Architect and build IPv6 networks on AWS

Alexandra Huides
Principal Network Specialist Solutions Architect
AWS
The WHYs
IPv6 adoption on AWS
WHY ADOPT IPv6 ON AWS?

- Improve network scalability
- Start building experience
- Minimize NAT (public & private)
- Simplify global connectivity
Improve network scalability

SIMPLY MORE ADDRESSES

NO MORE SUBNETTING CHALLENGES

IPV6-ONLY DEPLOYMENTS SUPPORTED
EASY TO DEPLOY & TEST
BUILD BACKWARDS COMPATIBILITY WITH IPV4
ADDRESS WHAT BRINGS VALUE

SIMPLY MORE ADDRESSES
NO MORE SUBNETTING CHALLENGES
IPV6-ONLY DEPLOYMENTS SUPPORTED

Start building experience

Improve network scalability
Improve network scalability:
- Simply more addresses
- No more subnetting challenges
- IPv6-only deployments supported

Start building experience:
- Easy to deploy & test
- Build backwards compatibility with IPv4
- Address what brings value

Minimize NAT (public & private):
- No need for public NAT
- No need for private NAT
- Improved visibility & security
Improve network scalability
- Simply more addresses
- No more subnetting challenges
- IPv6-only deployments supported

Start building experience
- Easy to deploy & test
- Build backwards compatibility with IPv4
- Address what brings value

Minimize NAT (public & private)
- No need for public NAT
- No need for private NAT
- Improved visibility & security

Simplify global connectivity
- No more overlapping IPs
- Integrate mergers and acquisitions
- Summarization and efficient routing
Improve network scalability
SIMPLY MORE ADDRESSES
NO MORE SUBNETTING CHALLENGES
IPV6-ONLY DEPLOYMENTS SUPPORTED

Start building experience
EASY TO DEPLOY & TEST
BUILD BACKWARDS COMPATIBILITY WITH IPV4
ADDRESS WHAT BRINGS VALUE

Minimize NAT (public & private)
NO NEED FOR PUBLIC NAT
NO NEED FOR PRIVATE NAT
IMPROVED VISIBILITY & SECURITY

Simplify global connectivity
NO MORE OVERLAPPING IPs
INTEGRATE Mergers and Acquisitions
SUMMARIZATION AND efficient ROUTING
Approaches

IPv6 adoption on AWS
IPv6 adoption approaches

Outside in (Edge first)

Inside out (Internal first)
Outside in (Edge first)

- Services layer
- Amazon VPC services
- VPC connectivity on AWS and hybrid
Outside in (Edge first)

- IPv6-enabled end-client experience
- Expanded user base in geographies with high IPv6 adoption
- No CGNAT in Service Provider networks for IPv6 clients
- Contribute to, and facilitate global IPv6 usage increase

¹Check [https://stats.labs.apnic.net/v6perf/XA](https://stats.labs.apnic.net/v6perf/XA)
We have enabled IPv6 on our load balancers (ALB) and CloudFront distributions so customers can already reach our services through IPv6. It turned out to be a very smooth process without any hiccups.

Within a short amount of time we were able to report nearly 40 percent of our customer traffic to be IPv6.

Hendrik Bergunde, Team Lead Technology - Aroundhome
Inside out (Internal first)
Unlock scale for container and platform deployments
Scale internal network connectivity
Accelerate the integration of mergers and acquisitions
Build familiarity with IPv6, adjust internal tooling
IPv6 adoption in the internal network enabled the full IP reachability Netflix needed across the thousands of VPCs without the need for Network Address Translation. Also, the Egress-only Internet Gateway helped maintain the private subnets security posture.

*Enabling IPv6 across the Netflix streaming platform in AWS enabled continued hyperscale growth, scalability and innovation.*

Donavan Fritz, Senior Network SRE - Netflix
IPv6 adoption on AWS

More customer stories
Focus areas
IPv6 adoption on AWS
IPv6 adoption focus areas

- Network
- Operating system
- App code
- Services & tools
Where to start with **IPv6 adoption** on AWS
IPv6 adoption
where to start

IPv6 addressing plan

Dual stack Amazon VPC
IPv6 addressing plan

Amazon-provided GUA (VPC-level)

Dual stack Amazon VPC
IPv6 addressing plan

10.1.0.0/16

2001:db8:1234:1a00::/56  (default IPv6 prefix size)

Amazon-provided GUA

Dual stack Amazon VPC
Dual stack Amazon VPC

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create
Create only the VPC resource or the VPC and other networking resources.
- VPC only
- VPC and more

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
- My-New-VPC

IPv4 CIDR block
- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block

IPv4 CIDR
- 10.1.0.0/16
  - CIDR block size must be between /16 and /28.

IPv6 CIDR block
- No IPv6 CIDR block
- IPAM-allocated IPv6 CIDR block
- Amazon-provided IPv6 CIDR block
- IPv6 CIDR owned by me

Network border group
A network border group is a unique group of Zones from where IPv4 and IPv6 IP addresses are advertised. All Availability Zones in this VPC will see this network border group.
- us-east-1

Tenancy
- Default
Dual stack Amazon VPC

Edit CIDRs
Add or remove CIDR blocks for your VPC.

IPv4 CIDRs
CIDR | Status
--- | ---
10.11.1.0/24 | Associated

Add new IPv4 CIDR

IPv6 CIDRs
CIDR (Network border group) | Pool
--- | ---

Add new IPv6 CIDR

Add IPv6 CIDR
IPv6 CDR block
- IPAM-allocated IPv6 CDR block
- Amazon-provided IPv6 CDR block
- IPv6 CDR owned by me

Network border group
A network border group is a unique group of Zones from where IPv4 and IPv6 IP addresses are advertised. All Availability Zones in this VPC will use this network border group.

You have no IPv6 CDR block.

Cancel | Select CDR
Dual stack Amazon VPC

Edit CIDRs

Add or remove CIDR blocks for your VPC.

**IPv4 CIDRs**

<table>
<thead>
<tr>
<th>CIDR</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.11.1.0/24</td>
<td>Associated</td>
</tr>
</tbody>
</table>

Add new IPv4 CIDR

**IPv6 CIDRs**

<table>
<thead>
<tr>
<th>CIDR (Network border group)</th>
<th>Pool</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2500::1f18:2992:5500::/56 (us-east-1)</td>
<td>Amazon</td>
<td>Associated</td>
</tr>
</tbody>
</table>

Add new IPv6 CIDR

Remove
Dual stack Amazon VPC

Amazon VPC

10.1.0.0/16

2001:db8:1234:1a00::/56

Amazon-provided GUA

- 10.1.0.0/24
  2001:db8:1234:1a00::/64

- 2001:db8:1234:1a01::/64

- 10.1.255.0/28
  2001:db8:1234:1a02::/64

- 2001:db8:1234:1a03::/64

- 10.1.64.0/22
  2001:db8:1234:1a04::/64

- 10.1.254.128/25
  2001:db8:1234:1a05::/64

- 2001:db8:1234:1a06::/64

- 10.1.155.0/24
  2001:db8:1234:1a07::/64
Dual stack Amazon VPC

Amazon VPC

10.1.0.0/16
IPv6 CIDR: /44 → /60 tiered IPv6 prefix size
Amazon-provided GUA
Dual stack Amazon VPC

IPv6 CIDR: /44 → /60

Amazon-provided GUA

- 10.1.0.0/24
  - /44 → /64
- 10.1.255.0/28
  - /44 → /64
- 10.1.64.0/22
  - /44 → /64
- 10.1.254.128/25
  - /44 → /64
- 10.1.55.0/24
  - /44 → /64
Dual stack Amazon VPC

10.1.0.0/16
Amazon-provided IPv6 Prefix
Randomly assigned by default
IPv6 addressing plan

Amazon-provided GUA (VPC-level)

Amazon-provided contiguous IPv6 GUA prefixes

Dual stack Amazon VPC
Amazon VPC IP Address Manager

Amazon-provided contiguous IPv6 prefixes
Amazon VPC IP Address Manager

Free tier
For IP management in a single AWS Region and account
Amazon-provided contiguous IPv6 blocks per Region and account

Advanced tier
For IP management across two or more AWS Regions and accounts
Amazon-provided contiguous IPv6 blocks across multiple Regions and accounts
IPv6 addressing plan

- Dual stack Amazon VPC
- Amazon-provided GUA (VPC-level)
- Amazon-provided contiguous IPv6 GUA prefixes
- Bring your own IPv6 (BYOIPv6) GUA prefixes
IPv6 addressing plan
BYOIPv6

In Amazon EC2
You can bring each address range to one AWS Region at a time.
You cannot share your IP address range with other accounts.
You can control if CIDRs in a pool can be publicly advertisable or not.
The most specific IPv6 address range that you can bring is /48 for CIDRs that are publicly advertisable and /56 for CIDRs that are not publicly advertisable.

With VPC IPAM
You can bring each address range to an IPAM top level Pool, and further split it across multiple Regional pools.
You can share your IP address range with other accounts.
You can control if CIDRs in a pool can be publicly advertisable or not.
The most specific IPv6 address range that you can bring is /48 for CIDRs that are publicly advertisable and /60 for CIDRs that are not publicly advertisable.
IPv6 addressing plan
BYOIPv6

Note: The prefix used for this presentation is an Amazon-owned IPv6 prefix, and prefix sizes are examples.
## IPv6 address planning summary

<table>
<thead>
<tr>
<th></th>
<th>Provisioning</th>
<th>Globally Unique</th>
<th>Internet advertisement</th>
<th>Internet Connectivity</th>
<th>NAT64 / NPT6</th>
<th>Summarization capabilities</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon-provided IPv6 GUA (VPC-level)</td>
<td>Directly at the VPC level</td>
<td>Yes</td>
<td>AWS advertised</td>
<td>Native on AWS</td>
<td>Not Required</td>
<td>Yes, for all VPCs created from the same IPAM Pool</td>
<td>Not recommended for large scale deployments (many VPCs)</td>
</tr>
<tr>
<td>Amazon-provided contiguous IPv6 prefixes</td>
<td>Amazon VPC IPAM free or advanced tiers</td>
<td>Yes</td>
<td>AWS advertised</td>
<td>Native on AWS</td>
<td>Not Required</td>
<td>No</td>
<td>No, for all VPCs created from the same IPAM Pool</td>
</tr>
<tr>
<td>BYOIPv6</td>
<td>Amazon EC2 or Amazon VPC IPAM</td>
<td>Yes</td>
<td>Configurable</td>
<td>Native on AWS if advertised from AWS</td>
<td>Not Required</td>
<td>Yes, for all VPCs created from the same BYOIPv6 pool</td>
<td>Facilitates growth on AWS, requires you to own IPv6 addresses, and prove ownership through the BYOIPv6 process.</td>
</tr>
</tbody>
</table>
IPv6 adoption

Inside out
Start with Dual stack Amazon VPC
### Dual stack Amazon VPC

#### IPv6 design

<table>
<thead>
<tr>
<th>Region</th>
<th>Amazon VPC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.0.0.0/16 + 2001:db8:1234:1a00::/56 (up to 5)</td>
</tr>
</tbody>
</table>

#### Availability Zone 1
- Subnet 10.0.0.0/24
- Subnet 10.0.1.0/24

#### Availability Zone 2
- Subnet 10.0.2.0/24
- Subnet 10.0.3.0/24
Dual stack Amazon VPC

IPv6 design

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56 (up to 5)

Destination | Target
10.0.0.0/16   | Local
2001:db8:1234:1a00::/56 | Local

VPC routing

Region

Availability Zone 1

Subnet 10.0.0.0/24

Subnet 10.0.1.0/24

Availability Zone 2

Subnet 10.0.2.0/24

Subnet 10.0.3.0/24
Dual stack Amazon VPC

IPv6 design

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56 (up to 5)

Availability Zone 1
Subnet 10.0.0.0/24

Subnet 10.0.1.0/24

Availability Zone 2
Subnet 10.0.2.0/24

Subnet 10.0.3.0/24

Amazon Route 53
VPC DNS

VPC CIDR +2
fd00:ec2::253

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Dual stack Amazon VPC
IPv6 design

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56 (up to 5)

Availability Zone 1
- Subnet 10.0.0.0/24
- Subnet 10.0.1.0/24
- Subnet 2001:db8:1234:1a01::/64

Availability Zone 2
- Subnet 10.0.2.0/24
- Subnet 10.0.3.0/24
- Subnet 2001:db8:1234:1a02::/64

VPC CIDR +2
fd00:ec2::253

VPC subnet types

Amazon Route 53
Build backwards compatibility

AWS DNS64 and NAT64
Dual stack Amazon VPC

IPv6 to IPv4 backwards compatibility

Q: Who is some-v4-only-domain.example.com?

Route 53 Resolver
IPv4 VPC CIDR+2
fd00:ec2::253

Answer: 1.2.3.4
Dual stack Amazon VPC
IPv6 to IPv4 backwards compatibility

DNS64

Region
Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56 (up to 5)

IPv6-only subnet
2001:db8:1234:1a00::/64

2001:db8:1234:1a00:ec2

 Recursive DNS lookup
Route 53 Resolver
IPv4 VPC CIDR+2
fd00:ec2::253

DNS64 settings
Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

Enable DNS64
Info
**Dual stack Amazon VPC**

**IPv6 to IPv4 backwards compatibility**

**DNS64**

---

**Amazon VPC**
- 10.0.0.0/16 + 2001:db8:1234:1a00::/56 (up to 5)

**IPv6 only subnet**
- 2001:db8:1234:1a00::/64

**Route 53 Resolver**
- IPv4 VPC CIDR+2
- fd00:ec2::253

**Recursive DNS lookup**

**Q: Who is some-v4-only-domain.example.com?**

**Answer:** 64:ff9b::1:2:3:4

**DNS64**

---

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Dual stack Amazon VPC
IPv6 to IPv4 backwards compatibility

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>2001:db8:1234:1a00::/56</td>
<td>Local</td>
</tr>
<tr>
<td>64:ff9b::/96</td>
<td>NATGW</td>
</tr>
</tbody>
</table>

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56 (up to 5)

IPv4 subnet 10.0.0.0/24
IP source = 10.0.0.20
IP destination = 1.2.3.4

IPv6-only subnet 2001:db8:1234:1a00::/64
IP source = 2001:db8:1234:1a00::ec2
IP destination = 64:ff9b::1:2:3:4

DNS64
NAT64

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Amazon Elastic Kubernetes Service

Simplify inside-out IPv6 adoption
IPv6 support for Amazon Compute Services

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56

Dual stack Subnet
10.0.0.0/24
2001:db8:1234:1a00::/64

Pod 1: 2001:db8:1234:1a00::1
Pod 1: 2001:db8:1234:1a00::2
...
Pod N: 2001:db8:1234:1a00::x

Pod 10.0.0.25
2001:db8:1234:1a00::ec2 + /80 assigned prefix

Amazon EKS
IPv6 support for Amazon EKS

POD ANATOMY

IPv6 prefix assignment only occurs at the EKS worker-node bootstrap time, which can help mitigate scenarios where high Pod churn EKS/IPv4 clusters are often delayed in Pod scheduling due to throttled API calls generated by the VPC CNI plug-in (ipamd) aimed to allocate Private IPv4 addresses in a timely fashion.
IPv6 support for Amazon EKS

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56

EKS implements a host-local CNI plugin, secondary to the VPC CNI plugin, which allocates and configures an IPv4 address for a Pod. The CNI plugin configures a host-specific non-routable IPv4 address for a Pod from the 169.254.172.0/22 range.

10.0.1.0/24
2001:db8:1234:1a01::/64

Worker Node
Pod
169.254.172.20
2001:db8:1234:1a01:1:2:3:4

CNI Host local
169.254.172.0/22

Primary ENI
10.0.0.25
2001:db8:1234:1a01::ec2
+/80 assigned prefix from subnet IPv6 CIDR

HOST LOCAL IPv4

The IPv4 address assigned to the Pod is unique to the worker-node and is not advertised or reachable beyond the worker-node.
ENABLE_V4_EGRESS (v1.15.1+)
Type: Boolean as a String
Default: true
Specifies whether PODs in an IPv6 cluster support IPv4 egress. If env is set to true, range 169.254.172.0/22 is reserved for IPv4 egress. When enabled, traffic egressing an IPv6 pod destined to an IPv4 endpoint will be SNAT’ed via the node IPv4 address. Note that enabling/disabling this feature only affects whether newly created pods have an IPv4 interface created. Therefore, it is recommended that you reboot existing nodes after enabling/disabling this feature.
IPv6 support for Amazon EKS

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

Pod
169.254.172.20
2001:db8:1234:1a01:12:3:4

Worker Node
CNI Host local
169.254.172.0/22

Primary ENI
10.0.0.25
2001:db8:1234:1a01::ec2
+ /80 assigned prefix from subnet IPv6 CIDR

Auto-assigned by AWS, immutable, not globally reachable – Private Network scope

Services / ClusterIP range
fd9e:89cb:a3d4::/108
IPv6 support for Amazon VPC

10.0.0.0/16 + 2001:db8:1234:1a00::/56

Dual stack Private Subnet

10.0.1.0/24
2001:db8:1234:1a01::/64

Pod to Pod on the same worker node
Any Pod-to-Pod communication across the nodes always uses an IPv6 address. VPC CNI configures iptables to handle IPv6 while blocking any IPv4 connections.
### IPv6 support for Amazon EKS

**Traffic Flows**

- **Pod to IPv6 endpoint outside of cluster**

**Amazon VPC**

10.0.0.0/16 + 2001:db8:1234:1a00::/56

**Dual stack Private Subnet**

10.0.1.0/24

2001:db8:1234:1a01::/64

**Worker Node**

Pod

169.254.172.20

2001:db8:1234:1a01:1:2:3:4

**IPv6**

- **IP source = POD IPv6 address**
- **IP destination = Endpoint IPv6 address**

**Route 53 Resolver**

**Internet Gateway**

**Egress-only Internet Gateway**

**The pod will perform a DNS query, and in this case, it receives an IPv6 address in return**
IPv6 support for Amazon EKS

Pod to an IPv6 endpoint on the internet

TRAFFIC FLOWS

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

Worker Node
169.254.172.20
2001:db8:1234:1a01:1:2:3:4

Primary ENI

Subnet route tables determine the path.

Destination | Target
--- | ---
10.0.0.0/16 | Local
2001:db8:1234:1a00::/56 | Local
0.0.0.0/0 | NATGW
::/0 | EIGW

Internet Gateway
Egress-only Internet Gateway

For egress to the internet, you can leverage the Egress-only internet gateway. Subnet route tables determine the path.
IPv6 support for Amazon VPC

10.0.0.0/16 + 2001:db8:1234:1a00::/56

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

Internet Gateway
Egress-only Internet Gateway
Route 53 Resolver

Q: Who is some-v4-only-domain.example.com?

Answer: 1:2:3:4 (An IPv4 address)

Pod to an IPv4 endpoint
IPv6 support for Amazon VPC

10.0.0.0/16 + 2001:db8:1234:1a00::/56

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

Pod
169.254.172.20
2001:db8:1234:1a01:1:2:3:4

Worker Node
IP = 169.254.172.20
IP destination = Endpoint IPv4 address

Primary ENI
10.0.1.25
2001:db8:1234:1a01:ec2
+ /80 assigned prefix from subnet IPv6 CIDR

Pod to an IPv4 endpoint

Traffic Flows

Amazon VPC
Internet Gateway
Egress-only Internet Gateway
Route 53 Resolver

IP source = 10.0.1.25
IP destination = Endpoint IPv4 address

Internet Gateway
Egress
only
Internet
Gateway

Primary ENI
10.0.1.25
2001:db8:1234:1a01:ec2
+ /80 assigned prefix from subnet IPv6 CIDR
IPv6 support for Amazon EKS

TRAFFIC FLOWS

Pod to an IPv4 endpoint on the internet
IPv6 support for Amazon VPC

Dual stack Private Subnet
10.0.0.0/16 + 2001:db8:1234:1a00::/56

Internet Gateway
Egress-only Internet Gateway
Route 53 Resolver

Traffic Flows
Pod to Kubernetes service (ClusterIP)

Pod
2001:db8:1234:1a02:1:2:3:4

IPv6 ClusterIP
fd9e:89cb:a3d4::38e7

Worker Node
Pod
2001:db8:1234:1a01:1:2:3:4

Internet Gateway
Egress-only Internet Gateway
Route 53 Resolver

IPv6 ClusterIP
fd9e:89cb:a3d4::38e7
IPv6 support for Amazon VPC

Availability Zone 1

10.0.0.0/16 + 2001:db8:1234:1a00::/56

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

Internet Gateway
Egress-only Internet Gateway
Route 53 Resolver

Traffic Flows

Ingress using dual stack load balancers: Public

Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56

Dual stack Public Subnet
10.0.0.0/24
2001:db8:1234:1a00::/64

AAAA record: IPv6 addresses
A record: Elastic IPv4 addresses

Dual stack Application Load Balancer

my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com

Destination Target
10.0.0.0/16 Local
2001:db8:1234:1a00::/56 Local
0.0.0.0/0 NAGW
/:0 IGW

Private subnets

Destination Target
10.0.0.0/16 Local
2001:db8:1234:1a00::/56 Local
0.0.0.0/0 NATGW
/:0 EIGW

Public subnets

Destination Target
10.0.0.0/16 Local
2001:db8:1234:1a00::/56 Local
0.0.0.0/0 NATGW
/:0 EIGW

Worker Node

Pod
169.254.172.20
2001:db8:1234:1a01:1:2:3:4
**IPv6 support for Amazon EKS**

Ingress using dual stack load balancers: Public

**TRAFFIC FLOWS**

<table>
<thead>
<tr>
<th>Private subnets</th>
<th>Public subnets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Target</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>2001:db8:1234:1a00::/56</td>
<td>Local</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>IGVW</td>
</tr>
<tr>
<td>::/0</td>
<td>IGVW</td>
</tr>
</tbody>
</table>

**Amazon VPC**

10.0.0.0/16 + 2001:db8:1234:1a00::/56

**Dual stack Public Subnet**

10.0.0.0/24
2001:db8:1234:1a00::/64

**Dual stack Private Subnet**

10.0.1.0/24
2001:db8:1234:1a01::/64

**IPv6**

169.254.172.20
2001:db8:1234:1a01::1234:5

**Internet Gateway**

**Egress-only Internet Gateway**

**Route 53 Resolver**

**Traffic Flows**

**Ingress using dual stack load balancers: Public**

**AAAA record: IPv6 addresses**

**A record: Elastic IPv4 addresses**

**Pod**

169.254.172.20
2001:db8:1234:1a01::1:2:3:4

my-loadbalancer-1234567890.us-east-1.elb.amazonaws.com
IPv6 support for Amazon VPC

Availability Zone 1

10.0.0.0/16
+ 2001:db8:1234:1a00::/56

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

Internet Gateway
Egress - only

TRAFFIC FLOWS

Ingress using dual stack load balancers: Private

ipv6.deny_all_igw_traffic blocks internet gateway (IGW) access to the load balancer, preventing unintended access to your internal load balancer through an internet gateway. It is set to true for internal load balancers.

Dual stack Public Subnet
10.0.0.0/24
2001:db8:1234:1a00::/64

AAAA record: IPv6 addresses
A record: Private IPv4 addresses

Dual stack Application / Network Load Balancer

Dual stack Private Subnet
10.0.1.0/24
2001:db8:1234:1a01::/64

Destination Target
10.0.0.0/16 Local
2001:db8:1234:1a00::/56 Local
0.0.0.0/0 EIGW
::/0 NATGW

10.0.0.0/16
2001:db8:1234:1a00::/56
0.0.0.0/0
::/0

169.254.172.20
2001:db8:1234:1a01:1:2:3:4

Worker Node
Pod
IPv6

IPv6 support for Amazon EKS

How about Pod v4 to Pod v6?
IPv6 support for 
Amazon EKS

IPv6 support for
TRAFFIC FLOWS

How about Pod v4 to Pod v6?

V6 cluster

Worker Node

Primary ENI
10.0.0.25
2001:db8:1234:1a01::ec2

Pod
169.254.172.20
2001:db8:1234:1a01:1:2:3:4

CNI Host local
169.254.172.0/22

V4 cluster

Worker Node

Primary ENI
10.1.1.25

Pod
10.1.1.20

V6 cluster

ENABLE_V6_EGRESS (v1.13.0+)

Type: Boolean as a String
Default: false

Specifies whether PODs in an IPv4 cluster support IPv6 egress. If set to true, range fd00::ac:00/118 is reserved for IPv6 egress. This feature also requires that the node has an IPv6 address assigned to its primary ENI, as this address is used for SNAT to IPv6 endpoints outside of the cluster. If the configuration prerequisites are not met, the egress-cni plugin is not enabled and an error log is printed in the aws-node container. Note that enabling/disabling this feature only affects whether newly created pods have an IPv6 interface created.
IPv6 support for Amazon EKS

Native v6 egress for v4 EKS clusters
Build IPv6 network connectivity
IPv6 network connectivity
Amazon VPC
10.0.0.0/16 + 2001:db8:1234:1a00::/56 (up to 5)

Public subnets

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>2001:db8:1234:1a00::/56</td>
<td>Local</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>IGW</td>
</tr>
<tr>
<td>::/0</td>
<td>IGW</td>
</tr>
</tbody>
</table>

Internet Gateway

IPv4
IPv6

EIP: 10.0.0.4 <> 18.4.2.1
EIP: 10.0.0.4 <> 53.1.23.4

Public subnets
### Dual stack Amazon VPC

**Internet connectivity**

**Public subnets**
- Destination: 10.0.0.0/16, Target: Local
- Destination: 2001:db8:1234:1a00::/56, Target: Local
- Destination: 0.0.0.0/0, Target: IGW

**Private subnets**
- Destination: 10.0.0.0/16, Target: Local
- Destination: 2001:db8:1234:1a00::/56, Target: Local
- Destination: ::/0, Target: EIGW

**Public subnets**
- Destination: 10.0.0.0/16, Target: Local
- Destination: 2001:db8:1234:1a00::/56, Target: Local
- Destination: 0.0.0.0/0, Target: IGW

**Subnets**
- Subnet 10.0.1.0/24: 10.0.1.4
- Subnet 10.0.2.0/24: 10.0.2.4
- Subnet 2001:db8:1234:1a00::ec2

**Internet Gateway**
- Egress-only Internet Gateway

**IPv4**
- Internet
  - IPv4
  - IPv6

**IPv6**
- Internet
  - IPv4
  - IPv6
**Dual stack Amazon VPC**

**Internet connectivity**

- **Public subnets**
- **Private subnets**

<table>
<thead>
<tr>
<th>Region</th>
<th>Amazon VPC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.0.0.0/16 + 2001:db8:1234:1a00::/56</td>
</tr>
</tbody>
</table>

- **Private IPv6-only subnets**
  - Destination | Target |
  - 10.0.0.0/16 | Local |
  - 2001:db8:1234:1a00::/56 | Local |
  - ::/0 | EIGW |
  - 64:ff9b::/96 | NATGW |

- **Subnets**
  - Subnet 10.0.1.0/24
  - Subnet 10.0.2.0/24
    - 2001:db8:1234:1a00::/64
  - Subnet 2001:db8:1234:1a01::/64

- **Internet Gateway**
  - Public NAT Gateway
  - Egress-only Internet Gateway

- **IPv4**
- **IPv6**
IPv6 network connectivity

Internet connectivity

VPC to VPC connectivity
### Dual stack Amazon VPC

**VPC to VPC connectivity**

<table>
<thead>
<tr>
<th>VPC Peering</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amazon VPC-1</strong></td>
</tr>
<tr>
<td>10.0.0.0/16 + 2001:db8:1234:1a00::/56</td>
</tr>
</tbody>
</table>

#### VPC-1 Route Table(s)

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>2001:db8:1234:1a00::/56</td>
<td>Local</td>
</tr>
<tr>
<td>10.1.0.0/16</td>
<td>PCX-ID</td>
</tr>
<tr>
<td>2001:db8:1234:1b00::/56</td>
<td>PCX-ID</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VPC Peering</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amazon VPC-2</strong></td>
</tr>
<tr>
<td>10.1.0.0/16 + 2001:db8:1234:1b00::/56</td>
</tr>
</tbody>
</table>

#### VPC-2 Route Table(s)

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>2001:db8:1234:1b00::/56</td>
<td>Local</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>PCX-ID</td>
</tr>
<tr>
<td>2001:db8:1234:1a00::/56</td>
<td>PCX-ID</td>
</tr>
</tbody>
</table>
Dual stack Amazon VPC

VPC to VPC connectivity

<table>
<thead>
<tr>
<th>Region</th>
<th>VPC-1 Route Table(s)</th>
<th>VPC-2 Route Table(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Destination</td>
<td>Target</td>
</tr>
<tr>
<td></td>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td>2001:db8:1234:1a00::/56</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td>::/0</td>
<td>IGW/EIGW</td>
</tr>
<tr>
<td></td>
<td>RFC1918</td>
<td>TGW</td>
</tr>
<tr>
<td></td>
<td>IPv6 summary route</td>
<td>TGW</td>
</tr>
</tbody>
</table>

Amazon VPC-1
10.0.0.0/16 + 2001:db8:1234:1a00::/56

DUAL STACK ATTACHMENT SUBNET

TGW ENI

AWS Transit Gateway

Internet Gateway

Egress-only Internet Gateway

Amazon VPC-2
10.1.0.0/16 + 2001:db8:1234:1b00::/56

DUAL STACK ATTACHMENT SUBNET

TGW ENI

TGW Route Table(s)

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>VPC-1 attachment</td>
</tr>
<tr>
<td>2001:db8:1234:1a00::/56</td>
<td>VPC-1 attachment</td>
</tr>
<tr>
<td>10.1.0.0/16</td>
<td>VPC-2 attachment</td>
</tr>
<tr>
<td>2001:db8:1234:1b00::/56</td>
<td>VPC-2 attachment</td>
</tr>
</tbody>
</table>
Dual stack Amazon VPC

VPC to VPC connectivity

VPC Peering

AWS Transit Gateway

AWS Cloud WAN

Region

VPC A
Dual stack

Network segment A

AWS Cloud WAN
IPv4 & IPv6

Network segment B

VPC C
IPv4-only

Network segment C
IPv6 network connectivity

- Internet connectivity
- VPC to VPC connectivity
- Hybrid connectivity
Dual stack Amazon VPC

Hybrid connectivity

AWS Direct Connect

IPv4 & IPv6 BGP PEERS

DX Point of presence

Customer gateway

Corporate data center

Region

DX Gateway

AWS Transit Gateway

Region

DX Gateway

AWS Transit Gateway

Transit VIF

DX Router

DC Router
Dual stack Amazon VPC

Hybrid connectivity

AWS Direct Connect
AWS Site-to-Site VPN

Region

AWS Transit Gateway

AWS Site-to-site VPN connection A – IPv4

AWS Site-to-site VPN connection B – IPv6

Internet

Corporate data center

192.168.0.0/16
2001:db8:5678::/56

/30 IPv4 inner Tunnel IPs
/126 IPv6 inner Tunnel IPs
Dual stack Amazon VPC

Hybrid connectivity

AWS Direct Connect
AWS Site-to-Site VPN

AWS Cloud WAN

Network segment C

AWS Site-to-site VPN connection A – IPv4

AWS Site-to-site VPN connection B – IPv6

AWS Site-to-site VPN connection C – IPv4

AWS Site-to-site VPN connection D – IPv6

192.168.0.0/16
2001:db8:5678::/56

Corporate data center

Customer Gateway

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
IPv6 adoption

Outside in
Configure IPv6 support for **Internal and external service delivery**
IPv6 for service delivery on AWS
IPv6 for service delivery on AWS

Application Load Balancer

Amazon VPC
10.0.0.0/16
2001:db8:1234:1a00::/56

Availability Zone 1
DUAL STACK SUBNET
ALB ENIs
IPv4 + IPv6

Availability Zone 2
DUAL STACK SUBNET
ALB ENIs
IPv4 + IPv6

Targets Subnet

my-loadbalancer-1234567890.elb.us-east-1.amazonaws.com

AAAA records: IPv6 addresses
A records: Elastic IPv4 addresses

Egress-only Internet Gateway

Targets can be IPv4 or IPv6
IPv6 for service delivery on AWS

Elastic Load Balancing

IPv6-ONLY INTERNET-FACING ALB

my-loadbalancer-1234567890.elb.us-east-1.amazonaws.com

Amazon VPC
10.0.0.0/16
2001:db8:1234:1a00::/56

Availability Zone 1
DUAL STACK SUBNET
ALB ENIs
IPv4 + IPv6

Availability Zone 2
DUAL STACK SUBNET
ALB ENIs
IPv4 + IPv6

Application Load Balancer

Egress-only Internet Gateway
AAA records: IPv6 addresses
A records: Elastic IPv4 addresses

Targets Subnet
Targets can be IPv4 or IPv6

Targets can be IPv4 or IPv6

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
IPv6 for service delivery on AWS

Elastic Load Balancing

Amazon VPC
10.0.0.0/16
2001:db8:1234:1a00::/56

Availability Zone 1

Availability Zone 2

Dual Stack Subnet
NLB Hyperplane ENI
IPv4 + IPv6

Targets Subnet

Network Load Balancer

AAA records: IPv6 addresses
A records: Elastic IPv4 addresses

Targets can be IPv4 or IPv6

my-loadbalancer-1234567890.elb.us-east-1.amazonaws.com

Egress-only Internet Gateway

Internet Gateway

IPv6 for service delivery on AWS

Application Load Balancer

Network Load Balancer

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
IPv6 for service delivery on AWS

Elastic Load Balancing

Application Load Balancer
Network Load Balancer
Gateway Load Balancer
IPv6 for service delivery on AWS

Elastic Load Balancing

Amazon VPC Lattice
VPCL FQDN: serviceA-e8f160e640d36ad99.7d67968.vpc-lattice-svcs.us-west-2.on.aws
• A: 169.254.x.x
• AAAA: fd00:ec2:80::x
IPv6 for service delivery on AWS

- Elastic Load Balancing
- Amazon VPC Lattice
- AWS PrivateLink
IPv6 for service delivery on AWS

AWS PrivateLink
Inside-out and Outside-in

Secure IPv6 connectivity
Secure IPv6 connectivity on AWS

VPC Network Access Control Lists

NATIVE IPv4 & IPv6
Secure IPv6 connectivity on AWS

VPC Security Groups

NATIVE IPv4 & IPv6
Secure IPv6 connectivity on AWS

AWS Network Firewall

Amazon VPC
10.0.0.0/16
2001:db8:1234:1a00::/56

Firewall Subnet
10.0.0.0/24

AWS Network Firewall endpoint
10.0.0.15
2001:db8:1234:1a00::/64

or

Firewall Subnet
10.0.1.0/24
2001:db8:1234:1a00::/64

AWS Network Firewall endpoint
10.0.1.15
2001:db8:1234:1a00::ec2

or

Firewall Subnet
2001:db8:1234:1a01::/64

AWS Network Firewall endpoint
2001:db8:1234:1a01::ec2

Secure IPv6 connectivity on AWS

AWS Network Firewall
Secure IPv6 connectivity on AWS

AWS WAF & AWS Shield

AWS WAF
Protects web applications by allowing you to write custom rules or choose managed rules from AWS or the AWS Marketplace.

AWS Shield & Shield Advanced
Managed threat protection that blocks DDoS attacks, vulnerability exploitation, and bad bots

IPv4 & IPv6
Build

Scalable IPv6 internet edge connectivity
Scalable IPv6 edge connectivity
Scalable IPv6 edge connectivity

DUAL STACK BY DEFAULT

Amazon CloudFront

IPv4

IPv6

AWS WAF

AWS Shield & Shield Advanced

Amazon CloudFront

Elastic Load Balancing

Amazon Elastic Compute Cloud

Amazon Simple Storage Service (S3)

Custom Origins
Scalable IPv6 edge connectivity

Amazon CloudFront

AWS Global Accelerator
Scalable IPv6 edge connectivity

AWS Global Accelerator

IPv4

IPv6

2 ANYCAST IPv4 ADDRESSES

2 ANYCAST IPv6 ADDRESSES

DUAL STACK

AWS Shield & Shield Advanced

AWS Global Accelerator

AWS WAF

Elastic Load Balancing

DUAL STACK

Amazon Elastic Compute Cloud

DUAL STACK
IPv6 on AWS
Service compatibility matrix
IPv6 on AWS

Start now

All resources
Thank you!