プライベートサブネットのインスタンスに SSH? EC2 Instance Connect Endpoint を試してみる！

Hiroki Yamazaki
Amazon Web Services Japan G.K.
Solutions Architect

2023/09/06

山崎 宏紀 (Yamazaki Hiroki)

Amazon Web Services Japan ソリューションアーキテクト

ソフトウェア・SaaS を開発されている皆様をご支援します！

得意分野:

- 組合せ最適化, 離散アルゴリズム
- Infrastructure as Code, Serverless

好きな AWS サービス: AWS CDK, AWS Step Functions

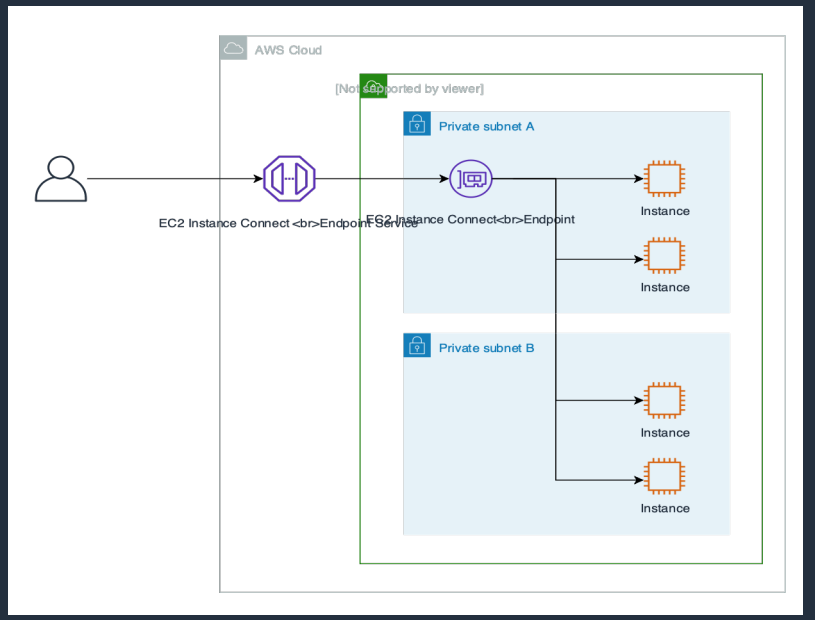
趣味: 将棋, ボードゲーム, ボルダリング

Agenda

- EC2 Instance Connect Endpoint (EIC Endpoint) 概要
- EC2 Instance Connect とは？
- Session Manager との違いを確認
- デモ
- おわりに
- Appendix

EC2 Instance Connect Endpoint (EIC Endpoint) 概要

- 2023/06: Public IP を持たないインスタンスに対し SSH/RDP 接続ができる EC2 Instance Connect Endpoint が発表
- 従来、インスタンスへの SSH/RDP での接続には Public IP や踏み台インスタンスを用意する必要があった



- EIC Endpoint の使用料金は無料 (別途データ転送料は発生)
- IAM・セキュリティグループによるアクセス制御
- AWS CloudTrail による監査
- インスタンスのセキュリティグループでは EIC Endpoint からの SSH/RDP を許可

Amazon EC2 Instance Connect でパブリック IP アドレスなしで SSH 接続と RDP 接続が可能に
https://aws.amazon.com/jp/about-aws/whats-new/2023/06/amazon-ec2-instance-connect-ssh-rdp-public-ip-address/

EC2 Instance Connect とは？

- インスタンスに SSH でアクセスするための機能
- SSH キーを自身で共有・管理する必要なし
- マネジメントコンソール・CLI 両対応
- 仕組み
  - Instance Connect API で SSH 公開鍵を インスタンスメタデータにプッシュ
  - インスタンスメタデータから取得した 公開鍵でユーザーを認証

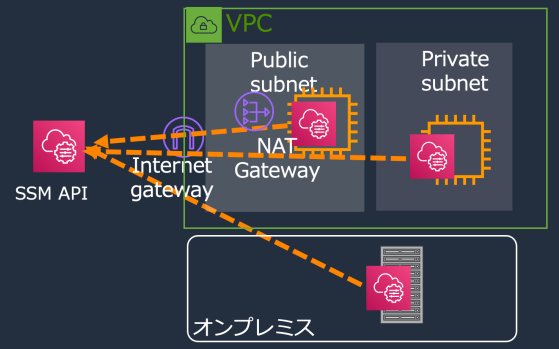
EC2 Instance Connect を使用して Linux インスタンスに接続する
https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/connect-linux-inst-eic.html

Session Manager との違いを確認

- インスタンスにアクセスするための AWS Systems Manager の一機能
- セキュリティグループでの Inbound 許可不要
- セッション中のコマンドと出力を記録可能
- インスタンス内 SSM Agent から SSM API への接続経路が必要

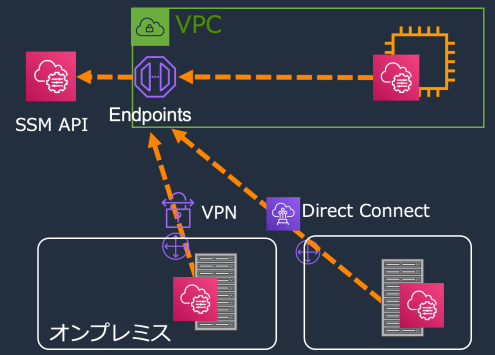
1, インターネット経由

・パブリックサブネットや
NAT Gateway を使用



2, VPC エンドポイント経由

・プライベートネットワークによる接続が可能
・オンプレミスからも AWS Direct Connect や
VPN 経由で閉域網経由のアクセスが可能



Outbound 設定の構成例

デモ

おわりに

- Public IP や踏み台なしで EC2 インスタンスに SSH/RDP 接続できる EC2 Instance Connect Endpoint を紹介
- 利用料金は無料で IAM やセキュリティグループによるアクセス制御に対応

- 2023/08 時点のクォータ
  - VPC ごと・サブネットごとに1つまで
- Multi-AZ 構成を利用している場合は Session Manager と適切な使い分けを！

Appendix

EIC Endpoint と Session Manager の比較観点 (2023/08 時点)

- 費用
  - EIC Endpoint: 無料
  - Session Manager: 無料。ただし、Private Subnet 内のインスタンスで利用する場合 SSM API への接続経路として NAT Gateway や VPC Endpoint が必要
- 可用性
  - EIC Endpoint: クォータの制約上、単一 AZ にのみ作成可能
  - Session Manager: NAT Gateway/VPC Endpoint を接続経路として利用する場合、Multi-AZ 構成可能
- 動作環境
  - EIC Endpoint: Amazon Linux 2 全てのバージョン, Ubuntu 16.04 以降
  - Session Manager: AWS Systems Manager の対応状況に準拠