SRA の技術情報誌
GS LetterNeo
Vol.163　2022 年 2 月

Amazon ECR の機能 Pull through cache repository

土田 拓実

DX 技術本部 DX 技術開発室

はじめに

AWS 上でコンテナを利用する際、Private Subnet から Public Registry のイメージを pull したいという要件が発生することもあると思います。この時、どのように対応すればよいでしょうか。Public Subnet に Nat Gateway を建ててインターネット越しにアクセスすることや、ECR Private Repository を作成して Public Registry のイメージを逐一 Push し、Private link からアクセスする運用等が考えられます。

この問題に対する新しい解決方法を提案する機能、「Pull through cache repository」が昨年の 11 月にリリース[1]されていたので、今回ご紹介＆試してみたいと思います。(GS LetterNeo12 月号[2]内でも Private Link から Public Registry にアクセスしたいという話がありましたが、こちらの機能を利用すれば解決します。)

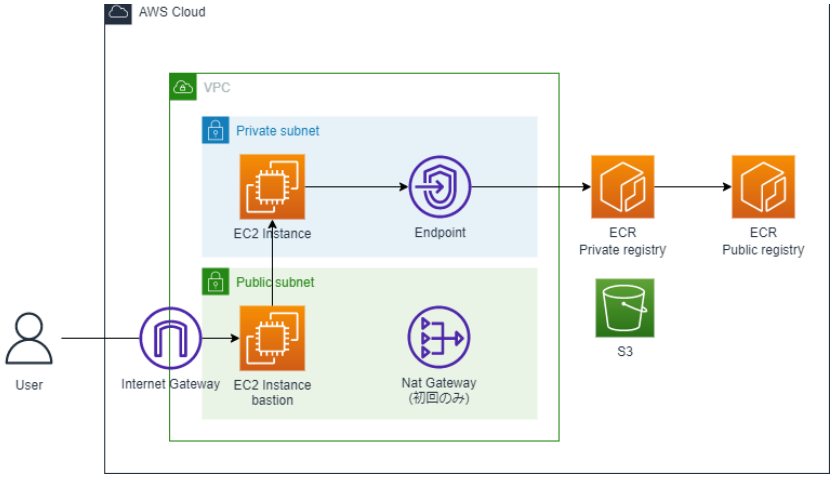
Pull through cache repository

ECR Private Registry 内に Public Repository のキャッシュリポジトリを作成・保持することができる機能です。この機能により、ECR Private Registry にしかアクセスできない環境でも、Public イメージのキャッシュリポジトリからイメージを pull することができます。それだけではなく、キャッシュリポジトリは 24 時間に一度、元の Public Repository に更新がないか確認します。

想定構成図

以下の構成で検証を行います。簡易な構成ですが、Private link で ECR Private Registry へのアクセスしかできない環境でも Public イメージが取れるぞ！というところをイメージして頂ければと思います。
Public Subnet に Nat Gateway がありますが、実は完全に Private Link のみというわけにはいかず、残念ながら初回の pull 時のみ Nat Gateway を作成する必要があります(公式ドキュメント[3]参照)。 一度 pull が完了すれば削除しても大丈夫です。

[1] https://aws.amazon.com/jp/about-aws/whats-new/2021/11/amazon-ecr-cache-repositories/
[2] https://www2.sra.co.jp/Portals/0/files/gsletter/pdf/GSLetterNeoVol161.pdf
[3] https://docs.aws.amazon.com/ja_jp/AmazonECR/latest/userguide/pull-through-cache.html



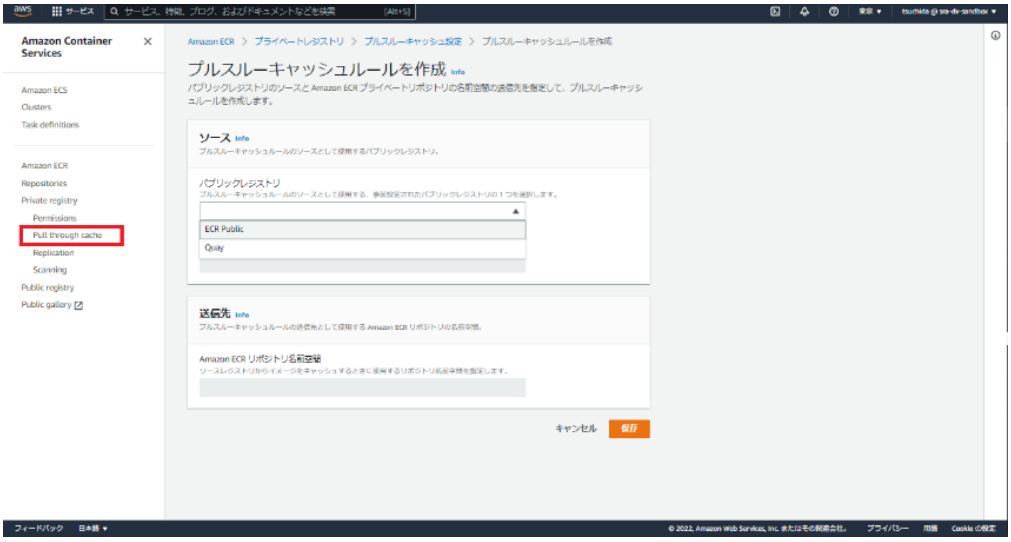
構築・検証

VPC , Subnet , EC2 , Nat Gateway , VPC エンドポイントの作成は本稿の趣旨ではないため省略します。VPC エンドポイントは(com.amazonaws.ap-northeast-1.ecr.dkr , com.amazonaws.ap-northeast-1.ecr.api , com.amazonaws.ap-northeast-1.s3)の 3 つを作成しています。S3 のエンドポイントは Gateway 型を利用しています。また、Private Subnet 内のインスタンスには必要な権限を付与しています。

Pull through cache repository の有効化

マネージメントコンソールから有効化することができます。「ECS → Private registry → Pull through cache」からプルスルーキャッシュルールを作成します。設定は以下のようにします。

- パブリックレジストリ(ECR Public or Quay)
  - ECR Public
- ソースレジストリ URL(固定)
  - public.ecr.aws
- Amazon ECR リポジトリ名前空間(デフォルト)
  - ecr-public



イメージを pull

踏み台インスタンス経由で Private Subnet 内のインスタンスに入り、イメージを pull してみます。ECR Private Registry に入り、Public Registry の amazon linux image を pull します。イメージの指定は`<Private Registry>/<リポジトリ名前空間>/<Public image>`のような形で行います。`aws_account_id`と`region`は環境に合ったものに置換します。

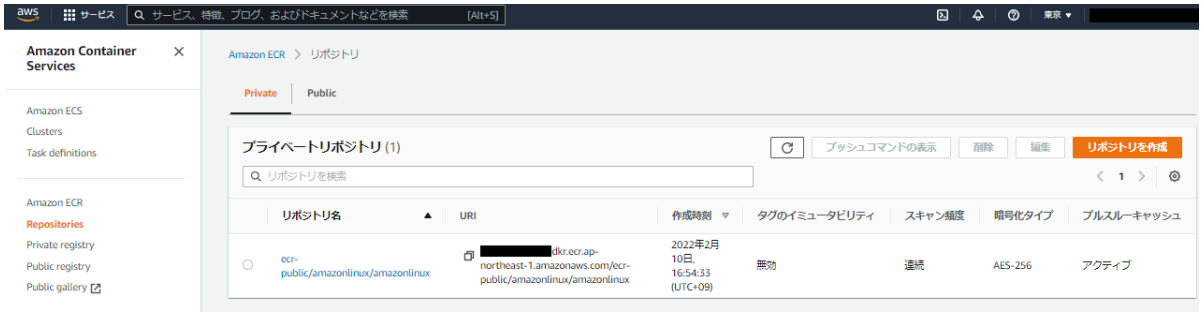
```
> export PRIVATE_REGISTRY="aws_account_id.dkr.ecr.region.amazonaws.com"
> aws ecr get-login-password \
    --region region | docker login \
    --username AWS \
    --password-stdin $PRIVATE_REGISTRY
Login Successded
```

```
> docker pull $PRIVATE_REGISTRY/ecr-public/amazonlinux/amazonlinux:latest
latest: Pulling from ecr-public/amazonlinux/amazonlinux
af353cabf27c: Pull complete
Digest:
sha256:15e6e0277d65375ba56b67b12e01103b3b3ff208e77b4af7be1166c06c97a57f
Status: Downloaded newer image for …(後略)
```

ローカルのイメージを確認すると、pull されていることがわかります。

```
> docker images
REPOSITORY TAG IMAGE_ID CREATED SIZE
<repository名> latest 5d4107984274 2 days ago 164MB
```

マネージメントコンソールから ECR を確認すると、キャッシュリポジトリが生成されていることがわかります。



1 度 pull してしまえば、Nat Gateway を削除してもイメージを pull できることも確認しました。

まとめ

Pull through cache repository を利用することで Private Subnet 内から Private Link で Public Registry のイメージを pull できることを確認しました。1 回目は Nat Gateway が必要になるものの、2 回目以降は不要になり、更にはイメージの更新も自動で行う便利な機能です。Private Link 分の課金が行われるものの、手動でイメージを更新するより楽になります。現状手動で運用している方は利用を検討してはいかがでしょうか。

GSLetterNeo Vol.163
2022 年 2 月 20 日発行
発行者　株式会社 SRA 先端技術研究所

編集者　熊澤努　方 学芬
バックナンバー https://www.sra.co.jp/public/sra/gsletter/
お問い合わせ　gsneo@sra.co.jp

株式会社SRA
〒171-8513 東京都豊島区南池袋 2-32-8

夢を。Yawaraka Innovation
やわらかいのべーしょん