@Jerid
投稿日 2020年09月18日　更新日 2020年09月18日

# VPCエンドポイントを試してみた

AWS , EC2 , IAM , vpc

vpcエンドポイントのハンズオンを体験したので、概要と作成方法の記録です。
勉強途中のため一部理解が追いついていない部分がありますが、ご了承ください。

## vpcエンドポイントとは

vpcエンドポイントは、グローバルIPを持つAWSサービスに対して、vpc内から直接アクセスするための出口のこと。

オンプレだと、専用線で自社サーバと、別地域のサーバやらストレージを接続するイメージです。(うん百万かかるのに・・・)

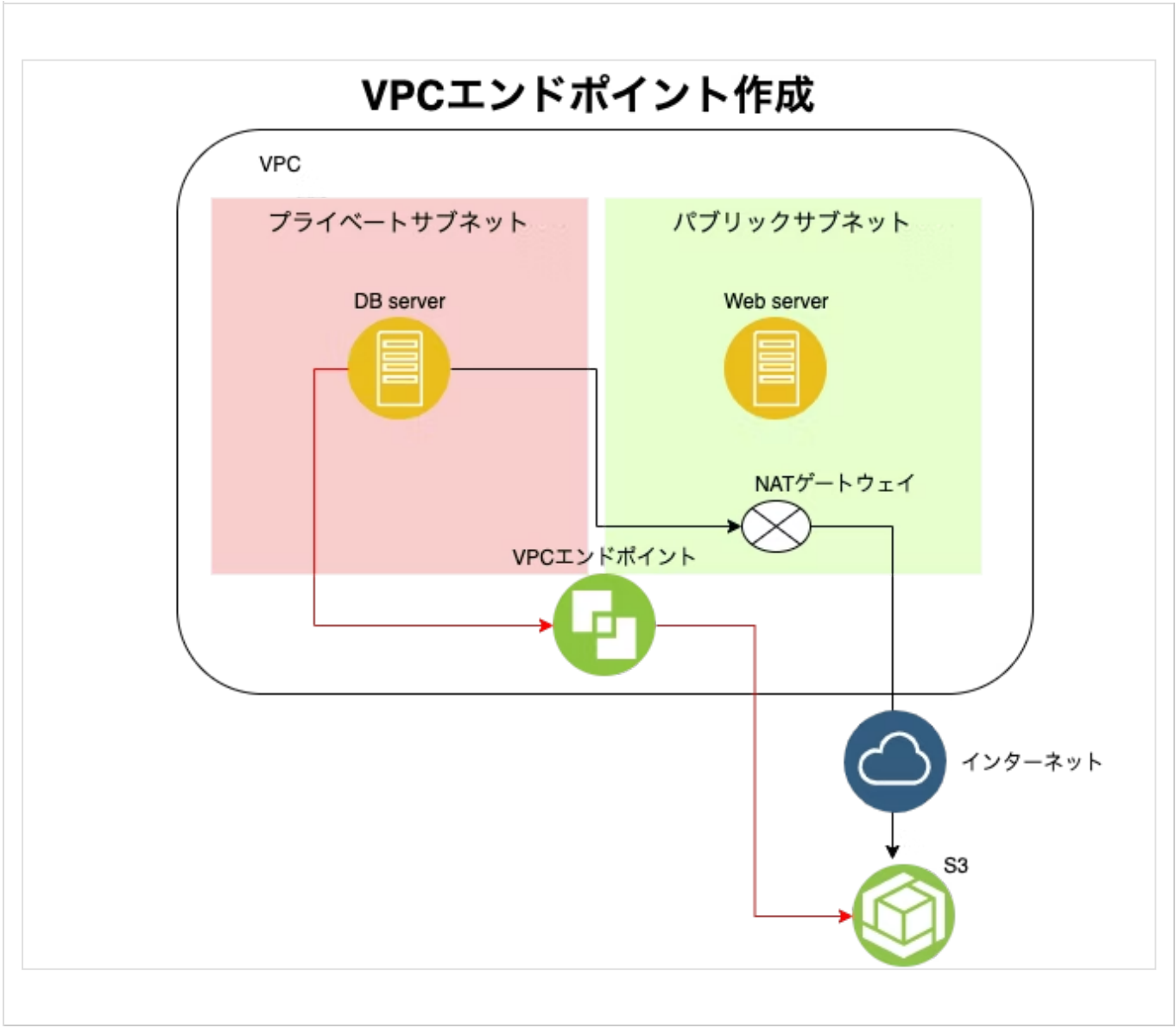
今回は、プライベートサブネット内のインスタンスから、S3へ直接アクセスするための、vpcエンドポイントを作成します。

以下の順に進んでいきますので、よろしくお願いいたします。
間違っている箇所があればコメントで教えていただけると大変助かります🙏


- 利用環境
- S3の作成
- IAMロールの作成・インスタンスへ割当
- VPCエンドポイントの作成・設定
- 動作確認
- VPCエンドポイントを使用しない場合のS3接続方法
- VPCエンドポイント諸々


# 利用環境

今までに作成したVPCやサブネット、インスタンスをそのまま利用しました。
下図の赤線ルートでS3へアクセスできることが目的です。(黒線はVPCエンドポイントを使用しない場合のアクセス例)




# S3の作成

今までS3は作成してこなかったため、最初にS3の作成を行います。

AWSマネジメントコンソールから「S3」と検索し、「S3マネジメントコンソール」に移動します。


S3マネジメントコンソールに移動したら、「バケットの作成」を選択します。

私はいくつかバケットを作成しているのでバケット名が表示されていますが、初回であれば何も表示されません。


S3バケットに名前をつけたら、今回は他に設定をしないので「作成」を選択します。

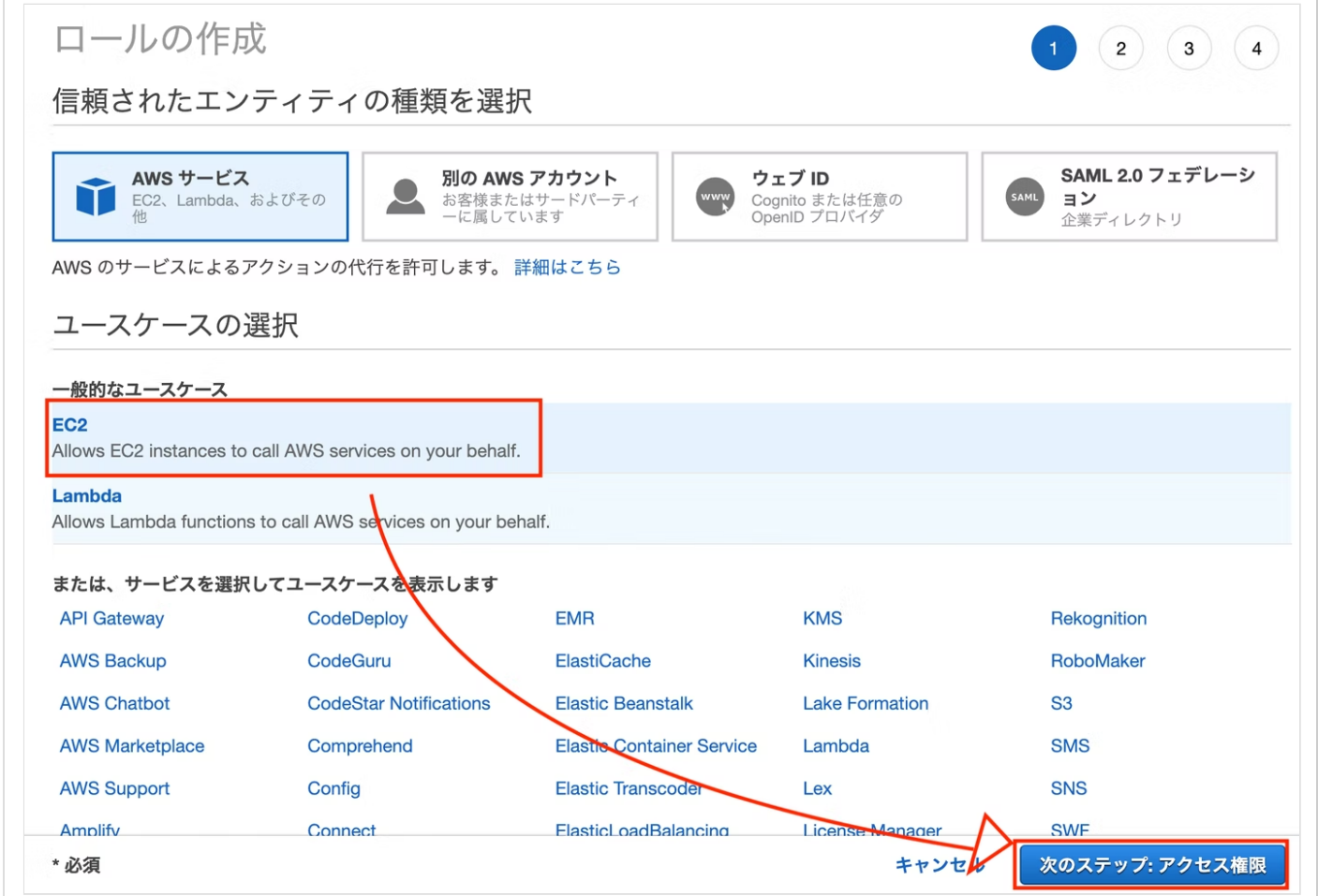
S3バケット名は一意の値である必要があるため、日付等を名前の後に付与すると良いようです。


# IAMロールの作成・インスタンスの割当

続いて、インスタンスがS3へアクセスするためのIAMロールを作成します。
(S3を作成しただけでは使えません!!まずはインスタンスがS3へアクセスできるよう権限設定をします)

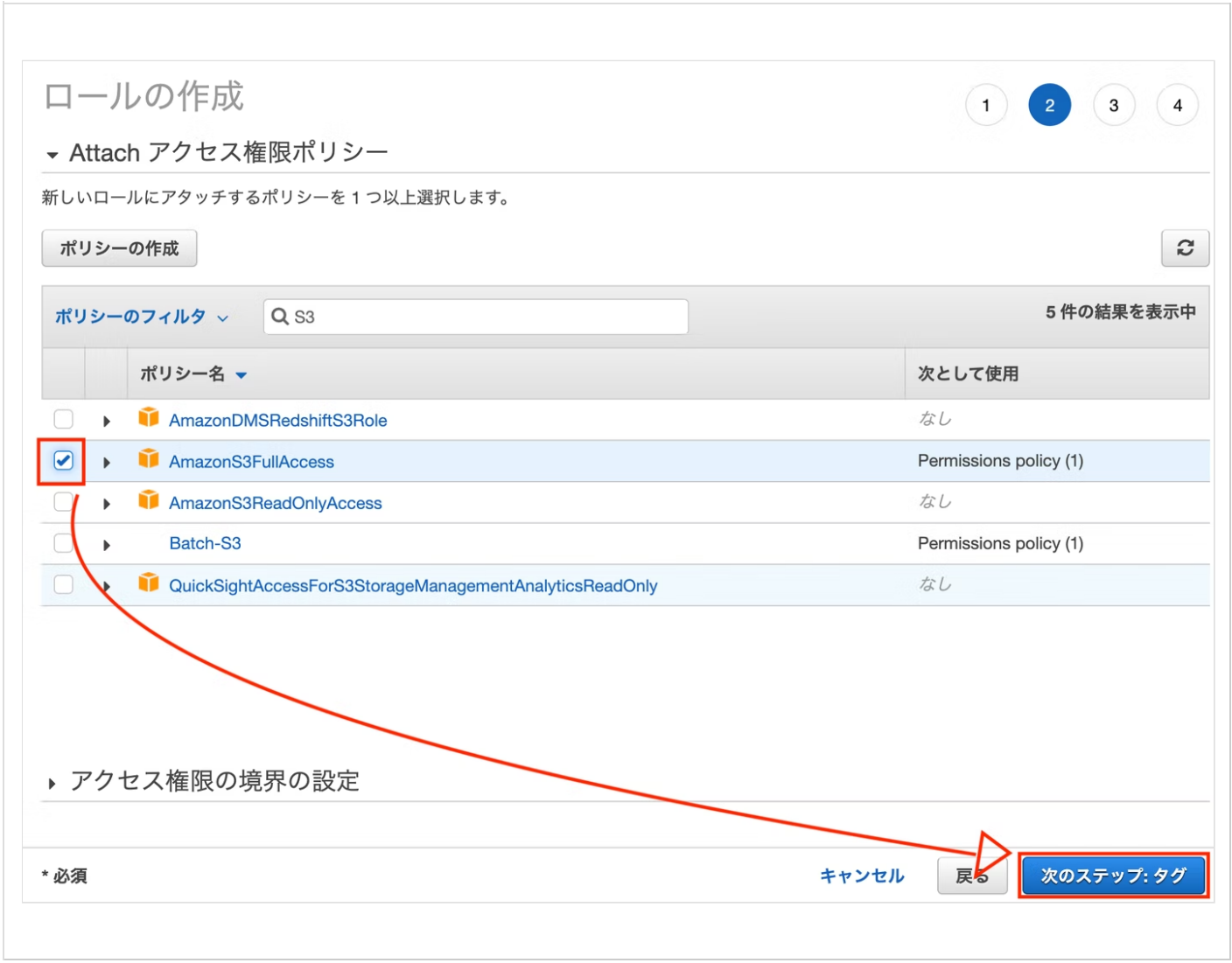
AWSマネジメントコンソールから「IAM」と検索し、「IAMマネジメントコンソール」に移動します。
IAMマネジメントコンソールの左ペイン、「ロール」を選択し、「ロールの作成」を選択します。


ユースケースは「EC2」を選択し「次のステップ」を選択します。




「AmazonS3FullAccess」を選択し、「次のステップ」を選択します。

※「ポリシーのフィルタ」で「S3」を入力すると良きです。




設定しなくても大丈夫ですが、「Name」キーの設定を行いました。


「ロール名」、「ロールの説明」を入力し、「ロールの作成」を選択します。

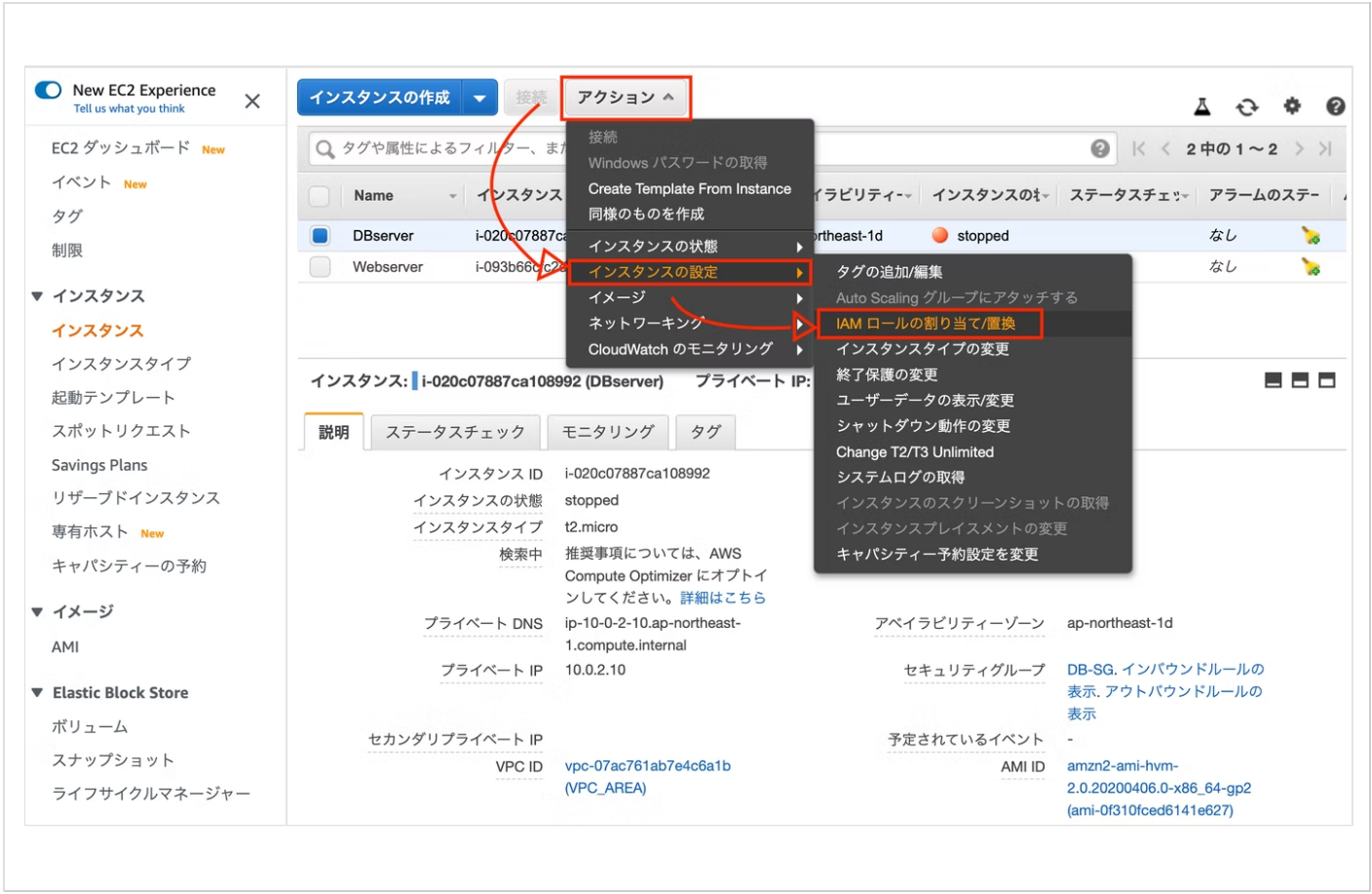
※ロール名は先ほどの「Name」キーと同様の値にしています。ロールの説明は適当でも大丈夫です。


ここまでで、S3へのアクセス権を持った、IAMロールの完成です。

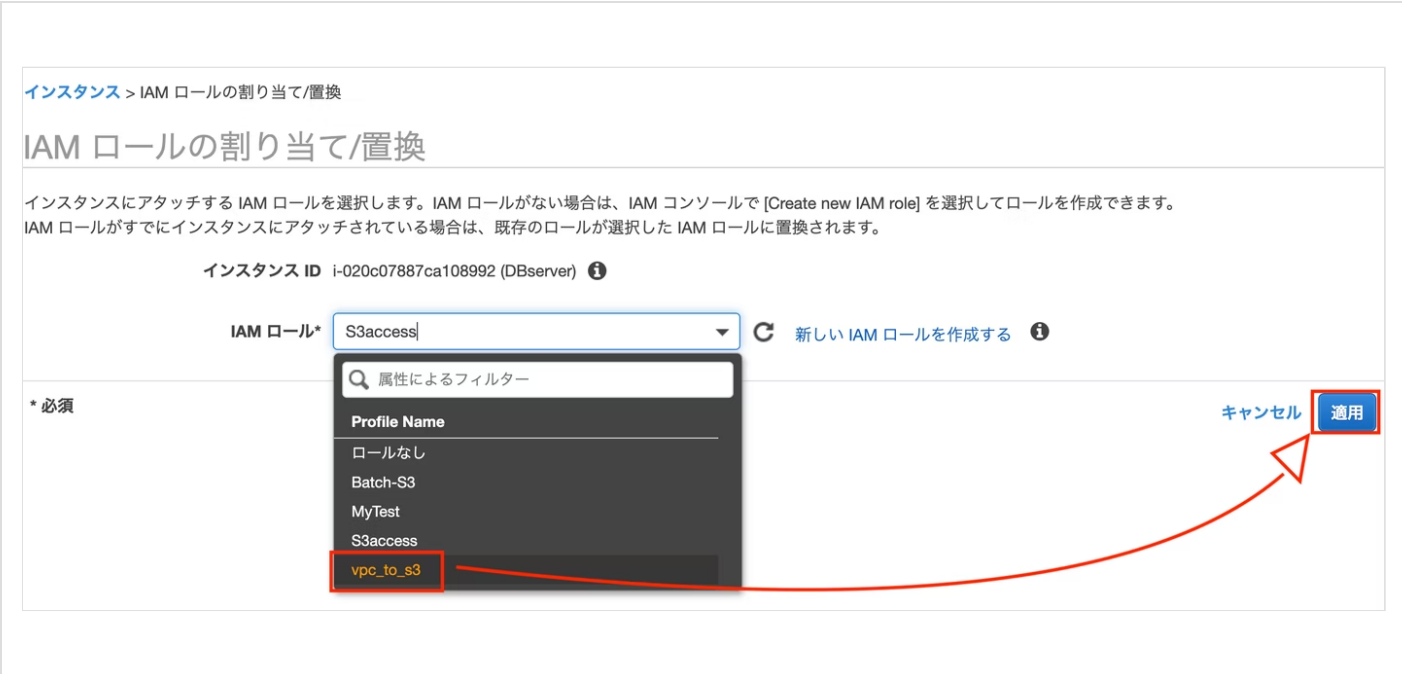
続けて、作成したIAMロールをインスタンスへ割り当てます。

「EC2マネジメントコンソール」に移動して、インスタンスを選択後、「アクション」、「インスタンスの設定」、「IAMロールの割り当て/置換」を選択します。

なお、インスタンスが停止していると割り当てに失敗しますので、起動状態でお願いします。
下の画面はインスタンスが停止しているので、この後失敗します。




先ほど作成したロールを選択して、「適用」を選択します。




これでIAMロールに準じたアクセス権限がインスタンスにされたことになります。
今回は、「AmazonS3FullAccess」がインスタンスに付与されたことになります。

また、プライベートサブネット内のインスタンスに割り当てたので、VPCエンドポイントもNATゲートウェイもない今の状態では、S3へは接続できません。

実際にプライベートサブネット内のインスタンスに接続して確認してみます。

```
# 自分のPCから
$ ssh ec2-user@18.177.121.50 -i my-key.pem
```

```
# パブリックサブネットのインスタンスから
[ec2-user@10.0.1.10 ~]$ ssh ec2-user@10.0.2.10 -i DBserver

# プライベートサブネットのインスタンスから
[ec2-user@10.0.2.10 ~]$ aws s3 ls
```

下図のようにプロンプトが戻ってきませんので、「Ctrl」＋「C」でAbortしましょう。

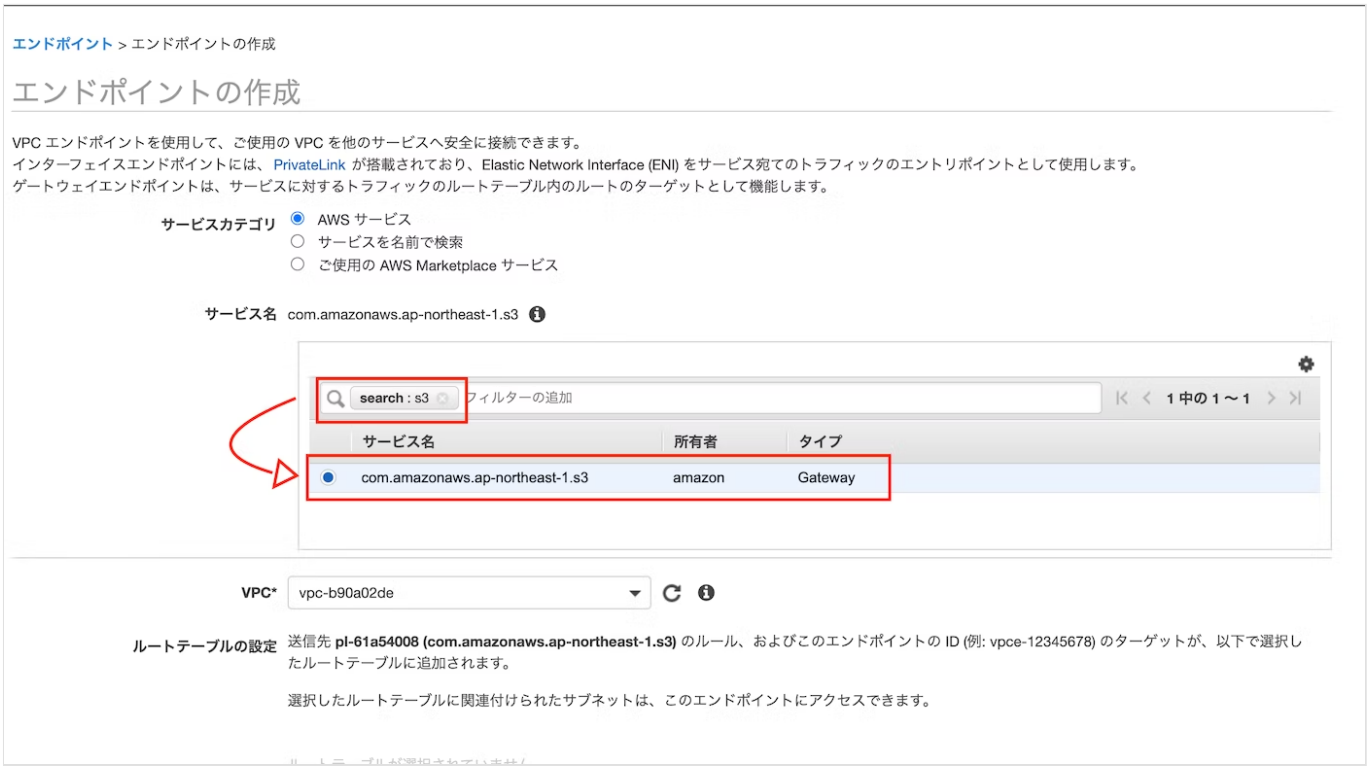
```
https://aws.amazon.com/amazon-linux-2/
26 package(s) needed for security, out of 62 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-2-10 ~]$
[ec2-user@ip-10-0-2-10 ~]$
[ec2-user@ip-10-0-2-10 ~]$
[ec2-user@ip-10-0-2-10 ~]$
[ec2-user@ip-10-0-2-10 ~]$ aws s3 ls
```

# VPCエンドポイントの作成・設定

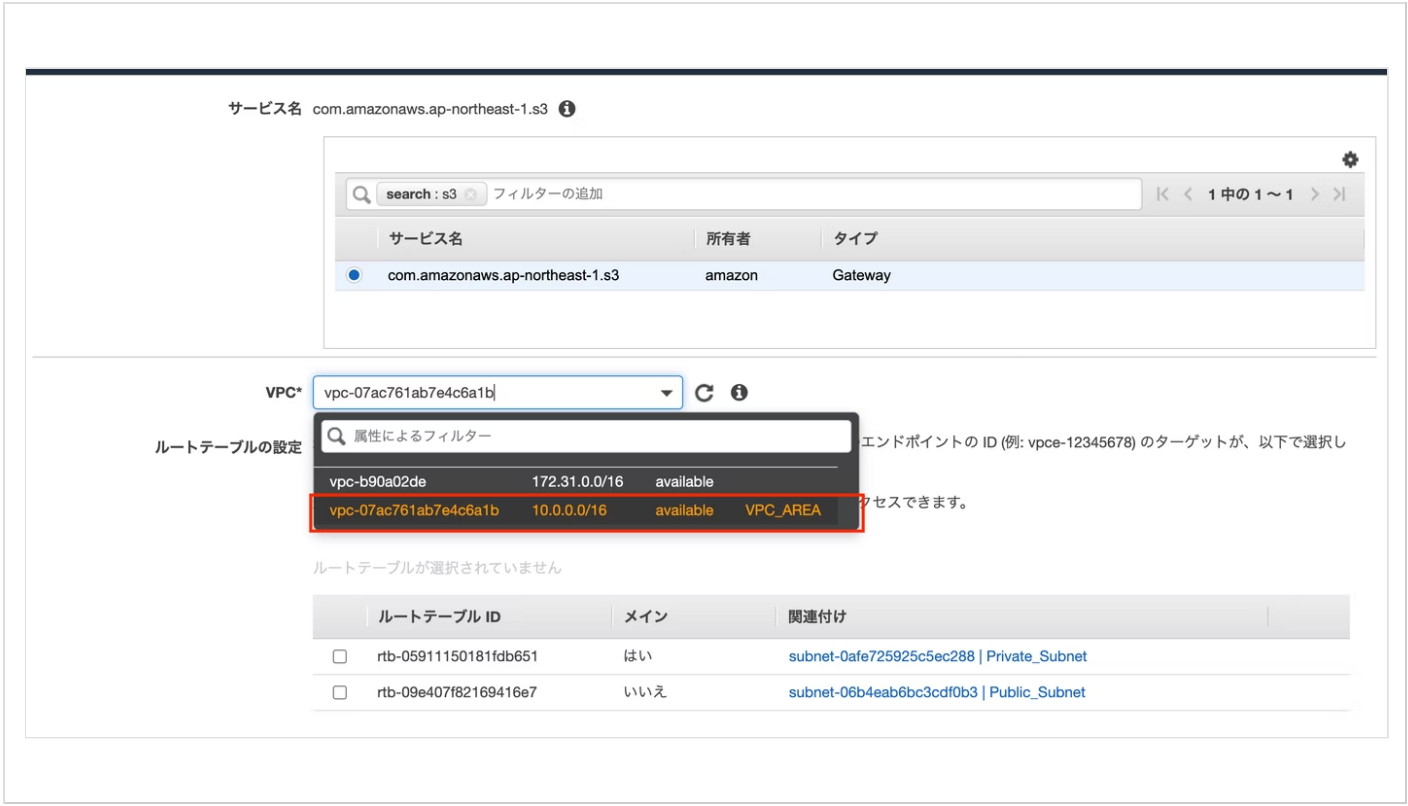
続いてVPCエンドポイントを作成します。

VPCダッシュボードから、左ペインの「エンドポイント」を選択します。

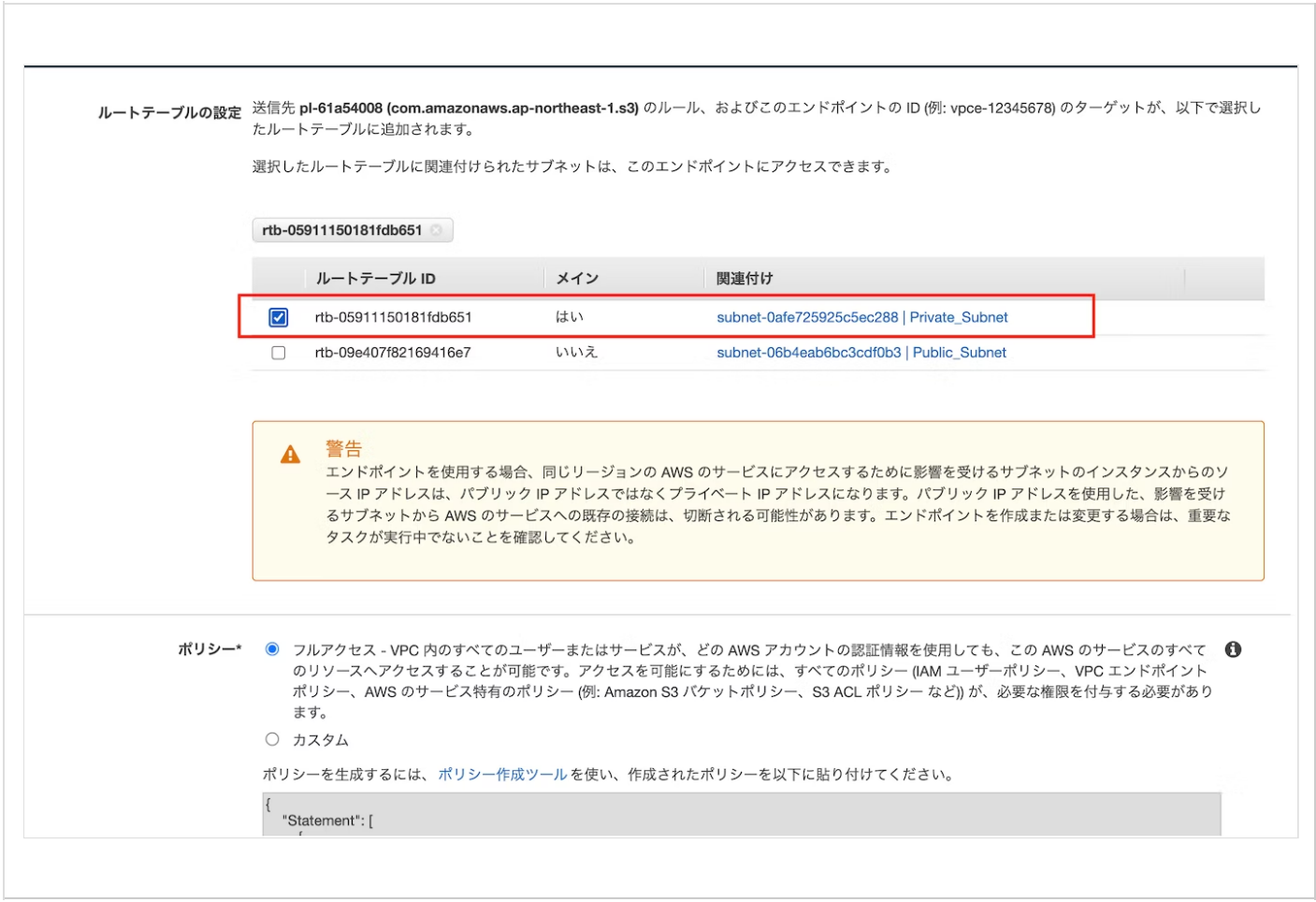

「S3」でフィルタをかけて、表示されたサービスを選択します。



vpcは自身で作成したvpcを選択します。

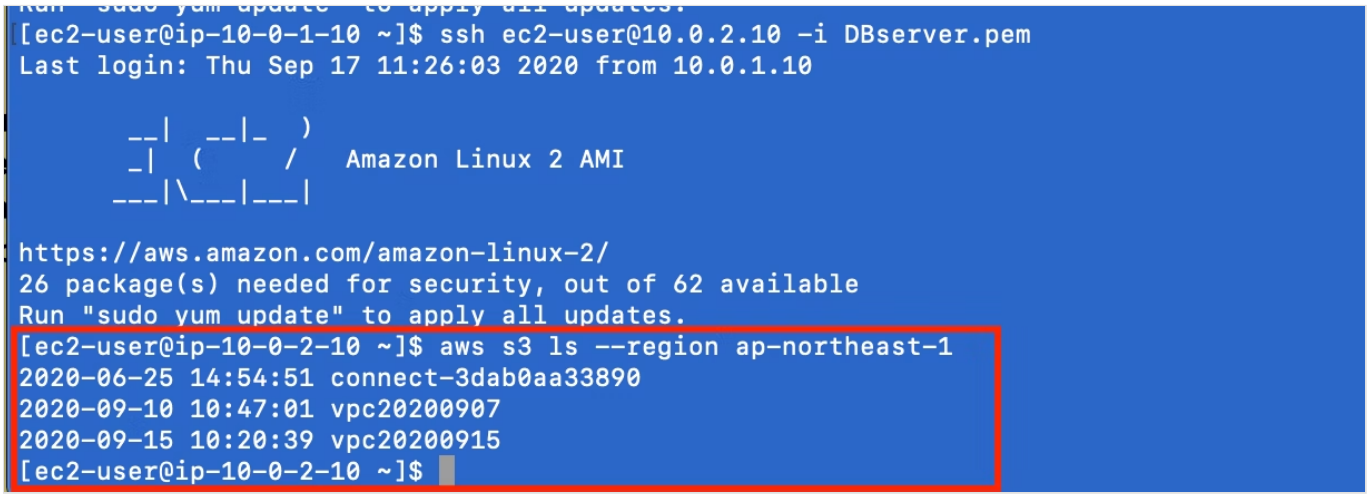



プライベートサブネットに属しているルートテーブルを選択します。




ポリシーは変更せず、「エンドポイントの作成」をすると完成です！！

先ほどと同様の手順で確認をしてみると。。。



「aws s3 ls」コマンドで応答が帰ってこなかったため、以下コマンドを使用しています。

```
$ aws s3 ls --region ap-northeast-1
```

# 少し補足

VPCエンドポイントには２種類あり、今回使用したのは無料のGateway型です。
Privatelink型は有料だそうです。

| 名前 | 実装方法 |
| --- | --- |
| Gateway型 | エンドポイントポリシーをルートテーブルに設定することで直接アクセスする |
| Privatelink型 | サブネットがエンドポイント用のIPを持ち、それをDNSが名前解決することでルーティングする |

# 参考文献

- これだけでOK！ AWS 認定ソリューションアーキテクト – アソシエイト試験突破講座（SAA-C02試験対応版

- そのトラフィック、NATゲートウェイを通す必要ありますか？適切な経路で不要なデータ処理料金は削減しましょう
- AWSの公式ドキュメント VPCエンドポイント

最後までお付き合いいただきありがとうございました💝