classmethod

AWS re:Invent ふりかえり勉強会

CLASSMETHOD

re:Growth2024

札幌

2024.12.12 木 18:30-21:00

classmethod

Amazon VPC Lattice 最新アップデート紹介

PrivateLink も似たようなアップデートあったけど違いとは

2024/12/12

AWS事業本部コンサルティング部

大村 保貴

自己紹介

大村 保貴 (Yasutaka Ohmura)

クラスメソッド株式会社
AWS事業本部 コンサルティング部
ソリューションアーキテクト

出身

- 網走
- 今年のふるさと納税に**網走のホタテ**はいかがでしょうか

仕事

- エンプラ企業中心にAWSやSaaSを利用した環境の設計などの技術支援
- HPC（スパコン）、ライフサイエンス分野を勉強中

経歴

- オンプレのインフラのコンサル→ IoTサービスのインフラ → クラスメソッド

受賞

- 2021, 2023, 2024 Japan AWS Top Engineers
- 2022 - 2024 Japan AWS All Certifications Engineers

セッション対象者とゴール

想定対象者

・VPC間接続できるサービスの種類はなんとなく知っている

ゴール

・VPCに追加された新しいリソースを知ってもらう

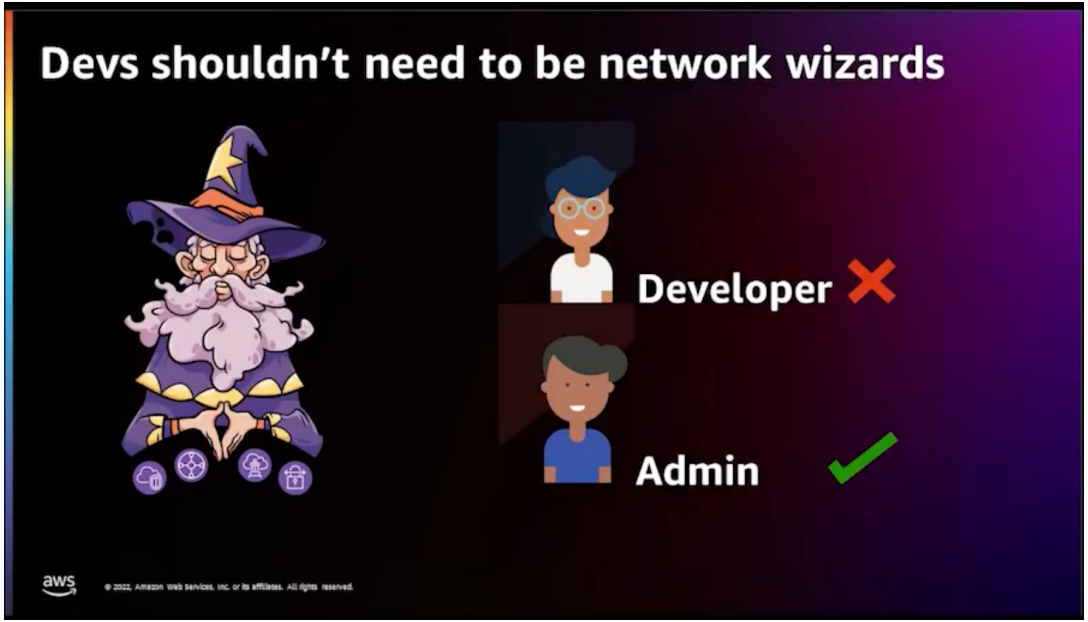
・VPC LatticeとPrivateLinkの接続方法の違いを知ってもらう

VPC Lattice 使ったことあるかた 🙋

VPC Lattice とは

VPC Lattice とは

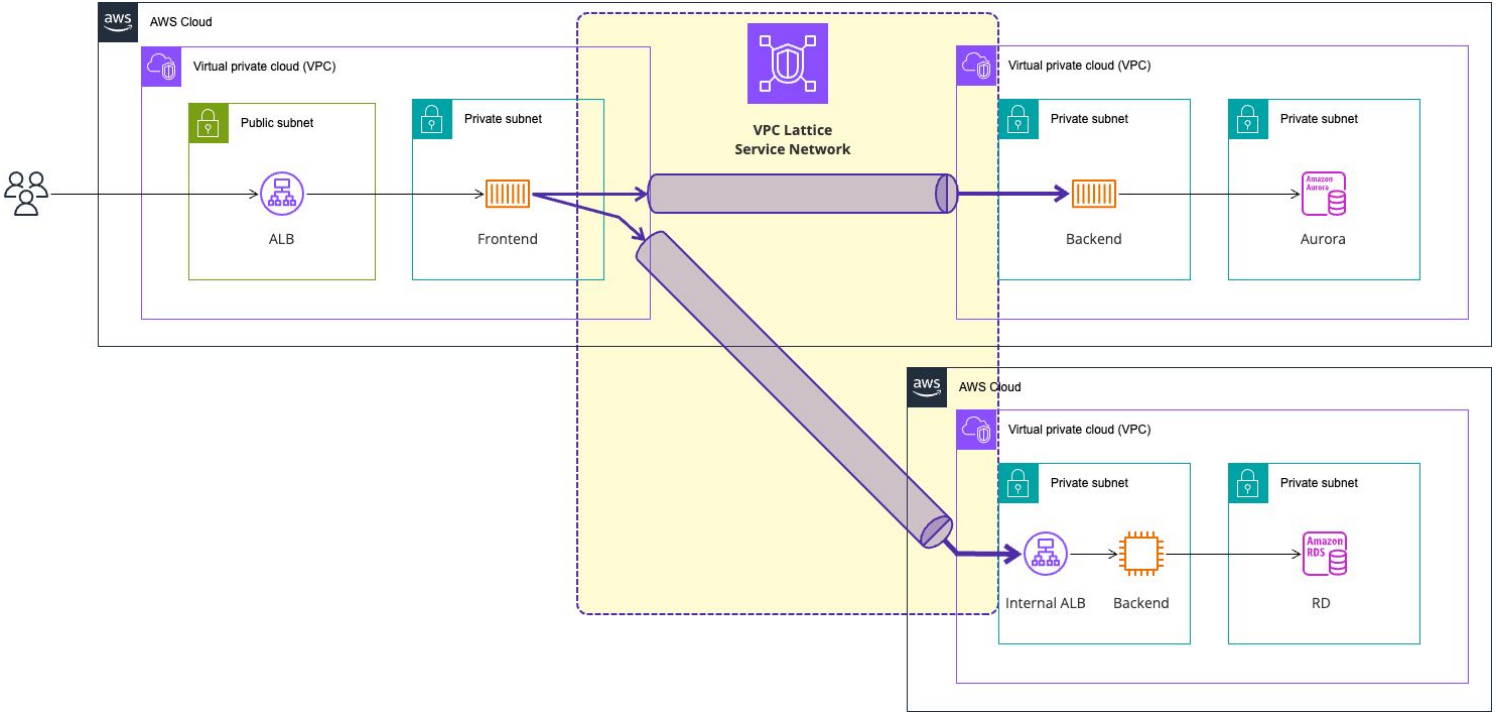
アプリケーション向けのVPC間通信サービス



引用: [AWS re:Invent 2022 - [NEW] Introducing Amazon VPC Lattice: Simplifying app networking (NET215)]

VPC Lattice とは

VPCやアカウントを跨いでAPIを提供するようなマイクロサービスにマッチ



VPC Lattice とは

ネットワーク周りの設定が抽象化されており、苦手意識のある人にも易しい

- L3のルーティング設定が不要（ルートテーブル自動作成）
- VPC間のCIDRが重複していても問題なし
- クロスアカウント接続もResource Access Maneger（RAM）で共有するだけ

TCP接続できるアップデートがあった

VPC Latticeアップデート

VPC Lattice now includes TCP support with VPC Resources

Posted on: Dec 2, 2024

With the launch of VPC Resources for Amazon VPC Lattice, you can now access all of your application dependencies through a VPC Lattice service network. You're able to connect to your application dependencies hosted in different VPCs, accounts, and on-premises using additional protocols, including TLS, HTTP, HTTPS, and now TCP. This new feature expands upon the existing HTTP-based services support, enabling you to share a wider range of resources across your organization.

With VPC Resource support, you can add your TCP resources, such as Amazon RDS databases, custom DNS, or IP endpoints, to a VPC Lattice service network. Now, you can share and connect to all your application dependencies, such as HTTP APIs and TCP databases, across thousands of VPCs, simplifying network management and providing centralized visibility with built-in access controls.

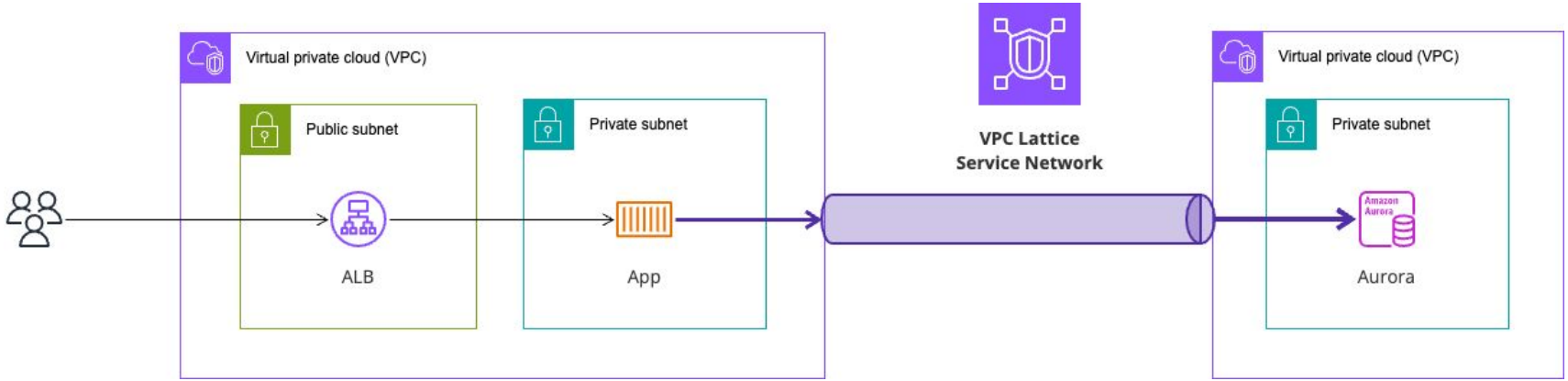
VPC Resources are generally available with VPC Lattice in Africa (Cape Town), Asia Pacific (Mumbai), Asia Pacific (Singapore), Asia Pacific (Sydney), Europe (Frankfurt), Europe (Ireland), Europe (Paris), Europe (Stockholm), Middle East (Bahrain), South America (Sao Paulo), US East (N. Virginia), US East (Ohio), US West (Oregon).

To get started, read the VPC Resources launch blog, architecture blog, and VPC Lattice User Guide. Learn more about VPC Lattice, visit Amazon VPC Lattice Getting Started.

引用: VPC Lattice now includes TCP support with VPC Resources

今回のアップデート

VPCを跨いで直接データベースに接続するような使い方もできるようになった



VPC Lattice アップデート

VPC Latticeアップデート

新たに3つのコンポーネントが追加され、TCP接続ができるようになりました

- Resource Configuration
- Resource Gateway
- サービスネットワークタイプのVPCエンドポイント

VPC Latticeアップデート

VPC Lattice now includes TCP support with VPC Resources

Posted on: Dec 2, 2024

With the launch of VPC Resources for Amazon VPC Lattice, you can now access all of your application dependencies through a VPC Lattice service network. You're able to connect to your application dependencies hosted in different VPCs, accounts, and on-premises using additional protocols, including TLS, HTTP, HTTPS, and now TCP. This new feature expands upon the existing HTTP-based services support, enabling you to share a wider range of resources across your organization.

With VPC Resource support, you can add your TCP resources, such as Amazon RDS databases, custom DNS, or IP endpoints, to a VPC Lattice service network. Now, you can share and connect to all your application dependencies, such as HTTP APIs and TCP databases, across thousands of VPCs, simplifying network management and providing centralized visibility with built-in access controls.

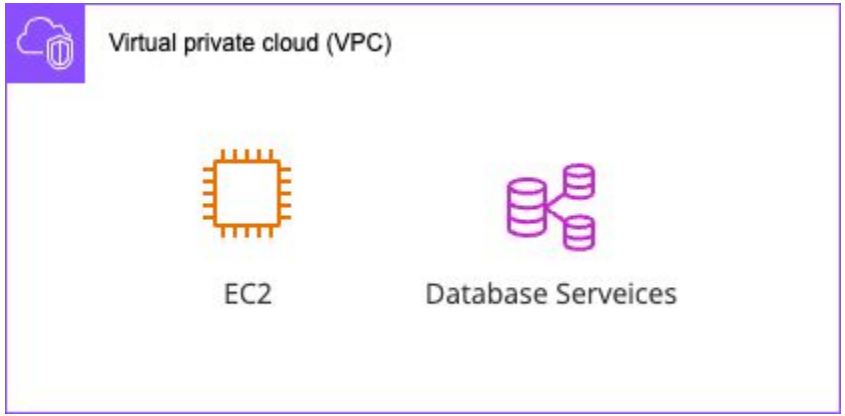
VPC Resources are generally available with VPC Lattice in Africa (Cape Town), Asia Pacific (Mumbai), Asia Pacific (Singapore), Asia Pacific (Sydney), Europe (Frankfurt), Europe (Ireland), Europe (Paris), Europe (Stockholm), Middle East (Bahrain), South America (Sao Paulo), US East (N. Virginia), US East (Ohio), US West (Oregon).

To get started, read the VPC Resources launch blog, architecture blog, and VPC Lattice User Guide. Learn more about VPC Lattice, visit Amazon VPC Lattice Getting Started.

引用: VPC Lattice now includes TCP support with VPC Resources

VPCリソースとは

VPC内にあるリソース全般のこと

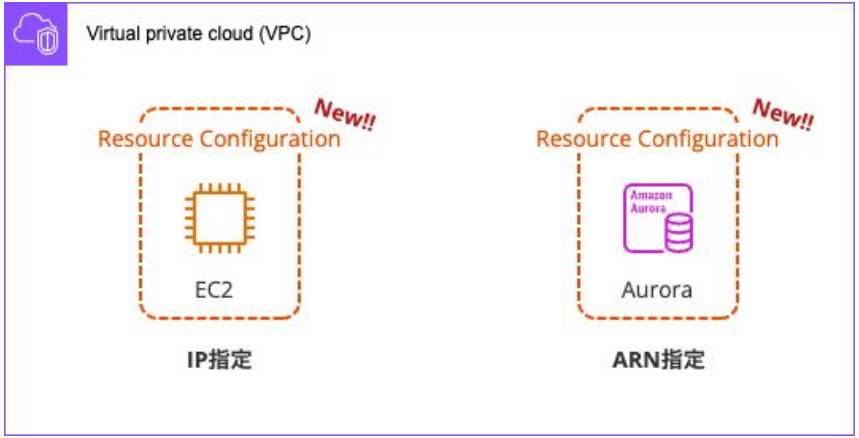


Resource Configurationとは

他のVPCから通信させたい**VPC内のリソースを指定**するのに使います

指定方法

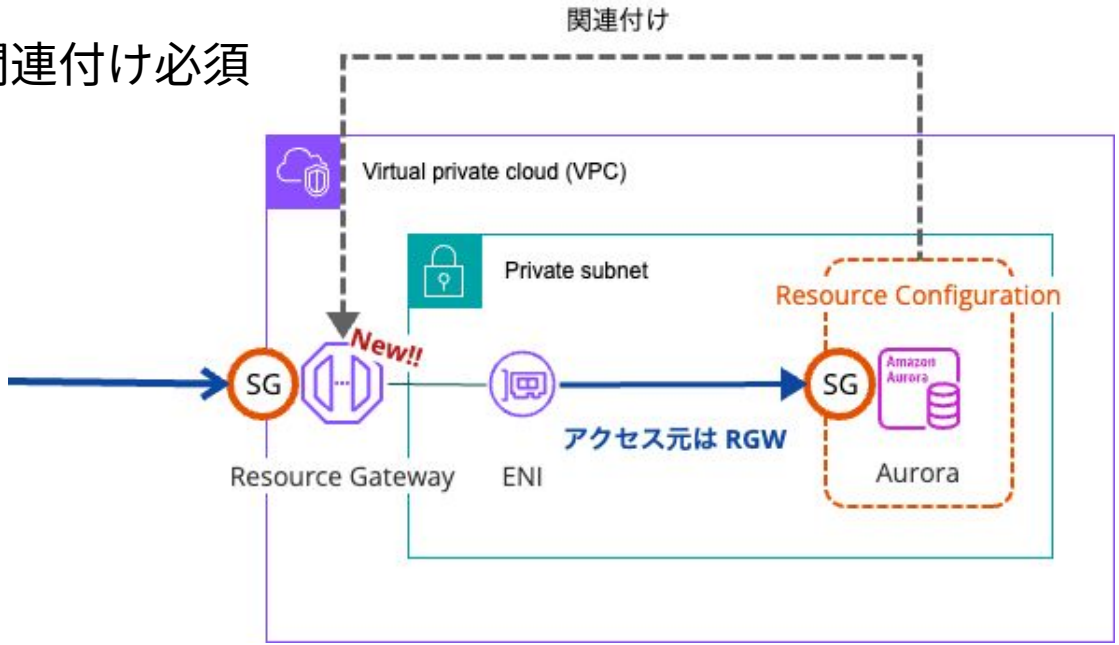
- VPC内のプライベートIPアドレス
- DNS名（プライベートホストゾーン未対応）
- ARN（現在はRDSのみ対応）



Resource Gatewayとは

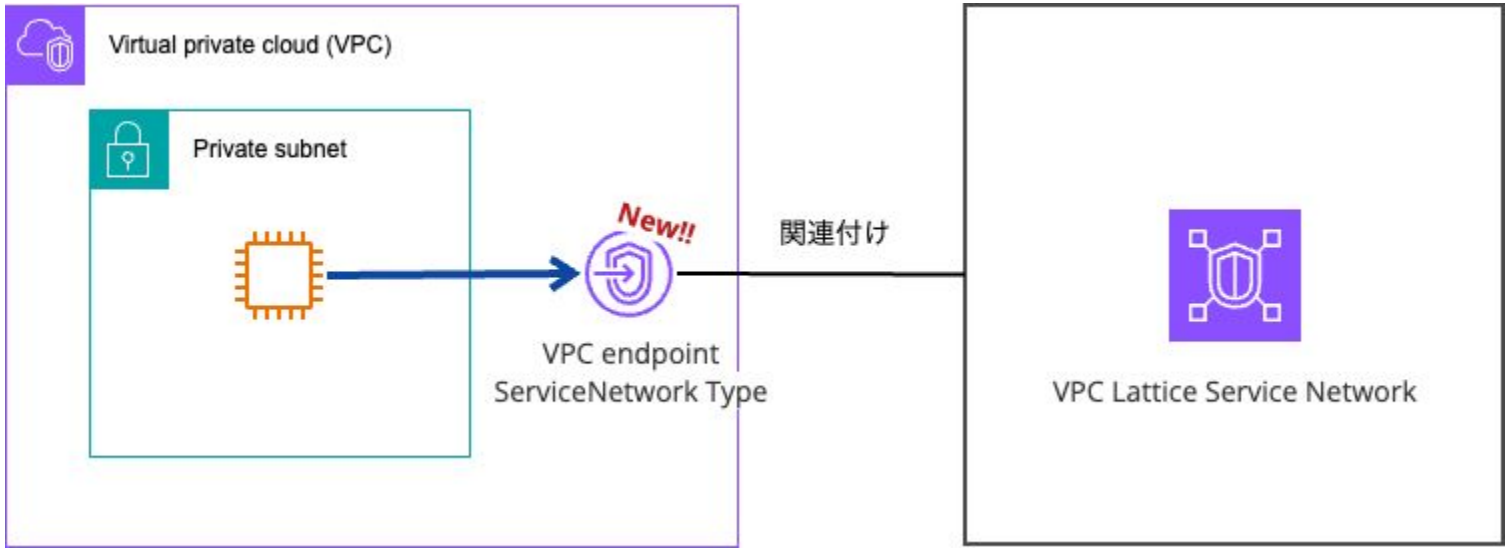
VPC内のリソースに**他のVPCからアクセスするための入口**

- VPCにアタッチ
- Resource Configurationと関連付け必須



VPCエンドポイントのサービスネットワークタイプ

VPC Latticeサービスネットワークへ接続するための専用経路



詳細

詳細はこちらのブログをご覧ください

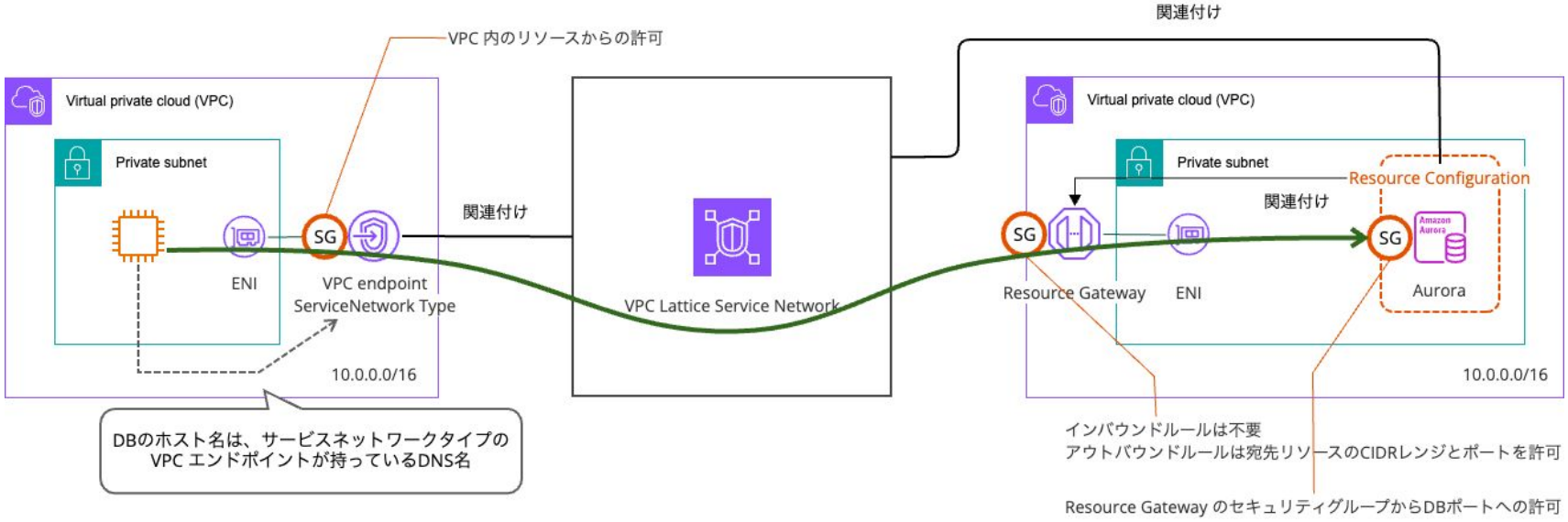
「ネットワークの新要素！Resource Gateway&Configuration関連アップデートまとめ」というタイトルでre:Growth 2024 東京に登壇しました #AWSreInvent #cmregrowth

とーち　2024.12.10

DevelopersIOブログリンク

DB接続するときの構成例

VPCエンドポイント利用する方法



DB接続するときの構成例

VPCエンドポイント利用する方法

vpce-0c6288af9ac0c9de9 / source-sn-endpoint

詳細 | サブネット | セキュリティグループ | 関連付け | タグ

エンドポイントの関連付け (2) 情報

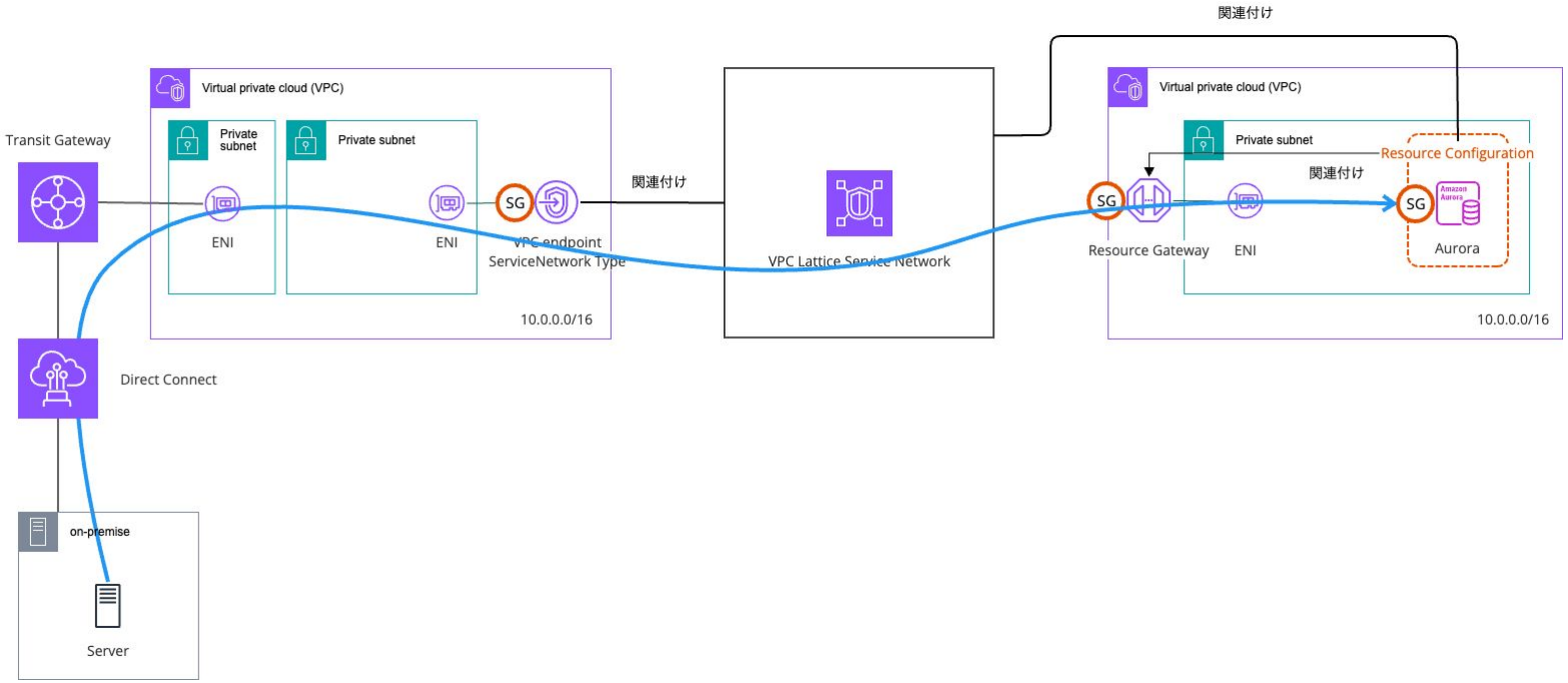
VPC エンドポイント 経由でアクセスするときの DNS 名

本当のDNS名

DNS 名	Private DNS
vpce-0c6288af9ac0c9de9-snra-0d636d8f66af6d41d.rcfg-0873e1ff6edba74b5.4232ccc.vpc-lattice-rsc.us-east-1.on.aws	database-1.cluster-cql5tgylta2m.us-east-1.rds.amazonaws.com
vpce-0c6288af9ac0c9de9-snra-041bd60a51f2cae2b.rcfg-0596e2c2c9bf03a2c.4232ccc.vpc-lattice-rsc.us-east-1.on.aws	database-1.cluster-ro-cql5tgylta2m.us-east-1.rds.amazonaws.com

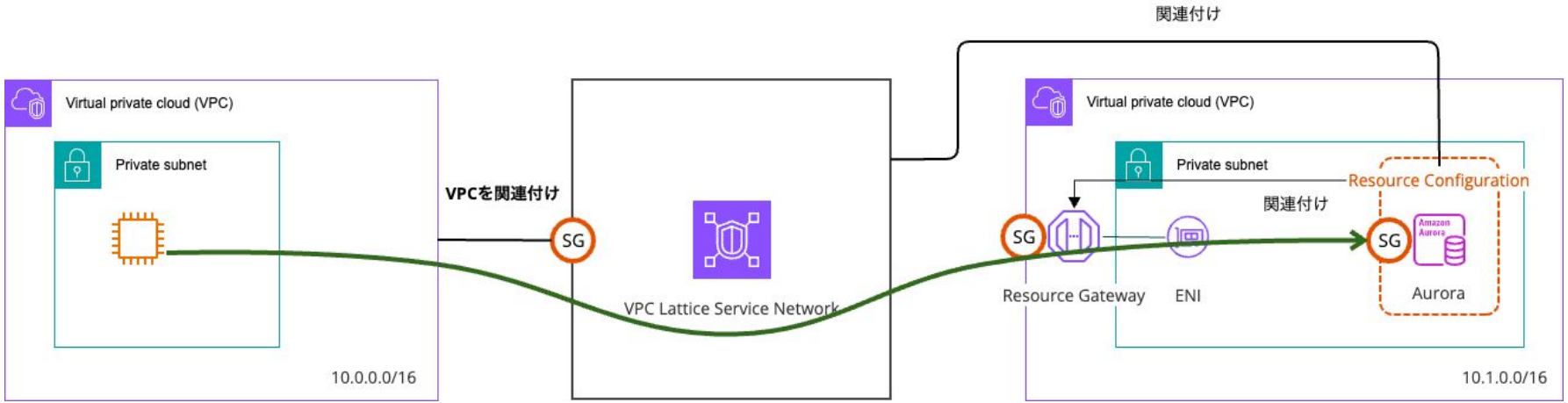
DB接続するときの構成例

VPCエンドポイント利用する方法



DB接続するときの構成例

サービスネットワークにアクセス元のVPCを関連付ける方法（未検証）



PrivateLink アップデート

PrivateLinkアップデート

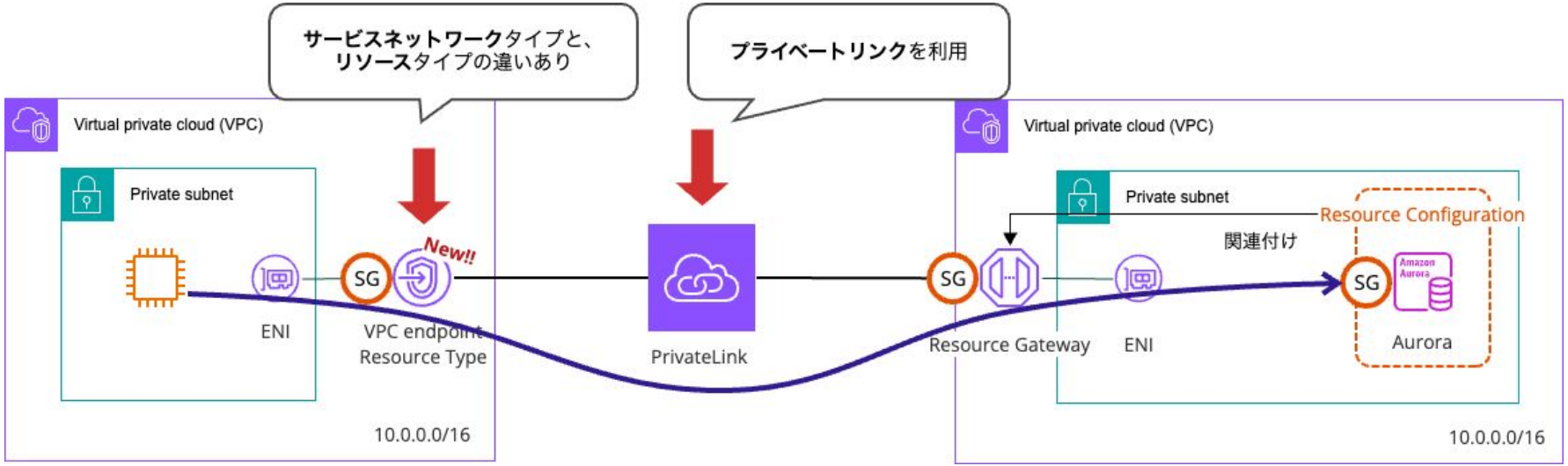
VPC内のリソースへのアクセスにNLBが不要になりました

- Resource Configuration
- Resource Gateway
- リソースタイプのVPCエンドポイント

DevelopersIOブログリンク

DB接続するときの構成例

VPC Latticeのときと同じ様に使います



既視感

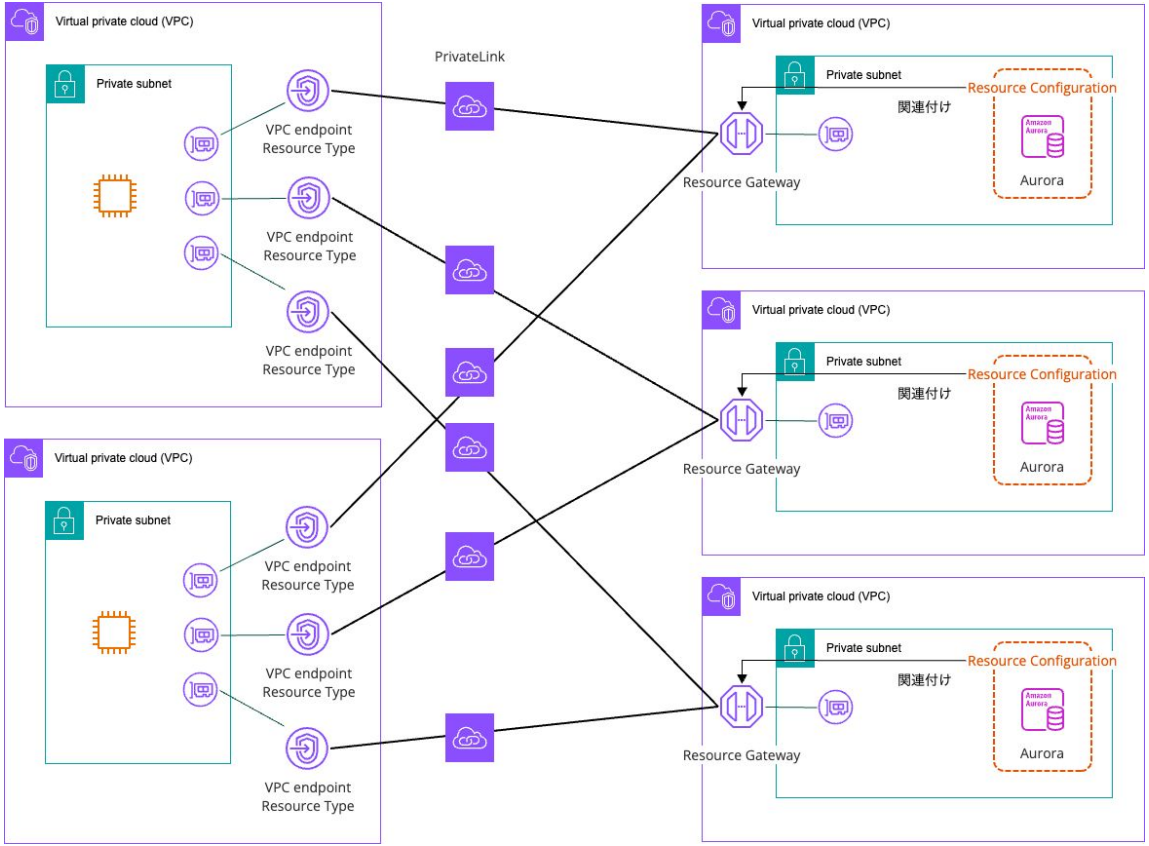
使い分けはどうしたら…

PrivateLink

1:1の接続

数が少ないなら問題なし

接続先増えると管理が大変

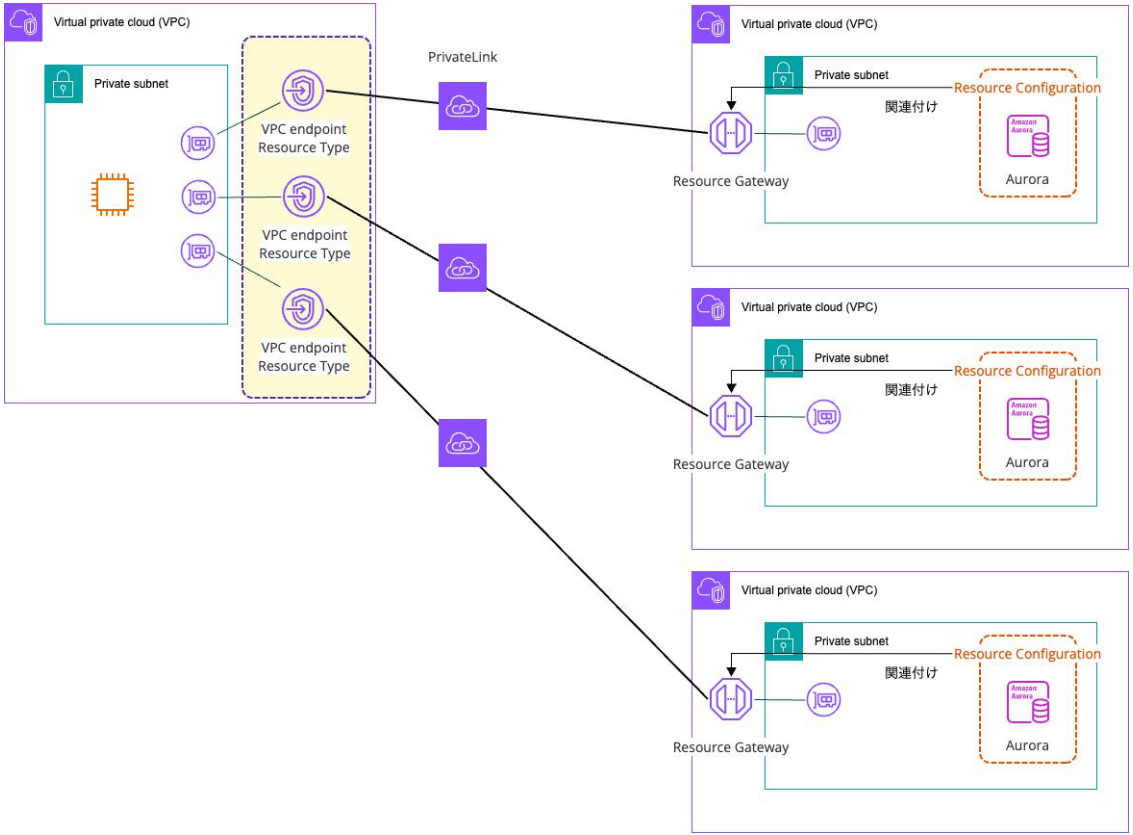


PrivateLink

1:1の接続

数が少ないなら問題なし

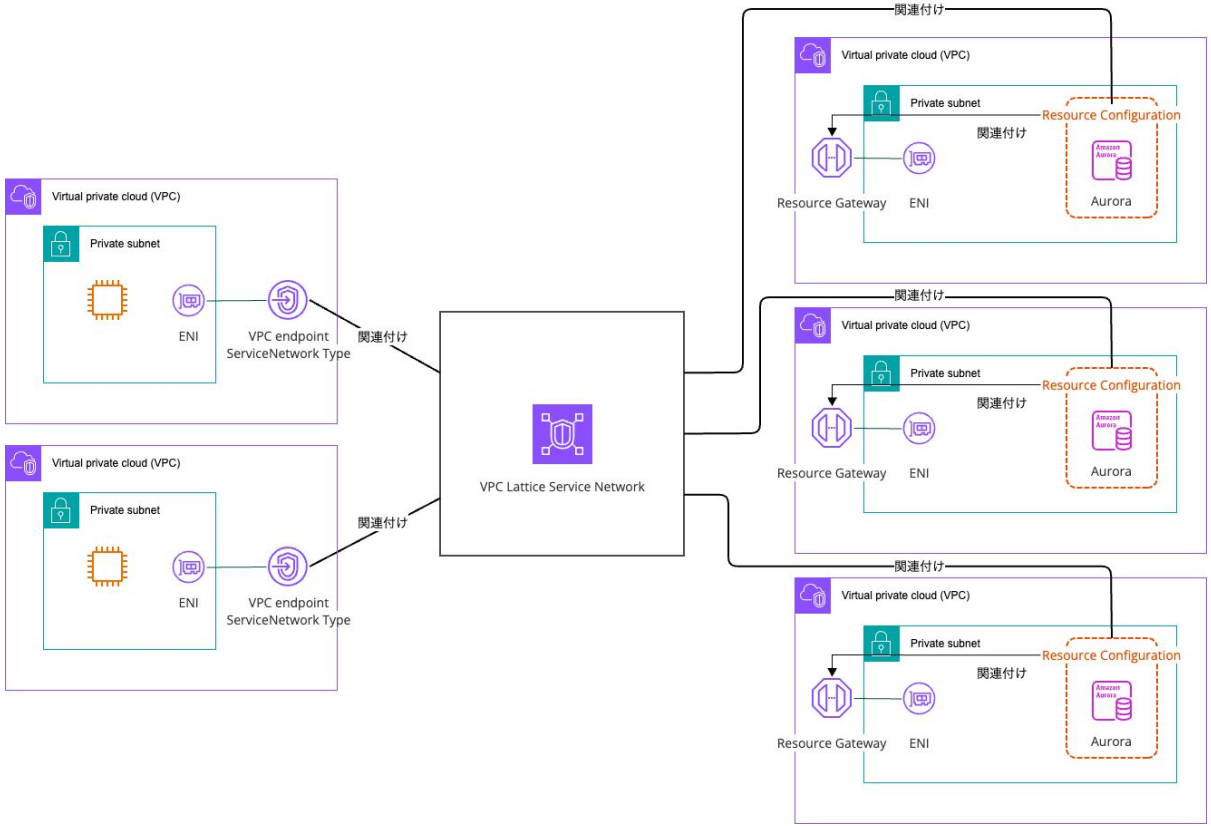
接続先増えると管理が大変



VPC Lattice

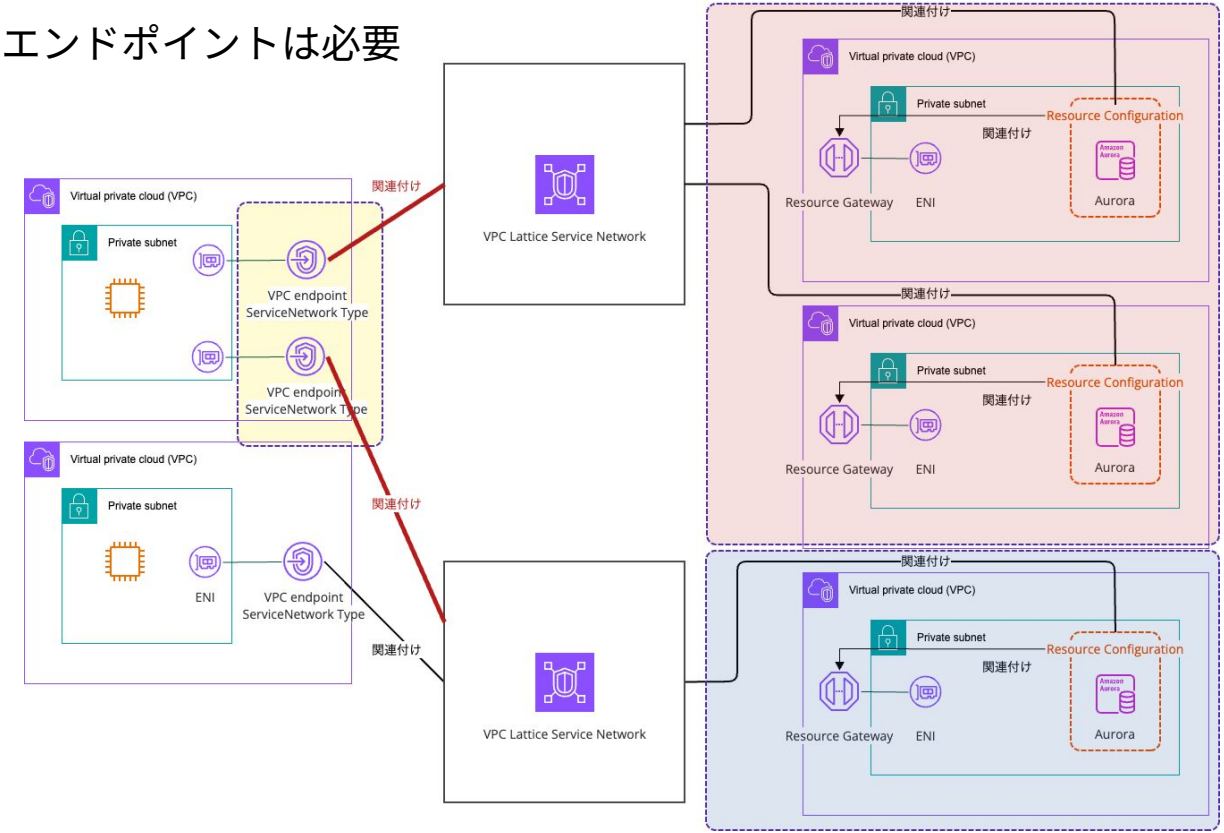
1:nの接続

複雑なときには良い



VPC Lattice

サービスネットワーク毎にVPCエンドポイントは必要



まとめ

まとめ

VPC関連のリソースとして以下が追加されました

- Resource Configuration
- Resource Gateway
- サービスネットワークタイプのVPCエンドポイント
- リソースタイプのVPCエンドポイント

VPC LatticeとPrivateLinkの接続の違いは...

- PrivateLinkは、1:1
- VPC Latticeは、1:n

今日のゴール

ゴール

- VPCに追加された新しいリソースを知ってもらう
- VPC LatticeとPrivateLinkの接続方法の違いを知ってもらう

classmethod