱必須含有 1 至 512 個 Unicode 字元。

   ii. 針對GitHub 容器登錄使用者名稱，指定您的 GitHub 容器登錄使用者

   iii. 對於GitHub 容器登錄存取權杖，請指定您的 GitHub 容器登錄存取權杖。有關創建 GitHub 訪問令牌的更多信息，請參閱 GitHub 文檔中的管理您的個人訪問令牌。

7. 在步驟 3：指定目的地頁面上，針對 Amazon ECR 儲存庫字首，指定快取從來源公有登錄檔提取的映像時要使用的儲存庫命名空間，接著選擇下一步。

   預設會填入命名空間，但也可以指定自訂命名空間。

8. 在步驟 4：檢閱並建立頁面上，檢閱提取快取規則組態，接著選擇建立。

9. 為要建立的每個提取快取重複前面的步驟。系統會針對每個區域分別建立提取快取規則。

對於 Microsoft Azure Container Registry

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。

2. 從導覽列選擇要在其中進行私有登錄檔設定的區域。

3. 在導覽窗格中，選擇 Private registry (私有登錄檔)、Pull through cache (提取快取)。

4. 在 Pull through cache configuration (提取快取組態) 頁面上，選擇 Add rule (新增規則)。

5. 在步驟 1：指定來源頁面上，執行下列動作。

   a. 針對登錄檔，選擇 Microsoft Azure Container Registry

   b. 針對來源登錄檔 URL，指定 Microsoft Azure Container Registry 的名稱，接著選擇下一步。

> **Important**
>
> 您只需要指定字首，因為會代表您填入 `.azurecr.io` 字尾。

6. 在步驟 2：設定身分驗證頁面上，針對上游憑證，您必須將 Microsoft Azure Container Registry 的身分驗證憑證儲存在 AWS Secrets Manager 秘密中。您可以指定現有秘密，或使用 Amazon ECR 主控台建立新秘密。

   a. 若要使用現有的密碼，請選擇 [使用現有 AWS 密碼]。針對秘密名稱，使用下拉式選單選取您現有的秘密，接著選擇下一步。

      > **Note**
      >
      > AWS Management Console 只會顯示名稱使用前綴的密碼 Secrets Manager 密`ecr-pullthroughcache/`碼。秘密也必須位於在其中建立提取快取規則的相同帳戶和區域中。

   b. 若要建立新秘密，請選擇建立 AWS 秘密，執行下列動作，接著選擇下一步。

      i. 針對秘密名稱，指定秘密的描述性名稱。秘密名稱必須含有 1 至 512 個 Unicode 字元。

      ii. 對於 Microsoft Azure Container Registry 使用者名稱，請指定您的 MMicrosoft Azure Container Registry 使用者名稱。

      iii. 對於 Microsoft Azure Container Registry 存取字符，請指定您的 Microsoft Azure Container Registry 存取字符。如需建立 Microsoft Azure Container Registry 存取字符的詳細資訊，請參閱 Microsoft Azure 文件中的建立字符 - 入口網站。

7. 在步驟 3：指定目的地頁面上，針對 Amazon ECR 儲存庫字首，指定快取從來源公有登錄檔提取的映像時要使用的儲存庫命名空間，接著選擇下一步。

   預設會填入命名空間，但也可以指定自訂命名空間。

8. 在步驟 4：檢閱並建立頁面上，檢閱提取快取規則組態，接著選擇建立。

9. 為要建立的每個提取快取重複前面的步驟。系統會針對每個區域分別建立提取快取規則。

對於 GitLab 容器註冊表

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列選擇要在其中進行私有登錄檔設定的區域。
3. 在導覽窗格中，選擇 Private registry (私有登錄檔)、Pull through cache (提取快取)。
4. 在 Pull through cache configuration (提取快取組態) 頁面上，選擇 Add rule (新增規則)。
5. 在 [步驟 1：指定來源] 頁面上，針對 [登錄] 選擇 [ GitLab 容器登錄]，[下一步]。

6. 在 [步驟 2：設定驗證] 頁面上，對於上游認證，您必須將 GitLab 容器登錄的驗證認證儲存在 AWS Secrets Manager 密碼中。您可以指定現有秘密，或使用 Amazon ECR 主控台建立新秘密。

   a. 若要使用現有的密碼，請選擇 [使用現有 AWS 密碼]。針對秘密名稱，使用下拉式選單選取您現有的秘密，接著選擇下一步。如需有關使用 Secrets Manager 主控台建立 Secrets Manager 秘密的詳細資訊，請參閱 將您的上游存儲庫憑據存儲在 AWS Secrets Manager 密鑰中。

      > **Note**
      >
      > AWS Management Console 只會顯示名稱使用前綴的密碼 Secrets Manager 密`ecr-pullthroughcache/`碼。秘密也必須位於在其中建立提取快取規則的相同帳戶和區域中。

   b. 若要建立新秘密，請選擇建立 AWS 秘密，執行下列動作，接著選擇下一步。

      i. 針對秘密名稱，指定秘密的描述性名稱。秘密名稱必須含有 1 至 512 個 Unicode 字元。

      ii. 針對GitLab 容器登錄使用者名稱，指定您的 GitLab 容器登錄使用者

      iii. 對於GitLab 容器登錄存取權杖，請指定您的 GitLab 容器登錄存取權杖。有關建立 GitLab 容器登錄存取權杖的詳細資訊，請參閱 GitLab 文件中的個人存取權杖、群組存取權杖或專案存取權杖。

7. 在步驟 3：指定目的地頁面上，針對 Amazon ECR 儲存庫字首，指定快取從來源公有登錄檔提取的映像時要使用的儲存庫命名空間，接著選擇下一步。

   預設會填入命名空間，但也可以指定自訂命名空間。

8. 在步驟 4：檢閱並建立頁面上，檢閱提取快取規則組態，接著選擇建立。

9. 為要建立的每個提取快取重複前面的步驟。系統會針對每個區域分別建立提取快取規則。

## 建立提取快取規則 (AWS CLI)

使用建立提取式快取規則 AWS CLI 命令，為 Amazon ECR 私有登錄建立直通快取規則。針對需要身分驗證的上游登錄檔，您必須將憑證儲存在 Secrets Manager 秘密中。若要使用 Secret 管理員主控台建立密碼，請參閱將您的上游存儲庫憑據存儲在 AWS Secrets Manager 密鑰中。

提供給每個受支援的登錄檔的下列範例。

對於 Amazon ECR Public

下列範例會為 Amazon ECR Public 登錄檔建立提取快取規則。其會指定 ecr-public 的儲存庫字首，這會導致使用提取快取規則建立的每個儲存庫具有 ecr-public/*upstream-repository-name* 的命名規則。

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

對於 Kubernetes 容器登錄檔

下列範例會為 Kubernetes 公有登錄檔建立提取快取規則。其會指定 kubernetes 的儲存庫字首，這會導致使用提取快取規則建立的每個儲存庫具有 kubernetes/*upstream-repository-name* 的命名規則。

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

對於 Quay

下列範例會為 Quay 公有登錄檔建立提取快取規則。其會指定 quay 的儲存庫字首，這會導致使用提取快取規則建立的每個儲存庫具有 quay/*upstream-repository-name* 的命名規則。

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

對於 Docker Hub

下列範例會為 Docker Hub 登錄檔建立提取快取規則。其會指定 docker-hub 的儲存庫字首，這會導致使用提取快取規則建立的每個儲存庫具有 docker-hub/*upstream-repository-name* 的命名規則。您必須指定秘密包含 Docker Hub 憑證的完整 Amazon Resource Name (ARN)。

```
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
```

對於 GitHub 容器註冊表

下列範例會為 GitHub 容器登錄建立提取快取規則。其會指定 docker-hub 的儲存庫字首，這會導致使用提取快取規則建立的每個儲存庫具有 github/*upstream-repository-name* 的命名規則。您必須指定包含 GitHub 容器登錄登入資料的密碼的完整 Amazon 資源名稱 (ARN)。

```
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
```

對於 Microsoft Azure Container Registry

下列範例會針對 Microsoft Azure 容器登錄建立快取規則提取。其會指定 azure 的儲存庫字首，這會導致使用提取快取規則建立的每個儲存庫具有 azure/*upstream-repository-name* 的命名規則。您必須指定秘密包含 Microsoft Azure Container Registry 憑證的完整 Amazon Resource Name (ARN)。

```
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
```

對於 GitLab 容器註冊表

下列範例會為 GitLab 容器登錄建立提取快取規則。其會指定 gitlab 的儲存庫字首，這會導致使用提取快取規則建立的每個儲存庫具有 gitlab/*upstream-repository-name* 的命名規則。您必須指定包含 GitLab 容器登錄登入資料的密碼的完整 Amazon 資源名稱 (ARN)。

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

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

## 後續步驟

建立提取快取規則之後，下列是後續步驟：

- 建立儲存庫建立範本。儲存庫建立範本賦予您控制權，於提取快取動作期間，定義用於 Amazon ECR 代表您建立的新儲存庫的設定。如需詳細資訊，請參閱 用於控制在提取快取動作期間建立的儲存庫的範本。
- 驗證提取快取規則。驗證提取快取規則時，Amazon ECR 會與上游登錄檔建立網路連線、驗證其是否可存取包含上游登錄檔憑證的 Secrets Manager 秘密，以及身分驗證是否成功。如需詳細資訊，請參閱 驗證 Amazon ECR 中的快取規則提取。
- 開始使用提取快取規則。如需詳細資訊，請參閱 在 Amazon ECR 中通過緩存規則拉動圖像。

# 用於控制在提取快取動作期間建立的儲存庫的範本

Amazon ECR 的儲存庫建立範本功能目前為預覽版本，可能會有所變更。在此公開預覽期間，只有 AWS Management Console 可用於管理存放庫建立範本。

使用 Amazon ECR 儲存庫建立範本，在提取快取動作期間，為 Amazon ECR 代表您建立的儲存庫定義設定。儲存庫建立範本中的設定只會在建立儲存庫期間套用，對使用任何其他方法建立的現有儲存庫或儲存庫沒有任何影響。

下列區域不支援儲存庫建立範本：

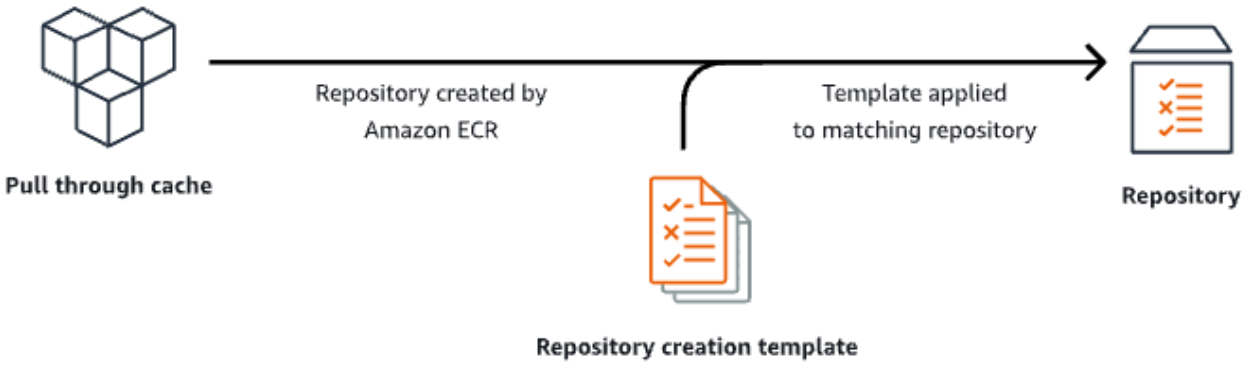
- 中國 (北京) (`cn-north-1`)
- 中國 (寧夏) (`cn-northwest-1`)
- AWS GovCloud (美國東部) (`us-gov-east-1`)
- AWS GovCloud (美國西部) (`us-gov-west-1`)

# 儲存庫建立範本的運作方式

有時 Amazon ECR 需要代表您建立新的私有儲存庫。例如，您第一次使用提取快取規則來擷取上游儲存庫的內容，並將其存放在 Amazon ECR 私有儲存庫時。如果沒有符合您提取快取規則的存放庫建立範本，Amazon ECR 會使用新儲存庫的預設設定。這些預設設定包括關閉標籤不變性、使用 AES-256 加密，以及不套用任何儲存庫或生命週期政策。

使用具有符合提取快取規則的字首之儲存庫建立範本，可讓您定義 Amazon ECR 套用於透過提取快取動作建立的新儲存庫之設定。您可以為新儲存庫定義標籤不變性、加密組態、儲存庫許可、生命週期政策和資源標籤。

下圖顯示使用儲存庫建立範本時 Amazon ECR 所使用的工作流程。




以下詳細說明儲存庫建立範本中的每個參數。

字首

字首是與範本相關聯的儲存庫命名空間字首。使用此字首建立的所有儲存庫都會套用此範本中定義的設定。例如，prod 字首會套用至開頭為 prod/ 的所有儲存庫。同樣地，prod/team 字首會套用至開頭為 prod/team/ 的所有儲存庫。

若要將範本套用至登錄檔中沒有關聯建立範本的所有儲存庫，您可以使用 ROOT 做為字首。

> **Important**
>
> 總會有一個假設 / 套用至字首的結尾。如果您指定 ecr-public 為字首，Amazon ECR 會將其視為 ecr-public/。使用提取快取規則時，您在規則建立期間指定的儲存庫字首，也應該將其指定為儲存庫建立範本字首。

描述

此範本描述是選用的，用於描述儲存庫建立範本的目的。

範本版本

要使用的儲存庫建立範本版本。目前僅支援 TV1 範本版本。

組態版本

範本要使用的儲存庫組態版本。每個範本都必須包含儲存庫組態。預設組態版本為 CV1，且包含映像標籤可變性、儲存庫政策和生命週期政策設定。

映像標籤可變性

用於使用範本建立的儲存庫之標籤可變性設定。如果省略此參數，則會使用可變預設設定，以允許覆寫映像標籤。建議使用此設定，用於透過提取快取動作所建立的儲存庫的範本。這可確保標籤相同時，Amazon ECR 可以更新快取的映像。

如果已指定不可變，儲存庫中的所有映像標籤不可變，這會阻止它們遭覆寫。

加密組態

用於使用範本建立之儲存庫的加密組態。

如果您使用 KMS 加密類型，儲存庫內容將搭配使用伺服器端加密與存放在 AWS KMS中的 AWS Key Management Service 金鑰進行加密。使用 AWS KMS 加密資料時，您可以使用 Amazon ECR 的預設 AWS 受管 AWS KMS 金鑰，也可以指定自己已建立的 AWS KMS 金鑰。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用儲存在 AWS Key Management Service (SSE-KMS) 的金 AWS Key Management Service 鑰使用伺服器端加密來保護資料。

如果您使用 AES256 加密類型，Amazon ECR 搭配使用伺服器端加密與 Amazon S3 受管加密金鑰，該方法使用 AES-256 加密演算法對儲存庫中的映像進行加密。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的透過 Amazon S3 受管加密金鑰 (SSE-S3) 使用伺服器端加密來保護資料。

儲存庫許可

套用至使用範本建立之儲存庫的儲存庫政策。儲存庫政策使用資源型許可來控制儲存庫的存取。資源型權限可讓您指定哪些 IAM 使用者或角色可以存取儲存庫，以及他們可以執行的動作。依預設，只有建立儲存庫的 AWS 帳戶才能存取存放庫。您可以套用政策文件，授予或拒絕對儲存庫的其他許可。如需詳細資訊，請參閱 Amazon ECR 中的私有儲存庫政策。

儲存庫生命週期政策

用於使用範本建立的儲存庫之生命週期政策。生命週期政策提供對私有儲存庫中映像的生命週期管理的更多控制。生命週期政策包含一個或多項規則，其中的每一項規則都會定義 Amazon ECR 的動作。這提供藉由依據年齡或計數讓映像過期的方式，自動清理您的容器映像。如需詳細資訊，請參閱 在 Amazon ECR 中使用生命週期政策自動清理映像檔。

資源標籤

資源標籤是要套用至儲存庫的中繼資料，可協助您分類和組織儲存庫。每個標籤皆包含由您定義的一個金鑰與一個選用值。

## 建立儲存庫建立範本的 IAM 許可

IAM 主體需要下列許可才能管理儲存庫建立範本。必須使用身分型 IAM 政策授予此許可。

- `ecr:CreateRepositoryCreationTemplate` – 准許建立儲存庫建立範本。
- `ecr:DeleteRepositoryCreationTemplate` – 准許刪除儲存庫建立範本。
- `ecr:PutLifecyclePolicy` – 准許建立生命週期政策，並將其套用至儲存庫。僅當儲存庫建立範本包含生命週期政策時，才需要此許可。
- `ecr:SetRepositoryPolicy` – 准許為儲存庫建立許可政策。僅當儲存庫建立範本包含儲存庫政策時，才需要此許可。
- `ecr:TagResource` – 准許將中繼資料標籤新增至資源。僅當儲存庫建立範本包含資源標籤時，才需要此許可。

## 在 Amazon ECR 中創建存儲庫創建模板

您可以建立儲存庫建立範本，以定義 Amazon ECR 在提取快取動作期間代表您建立的儲存庫所使用的設定。建立存放庫建立範本之後，所有在提取快取動作期間建立的新存放庫都會套用這些設定。這並不影響任何先前建立的儲存庫。

若要建立儲存庫建立範本 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列選擇要在其中建立儲存庫建立範本的區域。
3. 在導覽窗格中，選擇私有登錄檔，儲存庫建立範本。
4. 在儲存庫建立範本頁面上，選擇建立範本。

5. 在步驟 1：定義範本頁面上，針對範本詳細資料，選擇特定字首以將範本套用至特定儲存庫命名空間字首，或選擇 ECR 登錄檔中的任何字首，將範本套用至與區域中任何其他範本不相符的所有儲存庫。

   a. 如果您選擇特定字首，請針對字首指定要套用範本的儲存庫命名空間字首。總會有一個假設 / 套用至字首的結尾。例如，`prod` 字首會套用至開頭為 `prod/` 的所有儲存庫。同樣地，`prod/team` 字首會套用至開頭為 `prod/team/` 的所有儲存庫。

   b. 如果您選擇 ECR 登錄檔中的任何字首，字首將設定為 `ROOT`。

6. 針對範本描述，請指定範本的選擇性描述，然後選擇下一步。

7. 在步驟 2：新增儲存庫建立組態頁面中，指定要套用至使用範本建立之儲存庫的儲存庫設定組態。

   a. 針對 Image tag mutability (映像標籤可變性)，選擇要使用的標籤可變性設定。如需詳細資訊，請參閱 防止 Amazon ECR 中的圖像標籤被覆蓋。

      選取可變時，可以覆寫映像標籤。建議使用此設定，用於透過提取快取動作所建立的儲存庫的範本。這可確保標籤相同時，Amazon ECR 可以更新快取的映像。

      選取不可變時，會防止映像標籤遭到覆寫。儲存庫設定為不可變標籤後，如果有嘗試推送的映像具有已存在於儲存庫的標籤，將傳回 `ImageTagAlreadyExistsException` 錯誤。當為儲存庫開啟了標籤不變性時，這會影響所有標籤，並且您無法將某些標籤設為不可變，而將其他標籤設為可變。

   b. 針對加密組態，請選擇要使用的加密設定。如需詳細資訊，請參閱 靜態加密。

      選取 AES-256 時，Amazon ECR 會使用伺服器端加密與 Amazon Simple Storage Service 受管加密金鑰，該加密金鑰使用行業標準的 AES-256 加密演算法對靜態資料進行加密。此服務無須額外付費。

      選取 AWS KMS 時，Amazon ECR 會使用存放在 AWS Key Management Service (AWS KMS) 中的金鑰的伺服器端加密。使用 AWS KMS 加密資料時，您可以使用由 Amazon ECR AWS 管理的預設受管金鑰，或指定您自己的 AWS KMS 金鑰 (稱為客戶受管金鑰)。

      > **Note**
      >
      > 一旦建立儲存庫，就無法變更儲存庫的加密設定。

   c. 針對儲存庫許可，請指定要套用至使用此範本建立之儲存庫的儲存庫許可政策。您可以選擇性地使用下拉式清單，針對最常見的使用案例選取其中一個 JSON 範例。如需詳細資訊，請參閱 Amazon ECR 中的私有儲存庫政策。

d. 針對儲存庫生命週期政策，請指定要套用至使用此範本建立的儲存庫之儲存庫生命週期政策。您可以選擇性地使用下拉式清單，針對最常見的使用案例選取其中一個 JSON 範例。如需詳細資訊，請參閱 在 Amazon ECR 中使用生命週期政策自動清理映像檔。

e. 對於存放庫 AWS 標籤，請以鍵值配對形式指定中繼資料，以便與使用此樣板建立的儲存庫產生關聯，然後選擇下一步。如需詳細資訊，請參閱 在 Amazon ECR 中標記私有存儲庫。

8. 在步驟 3：檢閱和建立頁面上，檢閱您為儲存庫建立範本指定的設定。選擇編輯選項來進行變更。一旦完成，請選擇建立。

## 刪除 Amazon ECR 中的存儲庫創建模板

如果您使用完儲存庫建立範本，您可以將其刪除。刪除存放庫建立範本後，在提取快取動作期間建立的任何存放庫都會套用預設設定。

若要刪除儲存庫建立範本 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列上，選擇要刪除的儲存庫建立範本所在的區域。
3. 在導覽窗格中，選擇私有登錄檔，儲存庫建立範本。
4. 在儲存庫建立範本頁面上，選取要刪除的儲存庫建立範本。
5. 從動作下拉式選單中，選擇刪除。

# 驗證 Amazon ECR 中的快取規則提取

建立提取快取規則後，對於需要驗證的上游登錄，您可以驗證規則是否正常運作。驗證提取快取規則時，Amazon ECR 會與上游登錄建立網路連線、驗證其可存取包含上游登錄登入資料的 Secrets Manager 密碼，並驗證驗證是否成功。

在開始使用提取快取規則之前，請確認您擁有適當的 IAM 許可。如需詳細資訊，請參閱 將上游登錄與 Amazon ECR 私有登錄同步所需的 IAM 許可。

### 若要驗證提取快取規則 (AWS Management Console)

下列步驟說明如何使用 Amazon ECR 主控台驗證提取快取規則。

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列選擇包含提取快取規則的區域以進行驗證。

3. 在導覽窗格中，選擇 Private registry (私有登錄檔)、Pull through cache (提取快取)。
4. 在提取快取組態頁面上，選取要驗證的提取快取規則。接著，使用動作下拉式選單並選擇檢視詳細資料。
5. 在提取快取規則詳細資料頁面上，使用動作下拉式選單，然後選擇驗證身分驗證。Amazon ECR 將顯示寫著結果的橫幅。
6. 針對您要驗證的每個提取快取規則重複這些步驟。

### 若要驗證提取快取規則 (AWS CLI)

驗證提取快取規則 AWS CLI 命令用於驗證 Amazon ECR 私有登錄的直通快取規則。下列範例會使用 `ecr-public` 命名空間字首。以要驗證的提取快取規則的字首值取代該值。

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

在回應中，`isValid` 參數會指出驗證是否成功。如果出現 `true`，代表 Amazon ECR 可以連到上游登錄檔，且身分驗證成功。如果出現 `false`，代表出現問題並且驗證失敗。該 `failure` 參數會指出原因。

## 在 Amazon ECR 中通過緩存規則拉動圖像

下列範例顯示使用提取快取規則來提取映像時所要使用的命令語法。如果您在使用提取快取規則提取上游映像時收到錯誤，請參閱 疑難排解 Amazon ECR 中的快取問題 以查看最常見的錯誤以及解決方式。

在開始使用提取快取規則之前，請確認您擁有適當的 IAM 許可。如需詳細資訊，請參閱 將上游登錄與 Amazon ECR 私有登錄同步所需的 IAM 許可。

> **Note**
>
> 下列範例使用所使用的預設 Amazon ECR 儲存庫命名空間值。 AWS Management Console 確保使用已設定的 Amazon ECR 私有儲存庫 URI。

### 對於 Amazon ECR Public

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

### Kubernetes 容器登錄檔

```
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

針對 Docker Hub 官方映像：

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

> **Note**
>
> 針對 Docker Hub 官方映像，必須包含 `/library` 字首。對於所有其他 Docker Hub 儲存庫，您應該省略 `/library` 字首。

針對所有其他 Docker Hub 映像：

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

### GitHub 容器登錄

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

### Microsoft Azure Container Registry

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

### GitLab 容器登錄

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

## 將您的上游存儲庫憑據存儲在 AWS Secrets Manager 密鑰中

為需要身分驗證的上游儲存庫建立提取快取規則時，您必須將憑證儲存在 Secrets Manager 秘密中。使用 Secrets Manager 秘密可能需要付費。如需詳細資訊，請參閱 AWS Secrets Manager 定價。

下列程序將逐步指引您為每個支援的上游儲存庫建立 Secret Secrets Manager 秘密的方法。您可以選擇性地使用 Amazon ECR 主控台中的建立提取快取規則工作流程來建立秘密，而不是使用 Secrets Manager 主控台建立秘密。如需詳細資訊，請參閱 在 Amazon ECR 中創建提取緩存規則。

Docker Hub

若要為您的 Docker Hub 憑證建立 Secrets Manager 秘密 (AWS Management Console)

1. 前往以下位置開啟機密管理員控制台：https://console.aws.amazon.com/secretsmanager/。
2. 選擇 Store a new secret (存放新機密)。
3. 在選擇秘密類型頁面上，執行下列動作。
   a. 針對機密類型，選擇其他類型的機密。
   b. 在鍵值對中，為您的 Docker Hub 憑證建立兩個資料列。秘密當中最多可以存放 65536 個位元組。
      i. 針對第一個鍵值對，請指定 `username` 為鍵，並指定您的 Docker Hub 使用者名稱為值。
      ii. 針對第二個鍵值對，請指定 `accessToken` 為鍵，並指定您的 Docker Hub 存取字符為值。如需建立 Docker Hub 存取字符的詳細資訊，請參閱 Docker 文件中的建立和管理存取字符。

c. 針對加密金鑰，請保留預設的 aws/secretsmanager AWS KMS key 值，接著選擇下一步。使用此金鑰無需任何成本。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的 Secrets Manager 中的秘密加密和解密。

> **Important**
>
> 您必須使用預設 `aws/secretsmanager` 加密金鑰來加密秘密。Amazon ECR 不支援為此使用客戶自管金鑰 (CMK)。

4. 在設定秘密頁面上，執行下列動作。

a. 輸入描述性的 Secret name (機密名稱) 和 Description (描述)。秘密名稱必須含有 1 至 512 個 Unicode 字元,並且以 `ecr-pullthroughcache/` 作為字首。

> **Important**
>
> Amazon ECR AWS Management Console 只會使用前置詞顯示名稱的機 Secrets Manager 密`ecr-pullthroughcache/`碼。

b. (選用) 在 Tags (標籤) 區段，將標籤新增到秘密。關於標記策略，請參閱 《AWS Secrets Manager 使用者指南》中的標記 Secrets Manager 秘密。請勿在標籤中存放敏感資訊，因為標籤並未加密。

c. (選用) 若要將資源政策新增至秘密，請在 Resource permissions (資源使用權限) 中選擇 Edit permissions (編輯許可)。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的將許可政策連接至 Secrets Manager 秘密。

d. (選擇性) 在複製密碼中，若要將您的密碼複製到另一個機密 AWS 區域，請選擇複製密碼。您可以立即複寫秘密，也可以稍後返回複寫。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的將秘密複寫至其他地區。

e. 選擇下一步。

5. (選用) 在 Configure rotation (設定輪換) 頁面上，可開啟自動輪換。您也可以暫時關閉輪換，稍後再將其開啟。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的輪換 Secrets Manager 秘密。選擇 Next (下一步)。

6. 在 Review (檢閱) 頁面上，檢閱機密詳細資訊，然後選擇 Store (存放)。

Secrets Manager 會傳回秘密清單。如果您的新秘密沒有顯示，請選擇重新整理按鈕。

GitHub Container Registry

為您的 GitHub 容器登錄認證建立密碼管理員密碼 (AWS Management Console)

1. 前往以下位置開啟機密管理員控制台：https://console.aws.amazon.com/secretsmanager/。
2. 選擇 Store a new secret (存放新機密)。
3. 在選擇秘密類型頁面上，執行下列動作。
   a. 針對機密類型，選擇其他類型的機密。
   b. 在索引鍵/值配對中，為您 GitHub 的認證建立兩列。秘密當中最多可以存放 65536 個位元組。
      i. 對於第一個鍵/值對，指定`username`為密鑰，並將您的 GitHub用戶名指定為值。
      ii. 對於第二個鍵/值對，指定`accessToken`為密鑰，將 GitHub 訪問令牌指定為值。有關創建 GitHub 訪問令牌的更多信息，請參閱 GitHub 文檔中的管理您的個人訪問令牌。
   c. 針對加密金鑰，請保留預設的 aws/secretsmanager AWS KMS key 值，接著選擇下一步。使用此金鑰無需任何成本。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的 Secrets Manager 中的秘密加密和解密。

      > **Important**
      >
      > 您必須使用預設 `aws/secretsmanager` 加密金鑰來加密秘密。Amazon ECR 不支援為此使用客戶自管金鑰 (CMK)。

4. 在 Configure secret (設定秘密) 頁面上，執行下列動作：
   a. 輸入描述性的 Secret name (機密名稱) 和 Description (描述)。秘密名稱必須含有 1 至 512 個 Unicode 字元,並且以 `ecr-pullthroughcache/` 作為字首。

      > **Important**
      >
      > Amazon ECR AWS Management Console 只會使用前置詞顯示名稱的機 Secrets Manager 密`ecr-pullthroughcache/`碼。

   b. (選用) 在 Tags (標籤) 區段，將標籤新增到秘密。關於標記策略，請參閱 《AWS Secrets Manager 使用者指南》中的標記 Secrets Manager 秘密。請勿在標籤中存放敏感資訊，因為標籤並未加密。

c. (選用) 若要將資源政策新增至秘密，請在 Resource permissions (資源使用權限) 中選擇 Edit permissions (編輯許可)。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的將許可政策連接至 Secrets Manager 秘密。

d. (選擇性) 在複製密碼中，若要將您的密碼複製到另一個機密 AWS 區域，請選擇複製密碼。您可以立即複寫秘密，也可以稍後返回複寫。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的將秘密複寫至其他地區。

e. 選擇下一步。

5. (選用) 在 Configure rotation (設定輪換) 頁面上，可開啟自動輪換。您也可以暫時關閉輪換，稍後再將其開啟。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的輪換 Secrets Manager 秘密。選擇 Next (下一步)。

6. 在 Review (檢閱) 頁面上，檢閱機密詳細資訊，然後選擇 Store (存放)。

   Secrets Manager 會傳回秘密清單。如果您的新秘密沒有顯示，請選擇重新整理按鈕。

Microsoft Azure Container Registry

若要為您的 Microsoft Azure Container Registry 憑證建立 Secrets Manager 秘密 (AWS Management Console)

1. 前往以下位置開啟機密管理員控制台：https://console.aws.amazon.com/secretsmanager/。
2. 選擇 Store a new secret (存放新機密)。
3. 在選擇秘密類型頁面上，執行下列動作。

   a. 針對機密類型，選擇其他類型的機密。

   b. 在鍵/值對中，為您的 Microsoft Azure 憑證建立兩個資料列。秘密當中最多可以存放 65536 個位元組。

      i. 針對第一個鍵值對，請指定 `username` 為鍵，並指定您的 Microsoft Azure Container Registry 使用者名稱為值。

      ii. 針對第二個鍵值對，請指定 `accessToken` 為鍵，並指定您的 Microsoft Azure Container Registry 存取字符為值。如需建立 Microsoft Azure 存取字符的詳細資訊，請參閱 Microsoft Azure 文件中的建立字符 - 入口網站。

   c. 針對加密金鑰，請保留預設的 aws/secretsmanager AWS KMS key 值，接著選擇下一步。使用此金鑰無需任何成本。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的 Secrets Manager 中的秘密加密和解密。

> **Important**
>
> 您必須使用預設 `aws/secretsmanager` 加密金鑰來加密秘密。Amazon ECR 不支援為此使用客戶自管金鑰 (CMK)。

4. 在 Configure secret (設定秘密) 頁面上，執行下列動作：

   a. 輸入描述性的 Secret name (機密名稱) 和 Description (描述)。秘密名稱必須含有 1 至 512 個 Unicode 字元,並且以 `ecr-pullthroughcache/` 作為字首。

   > **Important**
   >
   > Amazon ECR AWS Management Console 只會使用前置詞顯示名稱的機 Secrets Manager 密`ecr-pullthroughcache/`碼。

   b. (選用) 在 Tags (標籤) 區段，將標籤新增到秘密。關於標記策略，請參閱 《AWS Secrets Manager 使用者指南》中的標記 Secrets Manager 秘密。請勿在標籤中存放敏感資訊，因為標籤並未加密。

   c. (選用) 若要將資源政策新增至秘密，請在 Resource permissions (資源使用權限) 中選擇 Edit permissions (編輯許可)。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的將許可政策連接至 Secrets Manager 秘密。

   d. (選擇性) 在複製密碼中，若要將您的密碼複製到另一個機密 AWS 區域，請選擇複製密碼。您可以立即複寫秘密，也可以稍後返回複寫。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的將秘密複寫至其他地區。

   e. 選擇下一步。

5. (選用) 在 Configure rotation (設定輪換) 頁面上，可開啟自動輪換。您也可以暫時關閉輪換，稍後再將其開啟。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的輪換 Secrets Manager 秘密。選擇 Next (下一步)。

6. 在 Review (檢閱) 頁面上，檢閱機密詳細資訊，然後選擇 Store (存放)。

   Secrets Manager 會傳回秘密清單。如果您的新秘密沒有顯示，請選擇重新整理按鈕。

GitLab Container Registry

為您的 GitLab 容器登錄認證建立密碼管理員密碼 (AWS Management Console)

1. 前往以下位置開啟機密管理員控制台：https://console.aws.amazon.com/secretsmanager/。
2. 選擇 Store a new secret (存放新機密)。
3. 在選擇秘密類型頁面上，執行下列動作。
   a. 針對機密類型，選擇其他類型的機密。
   b. 在索引鍵/值配對中，為您 GitLab 的認證建立兩列。秘密當中最多可以存放 65536 個位元組。
      i. 對於第一個索引鍵/值組，請指定`username`為機碼，並指定 GitLab 容器登錄使用者名稱做為值。
      ii. 對於第二個鍵/值對，指定`accessToken`為密鑰，並指定 GitLab 容器註冊表訪問令牌作為值。有關建立 GitLab 容器登錄存取權杖的詳細資訊，請參閱 GitLab 文件中的個人存取權杖、群組存取權杖或專案存取權杖。
   c. 針對加密金鑰，請保留預設的 aws/secretsmanager AWS KMS key 值，接著選擇下一步。使用此金鑰無需任何成本。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的 Secrets Manager 中的秘密加密和解密。

   > **Important**
   >
   > 您必須使用預設 `aws/secretsmanager` 加密金鑰來加密秘密。Amazon ECR 不支援為此使用客戶自管金鑰 (CMK)。

4. 在 Configure secret (設定秘密) 頁面上，執行下列動作：
   a. 輸入描述性的 Secret name (機密名稱) 和 Description (描述)。秘密名稱必須含有 1 至 512 個 Unicode 字元,並且以 `ecr-pullthroughcache/` 作為字首。

   > **Important**
   >
   > Amazon ECR AWS Management Console 只會使用前置詞顯示名稱的機 Secrets Manager 密`ecr-pullthroughcache/`碼。

b. (選用) 在 Tags (標籤) 區段，將標籤新增到秘密。關於標記策略，請參閱 《AWS Secrets Manager 使用者指南》中的標記 Secrets Manager 秘密。請勿在標籤中存放敏感資訊，因為標籤並未加密。

c. (選用) 若要將資源政策新增至秘密，請在 Resource permissions (資源使用權限) 中選擇 Edit permissions (編輯許可)。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的將許可政策連接至 Secrets Manager 秘密。

d. (選擇性) 在複製密碼中，若要將您的密碼複製到另一個機密 AWS 區域，請選擇複製密碼。您可以立即複寫秘密，也可以稍後返回複寫。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的將秘密複寫至其他地區。

e. 選擇下一步。

5. (選用) 在 Configure rotation (設定輪換) 頁面上，可開啟自動輪換。您也可以暫時關閉輪換，稍後再將其開啟。如需詳細資訊，請參閱 《AWS Secrets Manager 使用者指南》中的輪換 Secrets Manager 秘密。選擇 Next (下一步)。

6. 在 Review (檢閱) 頁面上，檢閱機密詳細資訊，然後選擇 Store (存放)。

   Secrets Manager 會傳回秘密清單。如果您的新秘密沒有顯示，請選擇重新整理按鈕。

# 疑難排解 Amazon ECR 中的快取問題

在使用提取快取規則提取上游映像時，以下是您可能會收到的最常見錯誤。

儲存庫不存在

指示儲存庫不存在的錯誤大多是因為儲存庫不存在於您的 Amazon ECR 私有登錄檔中，或是因為未授予 `ecr:CreateRepository` 許可給提取上游映像的 IAM 主體。若要解決此錯誤，您應該確認您提取命令中的儲存庫 URI 正確，已授予所需要的 IAM 許可給提取上游映像的 IAM 主體，或者在進行上游映像提取之前已在您的 Amazon ECR 私有登錄檔中建立了要將上游映像推送到的儲存庫。如需所需 IAM 許可的詳細資訊，請參閱 將上游登錄與 Amazon ECR 私有登錄同步所需的 IAM 許可。

以下為此錯誤的範例。

```
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'
```

找不到要求的影像

指示找不到映像的錯誤大多是因為映像不存在於上游登錄檔中，或是因為未授予 `ecr:BatchImportUpstreamImage` 許可給提取上游映像的 IAM 主體，但已在您的 Amazon ECR 私有登錄檔中建立了儲存庫。若要解決此錯誤，您應該確認上游映像和映像標籤名稱正確，且其已存在且已將所需要的 IAM 許可授予提取上游映像的 IAM 主體。如需所需 IAM 許可的詳細資訊，請參閱 [將上游登錄與 Amazon ECR 私有登錄同步所需的 IAM 許可]。

以下為此錯誤的範例。

```
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 從碼頭集線器存儲庫拉出時禁止

從標記為 Docker 官方映像的 Docker Hub 儲存庫中提取時，您必須在您使用的 URI 中包含 `/library/`。例如 *`aws_account_id`*`.dkr.ecr.`*`region`*`.amazonaws.com/docker-hub/`**`library/`***`image_name:tag`*。如果您省略 Docker Hub 官方映像檔的 `/library/`，當您嘗試使用提取快取規則提取映像時，將會傳回 `403 Forbidden` 錯誤。如需詳細資訊，請參閱 [在 Amazon ECR 中通過緩存規則拉動圖像]。

以下為此錯誤的範例。

```
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
```

# Amazon ECR 中的私有映像複寫

您可以設定 Amazon ECR 私有登錄檔，以支援儲存庫的複寫。Amazon ECR 支援跨區域和跨帳戶複寫。若要進行跨帳戶複寫，目的地帳戶必須設定登錄檔許可政策，以允許從來源登錄檔進行複寫。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表許可。

主題



## 私有映像複寫的考量

使用私有映像複寫時應考慮以下事項。

- 只會複寫於設定複寫後推送到儲存庫的儲存庫內容。不會複寫儲存庫中預先存在的任何內容。針對儲存庫設定複寫後，Amazon ECR 會讓目的地和來源同步保持。
- 發生複寫時，跨區域和帳戶的儲存庫名稱將保持不變。Amazon ECR 不支援在複寫期間變更儲存庫名稱。
- 第一次設定私有登錄檔進行複寫時，Amazon ECR 會代表您建立服務連結 IAM 角色。服務連結 IAM 角色授予 Amazon ECR 複寫服務在登錄檔中建立儲存庫和複寫映像所需的許可。如需詳細資訊，請參閱 使用 Amazon ECR 的服務連結角色。
- 若要進行跨帳戶複寫，私有登錄檔目的地必須授予許可，才能允許來源登錄複寫其映像。這是藉由設定私有登錄檔許可政策來完成。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表許可。
- 如果私有登錄檔的許可政策變更為移除許可，先前授予的任何進行中複寫都可能完成。
- 若要進行跨區域複寫，來源帳戶和目的地帳戶都必須先選擇加入區域，才能在該區域內或對該區域發生任何複寫動作。如需詳細資訊，請參閱《Amazon Web Services 一般參考》中的管理 AWS 區域。
- 不支援 AWS 磁碟分割之間的跨區域複寫。例如，無法將 `us-west-2` 中的儲存庫複寫到 `cn-north-1`。如需有關 AWS 分割區的詳細資訊，請參閱AWS 一般參考中的 ARN 格式。
- 私有登錄檔的複寫設定可能包含最多 25 個唯一目的地，跨越所有規則，最多有 10 個規則總計。每個規則最多可包含 100 個篩選條件。例如，這允許為包含用於生產和測試之映像的儲存庫指定個別規則。

- 複寫組態支援篩選藉由指定儲存庫字首來複寫私有登錄檔中的儲存庫。如需範例，請參閱範例：使用儲存庫篩選條件設定跨區域複寫。
- 每次映像推送時，複寫動作只會發生一次。例如，如果您將跨區域複寫從 us-west-2 至 us-east-1 和來自 us-east-1 至 us-east-2 進行設定，映像會推送至 us-west-2 僅複寫至 us-east-1，它不會再複寫至 us-east-2。這種行為適用於跨區域和跨帳戶複寫。
- 大多數映像可在不到 30 分鐘的時間內複製，但在極少數情況下，複製可能需要更長的時間。
- 登錄檔複寫不會執行任何刪除動作。當複寫映像和儲存庫不再使用時，您可以手動刪除複寫映像和儲存庫。
- 儲存庫政策 (包括 IAM 政策和生命週期政策) 不會進行複寫，除了它們定義的儲存庫外，也不會有任何影響。
- 不會複寫儲存庫設定。根據預設，所有因複寫動作而建立的儲存庫上會停用標籤不變性、映像掃描和 KMS 加密設定。建立儲存庫後，可以變更標籤不變性和映像掃描設定。不過，此設定僅適用於設定變更後推送的映像。
- 如果在儲存庫上啟用標籤不變性，而且複寫使用與現有映像相同標籤的映像，則會複寫映像，但不會包含重複的標籤。這可能導致映像未標籤。

# Amazon ECR 的私有映像複寫範例

以下範例顯示私有映像複寫作業的常見使用方式。如果您使用設定複寫 AWS CLI，您可以在建立 JSON 檔案時使用 JSON 範例做為起點。如果您使用設定複寫 AWS Management Console，當您在 [檢閱並提交] 頁面上檢閱複寫規則時，您會看到類似的 JSON。

## 範例：將跨區域複寫設定為單一目的地區域

下列顯示在單一登錄檔內設定跨區域複寫的範例。此範例假設您的帳戶 ID 為 111122223333 並且您正在 us-west-2 以外的區域中指定此複寫組態。

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

```
    ]
}
```

## 範例：使用儲存庫篩選條件設定跨區域複寫

下列範例說明為符合字首名稱值的儲存庫設定跨區域複寫。此範例假設您的帳戶 ID 為 111122223333 並且您正在 us-west-1 以外的區域中指定此複寫組態，並且儲存庫的字首為 prod。

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

## 範例：設定跨區域複寫至多個目的地區域

下列顯示在單一登錄檔內設定跨區域複寫的範例。此範例假設您的帳戶 ID 為 111122223333 並且您正在 us-west-1 或 us-west-2 以外的區域中指定此複寫組態。

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

```
    ]
}
```

## 範例：設定跨帳戶複寫

下列顯示為登錄檔設定跨帳戶複寫的範例。此範例會設定複寫到 444455556666 帳戶和 us-west-2 區域。

> **Important**
>
> 若要進行跨帳戶複寫，目的地帳戶必須設定登錄檔許可政策，以允許複寫發生。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表許可。

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

## 範例：指定組態中的多個規則

以下顯示為登錄檔設定多個複寫規則的範例。此範例使用規則設定 *111122223333* 帳戶的複寫，該規則將字首為 prod 的儲存庫複寫到 us-west-2 區域，並將字首為 test 的儲存庫複寫到 us-east-2 區域。複寫組態最多可包含 10 個規則，每個規則最多可指定 25 個目的地。

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

# 在 Amazon ECR 中設定私有映像複寫

針對您的私人登錄設定每個區域的複寫。您可以設定跨區域複寫或跨帳戶複寫。

如需複寫作業常見使用方式的範例，請參閱Amazon ECR 的私有映像複寫範例。

## 設定登錄檔複寫設定 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列，選擇要為其設定登錄檔複寫設定的區域。
3. 在導覽窗格中，選擇 Private registry (私有登錄檔)。
4. 在 Private registry (私有登錄檔) 頁面上，於 Replication (複寫) 區段中，選擇 Edit (編輯)。
5. 在 Replication (複寫) 頁面上，選擇 Add replication rule (新增複寫規則)。
6. 在 Destination types (目的地類型) 頁面上，選擇要啟用跨區域複寫、跨帳戶複寫或兩者，然後選擇 Next (下一步)。
7. 如果啟用跨區域複寫，則對於 Configure destination regions (設定目的地區域)，選擇一或多個 Destination regions (目的地區域)，然後選擇 Next (下一步)。
8. 如果啟用跨帳戶複寫，則對於 Cross-account replication (跨帳戶複寫)，選擇登錄檔的跨帳戶複寫設定。對於 Destination account (目的地帳戶)，輸入目的地帳戶的帳戶 ID 和一或多個 Destination regions (目的地區域) 以進行複寫。選擇 Destination account + (目的地帳戶 +)，將其他帳戶設定為複寫目的地。

> **Important**
>
> 若要進行跨帳戶複寫，目的地帳戶必須設定登錄檔許可政策，以允許複寫發生。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表許可。

9. (選用) 在 Add filters (新增篩選條件) 頁面上，指定複寫規則的一或多個篩選條件，然後選擇 Add (新增)。對於您要與複寫動作產生關聯的每個篩選條件重複此步驟。必須將篩選器指定為儲存庫名稱字首。如果未新增篩選器，則會複寫所有儲存庫的內容。一旦新增所有篩選條件，選擇 Next (下一步)。
10. 在 Review and submit (檢閱並提交) 頁面上，檢閱複寫規則組態，然後選擇 Submit rule (提交規則)。

## 設定登錄檔複寫設定 (AWS CLI)

1. 建立包含要為登錄檔定義的複寫規則的 JSON 檔案。複寫組態最多可包含 10 個規則，且所有規則最多 25 個唯一目的地，每個規則 100 個篩選條件。若要在您自己的帳戶內設定跨區域複寫，請指定您自己的帳戶 ID。如需更多範例，請參閱Amazon ECR 的私有映像複寫範例。

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

2. 登錄的複寫組態。

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

3. 確認您的登錄檔設定。

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

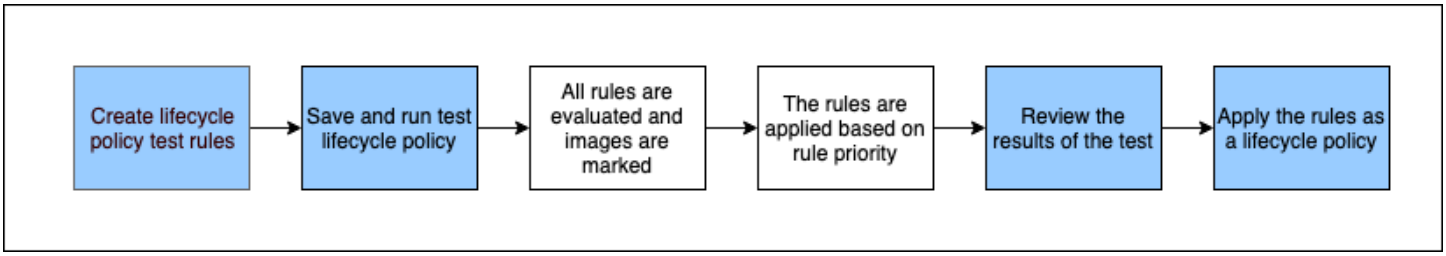
# 在 Amazon ECR 中使用生命週期政策自動清理映像檔

Amazon ECR 生命週期政策提供對私有儲存庫中映像的生命週期管理的更多控制。生命週期政策包含一或多個規則，每個規則都會針對 Amazon ECR 定義一個動作。根據生命週期政策中的到期條件，映像會根據 24 小時內的年齡或計數過期。當 Amazon ECR 根據生命週期政策執行動作時，此動作會擷取為中 AWS CloudTrail的事件。如需詳細資訊，請參閱 使用記錄 Amazon ECR 動作 AWS CloudTrail。

## 生命週期政策如何運作

生命週期政策由一或多個規則組成，用以決定儲存庫中的映像過期與否。在考慮使用生命週期政策時，請務必使用生命週期政策預覽來確認生命週期政策到期的映像，然後再將其套用至儲存庫。將生命週期政策套用至儲存庫後，您可預期映像將在符合到期條件後的 24 小時內過期。當 Amazon ECR 依據生命週期政策執行動作時，在 AWS CloudTrail中會將此動作視為事件。如需詳細資訊，請參閱 使用記錄 Amazon ECR 動作 AWS CloudTrail。

以下圖表顯示生命週期政策工作流程。




1. 建立一或多個測試規則。
2. 儲存測試規則並執行預覽。
3. 生命週期政策評估工具會檢視所有規則，並標記每個規則會影響的映像。
4. 然後，生命週期政策評估工具會根據規則優先順序套用規則，並顯示儲存庫中的哪些映像設定為過期。
5. 檢閱測試結果，確保標示為過期的映像符合您的預期。
6. 套用測試規則作為儲存庫的生命週期政策。
7. 建立生命週期政策後，您可預期映像將在符合到期條件後的 24 小時內過期。

# 生命週期政策評估規則

生命週期政策評估工具負責剖析生命週期政策的純文字 JSON、評估所有規則，然後根據規則優先順序套用這些規則至儲存庫中的映像。以下詳細說明生命週期政策評估工具的邏輯。如需範例，請參閱 Amazon ECR 中的生命週期政策範例。

- 不論規則優先順序，都會同時評估所有規則。評估所有規則之後，就會根據規則優先順序進行套用。
- 使用正好一個或零個規則來使映像過期。
- 不可使用優先順序低的規則使符合優先順序高的規則標記要求的映像過期。
- 規則絕不可標記以較高優先順序規則標記的映像，但是，優先順序低的規則仍能找出這些映像，就好像它們還沒有過期一樣。
- 規則組必須包含獨特的標籤前綴組合。
- 僅允許一個規則選擇未標記的映像。
- 如果清單檔案清單參考了映像檔，則映像檔無法在沒有先刪除清單檔案清單的情況下過期。
- 過期一律以 `pushed_at_time` 排列，且過期順序須為舊映像先、新映像後。
- 生命週期政策規則可指定 `tagPatternList` 或 `tagPrefixList`，但不能同時指定兩者。不過，生命週期策略可包含多項規則，不同規則可同時使用模式和字首清單。
- 唯有當 `tagStatus` 是 `tagged` 時，才能使用 `tagPatternList` 或 `tagPrefixList` 參數。
- 使用 `tagPatternList` 時，如果映像與萬用字元篩選條件相符，便會成功配對映像。例如，如果套用 `prod*` 篩選條件，系統會比對名稱以 `prod` 開頭的儲存庫，例如 `prod`、`prod1` 或 `production-team1`。同樣地，如果套用 `*prod*` 篩選條件，系統會比對名稱內包含 `prod` (例如 `repo-production` 或 `prod-team`) 的儲存庫。

  > **Important**
  >
  > 每個字串最多可有 4 個萬用字元 (*)，例如 `["*test*1*2*3", "test*1*2*3*"]` 是有效字串，但 `["test*1*2*3*4*5*6"]` 則為無效。

- 使用 `tagPrefixList` 時，若所有在 `tagPrefixList` 值中的標籤皆符合任何一個映像標籤，便會成功配對映像。
- 只有在 `countType` 是 `sinceImagePushed` 時才會使用 `countUnit` 參數。
- 使用 `countType = imageCountMoreThan`，映像會根據 `pushed_at_time` 來自最新至最舊排序，接著所有大於指定計數的映像皆會過期。
- 使用 `countType = sinceImagePushed`，所有 `pushed_at_time` 大於根據 `countNumber` 之指定天數的映像都會過期。

# 在 Amazon ECR 中建立生命週期政策預覽

您可以使用生命週期原則預覽來查看生命週期原則對映像儲存庫的影響，然後再套用它。在將生命週期政策套用至儲存庫之前，將預覽視為最佳實務。

> **Note**
>
> 如果您使用 Amazon ECR 複寫跨不同區域或帳戶複製儲存庫，請注意，生命週期政策只能對建立該儲存庫的區域中的儲存庫採取動作。因此，如果您已開啟複寫功能，您可能需要考慮在複寫儲存庫的每個區域和帳戶中建立生命週期政策。

建立生命週期政策預覽 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列上，選擇其中包含要執行生命週期政策預覽的儲存庫之區域。
3. 在導覽窗格中，依序選擇私有登錄檔和儲存庫。
4. 在私有儲存庫頁面中選取儲存庫，然後使用動作下拉式清單選擇生命週期政策。
5. 在儲存庫的生命週期政策規則頁面中，依序選擇編輯測試規則和建立規則。
6. 為每個生命週期政策測試規則輸入下列詳細資訊。

    a. 在 Rule priority (規則優先順序) 中，輸入規則優先順序的編號。規則優先順序會決定生命週期政策規則的套用順序。

    b. 在 Rule description (規則描述) 中，輸入生命週期政策規則的描述。

    c. 針對映像狀態，請選擇已標記 (萬用字元比對)、已標記 (前綴比對)、未標記或任何。

    d. 如果您在映像狀態選擇已標記 (萬用字元比對)，可針對指定萬用字元比對標籤指定含萬用字元 (*) 的映像標籤清單，以透過生命週期政策對其執行動作。例如，若您的映像已標記為 `prod`、`prod1`、`prod2` 等等，您可能需要指定 `prod*` 對所有映像執行動作。若您指定多個標籤，只會選擇含有所有指定標籤的映像。

    > **Important**
    >
    > 每個字串最多可有 4 個萬用字元 (*)，例如 `["*test*1*2*3", "test*1*2*3*"]` 是有效字串，但 `["test*1*2*3*4*5*6"]` 則為無效。

    e. 如果您在映像狀態選擇已標記 (前綴比對)，則可針對指定前綴比對標籤指定映像標籤清單，以透過生命週期政策對其執行動作。

f. 在比對條件中選擇自推送的映像或超過以下數目的映像，然後指定一個值。

g. 選擇儲存。

7. 重複操作步驟 5-7 來建立其他測試生命週期政策規則。
8. 若要執行生命週期政策預覽，請選擇 Save and run test (儲存並執行測試)。
9. 在 Image matches for test lifecycle rules (測試生命週期規則的映像符合數) 下，檢視您的生命週期政策預覽影響。
10. 若您對預覽結果感到滿意，請選擇 Apply as lifecycle policy (套用為生命週期政策) 來使用指定規則建立生命週期政策。在套用生命週期政策後，可預期受影響的映像會在 24 小時內過期。
11. 如果對預覽結果不滿意，您可以刪除一或多個測試生命週期規則，再建立一或多個規則加以取代，然後重複測試。

# 在 Amazon ECR 中建立儲存庫的生命週期政策

使用生命週期原則建立一組規則，使未使用的存放庫映像過期。建立生命週期原則後，受影響的映像會在 24 小時內過期。

> **Note**
>
> 如果您使用 Amazon ECR 複寫跨不同區域或帳戶複製儲存庫，請注意，生命週期政策只能對建立該儲存庫的區域中的儲存庫採取動作。因此，如果您已開啟複寫功能，您可能需要考慮在複寫儲存庫的每個區域和帳戶中建立生命週期政策。

## 先決條件

最佳做法：建立生命週期原則預覽，以確認您的生命週期原則規則所過期的映像是否符合您的需求。如需說明，請參閱在 Amazon ECR 中建立生命週期政策預覽。

### 建立生命週期政策 (AWS Management Console)

1. 在 https://console.aws.amazon.com/ecr/repositories 開啟 Amazon ECR 主控台。
2. 從導覽列上，選擇其中包含要建立生命週期政策的儲存庫之區域。
3. 在導覽窗格中，依序選擇私有登錄檔和儲存庫。
4. 在私有儲存庫頁面中選取儲存庫，然後使用動作下拉式清單選擇生命週期政策。

5. 在儲存庫生命週期政策頁面中，選擇建立規則。
6. 為您的生命週期政策規則輸入下列詳細資訊。
   a. 在 Rule priority (規則優先順序) 中，輸入規則優先順序的編號。規則優先順序會決定生命週期政策規則的套用順序。
   b. 在 Rule description (規則描述) 中，輸入生命週期政策規則的描述。
   c. 針對映像狀態，請選擇已標記 (萬用字元比對)、已標記 (前綴比對)、未標記或任何。
   d. 如果您在映像狀態選擇已標記 (萬用字元比對)，可針對指定萬用字元比對標籤指定含萬用字元 (*) 的映像標籤清單，以透過生命週期政策對其執行動作。例如，若您的映像已標記為 `prod`、`prod1`、`prod2` 等等，您可能需要指定 `prod*` 對所有映像執行動作。若您指定多個標籤，只會選擇含有所有指定標籤的映像。

      > **Important**
      >
      > 每個字串最多可有 4 個萬用字元 (*)，例如 `["*test*1*2*3", "test*1*2*3*"]` 是有效字串，但 `["test*1*2*3*4*5*6"]` 則為無效。

   e. 如果您在映像狀態選擇已標記 (前綴比對)，則可針對指定前綴比對標籤指定映像標籤清單，以透過生命週期政策對其執行動作。
   f. 在比對條件中選擇自推送的映像或超過以下數目的映像，然後指定一個值。
   g. 選擇儲存。
7. 重複操作步驟 5-7 來建立其他生命週期政策規則。

## 建立生命週期政策 (AWS CLI)

1. 取得要建立生命週期政策的儲存庫名稱。

```
aws ecr describe-repositories
```

2. 建立名為 `policy.json` 的本機檔案使用生命週期政策的內容。如需生命週期政策範例，請參閱「Amazon ECR 中的生命週期政策範例」。
3. 透過指定儲存庫名稱並參考您建立的生命週期政策 JSON 檔案來建立生命週期政策。

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

# Amazon ECR 中的生命週期政策範例

以下是顯示語法的生命週期原則範例。

若要查看有關策略內容的詳細資訊，請參閱Amazon ECR 中的生命週期政策屬性。如需使用建立生命週期原則的指示 AWS CLI，請參閱建立生命週期政策 (AWS CLI)。

## 生命週期政策範本

在與存放庫產生關聯之前，會先評估生命週期原則的內容。以下是生命週期政策的 JSON 語法範本。

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

## 篩選映像存在時間

以下範例顯示政策的生命週期政策語法，該政策能尋找以 prod 標籤開頭的映像，使用 prod* 的tagPatternList，將存在時間同樣超過 14 天的映像設為過期。

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Expire images older than 14 days",
```

```
            "selection": {
                "tagStatus": "tagged",
                "tagPatternList": ["prod*"],
                "countType": "sinceImagePushed",
                "countUnit": "days",
                "countNumber": 14
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

## 篩選映像計數

以下範例顯示政策的生命週期政策語法，該政策能只保留一個未標記的映像，並將其他所有映像設為過期。

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

## 篩選多個規則

以下是在生命週期政策中使用多個規則的範例。範例儲存庫與指定的生命週期政策與結果說明同時提供。

## 範例 A

儲存庫內容：

- Image A, Taglist: ["beta-1", "prod-1"], Pushed: 10 days ago
- Image B, Taglist: ["beta-2", "prod-2"], Pushed: 9 days ago
- Image C, Taglist: ["beta-3"], Pushed: 8 days ago

生命週期政策文字：

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

生命週期政策的邏輯會是：

- 規則 1 找出含有前綴 prod 標記的映像。將會從最舊的映像開始標記，直到沒有或剩餘很少符合的映像。標記映像 A 為過期。
- 規則 2 找出含有前綴 beta 標記的映像。將會從最舊的映像開始標記，直到沒有或剩餘很少符合的映像。標記映像 A 與映像 B 為過期。但是，映像 A 已被規則 1 看到，而若映像 B 已過期，則會因違反規則 1 而被略過。
- 結果：映像 A 已過期。

## 範例：B

這是與前一個範例相同的儲存庫，但是規則優先順序已變更以說明結果。

儲存庫內容：

- Image A, Taglist: ["beta-1", "prod-1"], Pushed: 10 days ago
- Image B, Taglist: ["beta-2", "prod-2"], Pushed: 9 days ago
- Image C, Taglist: ["beta-3"], Pushed: 8 days ago

生命週期政策文字：

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

生命週期政策的邏輯會是：

- 規則 1 找出含有前綴 beta 標記的映像。將會從最舊的映像開始標記，直到沒有或剩餘很少符合的映像。將看到所有三個映像並標記映像 A 與映像 B 為過期。
- 規則 2 找出含有前綴 prod 標記的映像。將會從最舊的映像開始標記，直到沒有或剩餘很少符合的映像。將不會看到映像，因所有可用映像已被規則 1 看到，因此將不會標記其他映像。
- 結果：映像 A 與 B 皆已過期。

## 篩選單一規則中的多個標籤

以下範例說明在單一規則中採用多標籤模式的生命週期政策語法。範例儲存庫與指定的生命週期政策與結果說明同時提供。

### 範例 A

當單一規則指定多個標籤模式，映像必須符合所有列出的標籤模式。

儲存庫內容：

- Image A, Taglist: ["alpha-1"], Pushed: 12 days ago
- Image B, Taglist: ["beta-1"], Pushed: 11 days ago
- Image C, Taglist: ["alpha-2", "beta-2"], Pushed: 10 days ago
- Image D, Taglist: ["alpha-3"], Pushed: 4 days ago
- Image E, Taglist: ["beta-3"], Pushed: 3 days ago
- Image F, Taglist: ["alpha-4", "beta-4"], Pushed: 2 days ago

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

生命週期政策的邏輯會是：

- 規則 1 找出含有前綴 `alpha` 和 `beta` 標籤的映像。看到映像 C 與 F。應標記存在時間大於五天的映像，應是映像 C。
- 結果：映像 C 已過期。

## 範例：B

下列範例說明非專屬的標籤。

儲存庫內容：

- Image A, Taglist: ["alpha-1", "beta-1", "gamma-1"], Pushed: 10 days ago
- Image B, Taglist: ["alpha-2", "beta-2"], Pushed: 9 days ago
- Image C, Taglist: ["alpha-3", "beta-3", "gamma-2"], Pushed: 8 days ago

```
{
    "rules": [
        {
            "rulePriority": 1,
```

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

生命週期政策的邏輯會是：

- 規則 1 找出含有前綴 alpha 和 beta 標籤的映像。看到所有映像。將會從最舊的映像開始標記，直到沒有或剩餘很少符合的映像。標記映像 A 與 B 為過期。
- 結果：映像 A 與 B 皆已過期。

## 篩選所有映像

以下生命週期政策範例說明含有不同篩選條件的映像。範例儲存庫與指定的生命週期政策與結果說明同時提供。

### 範例 A

下列顯示套用到所有規則的政策之生命週期政策語法，但是只保留一個映像並將其他所有映像設為過期。

儲存庫內容：

- Image A, Taglist: ["alpha-1"], Pushed: 4 days ago
- Image B, Taglist: ["beta-1"], Pushed: 3 days ago
- Image C, Taglist: [], Pushed: 2 days ago
- Image D, Taglist: ["alpha-2"], Pushed: 1 day ago

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

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

生命週期政策的邏輯會是：

- 規則 1 找出所有映像。會看到映像 A、B、C 與 D。除了最新映像外，應將所有映像設為過期。標記映像 A、B、C 為過期。
- 結果：映像 A、B 與 C 皆已過期。

## 範例：B

以下範例說明在單一規則中整合所有規則類型的生命週期政策。

儲存庫內容：

- Image A, Taglist: ["alpha-", "beta-1", "-1"], Pushed: 4 days ago
- Image B, Taglist: [], Pushed: 3 days ago
- Image C, Taglist: ["alpha-2"], Pushed: 2 days ago
- Image D, Taglist: ["git hash"], Pushed: 1 day ago
- Image E, Taglist: [], Pushed: 1 day ago

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

生命週期政策的邏輯會是：

- 規則 1 找出含有前綴 alpha 標記的映像。找出映像 A 與映像 C。應保留最新映像並將其他標記為過期。標記映像 A 為過期。
- 規則 2 找出未標記的映像。找出映像 B 與映像 E。應標記所有超過一天的映像為過期。標記映像 B 為過期。

- 規則 3 找出所有映像。找出映像 A、B、C、D 與 E。應保留最新映像並將其他標記為過期。但是，無法標記映像 A、B、C 或 E，因為會以較高的優先順序規則來找出它們。標記映像 D 為過期。
- 結果：映像 A、B 與 D 皆已過期。

# Amazon ECR 中的生命週期政策屬性

生命週期策略具有以下性質。

若要查看生命週期政策的範例，請參閱Amazon ECR 中的生命週期政策範例。如需使用建立生命週期原則的指示 AWS CLI，請參閱建立生命週期政策 (AWS CLI)。

## 規則優先順序

`rulePriority`

類型：整數

必要：是

設定套用的規則之順序，從最低值到最高值。優先順序1為的生命週期原則規則會先套用，下一個優先順序2為的規則為，依此類推。當您新增規則到生命週期政策時，必須指定唯一的 `rulePriority` 值。值不需要在策略中跨規則循序排列。擁有 `any` 的 `tagStatus` 值必須有 `rulePriority` 的最高值與最後評估的值。

## 描述

`description`

類型：字串

必要：否

(選用) 說明生命週期政策中的規則用途。

## 標籤狀態

`tagStatus`

類型：字串

必要：是

決定您新增的生命週期政策規則是否為映像指定標籤。可接受選項為 tagged、untagged、或 any。若您指定 any，所有映像都對規則進行評估。如果您指定 tagged，那麼您也必須指定 tagPrefixList 值。如果您指定 untagged，那麼您必須省略 tagPrefixList。

## 標籤模式清單

tagPatternList

類型：list[string]

必填：是，如果 tagStatus 設為已標記且未指定 tagPrefixList

為已標記的映像建立生命週期政策時，最佳做法是使用 tagPatternList 來指定預計會過期的標籤。您必須指定以逗號分隔的映像標籤模式清單，其中可能包含萬用字元 (*)，以便您透過生命週期政策執行動作。例如，若您的映像標記為 prod、prod1、prod2 等等，您可能需使用標籤模式清單 prod* 來指定所有標籤。若您指定多個標籤，只會選擇含有所有指定標籤的映像。

> **Important**
>
> 每個字串最多可有 4 個萬用字元 (*)，例如 ["*test*1*2*3", "test*1*2*3*"] 是有效字串，但 ["test*1*2*3*4*5*6"] 則為無效。

## 標籤字首清單

tagPrefixList

類型：list[string]

必填：是，如果 tagStatus 設為已標記且未指定 tagPatternList

僅在您指定 "tagStatus": "tagged" 且未指定 tagPatternList 時使用。您必須指定以逗號分隔的映像標籤前綴清單，用以使用生命週期政策來採取動作。例如，若您的映像被標記為 prod、prod1、prod2 以此類推，您可能需要使用標籤前綴 prod 來指定所有映像。若您指定多個標籤，只會選擇含有所有指定標籤的映像。

## 計數類型

countType

類型：字串

必要：是

指定計數類型以套用到映像。

若 countType 設為 imageCountMoreThan，您也指定 countNumber 來建立設定存在於您的儲存庫中的映像數量限制之規則。若 countType 設為 sinceImagePushed，您也指定 countUnit 與 countNumber 來指定存在於您的儲存庫中的映像時間限制。

## 計數單位

countUnit

類型：字串

必要：是，僅限 countType 設定為 sinceImagePushed 的情況

除了代表天數的 days 外，請指定 countNumber 的技術單位來作為時間單位。

只可在 countType 為 sinceImagePushed 時進行指定；若您在 countType 為其他值時指定計數單位，會發生錯誤。

## Count (計數)

countNumber

類型：整數

必要：是

指定計數號碼。可接受的值為正整數 (0 不是接受值)。

如果使用的 countType 為 imageCountMoreThan，那麼值便是您想要保留於儲存庫中的最大映像數量。如果使用的 countType 為 sinceImagePushed，那麼值便是您想要保留於儲存庫中的映像存在時間上限。

# 動作

`type`

類型：字串

必要：是

指定一種動作類型。支援的值為 `expire`。

# Amazon Elastic Container Registry 的安全性

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 Amazon ECR 的合規計劃，請參閱合規計劃範圍內的AWS 服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Amazon ECR 時套用共同責任模型。下列主題說明如何將 Amazon ECR 設定為符合您的安全與合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Amazon ECR 資源的服務。

主題

- Amazon Elastic Container Registry 的 Identity and Access Management
- Amazon ECR 中的資料保護
- Amazon Elastic Container Registry 的合規驗證
- Amazon Elastic Container Registry 的基礎設施安全性
- 預防跨服務混淆代理人

# Amazon Elastic Container Registry 的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員可以控制驗證 (已登入) 和授權 (具有許可) 來使用 Amazon ECR 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

- 物件
- 使用身分驗證

- 使用政策管理存取權
- Amazon Elastic Container Registry 如何與 IAM 搭配使用
- Amazon Elastic Container Registry 身分型政策的範例
- 使用標籤型存取控制
- AWS Amazon 彈性容器註冊表的受管政策
- 使用 Amazon ECR 的服務連結角色
- 針對 Amazon Elastic Container Registry Identity and Access 進行故障診斷

## 物件

您使用 AWS Identity and Access Management (IAM) 的方式會因您在 Amazon ECR 中執行的工作而有所不同。

服務使用者 – 如果您使用 Amazon ECR 執行任務，您的管理員會為您提供您需要的憑證和許可。隨著您為了執行作業而使用的 Amazon ECR 功能數量變多，您可能會需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Amazon ECR 中的功能，請參閱 針對 Amazon Elastic Container Registry Identity and Access 進行故障診斷。

服務管理員 – 若您在公司負責管理 Amazon ECR 資源，您應該具備 Amazon ECR 的完整存取權限。您的任務是判斷服務使用者應存取的 Amazon ECR 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司可搭配 Amazon ECR 使用 IAM 的方式，請參閱 Amazon Elastic Container Registry 如何與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 Amazon ECR 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的 Amazon ECR 身分型政策範例，請參閱 Amazon Elastic Container Registry 身分型政策的範例。

## 使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

### AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

### IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

### IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

# 使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

## 身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

## 資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

### 其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱 IAM 使用者指南中的工作階段政策。

### 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

## Amazon Elastic Container Registry 如何與 IAM 搭配使用

在您使用 IAM 管理對 Amazon ECR 的存取權之前，您應該瞭解哪些 IAM 功能可以與 Amazon ECR 搭配使用。若要深入瞭解 Amazon ECR 和其他 AWS 服務如何與 IAM 搭配使用，請參閱 IAM 使用者指南中的與 IAM 搭配使用的AWS 服務。

主題

- Amazon ECR 身分型政策
- Amazon ECR 資源型政策
- 以 Amazon ECR 標籤為基礎的授權
- Amazon ECR IAM 角色

## Amazon ECR 身分型政策

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。Amazon ECR 支援特定動作、資源和條件索引鍵。若要了解您在 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 JSON 政策元素參考。

動作

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

Amazon ECR 中的政策動作會在動作之前使用下列字首：`ecr:`。例如，若要授予某人使用 Amazon ECR `CreateRepository` API 操作建立 Amazon ECR 儲存庫的許可，請在其政策中加入 `ecr:CreateRepository` 動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Amazon ECR 會定義自己的一組動作，描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

```
"Action": [
      "ecr:action1",
      "ecr:action2"
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 `Describe` 文字的所有動作，請包含以下動作：

```
"Action": "ecr:Describe*"
```

若要查看 Amazon ECR 動作的清單，請參閱《IAM 使用者指南》中的 Amazon Elastic Container Registry 的動作、資源與條件索引鍵。

資源

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

Amazon ECR 儲存庫資源有以下 ARN：

```
arn:${Partition}:ecr:${Region}:${Account}:repository/${Repository-name}
```

如需 ARN 格式的詳細資訊，請參閱 Amazon 資源名稱 (ARN) 和 AWS 服務命名空間。

例如，若要在陳述式中指定 us-east-1 區域的 my-repo 儲存庫，請使用下列 ARN：

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
```

若要指定屬於特定帳戶的所有儲存庫，請使用萬用字元 (*)：

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/*"
```

若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

```
"Resource": [
      "resource1",
      "resource2"
```

若要查看 Amazon ECR 資源類型及其 ARN 的清單，請參閱《IAM 使用者指南》中的 Amazon Elastic Container Registry 定義的資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon Elastic Container Registry 定義的動作。

條件索引鍵

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

Amazon ECR 會定義自己的一組條件索引鍵，也支援使用一些全域條件索引鍵。若要查看所有 AWS 全域條件金鑰，請參閱 IAM 使用者指南中的AWS 全域條件內容金鑰。

大部分 Amazon ECR 動作均支援 aws:ResourceTag 和 ecr:ResourceTag 條件索引鍵。如需詳細資訊，請參閱 使用標籤型存取控制。

若要查看 Amazon ECR 條件索引鍵的清單，請參閱《IAM 使用者指南》中的 Amazon Elastic Container Registry 定義的條件索引鍵。若要了解您可以搭配哪些動作和資源使用條件索引鍵，請參閱 Amazon Elastic Container Registry 定義的動作。

範例

若要檢視 Amazon ECR 身分型政策的範例，請參閱 Amazon Elastic Container Registry 身分型政策的範例。

## Amazon ECR 資源型政策

資源型政策是 JSON 政策文件，這些文件會指定指定的委託人可對 Amazon ECR 資源以及在怎樣的條件下執行哪些動作。Amazon ECR 支援 Amazon ECR 存放庫的資源型許可政策。資源型政策可讓您依資源將使用許可授予至其他帳戶。您也可以使用資源型政策來允許 AWS 服務存取 Amazon ECR 儲存庫。

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的委託人。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源位於不同的 AWS 帳號中時，您也必須授與主參與者實體存取資源的權限。透過將身分型政策連接到實體來授予許可。不過，如果資源型政策會為相同帳戶中的委託人授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策有何差異。

Amazon ECR 服務僅支援一種稱為儲存庫政策之資源型政策，且已連接到儲存庫。此政策會定義哪些委託人實體 (帳戶、使用者、角色和聯合身分使用者) 可在該儲存庫上執行動作。若要了解如何將資源型政策連接到儲存庫，請參閱 Amazon ECR 中的私有儲存庫政策。

> **Note**
>
> 在 Amazon ECR 儲存器政策中，政策元素 `Sid` 支援 IAM 政策中不支援的附加字元和間距。

範例

若要檢視 Amazon ECR 資源型政策的範例，請參閱 Amazon ECR 中的私有儲存庫政策範例。

## 以 Amazon ECR 標籤為基礎的授權

您可以將標籤連接至 Amazon ECR 資源，或是在請求中將標籤傳遞至 Amazon ECR。若要根據標籤控制存取，請使用 `ecr:ResourceTag/`*`key-name`*、`aws:RequestTag/`*`key-name`* 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。如需標記 Amazon ECR 資源的詳細資訊，請參閱在 Amazon ECR 中標記私有存儲庫。

若要檢視身分型政策範例，以根據該資源上的標籤來限制存取資源，請參閱 使用標籤型存取控制。

## Amazon ECR IAM 角色

IAM 角色是您 AWS 帳戶中具有特定許可的實體。

搭配使用臨時憑證與 Amazon ECR

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫AssumeRole或GetFederation權杖等 AWS STS API 作業來取得臨時安全登入資料。

Amazon ECR 支援使用臨時憑證。

服務連結角色

服務連結角色可讓 AWS 服務存取其他服務中的資源，以代表您完成動作。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

Amazon ECR 支援服務連結角色。如需詳細資訊，請參閱 使用 Amazon ECR 的服務連結角色。

# Amazon Elastic Container Registry 身分型政策的範例

根據預設，使用者和角色不具備建立或修改 Amazon ECR 資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需 Amazon ECR 所定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱《服務授權參考》中的 Amazon Elastic Container Registry 的動作、資源和條件索引鍵。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 IAM 使用者指南中的在 JSON 索引標籤上建立政策。

主題

- 政策最佳實務
- 使用 Amazon ECR 主控台
- 允許使用者檢視自己的許可
- 存取一個 Amazon ECR 儲存庫

## 政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Amazon ECR 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動

作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。

- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

## 使用 Amazon ECR 主控台

若要存取 Amazon Elastic Container Registry 主控台，您必須擁有最基本的一組許可。這些許可必須允許您列出和檢視 AWS 帳戶中 Amazon ECR 資源的詳細資訊。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

若要確保這些實體仍可使用 Amazon ECR 主控台，請將`AmazonEC2ContainerRegistryReadOnly` AWS 受管政策新增至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

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

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合您嘗試執行之 API 操作的動作就可以了。

## 允許使用者檢視自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "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": "*"
```

```
        }
    ]
}
```

## 存取一個 Amazon ECR 儲存庫

在此範例中，您想要授與 AWS 帳戶中的使用者存取其中一個 Amazon ECR 儲存庫。my-repo您也希望允許使用者推送、提取及列出映像。

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

## 使用標籤型存取控制

Amazon ECR CreateRepository API 動作可讓您在建立儲存庫時指定標籤。如需詳細資訊，請參閱 在 Amazon ECR 中標記私有存儲庫。

若要讓使用者在建立時標記儲存庫，他們必須具備建立資源之動作 (如 `ecr:CreateRepository`) 的使用許可。若標籤於資源建立動作指定，Amazon 會針對 `ecr:CreateRepository` 動作執行其他授權，以確認使用者具備建立標籤的許可。

您可以透過 IAM 政策來使用標籤型存取控制，範例如下。

以下政策只允許使用者將儲存庫建立或標記為 `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"
                }
            }
        }
    ]
}
```

以下政策允許使用者存取所有儲存庫，除非被標記為 key=environment,value=prod。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ecr:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ecr:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecr:ResourceTag/environment": "prod"
                }
            }
        }
    ]
}
```

## AWS Amazon 彈性容器註冊表的受管政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

Amazon ECR 提供數個受管政策，您可以將這些政策附加到 IAM 身分或 Amazon EC2 執行個體。這些受管政策允許對 Amazon ECR 資源和 API 操作的存取進行不同層級的控制。如需這些政策中所提及之各 API 操作的詳細資訊，請參閱 Amazon Elastic Container Registry API 參考中的 Actions (動作)。

主題

- AmazonEC2ContainerRegistryFullAccess
- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryReadOnly
- AWSECRPullThroughCache_ServiceRolePolicy
- ECRReplicationServiceRolePolicy
- Amazon ECR 更新 AWS 受管政策

## AmazonEC2ContainerRegistryFullAccess

您可將 AmazonEC2ContainerRegistryFullAccess 政策連接到 IAM 身分。

您可以使用此受管政策作為根據您特定需求建立您自己 IAM 政策的起點。例如，您可以建立專門為使用者或角色提供完全管理員存取權限的政策，以管理對 Amazon ECR 的使用。藉由 Amazon ECR 生命週期政策功能，您可以在儲存庫中指定映像的生命週期管理。生命週期原則事件會報告為 CloudTrail 事件。Amazon ECR 與整合， AWS CloudTrail 因此它可以直接在 Amazon ECR 主控台中顯示您的生命週期政策事件。AmazonEC2ContainerRegistryFullAccess 受管 IAM 政策包括促進此行為的 cloudtrail:LookupEvents 許可。

許可詳細資訊

此政策包含以下許可：

- ecr – 允許委託人完整存取所有 Amazon ECR API。
- cloudtrail— 可讓主參與者查詢由 CloudTrail擷取的管理事件或「 AWS CloudTrail 見解」事件。

AmazonEC2ContainerRegistryFullAccess 政策如下所示。

```
{
    "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

您可將 AmazonEC2ContainerRegistryPowerUser 政策連接到 IAM 身分。

此政策授予管理許可，允許 IAM 使用者讀取和寫入儲存庫，但不允許他們刪除儲存庫或變更套用於他們的政策文件。

許可詳細資訊

此政策包含以下許可：

- ecr – 允許委託人讀取和寫入儲存庫，以及讀取生命週期政策。委託人不會被授予刪除儲存庫或變更套用至其生命週期政策的許可。

AmazonEC2ContainerRegistryPowerUser 政策如下所示。

```
{
    "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

您可將 AmazonEC2ContainerRegistryReadOnly 政策連接到 IAM 身分。

此政策向 Amazon ECR 授予唯讀許可。這包括在儲存庫中列出儲存庫和映像的功能。它還包括使用 Docker CLI 從 Amazon ECR 提取映像的能力。

許可詳細資訊

此政策包含以下許可：

- ecr – 允許委託人讀取儲存庫及其各自的生命週期政策。

AmazonEC2ContainerRegistryReadOnly 政策如下所示。

```
{
```

```
    "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

您無法將 AWSECRPullThroughCache_ServiceRolePolicy 受管 IAM 政策連接至 IAM 實體。此政策會連接至服務連結角色，可讓 Amazon ECR 透過提取快取工作流程將映像推送到儲存庫。如需詳細資訊，請參閱 用於提取快取的 Amazon ECR 服務連結角色。

### ECRReplicationServiceRolePolicy

您無法將 ECRReplicationServiceRolePolicy 受管 IAM 政策連接至 IAM 實體。此政策會連接到服務連結角色，而此角色可讓 Amazon ECR 代表您執行動作。如需詳細資訊，請參閱 使用 Amazon ECR 的服務連結角色。

## Amazon ECR 更新 AWS 受管政策

檢視自此服務開始追蹤這些變更以來，Amazon ECR AWS 受管政策的更新詳細資料。如需有關此頁面變更的自動提醒，請訂閱 Amazon ECR 文件歷史記錄頁面上的 RSS 摘要。

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWSECRPullThroughCache_ServiceRolePolicy – 更新現有政策 | Amazon ECR 將新的許可新增到 AWSECRPullThroughCache_ServiceRolePolicy 政策。這些許可允許 Amazon ECR 擷取 Secrets Manager 秘密的加密內容。這在使用提取快取規則從需要驗證的上游登錄檔快取映像時是必要的。 | 2023 年 11 月 15 日 |
| AWSECRPullThroughCache_ServiceRolePolicy – 新政策 | Amazon ECR 已新增新政策。此政策與提取快取功能的 AWSServiceRoleForECRPullThroughCache 服務連結角色相關聯。 | 2021 年 11 月 29 日 |
| ECR ReplicationServiceRolePolicy — 新政策 | Amazon ECR 已新增新政策。此政策與複寫功能的 AWSServiceRoleForECRReplication 服務連結角色相關聯。 | 2020 年 12 月 4 日 |
| 亞馬遜 EC2 ContainerRegistryFullAccess — 更新到現有政策 | Amazon ECR 將新的許可新增到 AmazonEC2ContainerRegistryFullAccess 政策。這些許可允許委託人建立 Amazon ECR 服務連結角色。 | 2020 年 12 月 4 日 |
| 亞馬遜 EC2 ContainerRegistryReadOnly — 更新到現有政策 | Amazon ECR 將新的許可新增到 AmazonEC2ContainerRegistryReadOnly 政策，允許委託人讀取生命週期政策、列出標籤，以及描述映像的掃描問題清單。 | 2019 年 12 月 10 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 亞馬遜 EC2 ContainerRegistry PowerUser — 更新到現有政策 | Amazon ECR 將新的許可新增到 AmazonEC2ContainerRegistryPowerUser 政策。它們允許委託人讀取生命週期政策、列出標籤，以及描述映像的掃描問題清單。 | 2019 年 12 月 10 日 |
| 亞馬遜 EC2 ContainerRegistry FullAccess — 更新到現有政策 | Amazon ECR 將新的許可新增到 AmazonEC2ContainerRegistryFullAccess 政策。它們可讓主參與者查詢由 CloudTrail擷取的管理事件或 AWS CloudTrail Insights 事件。 | 2017 年 11 月 10 日 |
| 亞馬遜 EC2 ContainerRegistry ReadOnly — 更新到現有政策 | Amazon ECR 將新的許可新增到 AmazonEC2ContainerRegistryReadOnly 政策。他們允許委託人描述 Amazon ECR 映像。 | 2016 年 10 月 11 日 |
| 亞馬遜 EC2 ContainerRegistry PowerUser — 更新到現有政策 | Amazon ECR 將新的許可新增到 AmazonEC2ContainerRegistryPowerUser 政策。他們允許委託人描述 Amazon ECR 映像。 | 2016 年 10 月 11 日 |
| 亞馬遜 EC2 ContainerRegistry ReadOnly — 新政策 | Amazon ECR 已新增新政策，授予唯讀許可給 Amazon ECR。這些許可包括在儲存庫中列出儲存庫和映像的功能。它們還包括使用 Docker CLI 從 Amazon ECR 提取映像的能力。 | 2015 年 12 月 21 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 亞馬遜 EC2 ContainerRegistry PowerUser — 新政策 | Amazon ECR 已新增授予管理許可的新政策，使用者可以對儲存庫進行讀取和寫入，但不可以刪除儲存庫或變更儲存庫套用的政策文件。 | 2015 年 12 月 21 日 |
| 亞馬遜 EC2 ContainerRegistry FullAccess — 新政策 | Amazon ECR 已新增新政策。此政策授予 Amazon ECR 的完整存取權限。 | 2015 年 12 月 21 日 |
| Amazon ECR 開始追蹤變更 | Amazon ECR 開始追蹤 AWS 受管政策的變更。 | 2021 年 6 月 24 日 |

## 使用 Amazon ECR 的服務連結角色

Amazon Elastic Container Registry (Amazon ECR) 使用 AWS Identity and Access Management (IAM) 服務連結角色提供使用複寫和提取快取功能所需的許可。服務連結角色是直接連結至 Amazon ECR 的一種特殊 IAM 角色類型。服務連結的角色是由 Amazon ECR 預先定義。其中包含了該服務需要的所有許可，可支援私有登錄檔的複寫和提取快取功能。設定登錄檔的複寫或提取快取之後，系統將代表您自動建立服務連結角色。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表設置。

服務連結角色可讓使用 Amazon ECR 設定複寫和提取快取的過程更為輕鬆。這是因為使用它，您不必手動新增所有必要的許可。Amazon ECR 定義其服務連結角色的許可，除非另有定義，否則僅有 Amazon ECR 可以擔任其角色。已定義的許可包括信任政策和許可政策。許可政策無法附加到其他任何 IAM 實體。

您只能在登錄檔停用複寫或提取快取後，才能刪除對應的服務連結角色。這可確保您不會意外移除 Amazon ECR 針對這些功能所要求的許可。

關於支援服務連結角色的其他服務，如需相關資訊，請參閱與 IAM 搭配運作的AWS 服務。在此連結至頁面上，在 Service-linked role (服務連結角色) 欄位中尋找具有 Yes (是) 的服務。選擇具有連結的 Yes (是)，以檢視該服務的相關服務連結角色文件。

主題

- Amazon ECR 服務連結角色的支援區域
- 用於複寫的 Amazon ECR 服務連結角色

- 用於提取快取的 Amazon ECR 服務連結角色

## Amazon ECR 服務連結角色的支援區域

Amazon ECR 在所有提供 Amazon ECR 服務的區域中支援使用服務連結的角色。如需 Amazon ECR 區域可用性的詳細資訊，請參閱《AWS 區域與端點》。

## 用於複寫的 Amazon ECR 服務連結角色

Amazon ECR 使用名為的服務連結角色，AWSServiceRoleForECRReplication該角色可讓 Amazon ECR 跨多個帳戶複寫映像。

Amazon ECR 的服務連結角色許可

服 AWSServiceRoleForECRReplication 務連結角色會信任下列服務擔任該角色：

- `replication.ecr.amazonaws.com`

以下 `ECRReplicationServiceRolePolicy` 角色許可政策允許 Amazon ECR 對資源使用以下動作：

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

> **Note**
>
> `ReplicateImage` 是 Amazon ECR 用於複寫的內部 API，無法直接呼叫。

您必須設定許可，IAM 實體 (例如，使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

建立 Amazon ECR 的服務連結角色

您不需要手動建立 Amazon ECR 服務連結角色。當您在 AWS Management Console、或 AWS API 中設定登錄的複寫設定時 AWS CLI，Amazon ECR 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您設定登錄檔的複寫設定時，Amazon ECR 會再次為您建立服務連結角色。

編輯 Amazon ECR 的服務連結角色

Amazon ECR 不允許手動編輯 AWSServiceRoleForECRReplication 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 Amazon ECR 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。不過，您必須在每個區域中先移除您登錄檔的複寫組態，才能手動刪除服務連結角色。

> **Note**
>
> 如果您嘗試在 Amazon ECR 服務仍在使用角色時刪除資源，則刪除動作可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試。

要刪除 Amazon ECR 資源使用 AWSServiceRoleForECRReplication

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列，選擇您複寫組態所設定的區域。
3. 在導覽窗格中，選擇 Private registry (私有登錄檔)。
4. 在私有登錄檔頁面上，於複寫組態區段中，選擇編輯。
5. 若要刪除所有複寫規則，請選擇全部刪除。此步驟需要確認。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除AWSServiceRoleForECRReplication服務連結角色。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

## 用於提取快取的 Amazon ECR 服務連結角色

Amazon ECR 使用名為的服務連結角色，AWSServiceRoleForECRPullThroughCache該角色授予 Amazon ECR 代表您執行動作的權限，以完成提取快取動作。如需提取快取的詳細資訊，請參閱「將上游註冊表與 Amazon ECR 私有註冊表同步」。

Amazon ECR 的服務連結角色許可

服AWSServiceRoleForECRPullThroughCache務連結角色會信任下列服務擔任該角色。

- `pullthroughcache.ecr.amazonaws.com`

許可詳細資訊

此 AWSECRPullThroughCache_ServiceRolePolicy 許可政策連接至服務連結角色。此受管政策授予 Amazon ECR 執行下列動作的許可。如需詳細資訊，請參閱 AWSECRPullThroughCache_ServiceRolePolicy。

- `ecr`：允許 Amazon ECR 服務將映像推送到私有儲存庫。
- `secretsmanager:GetSecretValue`— 允許 Amazon ECR 服務擷取密 AWS Secrets Manager 碼的加密內容。使用提取快取規則從需要在私有登錄檔中進行身分驗證的上游登錄檔快取映像時，需要此選項。該許可僅適用於具有 `ecr-pullthroughcache/` 名稱字首的秘密。

該 AWSECRPullThroughCache_ServiceRolePolicy 政策包含下列 JSON。

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

您必須設定許可，IAM 實體 (例如，使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

建立 Amazon ECR 的服務連結角色

您不需要為提取快取手動建立 Amazon ECR 服務連結角色。當您在 AWS Management Console、或 AWS API 中為私有登錄建立提取快取規則時 AWS CLI，Amazon ECR 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您為私有登錄檔建立提取快取規則時，Amazon ECR 會再次為您建立服務連結角色 (如果尚不存在)。

編輯 Amazon ECR 的服務連結角色

Amazon ECR 不允許手動編輯AWSServiceRoleForECRPullThroughCache服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 Amazon ECR 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。不過，您必須在每個區域中先刪除登錄檔的提取快取規則，才能手動刪除服務連結角色。

> **Note**
>
> 如果您嘗試在 Amazon ECR 服務仍在使用角色時刪除資源，則刪除動作可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試。

若要刪除由 AWSServiceRoleForECRPullThroughCache 服務連結角色所使用的 Amazon ECR 資源

1. 在 https://console.aws.amazon.com/ecr/ 開啟 Amazon ECR 主控台。
2. 從導覽列選擇您建立提取快取規則的區域。
3. 在導覽窗格中，選擇 Private registry (私有登錄檔)。
4. 在私有登錄檔頁面上，於提取快取組態區段中，選擇編輯。
5. 針對您建立的每個提取快取規則，請選取規則，然後選擇刪除規則。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除AWSServiceRoleForECRPullThroughCache服務連結角色。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

# 針對 Amazon Elastic Container Registry Identity and Access 進行故障診斷

請使用以下資訊來協助您診斷和修正使用 Amazon ECR 和 IAM 時可能遇到的常見問題。

主題

- 我未獲授權，不得在 Amazon ECR 中執行動作
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪 AWS 帳戶 問我的 Amazon ECR 資源

## 我未獲授權，不得在 Amazon ECR 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 ecr:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ecr:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 ecr:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

### 我沒有授權執行 iam：PassRole

如果您收到錯誤，告知您無權執行 iam:PassRole 動作，您的政策必須更新，允許您將角色傳遞給 Amazon ECR。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor 的 IAM 使用者嘗試使用主控台在 Amazon ECR 中執行動作時，發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

### 我想允許我以外的人訪 AWS 帳戶 問我的 Amazon ECR 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon ECR 是否支援這些功能，請參閱 Amazon Elastic Container Registry 如何與 IAM 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一個 AWS 帳戶 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。

- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

# Amazon ECR 中的資料保護

AWS 共同責任模型適用於 Amazon 彈性容器服務中的資料保護。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API 或 AWS 開發套件 AWS 服務 使用 Amazon ECS 或其他工作時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

主題

- 靜態加密

## 靜態加密

Amazon ECR 將映像存放在 Amazon ECR 管理的 Amazon S3 儲存貯體中。根據預設，Amazon ECR 會使用伺服器端加密與 Amazon S3 受管加密金鑰，該加密金鑰使用 AES-256 加密演算法對靜止資料進行加密。這不需要您採取任何動作，並且免費提供。如需詳細資訊，請參閱《Amazon Simple

Storage Service 使用者指南》中的透過 Amazon S3 受管加密金鑰 (SSE-S3) 使用伺服器端加密來保護資料。

若要進一步控制 Amazon ECR 儲存庫的加密，您可以使用存放於 AWS Key Management Service (AWS KMS) 中的 KMS 金鑰的伺服器端加密。使用 AWS KMS 加密資料時，您可以使用由 Amazon ECR 管理的預設值 AWS 受管金鑰，也可以指定自己的 KMS 金鑰 (稱為客戶受管金鑰)。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用存放於 AWS KMS (SSE-KMS) 的 KMS 金鑰使用伺服器端加密來保護資料。

每個 Amazon ECR 儲存庫都有一個加密組態，這是在建立儲存庫時所設定。您可以在每個儲存庫上使用不同的加密組態。如需詳細資訊，請參閱 建立 Amazon ECR 私有儲存庫來存放映像檔。

在啟用 AWS KMS 加密的情況下建立存放庫時，會使用 KMS 金鑰來加密存放庫的內容。此外，Amazon ECR 會將 AWS KMS 授權新增至 KMS 金鑰，並將 Amazon ECR 儲存庫做為受授權者主體。

以下提供了對 Amazon ECR 如何與 AWS KMS 整合以加密和解密您的儲存庫的高等程度的了解：

1. 建立儲存庫時，Amazon ECR 會傳送DescribeKey呼叫 AWS KMS 以驗證和擷取加密組態中指定的 KMS 金鑰的 Amazon 資源名稱 (ARN)。
2. Amazon ECR 會傳送兩個CreateGrant請求，以 AWS KMS 便在 KMS 金鑰上建立授權，以允許 Amazon ECR 使用資料金鑰加密和解密資料。
3. 推送映像時，會發出金GenerateData鑰要求，指 AWS KMS 定用於加密映像層和資訊清單的 KMS 金鑰。
4. AWS KMS 產生新的資料金鑰，在指定的 KMS 金鑰下加密，然後傳送要與影像層中繼資料和影像資訊清單一起儲存的加密資料金鑰。
5. 提取圖像時，會對「解密」請求進行 AWS KMS，指定加密的數據密鑰。
6. AWS KMS 解密加密的資料金鑰，並將解密的資料金鑰傳送到 Amazon S3。
7. 使用資料金鑰在提取映像層之前解密映像層。
8. 刪除儲存庫時，Amazon ECR 會傳送兩個RetireGrant請求，以淘汰 AWS KMS 為儲存庫建立的授權。

## 考量事項

使用 Amazon ECR AWS KMS 加密時，應考慮以下幾點。

- 如果您使用 KMS 加密建立 Amazon ECR 儲存庫，但未指定 KMS 金鑰，則 Amazon ECR 預設會使用 AWS 受管金鑰 與別名一起使`aws/ecr`用。當您第一次建立啟用 KMS 加密的儲存庫時，就會在您的帳戶中建立此 KMS 金鑰。
- 當您使用 KMS 加密搭配您自己的 KMS 金鑰時，金鑰必須與您的儲存庫位於相同的區域。
- 不應撤銷 Amazon ECR 代表您建立的授予。如果您撤銷授予 Amazon ECR 權限使用帳戶中 AWS KMS 金鑰的授權，Amazon ECR 無法存取此資料、加密推送到儲存庫的新映像，或在提取影像時將其解密。當您撤銷 Amazon ECR 的授予時，則會立即進行變更。若要撤銷存取權，請刪除儲存庫，而不是撤銷授權。刪除儲存庫後，Amazon ECR 會代表您淘汰授予。
- 使用 AWS KMS 金鑰會產生相關的費用。如需詳細資訊，請參閱 AWS Key Management Service 定價。

## 所需的 IAM 許可

使用 AWS KMS伺服器端加密建立或刪除 Amazon ECR 儲存庫時，所需的許可取決於您使用的特定 KMS 金鑰。

使用 Amazon ECR 時所需 AWS 受管金鑰 的 IAM 許可

依預設，如果 Amazon ECR 儲存庫已啟用 AWS KMS 加密，但未指定 KMS 金鑰，則會使用 AWS 受管金鑰 適用於 Amazon ECR 的。使用 Amazon ECR 的 AWS受管 KMS 金鑰加密儲存庫時，任何具有建立存放庫權限的主體也可以在存放庫上啟用 AWS KMS 加密。但是，刪除儲存庫的 IAM 委託人必須具有 `kms:RetireGrant` 許可。如此可在建立儲存庫時淘汰新增至 AWS KMS 索引鍵的授權。

下列範例 IAM 政策可以作為內嵌政策新增至使用者，以確保使用者具有刪除啟用加密的儲存庫所需的最低許可。使用資源參數可指定用於加密儲存庫的 KMS 金鑰。

```
{
    "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"
        }
```

```
    ]
}
```

使用客戶受管金鑰時所需的 IAM 許可

使用客戶受管金鑰建立啟用 AWS KMS 加密的存放庫時，KMS 金鑰政策和 IAM 政策同時具有建立存放庫之使用者或角色的必要許可。

建立您自己的 KMS 金鑰時，您可以使用預設金鑰政策 AWS KMS 建立，或者您可以自行指定。為了確保客戶受管金鑰可由帳戶擁有者管理，KMS 金鑰的金鑰原則應允許帳戶 root 使用者的所有 AWS KMS 動作。其他範圍的權限可能會新增至金鑰政策，但至少應該授予根使用者管理 KMS 金鑰的許可。若要允許 KMS 金鑰僅用於源自 Amazon ECR 的請求，您可以使用帶有值的 kms: ViaService 條件金鑰。`ecr.<region>.amazonaws.com`

下列範例金鑰原則提供擁有 KMS 金鑰完整存取權限的 AWS 帳戶 (root 使用者)。如需此金鑰政策範例的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的允許存取 AWS 帳戶並啟用 IAM 政策。

```
{
    "Version": "2012-10-17",
    "Id": "ecr-key-policy",
    "Statement": [
        {
            "Sid": "EnableIAMUserPermissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

除了必要的 Amazon ECR 許可之外，IAM 使用者`kms:CreateGrant`、`kms:RetireGrant`IAM 角色或建立儲存庫的 AWS 帳戶還必須具有、和`kms:DescribeKey`許可。

> **Note**
>
> 必須將 `kms:RetireGrant` 許可新增到建立儲存庫的使用者或角色的 IAM 政策中。可以將 `kms:CreateGrant` 和 `kms:DescribeKey` 許可新增到 KMS 金鑰的金鑰政策或建立儲存庫

的使用者或角色的 IAM 政策。如需有關 AWS KMS 權限運作方式的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的 AWS KMS API 權限：動作和資源參考。

下列範例 IAM 政策可以作為內嵌政策新增至使用者，以確保使用者具有建立啟用加密的儲存庫所需的最低許可，並在使用完儲存庫後刪除該儲存庫。使用資源參數可指定用於加密儲存庫的 AWS KMS key 。

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

允許使用者在建立儲存庫時在主控台中列出 KMS 金鑰

使用 Amazon ECR 主控台建立儲存庫時，您可以授予許可以允許使用者在為儲存庫啟用加密時列出區域中的客戶受管 KMS 金鑰。下列 IAM 政策範例顯示使用主控台時列出 KMS 金鑰和別名所需的許可。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases",
      "kms:DescribeKey"
    ],
```

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

## 使用 AWS KMS監控 Amazon ECR

您可以使用 AWS CloudTrail 來追蹤 Amazon ECR 代表您傳送 AWS KMS 的請求。記錄檔中的記 CloudTrail 錄項目包含加密內容金鑰，可讓它們更容易識別。

Amazon ECR 加密內容

加密內容是一組鍵/值組，其中包含任意非私密資料。當您在加密資料的要求中包含加密內容時， AWS KMS 密碼編譯會將加密內容繫結至加密的資料。若要解密資料，您必須傳遞相同的加密內容。

在其GenerateData金鑰和解密請求中 AWS KMS，Amazon ECR 使用具有兩個名稱 — 值對的加密內容，用於識別正在使用的儲存庫和 Amazon S3 儲存貯體。如以下範例所示。名稱不會改變，但組合的加密內容值對於每個值都是不同的。

```
"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"
}
```

您可以使用加密內容在稽核記錄和日誌 (例如和 Amazon CloudWatch Logs) 中識別這些加密操作，並做為政策和授權中授權的條件。AWS CloudTrail

Amazon ECR 加密內容包含兩個名稱值組。

- aws:s3:arn – 第一個名稱-值配對會識別儲存貯體。金鑰為 `aws:s3:arn`。值為 Amazon S3 儲存貯體 Amazon Resource Name (ARN)。

  ```
  "aws:s3:arn": "ARN of an Amazon S3 bucket"
  ```

  例如，如果儲存貯體的 ARN 是 `arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df`，加密內容會包含下列對組。

```
"arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-
ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df"
```

- aws:ecr:arn – 第二個名稱-值對會識別儲存庫的 Amazon Resource Name (ARN)。金鑰為 `aws:ecr:arn`。值為儲存庫的 ARN。

  ```
  "aws:ecr:arn": "ARN of an Amazon ECR repository"
  ```

  例如，如果儲存庫的 ARN 是 `arn:aws:ecr:us-west-2:111122223333:repository/repository-name`，加密內容會包含下列對組。

  ```
  "aws:ecr:arn": "arn:aws:ecr:us-west-2:111122223333:repository/repository-name"
  ```

## 故障診斷

使用主控台刪除 Amazon ECR 儲存庫時，如果儲存庫已成功刪除，但 Amazon ECR 無法淘汰新增至您儲存庫的 KMS 金鑰的授予，則會收到以下錯誤訊息。

```
The repository [{repository-name}] has been deleted successfully but the grants created
 by the kmsKey [{kms_key}] failed to be retired
```

發生這種情況時，您可以自行淘汰存放庫的 AWS KMS 授權。

手動淘汰儲存區域的 AWS KMS 授權

1. 列出用於儲存庫之 AWS KMS 金鑰的授權。此 `key-id` 值會包含在您從主控台收到的錯誤中。您也可以使用`list-keys`命令列出帳戶中特定區域中的 AWS 受管金鑰 和客戶受管 KMS 金鑰。

   ```
   aws kms list-grants \
        --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc
        --region us-west-2
   ```

   輸出包含 `EncryptionContextSubset`，其中包含儲存庫的 Amazon Resource Name (ARN)。這可用於確定新增到金鑰的哪個授予是您要淘汰的授予。`GrantId` 值會在下一個步驟中淘汰授予時使用。
2. 淘汰為儲存庫新增之 AWS KMS 金鑰的每個授權。將的值取代為*GrantId*上一個步驟輸出之授權的 ID。

```
aws kms retire-grant \
     --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc \
     --grant-id GrantId \
     --region us-west-2
```

# Amazon Elastic Container Registry 的合規驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。

- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求，例如 PCI DSS，滿足特定合規性架構所規定的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

# Amazon Elastic Container Registry 的基礎設施安全性

作為受管服務，Amazon 彈性容器登錄受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透過網路存取 Amazon ECR。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生臨時安全憑證來簽署請求。

您可從任何網路位置呼叫這些 API 操作，而 Amazon ECR 確實可支援基於資源的存取政策，以納入依據來源 IP 地址的限制。您也可以使用 Amazon ECR 政策，以便從特定 Amazon Virtual Private Cloud (Amazon VPC) 端點或特定 VPC 中控制存取權。實際上，這可以將對指定 Amazon ECR 資源的網路存取從網路內的特定 VPC 隔離出來。 AWS 如需詳細資訊，請參閱 Amazon ECR 接口 VPC 端端點 ()AWS PrivateLink。

## Amazon ECR 接口 VPC 端端點 ()AWS PrivateLink

您可以將 Amazon ECR 設定為使用介面 VPC 端點，進而提升 VPC 的安全狀態。VPC 私人雲端端點採用這項技術 AWS PrivateLink，可讓您透過私有 IP 地址私有存取 Amazon ECR API。 AWS PrivateLink 將 VPC 和 Amazon ECR 之間的所有網路流量限制在 Amazon 網路上。您不需要網際網路閘道、NAT 裝置或虛擬私有閘道。

如需 AWS PrivateLink 和 VPC 端點的詳細資訊，請參閱 Amazon VPC 使用者指南中的 VPC 端點。

## Amazon ECR VPC 端點的考量事項

在您設定 Amazon ECR 的 VPC 端點之前，請注意以下幾點考量。

- 若要允許託管在 Amazon EC2 執行個體上的 Amazon ECS 任務從 Amazon ECR 選取私有映像，請確保您還為 Amazon ECS 建立介面 VPC 端點。如需詳細資訊，請參閱 Amazon 彈性容器服務開發人員指南中的介面 VPC 端點 (AWS PrivateLink)。

  > **Important**
  >
  > Fargate 上託管的 Amazon ECS 任務不需要 Amazon ECS 介面 VPC 端點。

- 使用 Linux 平台版本 `1.3.0` 或更早版本的 Fargate 上託管的 Amazon ECS 任務只需要 com.amazonaws.***region***.ecr.dkr Amazon ECR VPC 端點和 Amazon S3 閘道端點即可利用此功能。
- 使用 Linux 平台版本 `1.4.0` 或更高版本託管在 Fargate 上的 Amazon ECS 任務需要 com.amazonaws.***region***.ecr.dkr 和 com.amazonaws.***region***.ecr.api Amazon ECR VPC 端點，以及 Simple Storage Service (Amazon S3) 閘道端點才能利用此功能。
- 使用 Windows 平台版本 `1.0.0` 或更高版本託管在 Fargate 上的 Amazon ECS 任務需要 com.amazonaws.***region***.ecr.dkr 和 com.amazonaws.***region***.ecr.api Amazon ECR VPC 端點，以及 Simple Storage Service (Amazon S3) 閘道端點才能利用此功能。
- Fargate 上託管的從 Amazon ECR 提取容器映像的 Amazon ECS 任務可以透過向任務的任務執行 IAM 角色新增條件索引鍵來限制對其任務使用的特定 VPC 和服務使用的 VPC 端點的存取。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的透過介面端點提取 Amazon ECR 映像的 Fargate 任務的可選 IAM 許可。
- 在 Fargate 上託管的 Amazon ECS 任務可從 Amazon ECR 提取容器映像，而這些容器映像也會使用日誌驅動程式將日`awslogs`誌資訊傳送到日誌，則需要 CloudWatch 日誌 VPC 端點。CloudWatch 如需詳細資訊，請參閱 建立記 CloudWatch 錄檔端點。
- 連接到 VPC 端點的安全群組，必須允許從 VPC 的私有子網路，透過 443 埠傳入的連線。
- VPC 端點目前不支援跨區域請求。請確實在打算向 Amazon ECR 發出 API 呼叫的相同區域中建立 VPC 端點。
- VPC 端點目前不支援 Amazon ECR Public 儲存庫。請考慮使用提取快取規則，將公有映像託管在與 VPC 端點位於相同區域的私有儲存庫中。如需詳細資訊，請參閱 將上游註冊表與 Amazon ECR 私有註冊表同步。
- VPC 端點僅支援透過 Amazon 路線 53 AWS 提供的 DNS。如果您想要使用自己的 DNS，您可以使用條件式 DNS 轉送。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 DHCP 選項集。

- 如果您的容器有現有的 Amazon S3 連線，則在您新增 Amazon S3 閘道端點時，其連線可能會短暫中斷。如果您想避免發生中斷情況，請建立採用 Amazon S3 閘道端點的新 VPC，然後將 Amazon ECS 叢集及其容器遷移至新的 VPC。
- 第一次使用提取快取規則提取映像時，如果您已使用 AWS PrivateLink 將 Amazon ECR 設定為使用介面 VPC 端點，那麼您需要在同一個 VPC 中使用 NAT 閘道建立公有子網路，然後將所有傳出流量從其私有子網路路由到 NAT 閘道，以便提取至工作。隨後的映像提取不需要這樣做。如需詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的案例：從私有子網路存取網際網路。

### Windows 映像的考量

基於 Windows 作業系統的映像包括受授權限制無法分配的成品。預設情況下，當您將 Windows 映像推送到 Amazon ECR 儲存庫時，不推送包含這些成品的層，因為它們被視為外來層。當成品由 Microsoft 提供時，外部層將從 Microsoft Azure 基礎設施中擷取。因此，為了讓您的容器能夠從 Azure 中提取這些外部層，除了建立 VPC 端點之外，還需要其他步驟。

當使用 Docker 常駐程式中的 `--allow-nondistributable-artifacts` 標誌將 Windows 映像推送到 Amazon ECR 時，可以覆寫此行為。啟用後，此標誌將把授權層推送到 Amazon ECR，這樣就可以透過 VPC 端點從 Amazon ECR 中提取這些映像，而無需額外存取 Azure。

> **Important**
>
> 使用 `--allow-nondistributable-artifacts` 標誌並不排除您遵守 Windows 容器基礎映像授權條款的義務；您不能發佈 Windows 內容以進行公有或第三方重新分佈。允許在您自己的環境中使用。

若要在 Docker 安裝中啟用此標誌，您必須修改 Docker 常駐程式組態檔案，其根據 Docker 的安裝情況，通常可以在 Docker Engine (Docker 引擎) 區段下的設定或偏好設定選單中設定，也可以直接編輯 `C:\ProgramData\docker\config\daemon.json` 檔案。

以下為所需組態的範例。將該值替換為要將映像推送到的儲存庫 URI。

```
{
    "allow-nondistributable-artifacts": [
        "111122223333.dkr.ecr.us-west-2.amazonaws.com"
    ]
}
```

修改 Docker 常駐程式組態檔案後，在嘗試推送映像之前，必須重新啟動 Docker 常駐程式。透過驗證基本層是否已推送到儲存庫來確認推送是否有效。

> **Note**
>
> Windows 映像的基本圖很大。層大小將導致較長的推送時間以及 Amazon ECR 中這些映像的額外存放成本。基於這些原因，我們建議僅在嚴格要求減少建置時間和持續儲存成本時使用此選項。例如，`mcr.microsoft.com/windows/servercore` 映像在 Amazon ECR 中壓縮時大約為 1.7 GiB。

## 為 Amazon ECR 建立 VPC 端點

若要為 Amazon ECR 服務建立 VPC 端點，請使用《Amazon VPC 使用者指南》中的 Creating an Interface Endpoint (建立介面端點) 程序。

在 Amazon EC2 執行個體上託管的 Amazon ECS 任務需要 Amazon ECR 端點和 Amazon S3 閘道端點。

使用平台版本 `1.4.0` 或更高版本在 Fargate 上託管的 Amazon ECS 任務需要 Amazon ECR VPC 終端節點和 Amazon S3 閘道端點。

使用平台版本 `1.3.0` 或更早版本的 Fargate 上託管的 Amazon ECS 任務只需要 com.amazonaws.***region***.ecr.dkr Amazon ECR VPC 端點和 Amazon S3 閘道端點。

> **Note**
>
> 建立端點的順序並不重要。

com.amazonaws.***region***.ecr.dkr

此端點用於 Docker 登錄檔 API。Docker 用戶端命令 (例如 `push` 和 `pull`) 會使用此端點。

當您建立此端點時，需確實啟用私有 DNS 主機名稱。若要執行此操作，請務必在建立 VPC 端點時，選取 Amazon VPC 主控台中的 Enable Private DNS Name (啟用私有 DNS 名稱) 選項。

com.amazonaws.*region*.ecr.api

> **Note**
>
> 指定的*##*代表 Amazon ECR 支援之 AWS 區域的區域識別碼，例如美國東部 (俄亥俄) 區域`us-east-2`。

此端點用於呼叫 Amazon ECR API。`DescribeImages` 和 `CreateRepository` 等 API 動作會移至此端點。

建立此端點時，您可以選擇啟用私有 DNS 主機名稱。當您建立 VPC 端點時，在 VPC 主控台中選取 Enable Private DNS Name (啟用私有 DNS 名稱) 來啟用此設計。如果您為 VPC 端點啟用私人 DNS 主機名稱，請更新您的 SDK 或 AWS CLI 最新版本，以便在使用 SDK 時或 AWS CLI 不需要指定端點 URL。

如果您啟用私人 DNS 主機名稱，且使用的 SDK 或 2019 年 1 月 24 日之前發行的 AWS CLI 版本，則必須使用`--endpoint-url`參數來指定介面端點。以下範例會顯示端點 URL 的格式。

```
aws ecr create-repository --repository-name name --endpoint-url https://
api.ecr.region.amazonaws.com
```

如果您不啟用 VPC 端點的私有 DNS 主機名稱，就必須透過 `--endpoint-url` 參數來指定介面端點的 VPC 端點 ID。 以下範例會顯示端點 URL 的格式。

```
aws ecr create-repository --repository-name name --endpoint-url
 https://VPC_endpoint_ID.api.ecr.region.vpce.amazonaws.com
```

## 建立 Amazon S3 閘道端點

若要讓您的 Amazon ECS 任務從 Amazon ECR 提取私有映像，您必須為所有 Amazon S3 建立閘道端點。閘道端點是必要的，因為 Amazon ECR 使用 Amazon S3 來存放映像分層。容器從 Amazon ECR 下載映像時，必須存取 Amazon ECR 以取得映像資訊清單，並透過 Amazon S3 下載實際映像層。以下是 Amazon S3 儲存貯體的 Amazon Resource Name (ARN)，該儲存貯體包含每個 Docker 映像的分層。

```
arn:aws:s3:::prod-region-starport-layer-bucket/*
```

使用《Amazon VPC 使用者指南》中的 Creating a gateway endpoint (建立閘道端點) 操作程序為 Amazon ECR 建立以下 Amazon S3 閘道端點。建立端點時，請務必為您的 VPC 選取路由表。

com.amazonaws.*region*.s3

Amazon S3 閘道端點會使用 IAM 政策文件來限制服務的存取權限。您可以使用 Full Access (完整存取) 政策，因為系統會以此政策為基礎，繼續套用您對任務 IAM 角色或其他 IAM 使用者政策的限制。如果您想將 Amazon S3 儲存貯體存取權限限制為使用 Amazon ECR 所需的最低許可，請參閱 Amazon ECR 的最低 Amazon S3 儲存貯體許可。

### Amazon ECR 的最低 Amazon S3 儲存貯體許可

Amazon S3 閘道端點會使用 IAM 政策文件來限制服務的存取權限。若要僅允許 Amazon ECR 的最低 Amazon S3 儲存貯體許可，請限制對 Amazon ECR 在為端點建立 IAM 政策文件時使用的 Amazon S3 儲存貯體的存取。

下表會說明 Amazon ECR 所需的 Amazon S3 儲存貯體政策許可。

| 權限 | 描述 |
| --- | --- |
| `arn:aws:s3:::prod-region-starport-layer-bucket/*` | 提供對包含每個 Docker 映像分層之 Amazon S3 儲存貯體的存取權限。表示 Amazon ECR 支援的 AWS 區域的區域識別符，例如美國東部 (俄亥俄) 區域的 `us-east-2` 。 |

### 範例

下方範例會說明如何提供 Amazon ECR 操作所需的 Amazon S3 儲存貯體存取權限。

```
{
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::prod-region-starport-layer-bucket/*"]
```

```
    }
  ]
}
```

## 建立記 CloudWatch 錄檔端點

使用 Fargate 啟動類型的 Amazon ECS 任務，該啟動類型使用沒有網際網路閘道的 VPC，也會使用日誌驅動程式將日**awslogs**誌資訊傳送到 CloudWatch 日誌，需要您建立 com.amazonaws。 *##* .logs 介面記錄檔的 CloudWatch VPC 人雲端端點。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用指南中的將日 CloudWatch 誌與界面 VPC 端點搭配使用。

## 為您的 Amazon ECR VPC 端點建立端點政策

當您建立或修改端點時，VPC 端點政策是您連接至端點的 IAM 資源政策。如果您在建立端點時未附加原則，請為您 AWS 附加允許完整存取服務的預設原則。端點政策不會覆寫或取代使用者政策或服務特定的政策。這個另行區分的政策會控制從端點到所指定之服務的存取。端點政策必須以 JSON 格式撰寫。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用 VPC 端點控制服務的存取。

我們建議建立單一 IAM 資源政策，並將其連接到兩個 Amazon ECR VPC 端點。

以下是 Amazon ECR 端點政策的範例。此政策可讓特定 IAM 角色從 Amazon ECR 提取映像。

```
{
 "Statement": [{
  "Sid": "AllowPull",
  "Principal": {
   "AWS": "arn:aws:iam::1234567890:role/role_name"
  },
  "Action": [
   "ecr:BatchGetImage",
   "ecr:GetDownloadUrlForLayer",
                  "ecr:GetAuthorizationToken"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

下列端點政策範例可防止指定的儲存庫遭到刪除。

```
{
```

```
 "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"
  }
 ]
}
```

下列端點政策範例會將前兩個範例結合成單一政策。

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

修改 Amazon ECR 的 VPC 端點政策

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 Endpoints (端點)。
3. 如果您尚未建立 Amazon ECR 的 VPC 端點，請參閱 為 Amazon ECR 建立 VPC 端點。
4. 選取要新增政策的 Amazon ECR VPC 端點，然後選擇畫面下半部的 Policy (政策) 索引標籤。
5. 選擇 Edit Policy (編輯政策)，並對政策做出變更。
6. 選擇 Save (儲存) 以儲存政策。

### 共用子網路

無法在與您共用的子網路中建立、描述、修改或刪除 VPC 端點。不過，可以在與您共用的子網路中使用 VPC 端點。

## 預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源政策中使用 `aws:SourceArn` 或 `aws:SourceAccount` 全域條件內容索引鍵，來限制 Amazon ECR 給予另一項服務對資源的許可。如果您想要僅允許一個資源與跨服務存取相關聯，則請使用 `aws:SourceArn`。如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 `aws:SourceAccount`。

防範混淆代理人問題的最有效方法是使用 `aws:SourceArn` 全域條件內容索引鍵，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 `aws:SourceArn` 全域內容條件索引鍵搭配萬用字元 (*) 來表示 ARN 的未知部分。例如 `arn:aws:servicename:region:123456789012:*`。

如果 aws:SourceArn 值不包含帳戶 ID (例如 Amazon S3 儲存貯體 ARN)，您必須使用這兩個全域條件內容索引鍵來限制許可。

aws:SourceArn 的值必須為 ResourceDescription。

下列範例顯示如何在 Amazon ECR 儲存庫政策中使用aws:SourceArn和aws:SourceAccount全域條件上下文金鑰，以允許存 AWS CodeBuild 取與該服務整合所需的 Amazon ECR API 動作，同時也可避免混淆的副問題。

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

# Amazon ECR 監控

您可以使用 Amazon 監控 Amazon ECR API 的使用情況 CloudWatch，這些 Amazon 會收集來自 Amazon ECR 的原始資料並將其處理為可讀且近即時的指標。這些統計資料會記錄兩週，因此您可以存取歷史資訊並深入了解 API 使用情況。Amazon ECR 指標資料會 CloudWatch 在一分鐘內自動傳送到。如需有關的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南。

Amazon ECR 會根據您的 API 用量，針對授權、映像推送和映像提取動作提供指標。

監控是維持 Amazon ECR 和 AWS 解決方案的可靠性、可用性和效能的重要組成部分。我們建議您從構成 AWS 解決方案的資源收集監控資料，以便在發生多點失敗時，可以更輕鬆地對多點失敗進行偵錯。不過，開始監控 Amazon ECR 之前，您應該建立監控計劃，其中回答下列問題：

- 監控目標是什麼？
- 要監控哪些資源？
- 監控這些資源的頻率為何？
- 要使用哪些監控工具？
- 誰將執行監控任務？
- 發生問題時應該通知誰？

下一步是在各個時間點和不同的負載條件下測量效能，以在您的環境中確立 Amazon ECR 正常效能的基準。當您監控 Amazon ECR 時，請存放歷史記錄監控資料，如此才能與新的效能資料做比較、辨識正常效能模式和效能異常狀況、規劃問題處理方式。

主題

- 視覺化您的服務配額和設定警報
- Amazon ECR 用量指標
- Amazon ECR 用量報告
- Amazon ECR 儲存庫指標
- Amazon ECR 活動和 EventBridge
- 使用記錄 Amazon ECR 動作 AWS CloudTrail

# 視覺化您的服務配額和設定警報

您可以使用 CloudWatch 主控台以視覺化方式呈現服務配額，並查看目前使用量與服務配額的比較。您也可以設定警示，以便在接近配額時收到通知。

視覺化服務配額並選擇是否設定警示

1. 開啟主 CloudWatch 控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格中，選擇 指標。
3. 在 All metrics (所有指標) 索引標籤上，選擇 Usage (用量)，然後選擇 By AWS Resource (依 AWS 資源)。

   服務配額用量指標清單隨即出現。
4. 選取其中一個指標旁的核取方塊。

   此圖表會顯示您目前該 AWS 資源的使用量。
5. 若要將服務配額新增至圖表，請執行下列動作：

   a. 選擇 Graphed metrics (圖表化指標) 標籤。

   b. 選擇 Math expression (數學表達式)、Start with an empty expression (以空表達式開始)。然後在新資料列的 Details (詳細資訊) 下，輸入 **`SERVICE_QUOTA(m1)`**。

      圖表中會新增一行，顯示指標所示資源的服務配額。
6. 若要查看目前用量的配額百分比，請新增表達式或變更目前的 SERVICE_QUOTA 表達式。新的表達式請使用 **`m1/60/SERVICE_QUOTA(m1)*100`**。
7. (選用) 若要設定接近服務配額的警示通知，請執行下列動作：

   a. 在 **`m1/60/SERVICE_QUOTA(m1)*100`** 資料列的 Actions (動作) 下，選擇警示圖示。它看起來像一個鈴鐺。

      警示建立頁面隨即出現。

   b. 確定在 Conditions (條件) 下，Threshold type (閾值類型) 為 Static (靜態)，而 Whenever Expression1 is (每當 Expression1) 設為 Greater (大於)。在 than (比較值) 下輸入 **`80`**。當您的用量超過配額的 80% 時，即會建立進入 ALARM 狀態的警示。

   c. 選擇下一步。

   d. 在下一頁中，選取 Amazon SNS 主題或建立新主題。當警示進入 ALARM 狀態時，即會通知此主題。然後選擇下一步。

e. 在下一頁中，輸入警示的名稱和說明，然後選擇 Next (下一步)。

f. 選擇 Create alarm (建立警示)。

# Amazon ECR 用量指標

您可以使用 CloudWatch 使用量度來提供您帳戶資源使用情況的可見度。使用這些指標，在 CloudWatch 圖形和儀表板上視覺化您目前的服務使用情況。

Amazon ECR 使用量指標對應於 AWS 服務配額。您可以設定警示，在您的用量接近服務配額時發出警示。如需 Amazon ECR 服務配額的詳細資訊，請參閱 Amazon ECR 服務配額。

Amazon ECR 在 `AWS/Usage` 命名空間中發佈下列指標。

| 指標 | 描述 |
| --- | --- |
| `CallCount` | 從您帳戶呼叫 API 動作的次數。資源由與指標相關聯的維度定義。<br><br>此指標最有用的統計資料為 `SUM`，代表所定義期間來自所有作者群之值的總和。 |

以下維度用於強化 Amazon ECR 發佈的用量指標。

| 維度 | 描述 |
| --- | --- |
| `Service` | 包含資源的 AWS 服務名稱。對於 Amazon ECR 用量指標，此維度的值為 `ECR`。 |
| `Type` | 正在報告的實體類型。目前，Amazon ECR 用量指標的唯一有效值為 `API`。 |
| `Resource` | 正在執行的資源類型。目前，Amazon ECR 會針對下列 API 動作傳回 API 用量的相關資訊。<br><br>• GetAuthorizationToken<br>• BatchCheckLayerAvailability<br>• InitiateLayerUpload |

| 維度 | 描述 |
| --- | --- |
| | • UploadLayerPart<br>• CompleteLayerUpload<br>• PutImage<br>• BatchGetImage<br>• GetDownloadUrlForLayer |
| `Class` | 正在追蹤的資源類別。目前，Amazon ECR 不會使用類別維度。 |

# Amazon ECR 用量報告

AWS 提供名為「Cost Explorer」的免費報告工具，可讓您分析 Amazon ECR 資源的成本和用量。

使用 Cost Explorer 來檢視用量和成本的圖表。您可以檢視前 13 個月的資料，以及預測未來三個月的可能花費。您可以使用 Cost Explorer 查看一段時間內在 AWS 資源上花費多少、找出需進一步調查的領域，以及查看您可用來了解成本的趨勢。您也可以指定資料的時間範圍，以及根據天或月檢視時間資料。

成本與用量報告中的計量資料會顯示所有 Amazon ECR 儲存庫的用量。如需詳細資訊，請參閱 標記您的資源以便計費。

有關「如何創建 AWS 成本和使用報表」的更多內容，敬請參閱《用AWS Billing 戶指南》中的「AWS 成本和使用報表」。

# Amazon ECR 儲存庫指標

Amazon ECR 將存儲庫提取計數指標發送到 Amazon CloudWatch。Amazon ECR 指標資料會 CloudWatch 在 1 分鐘內自動傳送到。如需有關的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南。

主題

- 啟用 CloudWatch 指標
- 可用的指標與維度
- 使用主控台檢視 Amazon ECR 指標 CloudWatch

# 啟用 CloudWatch 指標

Amazon ECR 為所有儲存庫自動傳送儲存庫指標。無需採取任何手動步驟。

# 可用的指標與維度

以下各節列出 Amazon ECR 傳送給 Amazon 的指標和維度。 CloudWatch

## Amazon ECR 指標

Amazon ECR 為您提供指標以監控儲存庫。您可以測量提取計數。

AWS/ECR 命名空間包含下列指標。

`RepositoryPullCount`

儲存庫中映像的提取總數。

有效維度：`RepositoryName`。

有效統計資訊：Average、Minimum、Maximum、Sum、Sample Count。最實用的統計是 Sum。

單位：整數。

## Amazon ECR 指標的維度

Amazon ECR 指標使用 AWS/ECR 命名空間，並提供下列維度的指標。

`RepositoryName`

此維度可篩選您為指定儲存庫中的所有容器映像請求的資料。

# 使用主控台檢視 Amazon ECR 指標 CloudWatch

您可以在 CloudWatch 主控台上檢視 Amazon ECR 儲存庫指標。主 CloudWatch 控台提供精細且可自訂的資源顯示。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

若要在 CloudWatch 主控台中檢視指標

1. 開啟主 CloudWatch 控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 在左側導覽中，選擇 Metrics (指標)、All metrics (所有指標)。

3. 在 Browse (瀏覽) 索引標籤中，在 AWS Namespaces ( 命名空間) 下，選擇 ECR。
4. 選擇要檢視的指標。儲存庫指標限定為 ECR > Repository Metrics (ECR > 儲存庫指標)。

# Amazon ECR 活動和 EventBridge

Amazon 可 EventBridge 讓您將 AWS 服務自動化，並自動回應系統事件，例如應用程式可用性問題或資源變更。來自 AWS 服務的事件會以近乎即時 EventBridge 的方式傳送到。您可撰寫簡單的規則，來指示您在意的事件，以及包含當事件符合規則時所要自動執行的動作。可以自動觸發的動作如下：

- 將事件新增至 CloudWatch 記錄檔中的記錄群組
- 調用函數 AWS Lambda
- 調用 Amazon EC2 執行命令
- 將事件轉傳至 Amazon Kinesis Data Streams
- 啟動 AWS Step Functions 狀態機
- 通知 Amazon SNS 主題或 Amazon SQS 佇列

如需詳細資訊，請參閱 Amazon EventBridge 使用者指南 EventBridge中的 Amazon 入門。

## 來自 Amazon ECR 的範例事件

以下是 Amazon ECR 的範例事件。盡可能發出事件。

已完成映像推送的事件

每次完成映像推送時，會傳送下列事件。如需詳細資訊，請參閱 將碼頭映像推送到 Amazon ECR 私有存儲庫。

```
{
    "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"
    }
}
```

提取快取動作的事件

嘗試提取快取動作時，會傳送下列事件。如需詳細資訊，請參閱 將上游註冊表與 Amazon ECR 私有註冊表同步。

```
{
    "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",
    }
}
```

已完成映像掃描的事件 (基本型掃描)

啟用登錄檔的基本型掃描時，當每個映像掃描完成時，就會傳送下列事件。finding-severity-counts 參數只會在出現嚴重性等級時才傳回嚴重性等級的值。例如，如果映像在 CRITICAL 等級沒有問題清單，則不會傳回任何重要等級數值。如需詳細資訊，請參閱 掃描影像以查看 Amazon ECR 中的作業系統漏洞。

> **Note**
>
> 如需有關 Amazon Inspector 在啟用增強型掃描時發出之事件的詳細資訊，請參閱 EventBridge 在 Amazon ECR 中為增強掃描而傳送的事件。

```
{
    "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": []
    }
}
```

啟用增強型掃描之資源上的變更通知事件 (增強掃描)

為登錄檔啟用增強型掃描時，Amazon ECR 會在啟用了增強型掃描的資源發生變更時傳送下列事件。這包括正在建立的新儲存庫、正在變更的儲存庫掃描頻率，或是在啟用了增強型掃描的儲存庫中建立或刪除映像時。如需詳細資訊，請參閱 掃描影像以查看 Amazon ECR 中的軟體漏洞。

```
{
 "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"
 }
}
```

### 映像刪除的事件

刪除映像時傳送以下事件。如需詳細資訊，請參閱 [刪除 Amazon ECR 中的圖像](#)。

```
{
    "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"
    }
}
```

# 使用記錄 Amazon ECR 動作 AWS CloudTrail

Amazon ECR 與這項服務整合在一起 AWS CloudTrail，可提供 Amazon ECR 中使用者、角色或服務所採取的動作記錄的 AWS 服務。 CloudTrail 將下列 Amazon ECR 動作擷取為事件：

- 所有 API 呼叫，包括來自 Amazon ECR 主控台的呼叫
- 由於儲存庫上的加密設定而採取的所有動作
- 根據生命週期政策規則採取的所有動作，包括成功和失敗的動作

> **Important**
>
> 由於個別 CloudTrail 事件的大小限制，對於 10 個或更多映像到期的生命週期政策動作，Amazon ECR 會將多個事件傳送至 CloudTrail。此外，Amazon ECR 每個映像最多包含 100 個標籤。

建立追蹤後，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Amazon ECR 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用此資訊，您就可以判斷傳送至 Amazon ECR 的請求、提出請求的 IP 地址、提出請求的對象、提出請求的時間，以及其他詳細資訊。

如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/。

## Amazon ECR 信息 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。當 Amazon ECR 中發生活動時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以在帳戶中查看，搜索和下載最近的事 AWS 件。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

如需 AWS 帳戶中持續的事件記錄 (包括 Amazon ECR 的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。當您在主控台建立追蹤記錄時，可以將追蹤記錄套用至單一區域或所有區域。追蹤記錄 AWS 分區中的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務來分析 CloudTrail 記錄檔中收集的事件資料，並採取行動。如需詳細資訊，請參閱：

- 為您的 AWS 帳戶建立追蹤
- AWS 與 CloudTrail 日誌的服務整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件和從多個帳戶接收 CloudTrail 日誌文件

所有 Amazon ECR API 動作都會記錄下來， CloudTrail 並記錄在 Amazon 彈性容器登錄檔 API 參考中。當您執行一般工作時，會在 CloudTrail 記錄檔中為該工作的每個 API 動作產生區段。例如，當您建立存放庫時 `GetAuthorizationTokenCreateRepository`，會在 CloudTrail 記錄檔中產生和`SetRepositoryPolicy`區段。將映像推送至儲存庫時，會產生 `InitiateLayerUpload`、`UploadLayerPart`、`CompleteLayerUpload` 和 `PutImage` 區段。提取映像時，會產生 `GetDownloadUrlForLayer` 和 `BatchGetImage` 區段。如需這些常見任務的範例，請參閱CloudTrail 記錄項目範例。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或 使用者登入資料提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 請求是否由其他 AWS 服務提出

如需詳細資訊，請參閱CloudTrail`userIdentity`元素。

# 了解 Amazon ECR 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單個請求，包括有關請求的操作，操作的日期和時間，請求參數和其他信息的信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

## CloudTrail 記錄項目範例

以下是一些常見 Amazon ECR 任務的 CloudTrail 日誌項目範例。

> **Note**
>
> 這些範例已格式化，以提升可讀性。在記 CloudTrail 錄檔中，所有項目和事件都會串連成一行。此外，這個範例中受限於單一 Amazon ECR 項目。在真實的 CloudTrail 記錄檔中，您會看到來自多個 AWS 服務的項目和事件。

主題



## 範例：建立儲存庫動作

下列範例顯示示範`CreateRepository`動作的 CloudTrail 記錄項目。

```
{
    "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"
}
```

範例：建立 Amazon ECR 儲存庫時的 AWS KMS CreateGrant API 動作

下列範例顯示一個 CloudTrail 記錄項目，示範在建立已啟用 KMS 加密的 Amazon ECR 儲存庫時採取的 AWS KMS CreateGrant 動作。對於啟用 KMS 加密建立的每個存放庫，您應該會在中看到兩個 CreateGrant 記錄項目 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"
}
```

範例：映像推送動作

下列範例顯示示範使用PutImage動作之影像推送的 CloudTrail 記錄項目。

> **Note**
>
> 推送影像時，您也會在 CloudTrail 記錄檔中看到InitiateLayerUploadUploadLayerPart、和CompleteLayerUpload參照。

```
{
    "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"
}
```


範例：映像提取動作

下列範例顯示示範使用`BatchGetImage`動作的影像提取的 CloudTrail 記錄項目。

> **Note**
>
> 提取圖像時，如果您尚未在本地擁有映像，則還將在 CloudTrail 日誌中看到`GetDownloadUrlForLayer`引用。


```
{
    "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"
}
```

### 範例：映像生命週期政策動作

下列範例顯示一個 CloudTrail 記錄項目，說明影像何時因生命週期原則規則而到期。您可以藉由為事件名稱欄位篩選 `PolicyExecutionEvent`，找出事件類型。

> **Important**
>
> 由於個別 CloudTrail 事件的大小限制，對於 10 個或更多映像到期的生命週期政策動作，Amazon ECR 會將多個事件傳送至 CloudTrail。此外，Amazon ECR 每個映像最多包含 100 個標籤。

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

# 搭配開發套件 AWS 使用 Amazon ECR

AWS 軟件開發套件（SDK）可用於許多流行的編程語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。

| SDK 文件 | 代碼範例 |
| --- | --- |
| AWS SDK for C++ | AWS SDK for C++ 程式碼範例 |
| AWS CLI | AWS CLI 程式碼範例 |
| AWS SDK for Go | AWS SDK for Go 程式碼範例 |
| AWS SDK for Java | AWS SDK for Java 程式碼範例 |
| AWS SDK for JavaScript | AWS SDK for JavaScript 程式碼範例 |
| 適用於 Kotlin 的 AWS SDK | 適用於 Kotlin 的 AWS SDK 程式碼範例 |
| AWS SDK for .NET | AWS SDK for .NET 程式碼範例 |
| AWS SDK for PHP | AWS SDK for PHP 程式碼範例 |
| AWS Tools for PowerShell | PowerShell 程式碼範例的工具 |
| AWS SDK for Python (Boto3) | AWS SDK for Python (Boto3) 程式碼範例 |
| AWS SDK for Ruby | AWS SDK for Ruby 程式碼範例 |
| 適用於 Rust 的 AWS SDK | 適用於 Rust 的 AWS SDK 程式碼範例 |
| 適用於 SAP ABAP 的 AWS SDK | 適用於 SAP ABAP 的 AWS SDK 程式碼範例 |
| 適用於 Swift 的 AWS SDK | 適用於 Swift 的 AWS SDK 程式碼範例 |

**可用性範例**

找不到所需的內容嗎？ 請使用本頁面底部的提供意見回饋連結申請程式碼範例。

# 使 AWS 用開發套件的 Amazon ECR 程式碼範例

下列程式碼範例說明如何搭配 AWS 軟體開發套件 (SDK) 使用 Amazon ECR。

Actions 是大型程式的程式碼摘錄，必須在內容中執行。雖然動作會告訴您如何呼叫個別服務函數，但您可以在其相關情境和跨服務範例中查看內容中的動作。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配開發套件 AWS 使用 Amazon ECR。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

程式碼範例

- 使 AWS 用開發套件為 Amazon ECR 執行的動作
  - 搭DescribeRepositories配 AWS 開發套件或 CLI 使用
  - 搭ListImages配 AWS 開發套件或 CLI 使用

# 使 AWS 用開發套件為 Amazon ECR 執行的動作

下列程式碼範例示範如何使用 AWS 開發套件執行個別 Amazon ECR 動作。這些摘錄呼叫 Amazon ECR API，是來自必須在內容中執行的大型程式碼摘錄。每個範例都包含一個連結 GitHub，您可以在其中找到設定和執行程式碼的指示。

下列範例僅包含最常使用的動作。如需完整清單，請參閱亞馬遜彈性容器登錄 (Amazon ECR) API 參考。

範例

- 搭DescribeRepositories配 AWS 開發套件或 CLI 使用
- 搭ListImages配 AWS 開發套件或 CLI 使用

## 搭`DescribeRepositories`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`DescribeRepositories`。

CLI

AWS CLI

描述登錄中的儲存庫

此範例說明帳戶預設登錄中的儲存庫。

命令：

```
aws ecr describe-repositories
```

輸出：

```
{
    "repositories": [
        {
            "registryId": "012345678910",
            "repositoryName": "ubuntu",
            "repositoryArn": "arn:aws:ecr:us-west-2:012345678910:repository/
ubuntu"
        },
        {
            "registryId": "012345678910",
            "repositoryName": "test",
            "repositoryArn": "arn:aws:ecr:us-west-2:012345678910:repository/test"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeRepositories中的。

Rust

適用於 Rust 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
async fn show_repos(client: &aws_sdk_ecr::Client) -> Result<(),
 aws_sdk_ecr::Error> {
    let rsp = client.describe_repositories().send().await?;
```

```
    let repos = rsp.repositories();

    println!("Found {} repositories:", repos.len());

    for repo in repos {
        println!("  ARN:  {}", repo.repository_arn().unwrap());
        println!("  Name: {}", repo.repository_name().unwrap());
    }

    Ok(())
}
```

- 如需 API 的詳細資訊，請參閱 AWS SDK DescribeRepositories中的 Rust API 參考資料。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配開發套件 AWS 使用 Amazon ECR。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

## 搭**ListImages**配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用ListImages。

CLI

AWS CLI

列出儲存庫中的影像

下列list-images範例會顯示cluster-autoscaler儲存庫中的影像清單。

```
aws ecr list-images \
    --repository-name cluster-autoscaler
```

輸出：

```
{
    "imageIds": [
        {
            "imageDigest":
 "sha256:99c6fb4377e9a420a1eb3b410a951c9f464eff3b7dbc76c65e434e39b94b6570",
            "imageTag": "v1.13.8"
        },
```

```
        {
            "imageDigest":
 "sha256:99c6fb4377e9a420a1eb3b410a951c9f464eff3b7dbc76c65e434e39b94b6570",
            "imageTag": "v1.13.7"
        },
        {
            "imageDigest":
 "sha256:4a1c6567c38904384ebc64e35b7eeddd8451110c299e3368d2210066487d97e5",
            "imageTag": "v1.13.6"
        }
    ]
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考ListImages中的。

Rust

適用於 Rust 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
async fn show_images(
    client: &aws_sdk_ecr::Client,
    repository: &str,
) -> Result<(), aws_sdk_ecr::Error> {
    let rsp = client
        .list_images()
        .repository_name(repository)
        .send()
        .await?;

    let images = rsp.image_ids();

    println!("found {} images", images.len());

    for image in images {
        println!(
            "image: {}:{}",
```

```
            image.image_tag().unwrap(),
            image.image_digest().unwrap()
        );
    }

    Ok(())
}
```

- 如需 API 的詳細資訊，請參閱 AWS SDK ListImages中的 Rust API 參考資料。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配開發套件 AWS 使用 Amazon ECR。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

# Amazon ECR 服務配額

下表提供 Amazon Elastic Container Registry (Amazon ECR) 的預設服務配額。

| 名稱 | 預設 | 可調整 | 描述 |
| --- | --- | --- | --- |
| 複寫組態中每個規則的篩選條件 | 每個受支援的區域：100 | 否 | 複寫組態中每個規則的篩選條件的數量上限。 |
| 每個儲存庫的映像 | 每個支援的區域：10,000 | 是 | 每個儲存庫映像的數量上限。 |
| 分層部分 | 每個支援的區域：4,200 | 否 | 分層部分數目上限。這僅適用於直接使用 Amazon ECR API 動作來啟動分段上傳以進行映像推送操作時。 |
| 生命週期政策長度 | 每個支援的區域：30,720 | 否 | 生命週期政策中的字元數上限。 |
| 最大分層部分大小 | 每個受支援的區域：10 | 否 | 分層部分大小上限 (MiB)。這僅適用於直接使用 Amazon ECR API 動作來啟動分段上傳以進行映像推送操作時。 |
| 最大分層大小 | 每個受支援的區域：52,000 個 | 否 | 每層的大小上限 (MiB)。 |
| 最小分層部分大小 | 每個受支援的區域：5 | 否 | 分層部分大小下限 (MiB)。這僅適用於直接使用 Amazon ECR API 動作來啟動分段上傳以進行映像推送操作時。 |

| 名稱 | 預設 | 可調整 | 描述 |
| --- | --- | --- | --- |
| 依登錄檔提取快取規則 | 每個受支援的區域：50 | 否 | 提取快取規則的數量上限。 |
| BatchCheckLayerAvailability 請求的速率 | 每個受支援的區域：每秒 1,000 | 是 | 目前區域中每秒可進行 BatchCheckLayerAvailability 請求的數量上限。將映像推送至儲存器時會檢查每個映像圖層，驗證之前是否上傳過。如果已上傳，則會略過映像圖層。 |
| BatchGetImage 請求的速率 | 每個支援的區域：每秒 2,000 | 是 | 目前區域中每秒可進行 BatchGetImage 請求的數量上限。提取映像時，系統會叫用 BatchGetImage API 一次以擷取映像資訊清單。如果您請求增加此 API 的配額，請同時檢視 GetDownloadUrlForLayer 使用量。 |
| CompleteLayerUpload 請求的速率 | 每個支援的區域：每秒 100 | 是 | 目前區域中每秒可進行 CompleteLayerUpload 請求的數量上限。推送映像時，每個新映像圖層都會叫用 CompleteLayerUpload API 一次，以確認上傳已完成。 |
| GetAuthorizationToken 請求的速率 | 每個支援的區域：每秒 500 | 是 | 目前區域中每秒可進行 GetAuthorizationToken 請求的數量上限。 |

| 名稱 | 預設 | 可調整 | 描述 |
| --- | --- | --- | --- |
| GetDownloadUrlForLayer 請求的速率 | 每個支援的區域：每秒 3,000 | 是 | 目前區域中每秒可進行 GetDownloadUrlForLayer 請求的數量上限。提取映像時，未快取的每個映像圖層都會叫用一次 GetDownloadUrlForLayer API。如果您請求增加此 API 的配額，請同時檢視 BatchGetImage 使用量。 |
| InitiateLayerUpload 請求的速率 | 每個支援的區域：每秒 100 | 是 | 目前區域中每秒可進行 InitiateLayerUpload 請求的數量上限。推送映像時，未上傳的每個映像圖層都會叫用 InitiateLayerUpload API 一次。是否上傳映像圖層會由 BatchCheckLayerAvailability API 動作決定。 |
| PutImage 請求的速率 | 每個支援的區域：每秒 10 | 是 | 目前區域中每秒可進行 PutImage 請求的數量上限。推送映像並上傳所有新映像圖層時，系統會叫用 PutImage API 一次，以建立或更新與映像關聯標籤的映像資訊清單。 |

| 名稱 | 預設 | 可調整 | 描述 |
| --- | --- | --- | --- |
| UploadLayerPart 請求的速率 | 每個支援的區域：每秒 500 | 是 | 目前區域中每秒可進行 UploadLayerPart 請求的數量上限。推送映像時，每個新映像層都會分成多個部分上傳，而每個新映像層部分都會呼叫一次 UploadLayerPart API。 |
| 映像掃描速率 | 每個支援的區域：1 | 否 | 每 24 小時每張映像的映像掃描次數上限。 |
| 已註冊的儲存庫 | 每個支援的區域：10,000 | 是 | 目前區域中，您可以在此帳戶中建立的儲存庫數量上限。 |
| 每個生命週期政策的規則 | 每個受支援的區域：50 | 否 | 生命週期政策中規則的數量上限 |
| 每個複寫組態的規則 | 每個受支援的區域：10 | 否 | 複寫組態中規則的數量上限。 |
| 每個映像的標籤 | 每個支援的區域：1,000 | 否 | 每個映像的標籤數目上限。 |
| 複寫組態中跨所有規則的唯一目的地 | 每個受支援的區域：25 | 否 | 複寫組態中跨所有規則的唯一目的地的數量上限。 |

# 在 AWS Management Console 中管理您的 Amazon ECR 服務配額

Amazon ECR 已與 Service Quotas 整合，這是可讓您集中檢視和管理配額的 AWS 服務。如需詳細資訊，請參閱Service Quotas 使用者指南中的什麼是 Service Quotas？。

Service Quotas 可讓您輕鬆查詢所有 Amazon ECR 服務配額的值。

檢視 Amazon ECR 服務配額 (AWS Management Console)

1. 開啟 Service Quotas 主控台，網址為 https://console.aws.amazon.com/servicequotas/。
2. 在導覽窗格中，選擇 AWS services (AWS 服務)。
3. 從 AWS 服務清單中，搜尋並選取 Amazon Elastic Container Registry (Amazon ECR)。

   在 Service quotas (服務配額) 清單中，您可以看到服務配額名稱、套用的值 (如果有的話)、AWS 預設配額，以及配額值是否可調整。
4. 若要檢視服務配額的其他資訊 (例如說明)，請選擇配額名稱。

若要請求提高配額，請參閱《Service Quotas 使用者指南》https://docs.aws.amazon.com/servicequotas/latest/userguide/request-increase.html中的請求提高配額。

## 建立 CloudWatch 警示以監控 API 用量指標

Amazon ECR 提供 CloudWatch 用量指標，這些指標對應至涉及登錄驗證、映像推送和映像提取動作之每個 API 的 AWS 服務配額。在 Service Quotas 控制台中，您可以在圖形上視覺化您的用量，並設定在用量接近服務配額時警示您。如需詳細資訊，請參閱 Amazon ECR 用量指標。

使用下列步驟，根據其中一個 Amazon ECR API 用量指標來建立 CloudWatch 警示。

根據您的 Amazon ECR 用量配額建立警示 (AWS Management Console)

1. 開啟 Service Quotas 主控台，網址為 https://console.aws.amazon.com/servicequotas/。
2. 在導覽窗格中，選擇 AWS services (AWS 服務)。
3. 從 AWS 服務清單中，搜尋並選取 Amazon Elastic Container Registry (Amazon ECR)。
4. 在 Service quotas (服務配額) 清單中，選取您要為其建立警示的 Amazon ECR 用量配額。
5. 在 Amazon CloudWatch Events 警示區段中，選擇 Create (建立)。
6. 針對 Alarm threshold (警示閾值)，選擇您想要多少百分比的套用配額值設為警示值。
7. 針對 Alarm name (警示名稱)，輸入警示的名稱，然後選擇 Create (建立)。

# Amazon ECR 故障診斷

本章可協助您尋找 Amazon ECR 的診斷資訊，並提供常見問題和錯誤訊息的疑難排解步驟。

主題



## 使用 Amazon ECR 時的泊塢視窗命令和問題疑難排解

在某些情況下，針對 Amazon ECR 執行 Docker 命令可能會導致錯誤訊息。以下說明了一些一般錯誤訊息與潛在解決方案。

主題



### Docker 日誌不包含預期的錯誤消息

要開始調試任何與 Docker 相關的問題，請首先在主機實例上運行的 Docker 守護程序上打開 Docker 調試輸出。如果您在 Amazon ECS 容器執行個體上使用從 Amazon ECR 擷取的映像檔，請參閱 Amazon 彈性容器服務開發人員指南中的從 Docker 精靈設定詳細輸出。

### 當從 Amazon ECR 儲存庫提取映像時，出現錯誤：「Filesystem Verification Failed」(檔案系統驗證失敗) 或「404: Image Not Found」(404：找不到映像)

在 Docker 1.9 或以上版本中使用 docker pull 命令從 Amazon ECR 儲存庫映像時，您可能收到錯誤 `Filesystem verification failed`。當您使用 Docker 1.9 以前的版本時，您可能會收到錯誤 `404: Image not found`。

以下列出一些可能的原因及其說明。

本機磁碟已滿

若您正在執行 docker pull 的本機磁碟已滿，則在本機檔案上計算的 SHA-1 雜湊，可能與 Amazon ECR 計算的 SHA-1 雜湊不同。檢查您的本機磁碟有足夠的剩餘空間以儲存您提取的 Docker 映像。您也可以刪除舊的映像，以為新的映像騰出空間。使用 docker images 命令以查看所有本機下載且包含容量大小的 Docker 映像清單。

由於網路錯誤，用戶端無法連接至遠端儲存庫

對 Amazon ECR 儲存庫的呼叫需要正常運作的網路連線。確認您的網路設定，並確認其他工具與應用程式可正常存取網路資源。如果您在私有子網路中的 Amazon EC2 執行個體上執行 docker pull，請確認該子網路擁有對網際網路的路由。使用網路地址轉譯 (NAT) 伺服器或受管 NAT 閘道。

目前，對 Amazon ECR 儲存庫的呼叫也需要透過您的企業防火牆的網路存取至 Amazon Simple Storage Service (Amazon S3)。如果您的組織使用允許服務端點的防火牆軟體或 NAT 裝置，請務必確保您目前區域的 Amazon S3 服務端點是受到允許的。

如果您正在 HTTP 代理後使用 Docker，您可以使用適當的代理設定來設定 Docker。如需詳細資訊，請參閱 Docker 文件中的 HTTP 代理。

## 當從 Amazon ECR 提取映像時出現錯誤：「Filesystem Layer Verification Failed」(檔案系統分層驗證失敗)

當您使用 docker pull 命令提取映像時，您可能會收到錯誤 `image image-name not found`。若您檢查 Docker 日誌時，您可能會看到像下列的錯誤：

```
filesystem layer verification failed for digest sha256:2b96f...
```

此錯誤表示一個或更多的映像分層下載失敗。以下列出一些可能的原因及其說明。

您可能正在使用較舊版本的 Docker

在您使用低於 1.10 版本的 Docker 時，有少許機率會出現此錯誤。將您的 Docker 用戶端更新為 1.10 或更新的版本。

您的用戶端遭遇網路或磁碟錯誤

完全的磁碟或網路錯誤可能阻礙一個或更多分層的下載，如同稍早討論過的 `Filesystem verification failed` 訊息。遵循上述建議，以確保您的檔案系統未滿，且已在您的網路中啟用存取 Amazon S3。

## 當推送至儲存庫時，出現 HTTP 403 錯誤或「無基本身分驗證憑證」錯誤

即使您已透過 aws ecr get-login-password 命令成功驗證至 Docker，有時候您可能仍會收到 HTTP `403 (Forbidden)` 錯誤，或是從 docker push 或 docker pull 命令收到錯誤訊息 `no basic auth credentials`。以下是此問題的一些已知原因：

您已驗證至不同區域

驗證請求是繫結至特定區域的，且無法跨區域使用。例如，如果您從美國西部 (奧勒岡) 取得了授權字符，您便不得將其用於驗證您美國東部 (維吉尼亞北部) 中的儲存庫。若要解決此問題，請確認您已從與儲存器所在相同的區域擷取身分驗證字符。如需詳細資訊，請參閱 the section called “登錄檔身分驗證”。

您已完成身分驗證，可推送至您沒有權限的儲存庫

您沒有推送至儲存庫的必要權限。如需詳細資訊，請參閱 Amazon ECR 中的私有儲存庫政策。

您的字符已過期

使用 `GetAuthorizationToken` 操作取得的授權字符預設過期期間是 12 小時。

`wincred` 憑證管理工具中的錯誤

某些適用 Windows 的 Docker 版本使用稱作 `wincred` 的憑證安全管理工具，該工具並不會適當的處理由 aws ecr get-login-password 產生的 Docker 登入命令 (如需詳細資訊，請參閱 https://github.com/docker/docker/issues/22910)。您可以執行輸出的 Docker 登入命令，但若您試著推送或提取映像時，那些命令將失敗。您可以透過從 aws ecr get-login-password 輸出 Docker 登入命令的登錄檔引數中移除 `https://` 機制以解決此錯誤。無 HTTPS 機制的範例 Docker 登入命令如下所示。

```
docker login -u AWS -p <password> <aws_account_id>.dkr.ecr.<region>.amazonaws.com
```

# Amazon ECR 錯誤訊息故障診斷

在某些情況下，您已透過 Amazon ECR 主控台啟動的 API 呼叫，或 AWS CLI 結束時顯示錯誤訊息。以下說明了一些一般錯誤訊息與潛在解決方案。

## 要求過多或 ThrottleException

您可能會收到來自一個或多個 Amazon ECR 動作或 API 呼叫的`ThrottleException`錯誤或錯誤。`429: Too Many Requests`這表示您正在以短間隔重複呼叫 Amazon ECR 中的單一端點，因此您的請求已被調節。調節會發生在當從單一使用者至單一端點的呼叫在一段時間內超出特定閾值時。

Amazon ECR 中的每個 API 操作都有一個與其相關聯的速率節流。例如，`GetAuthorizationToken` 動作的調節為每秒 20 次交易 (TPS)，爆增上限允許為每秒 200 次交易。在每一區域中，每一帳戶都會接收到可儲存高達 200 `GetAuthorizationToken` 點的儲存貯體。這些點數以每秒 20 次的速率補充。如果您的儲存貯體有 200 點，您一秒可以達到每秒 200 次的 `GetAuthorizationToken` API 交易，然後再無限期保持每秒 20 次交易。如需 Amazon ECR API 速率限制的詳細資訊，請參閱Amazon ECR 服務配額。

欲處理調節錯誤，以增量退避實施重試功能至您的程式碼。如需詳細資訊，請參閱 AWS SDK 和工具參考指南中的重試行為。另一個選項是要求提高速率限制，您可以使用 Service Quotas 控制台執行此操作。 如需詳細資訊，請參閱在 AWS Management Console 中管理您的 Amazon ECR 服務配額。

## HTTP 403: "User [arn] is not authorized to perform [operation]" (使用者 [arn] 未授權您執行此 [操作])

當您嘗試以 Amazon ECR 執行動作時，您可能會接收到下列錯誤：

```
$ 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: *
```

這表示您的使用者沒有被授予使用 Amazon ECR 的權限，或者那些權限未正確設定。特別是，如果您正在針對一個 Amazon ECR 儲存庫執行動作，確認使用者已被授予權限以存取該儲存庫。如需相關建立和驗證 Amazon ECR 許可的詳細資訊，請參閱 Amazon Elastic Container Registry 的 Identity and Access Management。

## HTTP 404：「儲存庫不存在」錯誤

如果您指定的 Docker Hub 儲存庫目前尚未存在，Docker Hub 會自動建立。使用 Amazon ECR，新的儲存庫必須在可使用前確實建立。這會避免新的儲存庫被意外的建立 (例如輸入了錯別字)，並且也確保了適當的安全性存取政策確實的指派至任何新的儲存庫。如需有關建立儲存庫的詳細資訊，請參閱 Amazon ECR 私有儲存庫。

## 錯誤：無法從非 TTY 裝置執行互動式登入

如果您收到錯誤訊息 `Cannot perform an interactive login from a non TTY device`，以下疑難排解步驟應該會有所幫助。

- 請確認您使用的是 AWS CLI 版本 2，而且您的系統上沒有衝突的 AWS CLI 版本 1。如需詳細資訊，請參閱安裝或更新最新版本的 AWS CLI。
- 確認您已 AWS CLI 使用有效的認證設定。如需詳細資訊，請參閱安裝或更新最新版本的 AWS CLI。
- 驗證命 AWS CLI 令的語法是否正確。

# 文件歷史紀錄

下表說明自上次發行 Amazon ECR 後，對文件的重要變更。我們也會經常更新文件，以處理您傳送給我們的意見回饋。

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 新增跨區域和跨帳戶複寫至中國區域 | Amazon ECR 新增了對中國區域的支援，以篩選複寫哪些儲存庫。 | 2024 年五月十五日 |
| 添加了 GitLab 容器註冊表以通過緩存規則提取 | Amazon ECR 增加了對為 GitLab 容器登錄建立提取快取規則的支援。 | 2024 年五月八日 |
| Amazon ECR 生命週期政策新增萬用字元使用支援 | Amazon ECR 在生命週期政策規則中使用 `tagPatternList` 參數，藉以新增在生命週期政策中使用萬用字元的支援。如需詳細資訊，請參閱 在 Amazon ECR 中使用生命週期政策自動清理映像檔。 | 2023 年 12 月 18 日 |
| Amazon ECR 儲存庫建立範本 | Amazon ECR 新增儲存庫建立範本支援。如需詳細資訊，請參閱 用於控制在提取快取動作期間建立的儲存庫的範本。 | 2023 年 11 月 15 日 |
| Amazon ECR 提取快取已新增支援已驗證的上游登錄檔 | Amazon ECR 已新增支援，開放使用需驗證才能提取快取規則的上游登錄檔。如需詳細資訊，請參閱 將上游註冊表與 Amazon ECR 私有註冊表同步。 | 2023 年 11 月 15 日 |
| AWSECRPullThroughCache_ServiceRolePolicy – 更新現有政策 | Amazon ECR 將新的許可新增到 `AWSECRPullThroughCache_ServiceRolePolicy` 政策。這些許可允許 Amazon ECR 擷取 Secrets Manager 秘密的加密內容。這在使用提取快取規則從需要驗證的上游登錄檔快取映像時是必要的。 | 2023 年 11 月 15 日 |
| Amazon ECR 映像簽署 | Amazon ECR 並 AWS Signer 增加了對使用公證用戶端建立和推送容器映像簽名的支援。如需詳細資訊，請參閱 簽署儲存在 Amazon ECR 私有儲存庫中的映像。 | 2023 年 6 月 6 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 新增了 Kubernetes 容器登錄檔以提取快取規則 | Amazon ECR 新增了對 Kubernetes 容器登錄檔建立提取快取規則的支援。如需詳細資訊，請參閱 將上游註冊表與 Amazon ECR 私有註冊表同步。 | 2023 年 6 月 1 日 |
| Amazon ECR 增強型掃描持續時間支援 | Amazon Inspector 新增在啟用增強型掃描時設定儲存庫監控的持續時間的支援。如需詳細資訊，請參閱 在 Amazon Inspector 中更改圖像的增強掃描持續時間。 | 2022 年 6 月 28 日 |
| Amazon ECR 將存儲庫提取計數指標發送到 Amazon CloudWatch | Amazon ECR 將存儲庫提取計數指標發送到 Amazon CloudWatch。如需詳細資訊，請參閱 Amazon ECR 儲存庫指標。 | 2022 年 1 月 6 日 |
| 擴展複寫支援 | Amazon ECR 已新增用於篩選要複寫哪些儲存庫的支援。如需詳細資訊，請參閱 Amazon ECR 中的私有映像複寫。 | 2021 年 9 月 21 日 |
| AWS Amazon ECR 的受管政策 | Amazon ECR 新增了 AWS 受管政策的文件。如需詳細資訊，請參閱 AWS Amazon 彈性容器註冊表的受管政策。 | 2021 年 6 月 24 日 |
| 跨區域和跨帳戶複寫 | Amazon ECR 已新增為您的私有登錄檔設定複寫設定的支援。如需詳細資訊，請參閱 Amazon ECR 中的私有註冊表設置。 | 2020 年 12 月 8 日 |
| OCI 成品支援 | Amazon ECR 已新增推送和提取開放容器計畫 (OCI) 成品的支援。新的參數 `artifactMediaType` 已新增至 `DescribeImages` API 回應來指出成品的類型。<br><br>如需詳細資訊，請參閱 將頭盔圖推送到 Amazon ECR 私有存儲庫。 | 2020 年 8 月 24 日 |
| 靜態加密 | Amazon ECR 已新增對使用存放在 AWS Key Management Service (AWS KMS) 中的客戶受管金鑰的伺服器端加密為您的儲存庫設定加密的支援。<br><br>如需詳細資訊，請參閱 靜態加密。 | 2020 年 7 月 29 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 多架構映像 | Amazon ECR 已新增對建立和推送用於多架構映像之 Docker 資訊清單列表的支援。<br><br>如需詳細資訊，請參閱 將多架構映像推送到 Amazon ECR 私有儲存庫。 | 2020 年 4 月 28 日 |
| Amazon ECR 用量指標 | Amazon ECR 新增了 CloudWatch 使用量指標，提供您帳戶資源使用量的可見性。您也可以從 CloudWatch 和 Service Quotas 主控台建立 CloudWatch警示，以便在使用量接近套用的服務配額時收到警示。<br><br>如需詳細資訊，請參閱 Amazon ECR 用量指標。 | 2020 年 2 月 28 日 |
| 更新 Amazon ECR 服務配額 | 已更新 Amazon ECR 服務配額以包含每個 API 配額。<br><br>如需詳細資訊，請參閱 Amazon ECR 服務配額。 | 2020 年 2 月 19 日 |
| 新增 `get-login-password` 的命令 | 已新增 get-login-password 的支援，可提供簡單且安全的授權字符擷取方式。<br><br>如需詳細資訊，請參閱 使用授權字符。 | 2020 年 2 月 4 日 |
| 映像掃描 | 新增對映像掃描的支援，這有助於識別容器映像中的軟體漏洞。Amazon ECR 使用開放原始碼 CoreOS Clair 專案的 Common Vulnerabilities and Exposures (CVE) 資料庫，並提供您掃描結果的清單。<br><br>如需詳細資訊，請參閱 掃描影像以查看 Amazon ECR 中的軟體漏洞。 | 2019 年 10 月 24 日 |
| VPC 端點政策 | 新增對 Amazon ECR 介面 VPC 端點設定 IAM 政策的支援。<br><br>如需詳細資訊，請參閱 為您的 Amazon ECR VPC 端點建立端點政策。 | 2019 年 9 月 26 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 映像標籤可變性 | 新增支援將儲存庫設定為不可變的，以防止映像標籤被覆寫。<br><br>如需詳細資訊，請參閱 防止 Amazon ECR 中的圖像標籤被覆蓋。 | 2019 年 7 月 25 日 |
| 介面 VPC 端點 (AWS PrivateLink) | 增加了對配置由 AWS PrivateLink支持的接口 VPC 端點的支持。這可讓您在 VPC 與 Amazon ECR 之間建立私有連線，而不需要透過網際網路、NAT 執行個體、VPN 連接或 AWS Direct Connect進行存取。<br><br>如需詳細資訊，請參閱 Amazon ECR 接口 VPC 端端點 ()AWS PrivateLink。 | 2019 年 1 月 25 日 |
| 資源標記 | Amazon ECR 新增支援將中繼資料標籤新增至您的儲存庫。<br><br>如需詳細資訊，請參閱 在 Amazon ECR 中標記私有存儲庫。 | 2018 年 12 月 18 日 |
| Amazon ECR 名稱變更 | Amazon Elastic Container Registry 已重新命名 (之前稱為 Amazon EC2 Container Registry)。 | 2017 年 11 月 21 日 |
| 生命週期政策 | Amazon ECR 生命週期政策可讓您指定儲存庫中映像的生命週期管理。<br><br>如需詳細資訊，請參閱 在 Amazon ECR 中使用生命週期政策自動清理映像檔。 | 2017 年 10 月 11 日 |
| Amazon ECR 對 Docker 映像資訊清單 2 結構描述 2 的支援 | Amazon ECR 現在支援 Docker 映像工作資訊清單檔案 V2 結構描述 2 (需搭配 1.10 或更新版本的 Docker 使用)。<br><br>如需詳細資訊，請參閱 Amazon ECR 中的容器映像資訊清單格式支援。 | 2017 年 1 月 27 日 |
| Amazon ECR 一般可用性 | 亞馬遜彈性容器註冊表 (Amazon ECR) 是一種受管的 AWS Docker 登錄服務，具有安全、可擴展和可靠性。 | 2015 年 12 月 21 日 |

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。