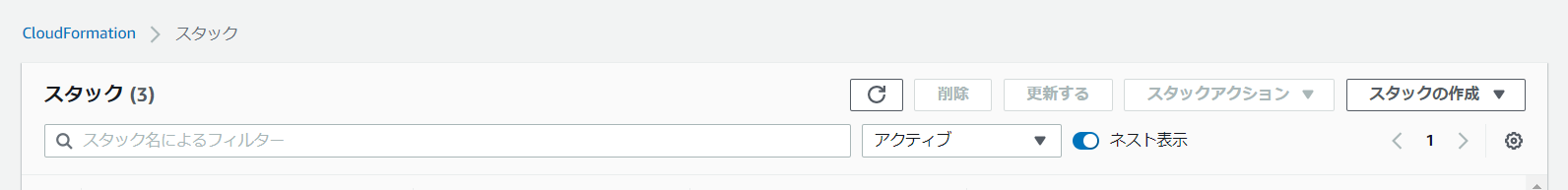
VPC Reachability Analyzer ワークショップ

2021/03/12

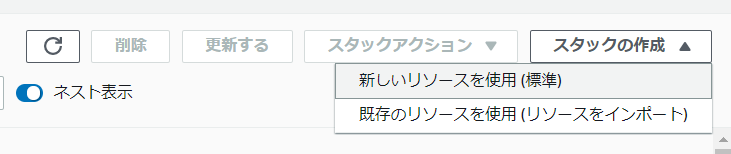
亀田 治伸

シニアエバンジェリスト

1. CloudFormationによる環境の構築
   1. 作業はすべてバージニア北部で行います。CloudFormationのマネージメントコンソール上で「スタックの作成」ボタンをおします



* 1. 「新しいリソースを仕様（標準）を押します」

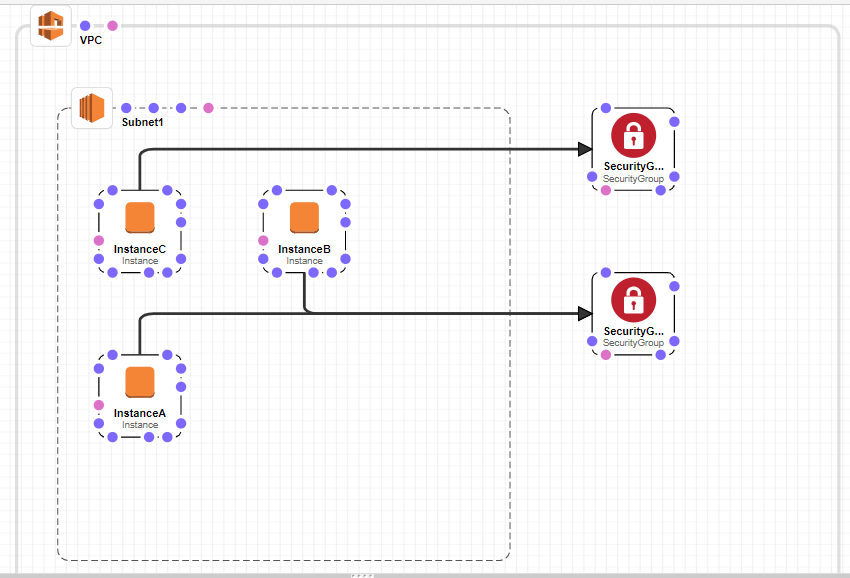


* 1. 以下のURLからファイルをダウンロードしどこか適当なところに保存します

<https://github.com/harunobukameda/VPC-Reachability-Analyzer/blob/main/vpcreachabilityanalyzertestenvironment.yaml>

* 1. 「テンプレートファイルのアップロード」から上記でダウンロードしたテンプレートをアップロードし、「次へ」ボタンをおします。中身に興味がある方は、「次へ」を押す前に「デザイナーで表示」ボタンをおして今から作成しようとしている環境のダイアグラムを見てみてください。



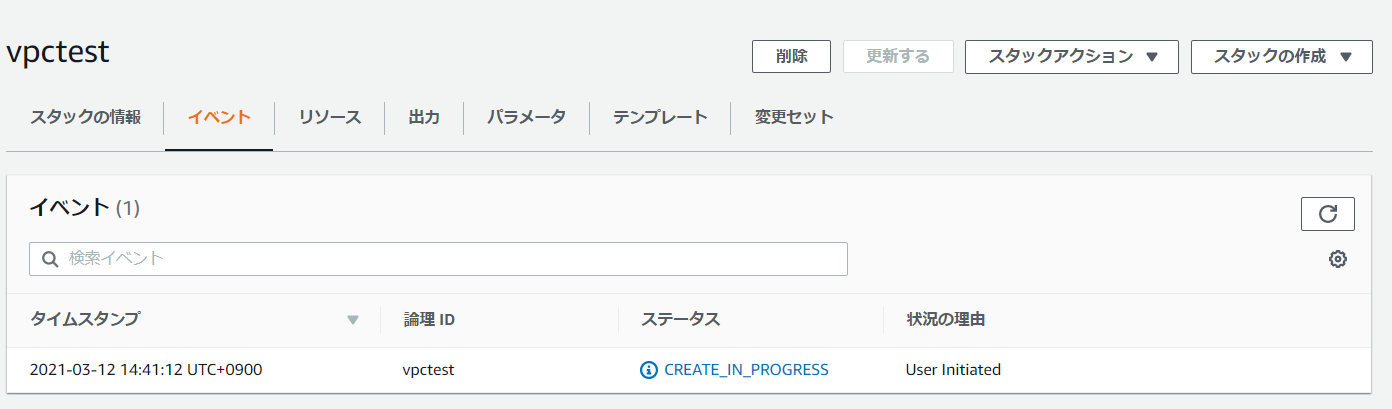


この環境では、1つのVPC,3つのEC2インスタンス、2つのセキュリティグループを作ります。インスタンス A と B は相互に通信できますが、インスタンス C にアタッチされたセキュリティグループでは着信トラフィックが許可されないため、それら 2 つのインスタンスはインスタンス C と通信ができません。

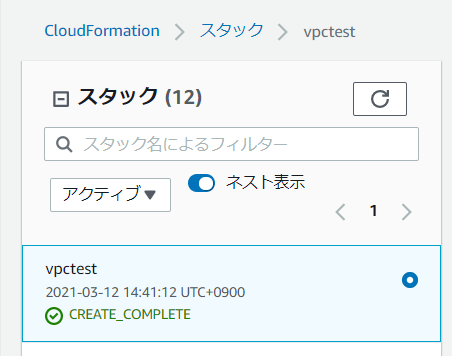
* 1. スタックの適当な名前を付けて「次へ」を押します。次の画面は全てデフォルトのまま「次へ」を再度押します。



* 1. 最後の確認画面で「スタックの作成」を押します。以下の様に構築中の画面になりますので少しまちます。



* 1. 以下のようになれば構築が完了です。



CloudFormationのリソースタブで出力されたVPCID、3つのインスタンスIDを控えておきます。

* 1. EC2マネージメントコンソールで、それぞれ[A][B][C]という名前を生成された3つのインスタンスに指定します。（A,BとCは技術統制が異なるので、必ず上記手順と同じ指定となるようにしてください）

1. VPC Reachability Analyzerの確認
   1. VPCマネージメントコンソールの左ペインで、[Reachability Analyzer]をクリックします

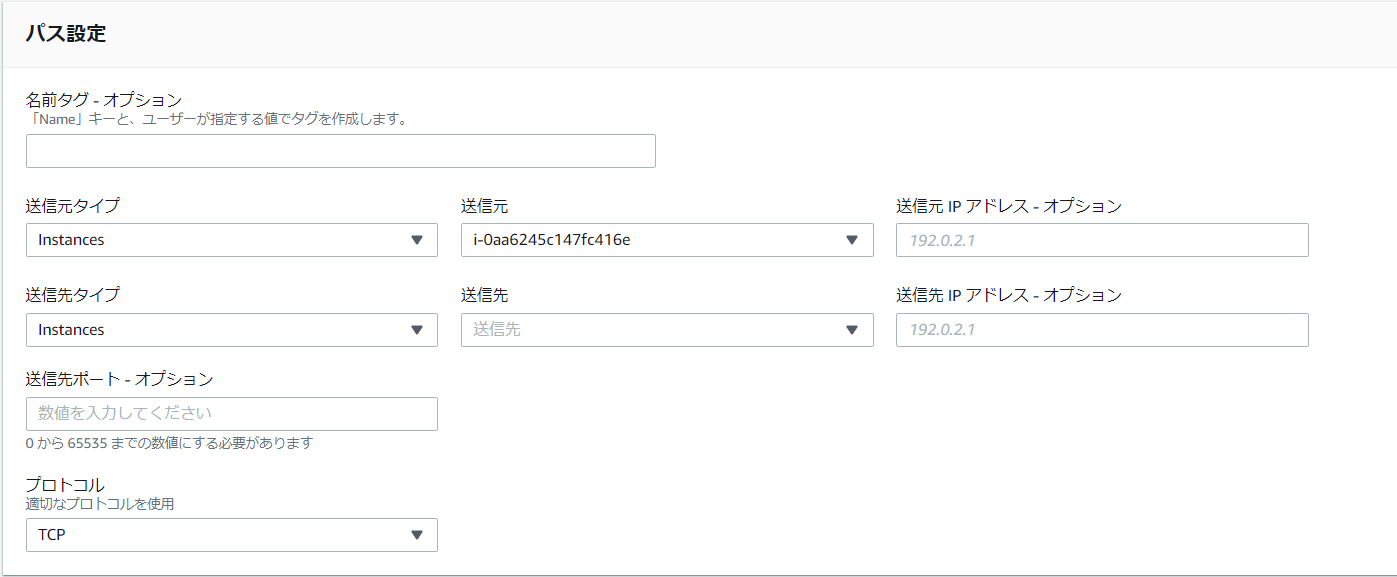


* 1. 「パスの作成と分析」をおします



* 1. 適当な名前を入力し、送信元タイプで「Instances」、送信元で「A」、を選択します。同様に2番目の送信元タイプで「Instances」、送信先で「B」、を選択します。

ポート、プロトコルはそのままで「パスの分析と作成」を押します



* 1. しばらく待つと、分析結果が表示されます

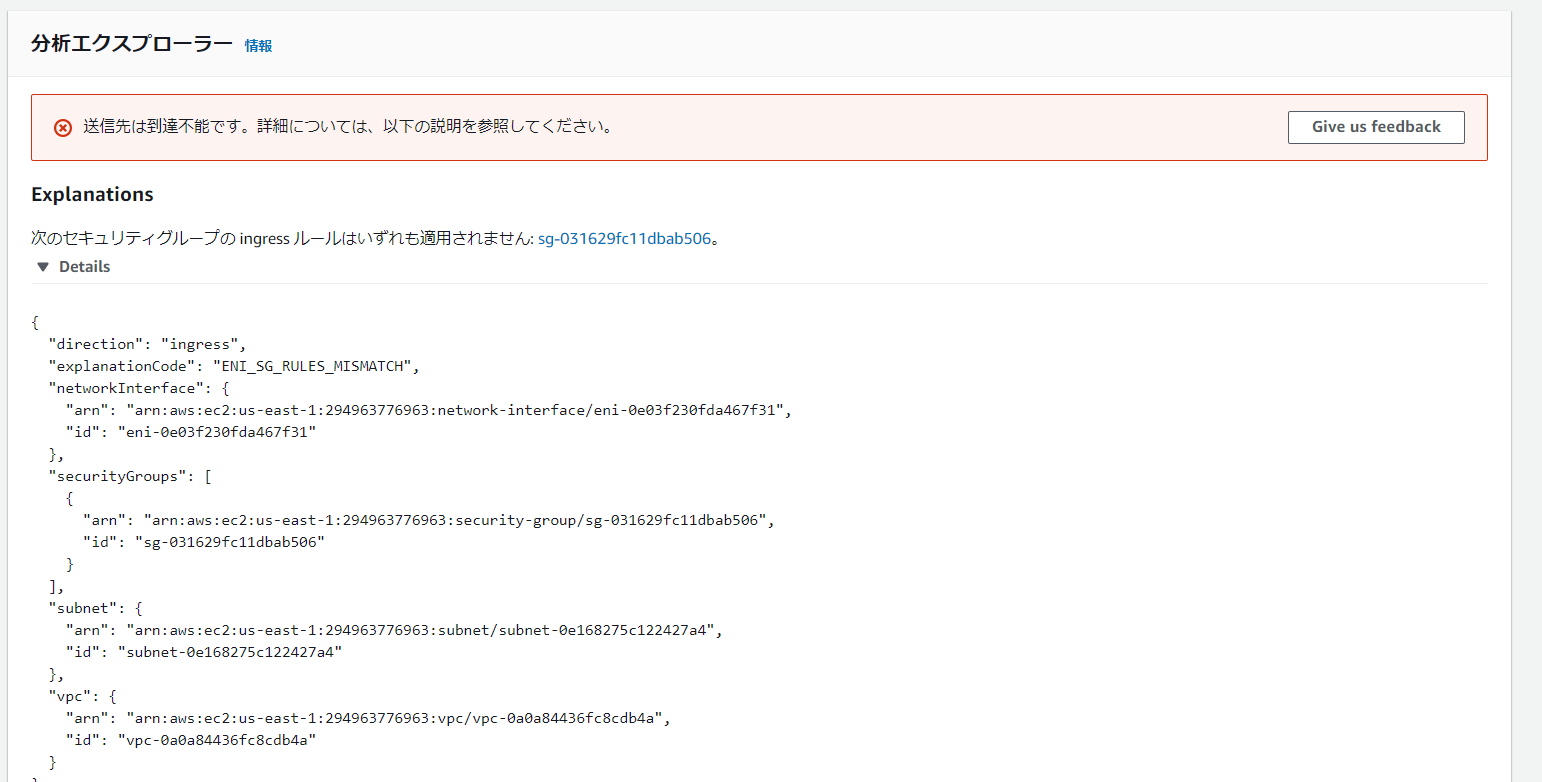


AからBは疎通できていることが確認できます。

* 1. 新しくAからCへの分析を同様の手順で作成します。しばらく待つと「到達不可能」として分析が完了します



* 1. 以下のように、とあるセキュリティグループがingressルール（インバウンド通信）を許可していないため、不達となったことがわかります。



* 1. セキュリティグループをクリックします。「インバウンドルールを編集」を押します



* 1. 以下のようにTCPをインバウンドで設定し、「ルールを保存」を押します



* 1. 先ほどの分析に戻り、「パスの分析」を押して、再実行します



* 1. オプションで通るべきパスを指定する画面がでてきますが、空欄のまま「確認」をおします



* 1. 次は到達可能として分析が成功します



1. 異なるVPCへの疎通 VPC Peering
   1. これからの手順は複数のVPCを利用するため、非常にID表示などがややこしく、以下のパラメータをまずメモ帳などにメモったのち作業を始めましょう。

・今日作成したVPCID

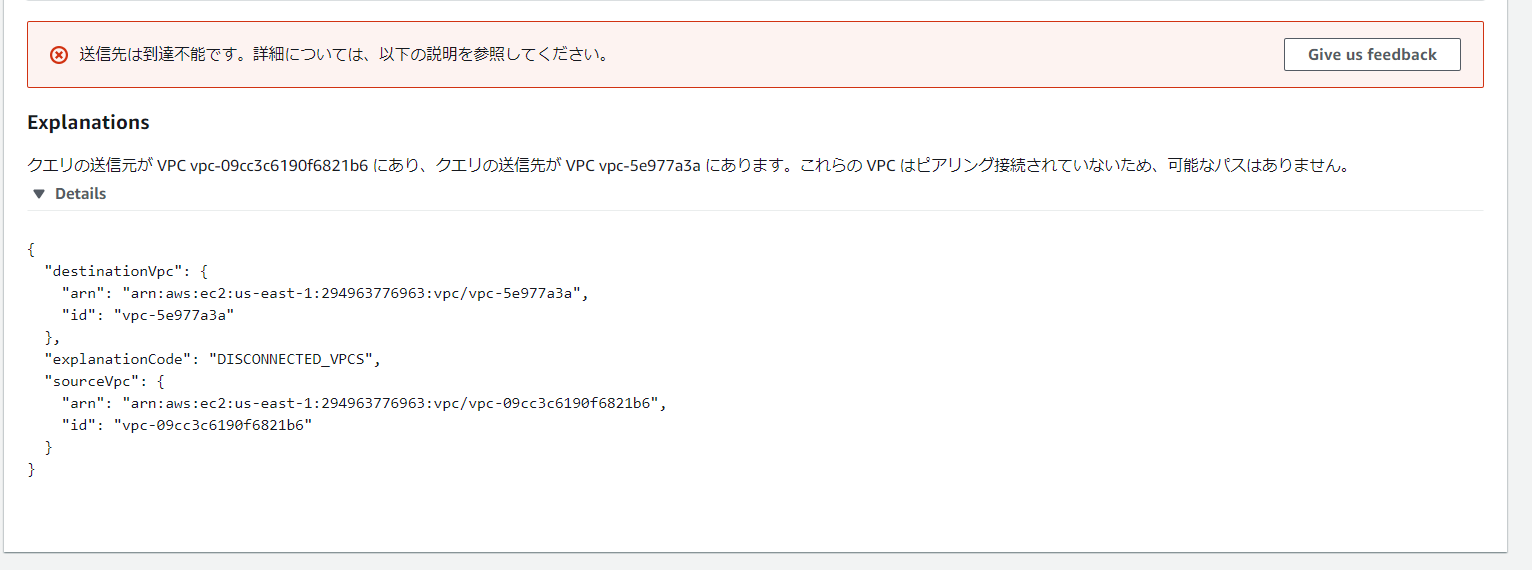
・今日作成したVPCIDのIPv4 CIDR

・AインスタンスのID

・バージニア北部リージョンのデフォルトVPCID

・上記デフォルトVPCのIPv4 CIDR

* 1. デフォルトVPCが存在していない場合、別のVPCでも作業可能です。まずVPC内にEC2を1個作成します。OS、インスタンスタイプ、サブネットはなんでもかまいません。ログインしませんので、pemキーの保存などは不要です。EC2のidを上記メモに追記します。
  2. 作成されたインスタンスに[handson-target]と名前を付けておきます
  3. 先ほどと同じ手順でVPC Reachability Analyzerの分析を、送信元「A」、送信先「handson-target」で作成し、実行します。以下のエラーが出力されます。

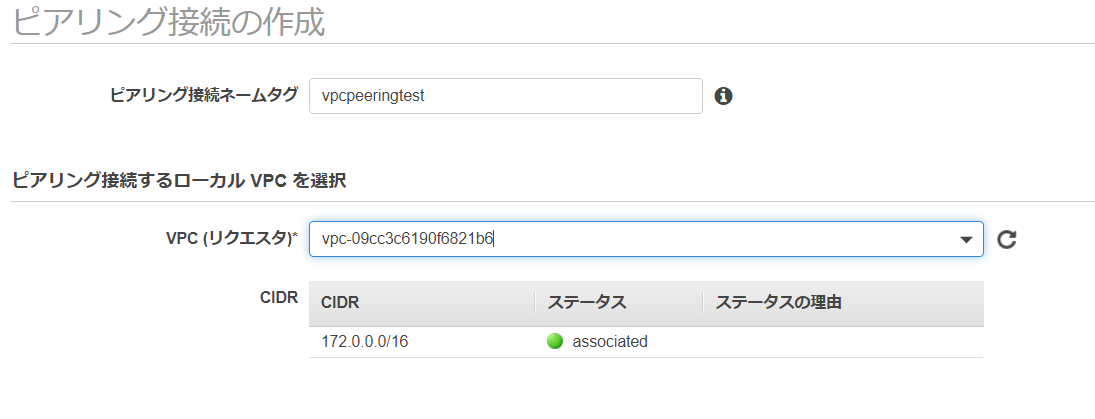


* 1. VPCマネージメントコンソールの左ペインから「ピアリング接続」を選び、「ピアリング接続の作成」ボタンをおします





* 1. ネームタグに「vpcpeeringtest」と名付け、リクエスタに今日作成したVPCのIDを設定します



* 1. もうひとつのVPCを選択、の画面でデフォルトVPCのIDを選び、「ピアリング接続の作成」ボタンをおします



* 1. 「承諾の保留中」スタータスの接続がありますので、そちらを選んでアクションから「リクエストの承諾」を選びます。ダイアログが出てきますので「はい、承諾する」をおします



次の画面ではお互いのVPCの相互通信を成立させるために必要なルートテーブルの設定喚起が出ていますが、一旦画面を閉じます。メモ帳に作成されPeeringのIDを記載しておきます。（pcx-xxxxxxx…）

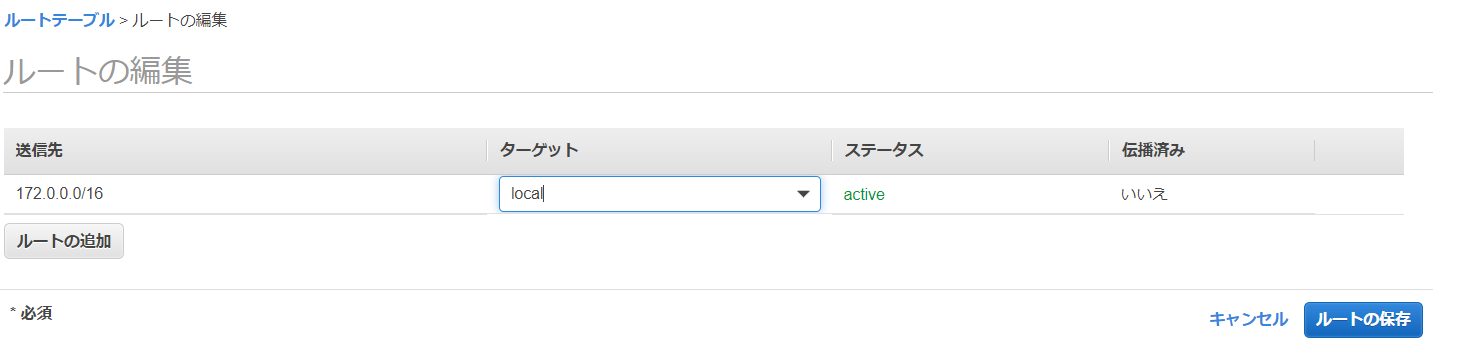
* 1. 再度VPC Reachability Analyzerの画面で新しい分析を作成します。今度は送信元をインスタンスA、送信先を「VPC Peering test」とします。以下の通り今日作成したVPCからデフォルトVPCへ通信をルーティングさせる設定がないため、失敗します



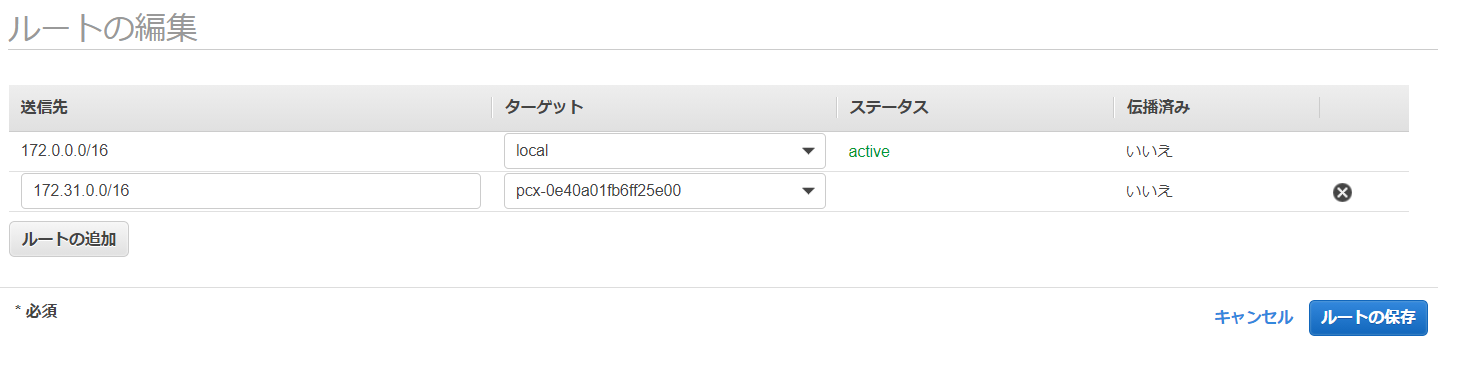
* 1. VPCのマネージメントコンソールから今日作成したVPCの詳細画面へいき、ルートテーブルIDを特定します。(上記エラーで表示されているルートテーブルIDを右クリックでも遷移します)　クリックするとルートテーブル設定画面へ遷移します



* 1. アクションから、「ルートの編集」をえらびます



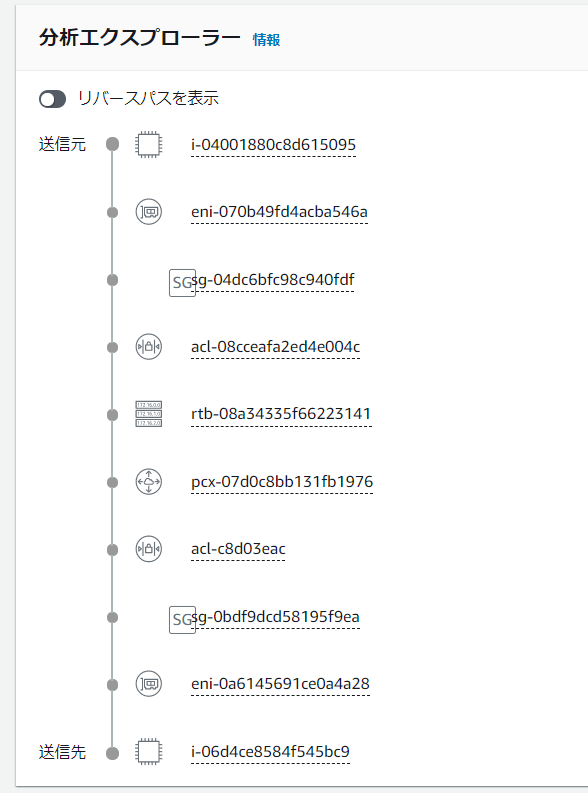
* 1. 現時点での設定では、今日作成したVPC内部のみが設定されていますので、先ほどPeeringしたデフォルトVPCへのルートを追加します。ターゲットにはデフォルトVPCのIDではなく、Peering Connectionを選びます。以下のような画面になったら「ルートの保存」を押します。ここで入力されているIPアドレスブロックは、先ほどメモをしたデフォルトVPCのブロックです



* 1. 再度先ほどの分析を実行すると以下のようにVPC Peeringまでの疎通の確認ができました。ルートテーブルの反映は少し時間がかかるため、エラーとなる場合は、1分程度たってから再度分析を実行してみてください



* 1. 再度新しい分析を作成して、送信元とA,送信先をhandson-targetとして、分析を実行します。以下のエラーが出力されます。作成したVPCからデフォルトVPCへのルートはできましたが、デフォルトVPCから今日作成したVPCへのルートがないためです。同様の手順でルートテーブルを設定し、分析を実行すると以下のように成功します。

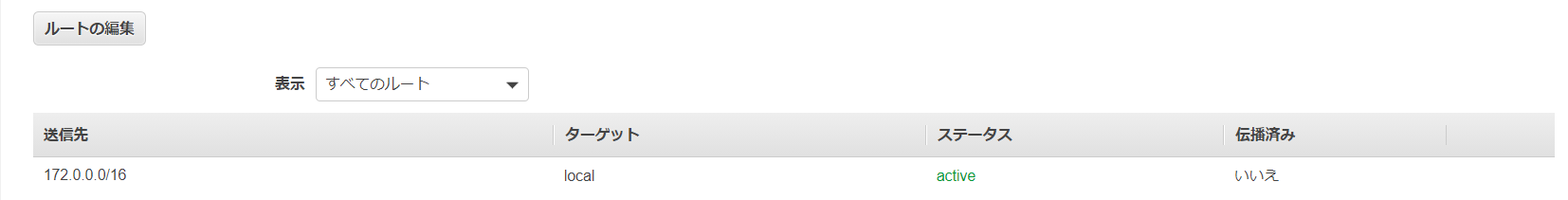


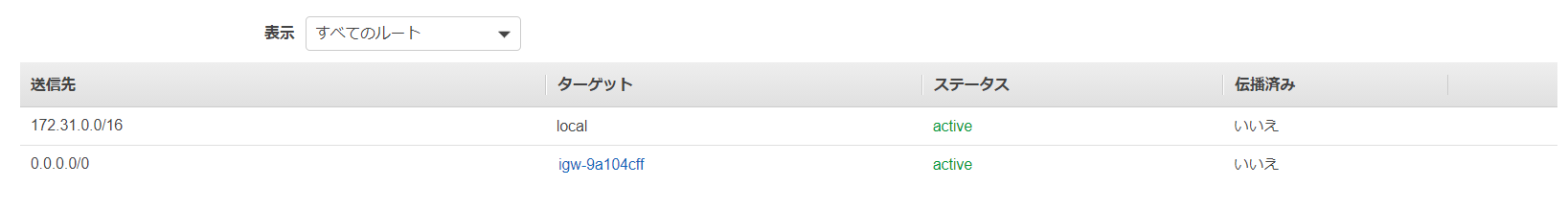
* 1. VPマネージメントコンソール、左ペインからピアリング接続の設定を、アクションボタンのドロップダウンから削除して、再度分析を行ってください。以下のように到達不可能となります。タイミングで異なるエラーが出る場合がありますが、到達不可能となっていればこの手順では正解です



* 1. ２つのルートテーブルから、VPC Peering向けのルートを削除します。

それぞれ以下が正しい状態です。





1. おつかれさまでした

削除は、

CloudFormationスタック

デフォルトVPCのEC2インスタンス

を行ってください。