Architektur-Diagramme

Stellen Sie Microservices mithilfe von Amazon EKS zur Verfügung

Stellen Sie Microservices mithilfe von Amazon EKS zur Verfügung: Architektur-Diagramme

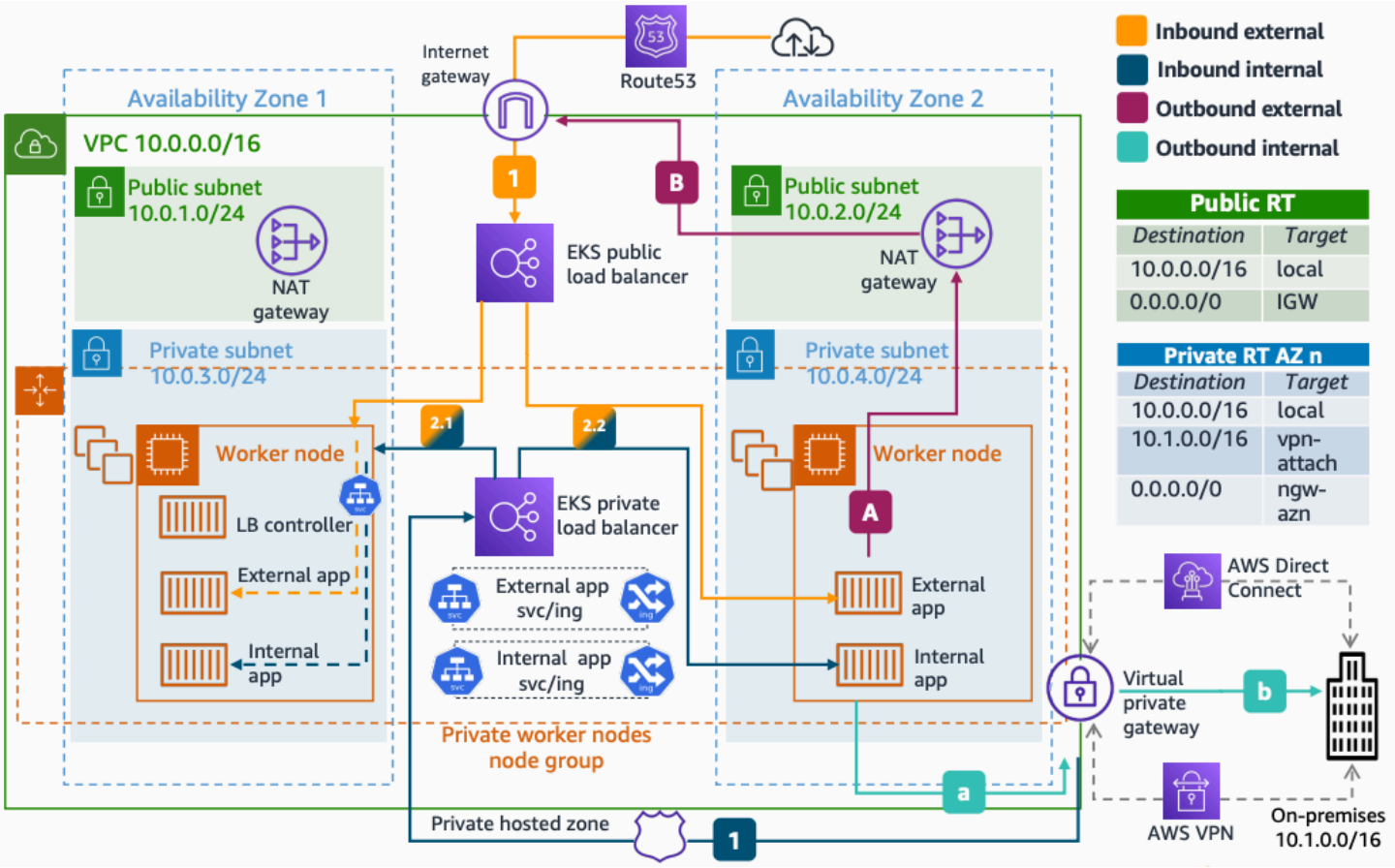
Table of Contents

Stellen Sie Microservices in einem Hybridszenario mithilfe von Amazon EKS bereit

Veröffentlichungsdatum: 22. Februar 2022 () Geschichte des Diagramms

Diese Architektur zeigt, wie Amazon Elastic Kubernetes Service-Microservices, die in privaten Subnetzen gehostet werden, für das Internet und lokale Netzwerke verfügbar gemacht werden. Der AWS Load Balancer Controller verwaltet Elastic Load Balancer (ELBs) für Dienste und Eingänge. Kubernetes

Stellen Sie Microservices in einem Hybridszenario mithilfe von Amazon EKS bereit



Die folgenden Schritte beschreiben den eingehenden externen Datenfluss:

1. Amazon Route 53 löst eingehende Anfragen an das öffentliche ELB auf, das vom AWS Load Balancer Controller bereitgestellt wird.
2. Die ELBs leiten den Datenverkehr an Anwendungen weiter. Sie können zwischen zwei Modi wählen: Instanzmodus (Datenverkehr wird an einen Worker-Knoten gesendet, dann leitet der Dienst den Verkehr an den Pod weiter) oder IP-Modus (Datenverkehr, der direkt an die IP des Pods geleitet wird). Weitere Informationen finden Sie in den Details zum Cluster-Netzwerk.

Die folgenden Schritte beschreiben den internen Eingangsfluss:

1. Amazon Route 53 löst eingehende Anfragen an den privaten ELB auf, der vom AWS Load Balancer Controller mithilfe einer privat gehosteten Zone bereitgestellt wird.
2. Die ELBs leiten den Datenverkehr an Anwendungen im Instanzmodus oder IP-Modus weiter.

Die folgenden Schritte beschreiben den ausgehenden externen Datenfluss:

A. Wenn ein Pod in einem privaten Subnetz eine ausgehende Anfrage an das Internet initiiert, leitet die private Routing-Tabelle den Datenverkehr an das NAT-Gateway (NGW) weiter.

B. Die öffentliche Routing-Tabelle leitet den Datenverkehr vom NGW an das Internet-Gateway (IGW) weiter.

Die folgenden Schritte beschreiben den ausgehenden internen Datenfluss:

a. Ein Pod in einem privaten Subnetz initiiert eine ausgehende Anfrage an das lokale Netzwerk. Die private Routing-Tabelle leitet den Datenverkehr an das Virtual Private Gateway (VGW) weiter.

b. Der Datenverkehr erreicht das lokale Netzwerk über die VPN- oder AWS Direct Connect-Verbindung.

> **Note**
>
> Sie können Ingress-Controller wie den NGINX-Ingress-Controller als Alternative zum AWS Load Balancer Controller verwenden. Wenn Sie AWS Fargate für Amazon EKS verwenden, haben Sie nur Pod-ENIs in den privaten Subnetzen und müssen ELBs mit IP-Modus verwenden.

Weitere Informationen

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS Architektur-Ikonen
- AWS Zentrum für Architektur
- AWS Well-Architected

Geschichte des Diagramms

Abonnieren Sie den RSS-Feed, um über Aktualisierungen dieses Referenzarchitekturdiagramms informiert zu werden.

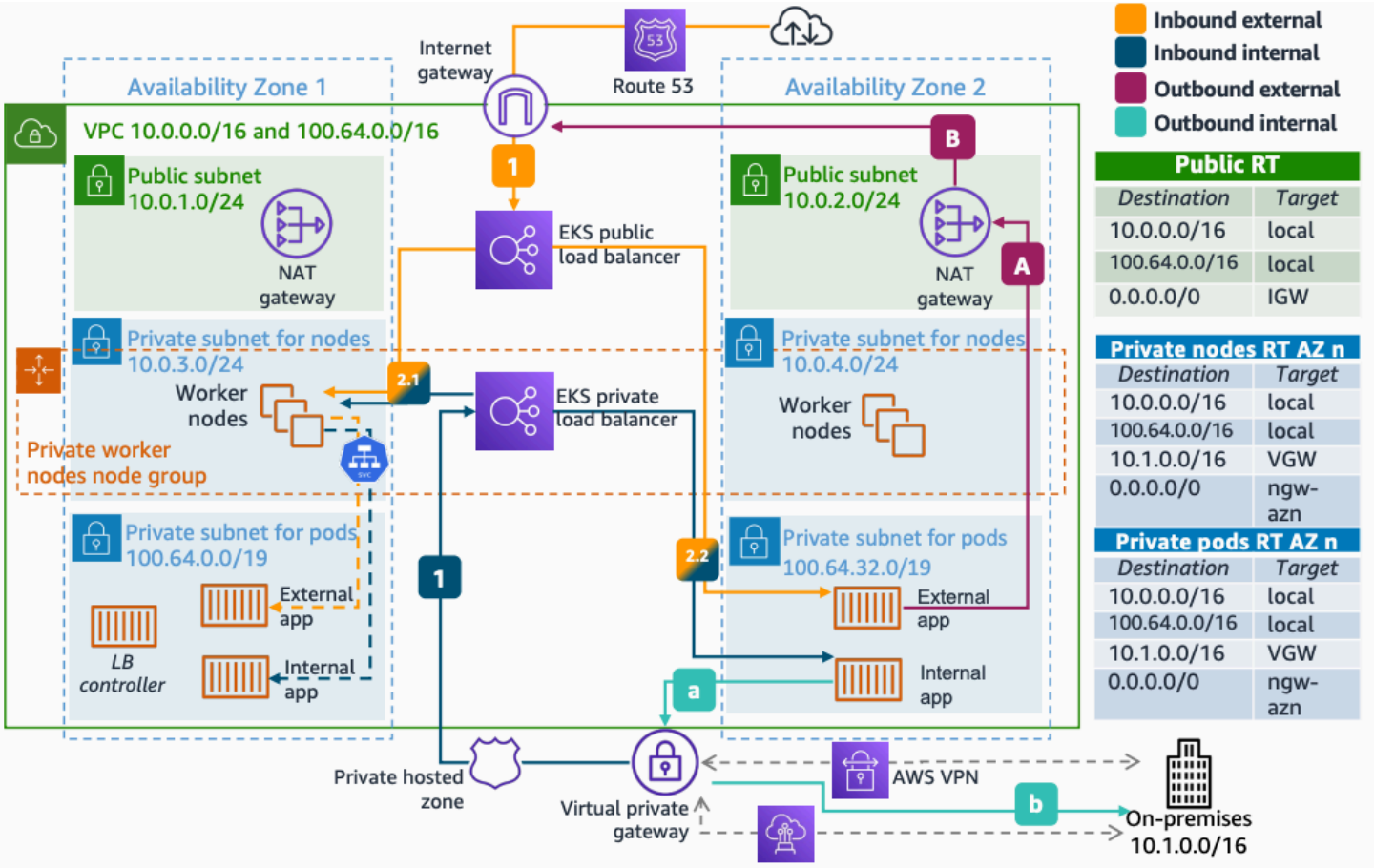
Änderung	Beschreibung	Datum
Erste Veröffentlichung	Das Referenzarchitekturdiagramm wurde zuerst veröffentlicht.	22. Februar 2022
Erste Veröffentlichung	Das Referenzarchitekturdiagramm wurde erstmals veröffentlicht.	22. Februar 2022
Erste Veröffentlichung	Das Referenzarchitekturdiagramm wurde erstmals veröffentlicht.	22. Februar 2022

> **Note**
>
> Um RSS-Updates zu abonnieren, muss ein RSS-Plugin für den von Ihnen verwendeten Browser aktiviert sein.

Umgang mit Pod-IP-Erschöpfung

Diese Architektur zeigt, wie Sie mit der Erschöpfung von Pod-IP-Adressen umgehen können, indem Sie Ihrer Amazon VPC sekundäre CIDR-Blöcke aus dem RFC 6598-Adressraum hinzufügen. https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html Mithilfe der CNI Custom Networking-Funktion verwenden Pods keine RFC 1918-IP-Adressen mehr in der VPC.

Gehen Sie mit der Erschöpfung der Pod-IP um



Die folgenden Schritte beschreiben den eingehenden externen Datenfluss:

1. Amazon Route 53 löst eingehende Anfragen an das öffentliche ELB auf, das vom AWS Load Balancer Controller bereitgestellt wird.
2. Die ELBs leiten den Datenverkehr an Anwendungen weiter. Sie wählen zwischen dem Instanzmodus (Datenverkehr, der an einen Worker-Knoten gesendet wird, dann leitet der Dienst zum Pod weiter) oder dem IP-Modus (Datenverkehr, der direkt an die Pod-IP weitergeleitet wird).

Die folgenden Schritte beschreiben den internen Eingangsfluss:

1. Amazon Route 53 löst eingehende Anfragen an den privaten ELB auf, der vom AWS Load Balancer Controller mithilfe einer privat gehosteten Zone bereitgestellt wird.
2. Die ELBs leiten den Datenverkehr an Anwendungen im Instanzmodus oder IP-Modus weiter.

Die folgenden Schritte beschreiben den ausgehenden externen Datenfluss:

A. Ein Pod in einem privaten Subnetz initiiert eine ausgehende Anfrage an das Internet. Die private Routing-Tabelle leitet den Datenverkehr an das NAT-Gateway (NGW) weiter.
B. Die öffentliche Routing-Tabelle leitet den Datenverkehr vom NGW an das Internet-Gateway (IGW) weiter.

Die folgenden Schritte beschreiben den ausgehenden internen Datenfluss:

a. Ein Pod in einem privaten Subnetz initiiert eine ausgehende Anfrage an das lokale Netzwerk. Die private Routing-Tabelle leitet den Datenverkehr an das Virtual Private Gateway (VGW) weiter.
b. Der Datenverkehr erreicht das lokale Netzwerk über die VPN- oder AWS Direct Connect-Verbindung.

> **Note**
>
> Das Standardverhalten von Amazon EKS besteht darin, den NAT-Pod-Verkehr an die primäre IP-Adresse des Hosting-Worker-Knotens weiterzuleiten. AWS Fargate for Amazon EKS unterstützt zusätzliche CIDRs. Die benutzerdefinierte Ressource EniConfig definiert das Subnetz, in dem Pods geplant sind. In diesem Blogbeitrag finden Sie Einstellungen für mehrere Konten.

Weitere Informationen

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS Architektur-Ikonen
- AWS Zentrum für Architektur
- AWS Well-Architected

Geschichte des Diagramms

Abonnieren Sie den RSS-Feed, um über Aktualisierungen dieses Referenzarchitekturdiagramms informiert zu werden.

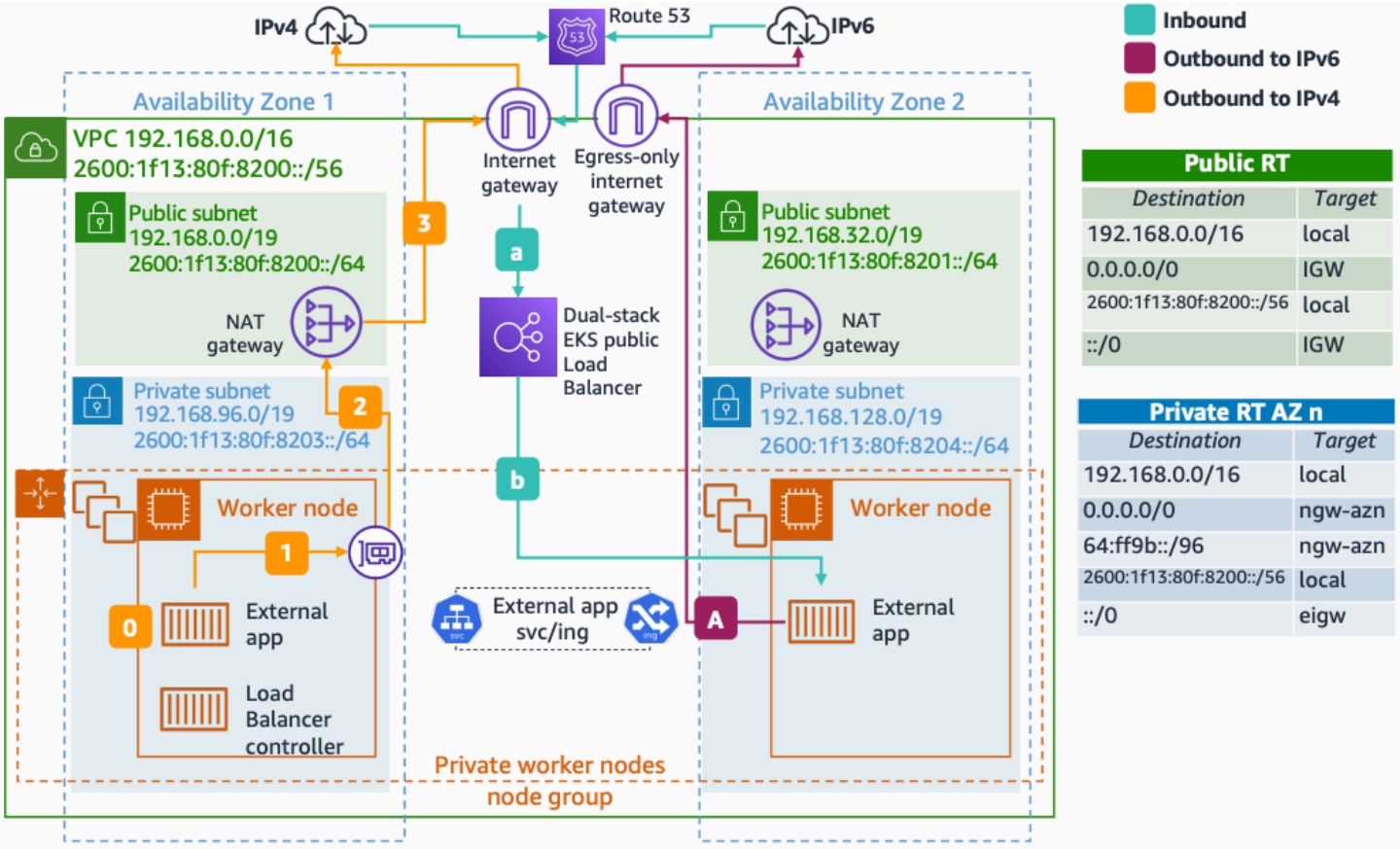
Änderung	Beschreibung	Datum
Erste Veröffentlichung	Das Referenzarchitektu rdiagramm wurde zuerst veröffentlicht.	22. Februar 2022
Erste Veröffentlichung	Das Referenzarchitektu rdiagramm wurde erstmals veröffentlicht.	22. Februar 2022
Erste Veröffentlichung	Das Referenzarchitektu rdiagramm wurde erstmals veröffentlicht.	22. Februar 2022

> **Note**
>
> Um RSS-Updates zu abonnieren, muss ein RSS-Plugin für den von Ihnen verwendeten Browser aktiviert sein.

Stellen Sie Amazon EKS-Microservices in IPv6-Clustern bereit

Diese Architektur zeigt, wie Amazon EKS-Microservices mit IPv6 verfügbar gemacht und eine Verbindung zu IPv6- und IPv4-Endpunkten im Internet hergestellt werden. Die Umstellung auf IPv6 behebt auch die Erschöpfung der Pod-IP-Adressen, da Sie die IPv4-Grenzwerte nicht umgehen müssen.

Stellen Sie Amazon EKS-Microservices in IPv6-Clustern bereit



Die folgenden Schritte beschreiben den eingehenden Fluss:

a. Amazon Route 53 löst eingehende Anfragen an die öffentlichen ELBs im Dual-Stack-Modus auf, der vom AWS Load Balancer Controller bereitgestellt wird.

b. Der ELB leitet den Datenverkehr im IP-Modus an die IPv6-Pods weiter.

Die folgenden Schritte beschreiben den ausgehenden IPv6-Fluss:

A. Jegliche Pod-Kommunikation von privaten Subnetzen zu IPv6-Endpunkten außerhalb des Clusters wird über ein Internet-Gateway (EIGW) nur für ausgehenden Datenverkehr geleitet.

Die folgenden Schritte beschreiben den ausgehenden IPv4-Fluss:

1. Ein Pod in einem privaten Subnetz initiiert eine ausgehende Anfrage an eine IPv4-Adresse im Internet und führt eine DNS-Suche durch. Nach Erhalt einer IPv4-Antwort „A“ stellt der Pod eine Verbindung her, indem er die IPv4-Adresse vom lokalen Host 169.254.172 verwendet. https://github.com/aws/amazon-vpc-cni-k8s/blob/master/misc/10-aws.conflist 0/22 IP-Bereich.
2. Die eindeutige IPv4-Adresse des Pods wird über NAT in die IPv4-Adresse (VPC) der primären Netzwerkschnittstelle übersetzt, die an den Knoten angeschlossen ist.
3. Die private Routing-Tabelle leitet den Datenverkehr an das NAT-Gateway weiter, und die private IPv4-Adresse eines Knotens wird in die öffentliche IPv4-Adresse des Gateways übersetzt.

> **Note**
>
> Zum Zeitpunkt der Erstellung dieses Artikels unterstützen ALB und NLB Dual-Stack nur für Endpunkte mit Internetanschluss. Amazon EKS implementiert ein hostlokales CNI-Plugin, das zusammen mit VPC CNI verkettet ist, um eine IPv4-Adresse für einen Pod aus 169.254.172 zuzuweisen und zu konfigurieren. 0/22 Bereich.

Weitere Informationen

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS Architektur-Ikonen
- AWS Zentrum für Architektur
- AWS Well-Architected

Geschichte des Diagramms

Abonnieren Sie den RSS-Feed, um über Aktualisierungen dieses Referenzarchitekturdiagramms informiert zu werden.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	Das Referenzarchitektu rdiagramm wurde zuerst veröffentlicht.	22. Februar 2022
Erste Veröffentlichung	Das Referenzarchitektu rdiagramm wurde erstmals veröffentlicht.	22. Februar 2022
Erste Veröffentlichung	Das Referenzarchitektu rdiagramm wurde erstmals veröffentlicht.	22. Februar 2022

> **Note**
>
> Um RSS-Updates zu abonnieren, muss ein RSS-Plugin für den von Ihnen verwendeten Browser aktiviert sein.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.