



架構圖表

# 使用 Amazon EKS 公開微服務



## 使用 Amazon EKS 公開微服務: 架構圖表

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

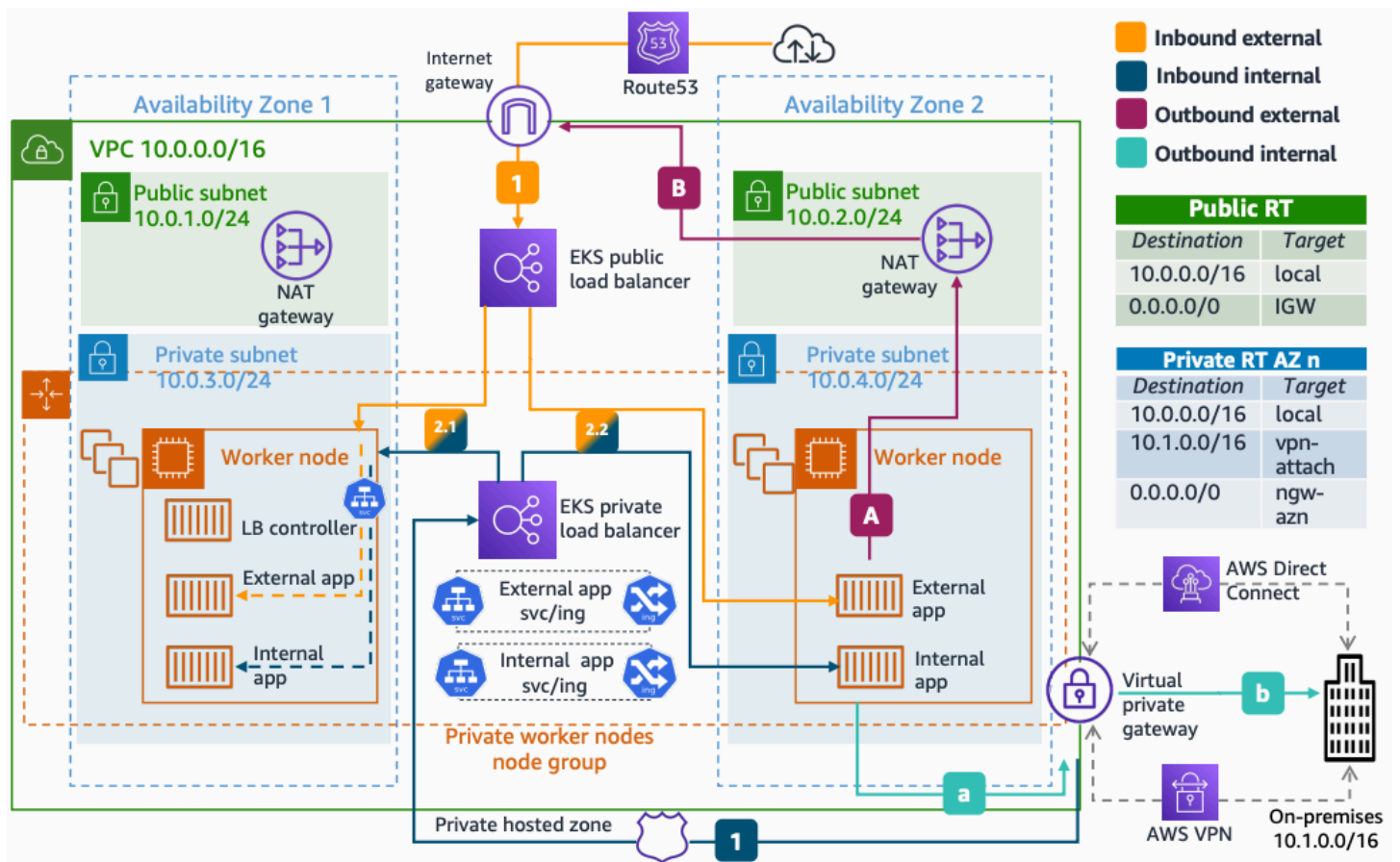
|                                   |   |
|-----------------------------------|---|
| 混合 EKS IPv4 .....                 | 1 |
| 使用 Amazon EKS 在混合案例中公開微服務 .....   | 1 |
| 深入閱讀 .....                        | 2 |
| 圖表歷史記錄 .....                      | 2 |
| 自訂聯網 .....                        | 4 |
| 處理 Pod IP 耗盡 .....                | 4 |
| 深入閱讀 .....                        | 5 |
| 圖表歷史記錄 .....                      | 5 |
| IPv6 叢集 .....                     | 7 |
| 在 IPv6 叢集中公開 Amazon EKS 微服務 ..... | 7 |
| 深入閱讀 .....                        | 8 |
| 圖表歷史記錄 .....                      | 8 |
| .....                             | x |

# 使用 Amazon EKS 在混合案例中公開微服務

發佈日期：2022 年 2 月 22 日 ([圖表歷史記錄](#))

此架構說明如何將私有子網路中託管的 [Amazon Elastic Kubernetes Service](#) 微服務公開至網際網路和內部部署網路。[AWS Load Balancer 控制器](#) 會管理 Kubernetes 服務和輸入的 Elastic Load Balancer (ELBs)。

## 使用 Amazon EKS 在混合案例中公開微服務



下列步驟說明傳入外部流程：

1. [Amazon Route 53](#) 會將傳入請求解析為 [AWS Load Balancer 控制器](#) 所部署的公有 ELB。
2. ELBs 流量轉送至應用程式。您可以選擇兩種模式：執行個體模式（傳送至工作者節點的流量，然後服務會將流量重新導向至 Pod）或 IP 模式（直接導向至 Pod IP 的流量）。如需詳細資訊，請參閱 [叢集聯網詳細資訊](#)。

下列步驟說明傳入內部流程：

1. Amazon Route 53 會使用私有託管區域，將傳入請求解析為 AWS Load Balancer 控制器所部署的私有 ELB。
2. ELBs 流量轉送至執行個體模式或 IP 模式的應用程式。

下列步驟說明傳出外部流程：

- A. 當私有子網路中的 Pod 起始傳出請求至網際網路時，私有路由表會將流量轉送至 NAT 閘道 (NGW)。
- B. 公有路由表會將流量從 NGW 轉送到網際網路閘道 (IGW)。

下列步驟說明傳出內部流程：

- a. 私有子網路中的 Pod 會起始對內部部署網路的傳出請求。私有路由表會將流量轉送至虛擬私有閘道 (VGW)。
- b. 流量會透過 VPN 或 AWS Direct Connect 連線到達內部部署網路。

#### Note

您可以使用 NGINX [輸入控制器](#) 等輸入控制器做為 AWS Load Balancer 控制器的替代方案。  
<https://kubernetes.github.io/ingress-nginx/deploy/> 如果您使用 [AWS Fargate](#) for Amazon EKS，則只有私有子網路中的 Pod ENIs，而且必須使用具有 IP 模式 ELBs。

## 深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS 架構中心](#)
- [AWS Well-Architected](#)

## 圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

| 變更                   | 描述         | 日期              |
|----------------------|------------|-----------------|
| <a href="#">初次出版</a> | 首先發佈參考架構圖。 | 2022 年 2 月 22 日 |
| <a href="#">初次出版</a> | 首先發佈參考架構圖。 | 2022 年 2 月 22 日 |
| <a href="#">初次出版</a> | 首先發佈參考架構圖。 | 2022 年 2 月 22 日 |

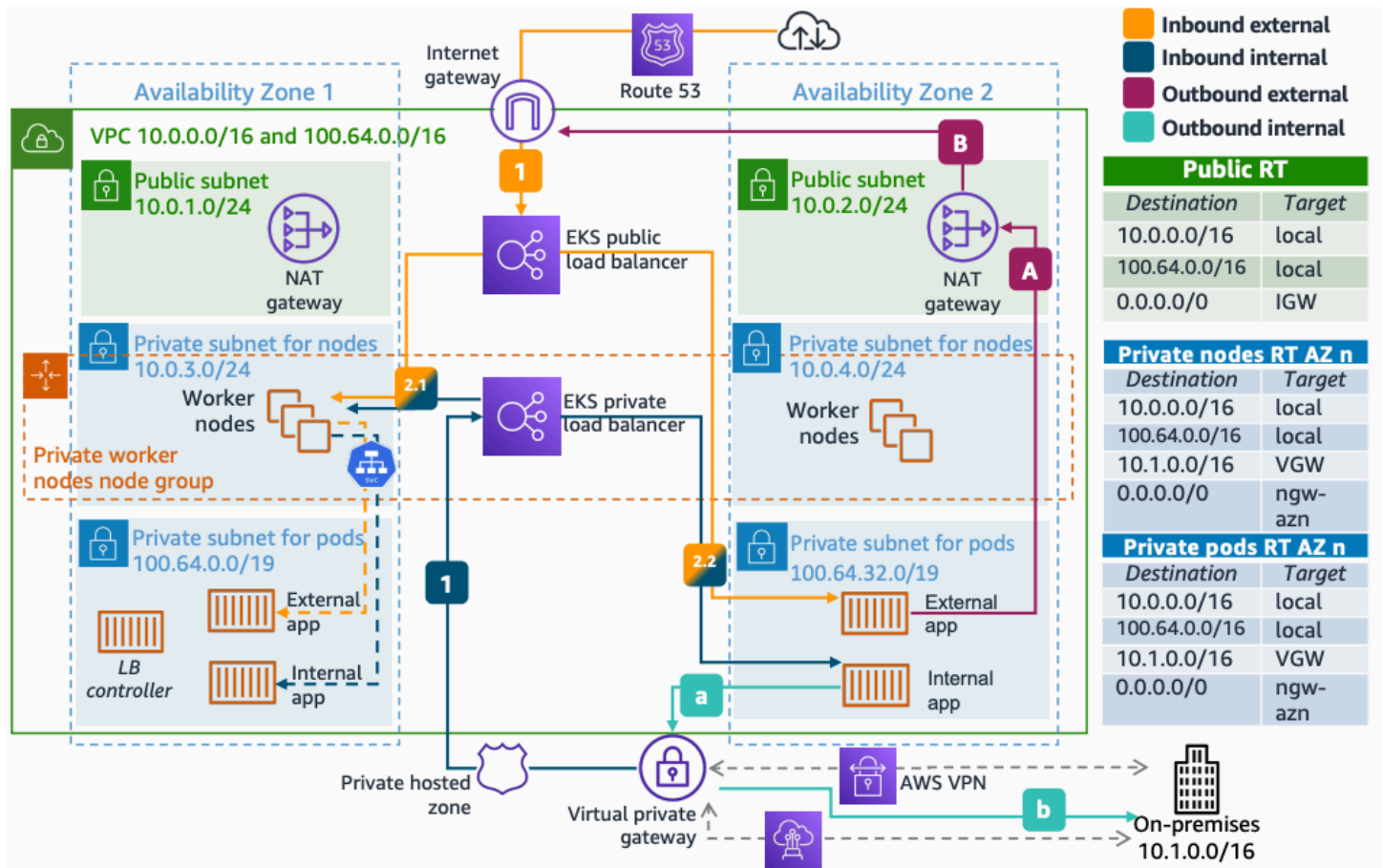
 Note

若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

## 處理 Pod IP 耗盡

此架構說明如何處理 Pod IP 耗盡，方法是將次要 CIDR 區塊從 [RFC 6598](#) 地址空間新增至您的 [Amazon VPC](#)。使用 [CNI 自訂網路](#) 功能，Pod 不再使用 VPC 中的 [RFC 1918](#) IP 地址。

## 處理 Pod IP 耗盡



下列步驟說明傳入外部流程：

1. Amazon Route 53 會將傳入請求解析為 AWS Load Balancer 控制器所部署的公有 ELB。
2. ELBs 流量轉送至應用程式。您可以選擇執行個體模式（傳送至工作者節點的流量，然後服務重新導向至 Pod）或 IP 模式（直接導向至 Pod IP 的流量）。

下列步驟說明傳入內部流程：

1. Amazon Route 53 會使用私有託管區域，將傳入請求解析為 [AWS Load Balancer 控制器](#) 所部署的私有 ELB。

## 2. ELBs 流量轉送至執行個體模式或 IP 模式的應用程式。

下列步驟說明傳出外部流程：

- A. 私有子網路中的 Pod 會起始對網際網路的傳出請求。私有路由表會將流量轉送至 NAT 閘道 (NGW)。
- B. 公有路由表會將流量從 NGW 轉送到網際網路閘道 (IGW)。

下列步驟說明傳出內部流程：

- a. 私有子網路中的 Pod 會起始對內部部署網路的傳出請求。私有路由表會將流量轉送至虛擬私有閘道 (VGW)。
- b. 流量會透過 VPN 或 AWS Direct Connect 連線到達內部部署網路。

### Note

Amazon EKS 的預設行為是將 NAT Pod 流量來源至託管工作者節點的主要 IP 地址。[AWS Fargate](#) for Amazon EKS 支援其他 CIDRs。[ENIConfig 自訂資源](#)會定義排程 Pod 的子網路。如需多帳戶設定，請參閱此[部落格文章](#)。

## 深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS 架構中心](#)
- [AWS Well-Architected](#)

## 圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

變更

描述

日期

|                      |            |                 |
|----------------------|------------|-----------------|
| <a href="#">初次出版</a> | 首先發佈參考架構圖。 | 2022 年 2 月 22 日 |
| <a href="#">初次出版</a> | 首先發佈參考架構圖。 | 2022 年 2 月 22 日 |
| <a href="#">初次出版</a> | 首先發佈參考架構圖。 | 2022 年 2 月 22 日 |

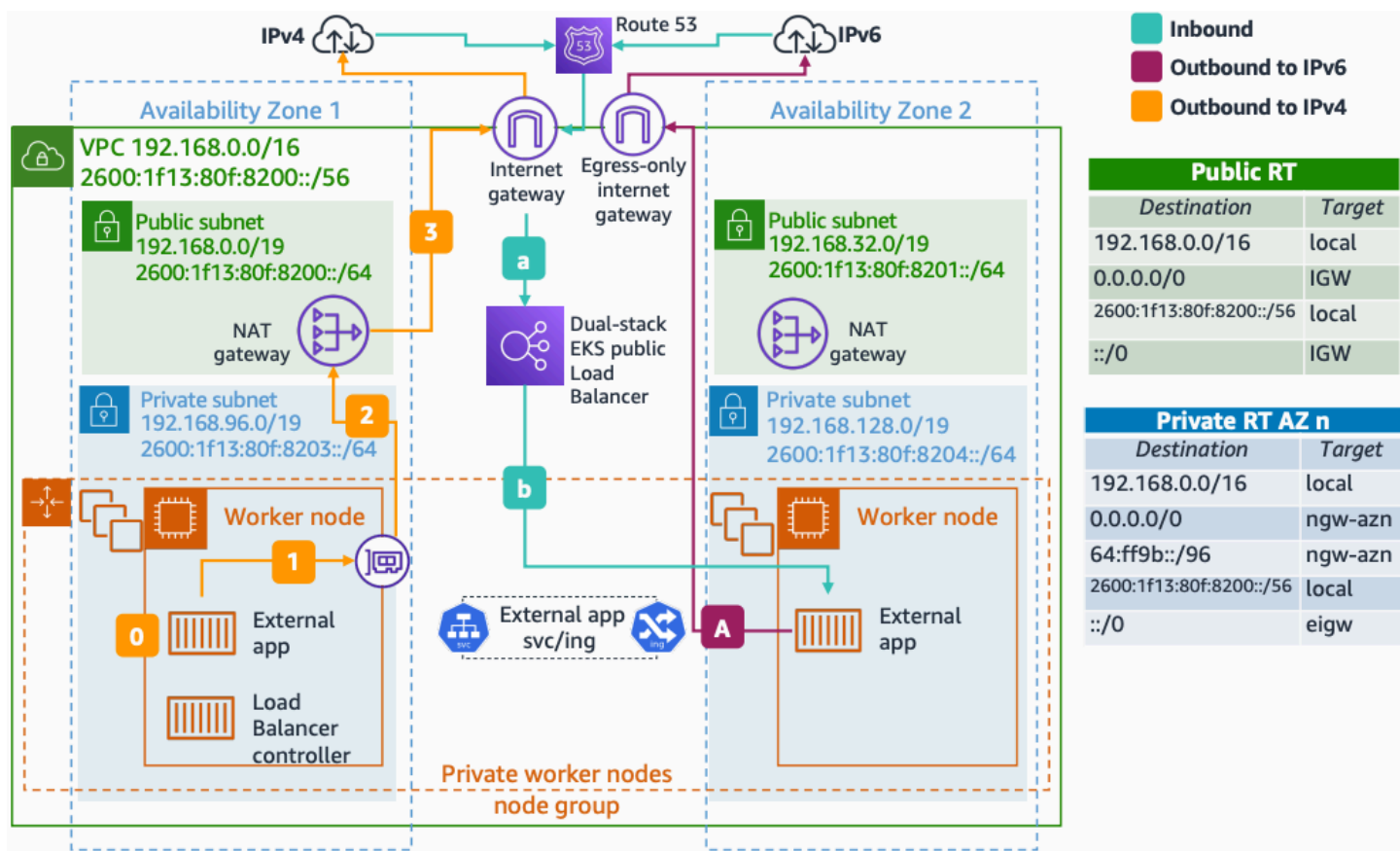
 Note

若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

## 在 IPv6 叢集中公開 Amazon EKS 微服務

此架構說明如何使用 IPv6 公開 Amazon EKS 微服務，並連線到網際網路上的 IPv6 和 IPv4 端點。移至 IPv6 也可解決 Pod IP 耗盡，因為您不需要處理 IPv4 限制。

## 在 IPv6 叢集中公開 Amazon EKS 微服務



下列步驟說明傳入流程：

- Amazon Route 53 會以 AWS Load Balancer 控制器部署的**雙堆疊模式**，將傳入請求解析至公有 ELBs。
- ELB 會使用 IP 模式將流量轉送至 IPv6 Pod。

下列步驟說明傳出 IPv6 流程：

- 從私有子網路內到叢集外部 IPv6 端點的任何 Pod 通訊都會透過輸出限定網際網路閘道 (EIGW) 路由。

下列步驟說明傳出 IPv4 流程：

1. 私有子網路中的 Pod 會對網際網路上的 IPv4 地址啟動傳出請求，並執行 DNS 查詢。收到 IPv4 "A" 回應時，Pod 會使用來自 [host-local](#) 169.254.172.0/22 IP 範圍的 IPv4 地址建立連線。
2. Pod 的節點限定唯一 IPv4 地址會透過 NAT 轉譯為連接至節點之主要網路介面的 IPv4 (VPC) 地址。
3. 私有路由表會將流量轉送至 NAT 閘道，而節點的私有 IPv4 地址會轉譯為閘道的公有 IPv4 地址。

#### Note

撰寫本文時，ALB 和 NLB 僅支援面向網際網路端點的雙堆疊。Amazon EKS 實作與 VPC CNI 連結的主機本機 CNI 外掛程式，為 169.254.172.0/22 範圍的 Pod 配置和設定 IPv4 地址。

## 深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS 架構中心](#)
- [AWS Well-Architected](#)

## 圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

| 變更                   | 描述         | 日期              |
|----------------------|------------|-----------------|
| <a href="#">初次出版</a> | 首先發佈參考架構圖。 | 2022 年 2 月 22 日 |
| <a href="#">初次出版</a> | 首先發佈參考架構圖。 | 2022 年 2 月 22 日 |
| <a href="#">初次出版</a> | 首先發佈參考架構圖。 | 2022 年 2 月 22 日 |

 Note

若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。