The Cloud, IPv6 and the Enterprise

Radek Zajíc, radek@zajic.v.pytli.cz • Enterprise & IPv6 Workshop, 2023-04-24

Dark Clouds by *Christoph Kummer*, *CC BY-NC-SA 2.0*

about::myself

Radek Zajíc

WORLD IPv6 LAUNCH

SEZNAM.CZ

T · · Mobile ·

sky | showmax

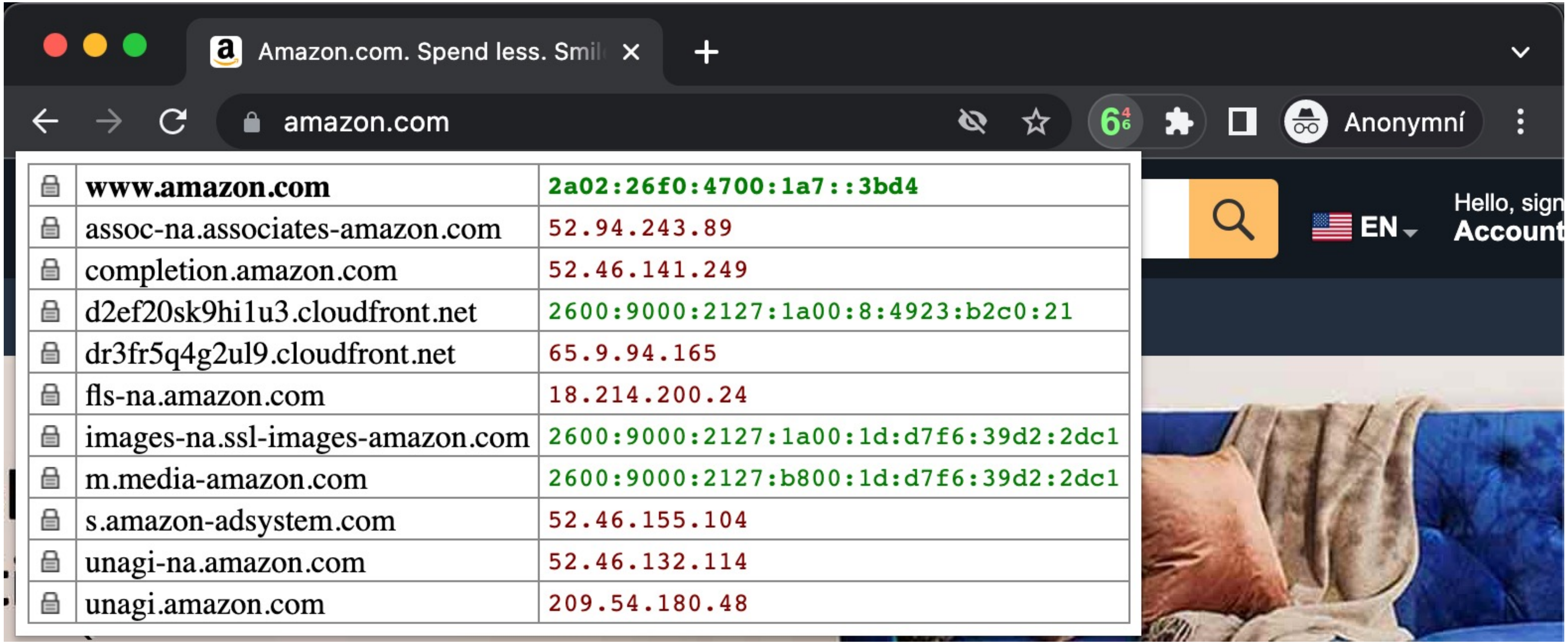
Blog: showmax.engineering
Twitter: @ShowmaxDevs

Enterprises

have traditionally operated an on-premises infrastructure

Enterprises

some even enabled IPv6



🔒	**www.amazon.com**	2a02:26f0:4700:1a7::3bd4
🔒	assoc-na.associates-amazon.com	52.94.243.89
🔒	completion.amazon.com	52.46.141.249
🔒	d2ef20sk9hi1u3.cloudfront.net	2600:9000:2127:1a00:8:4923:b2c0:21
🔒	dr3fr5q4g2ul9.cloudfront.net	65.9.94.165
🔒	fls-na.amazon.com	18.214.200.24
🔒	images-na.ssl-images-amazon.com	2600:9000:2127:1a00:1d:d7f6:39d2:2dc1
🔒	m.media-amazon.com	2600:9000:2127:b800:1d:d7f6:39d2:2dc1
🔒	s.amazon-adsystem.com	52.46.155.104
🔒	unagi-na.amazon.com	52.46.132.114
🔒	unagi.amazon.com	209.54.180.48

```
# whois 2a02:26f0:4700:1a7::3bd4

inet6num:       2a02:26f0:4700::/48
netname:        AKAMAI-PA
descr:          Akamai Technologies
country:        EU
```

Today we're all moving to *The Cloud*

Even enterprises.

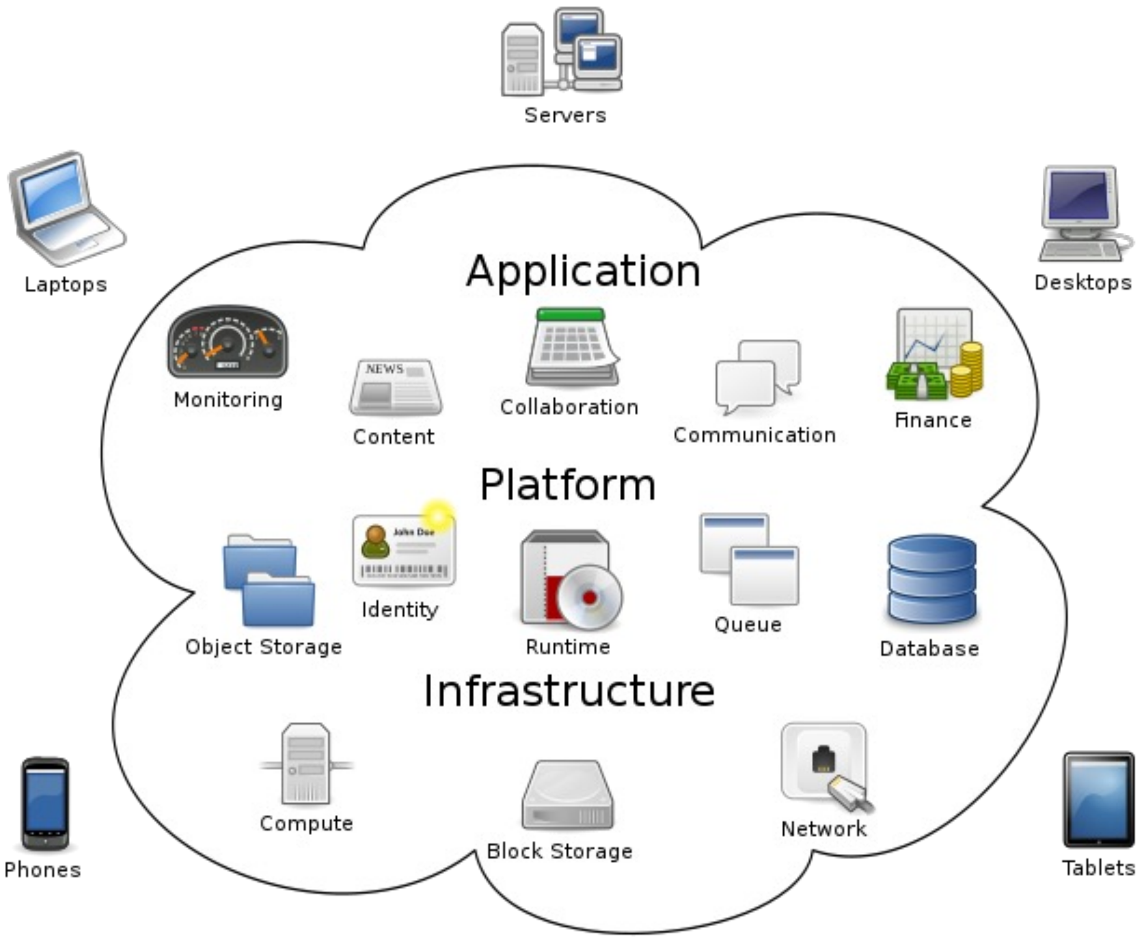
And some want (or need) IPv6.

But what is *The Cloud?*

Feature disparity as a service.

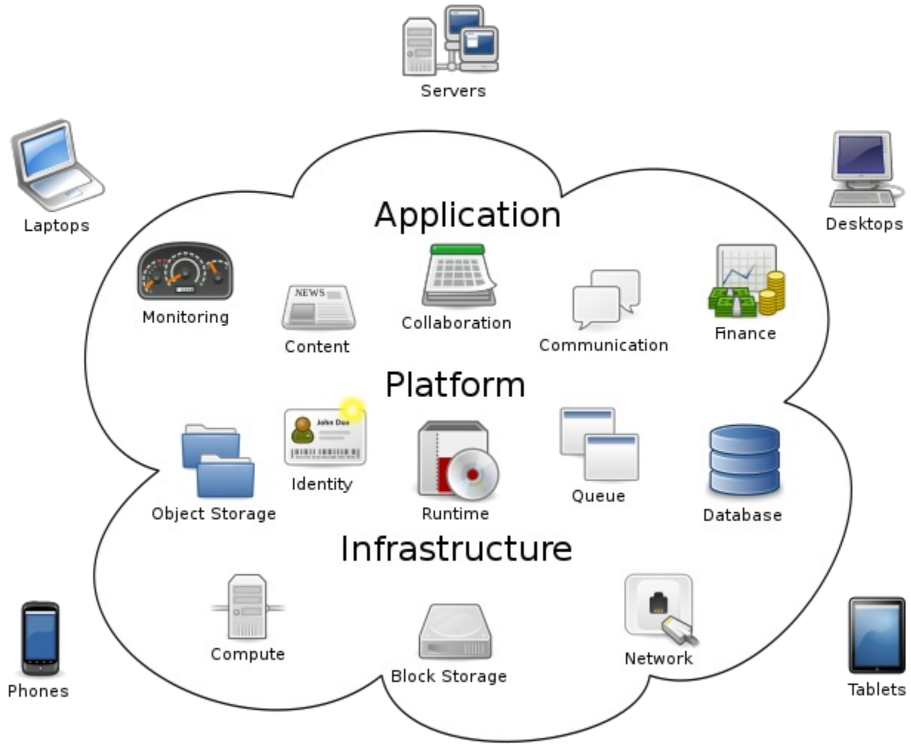
Everything as a service.

What is *The Cloud?*

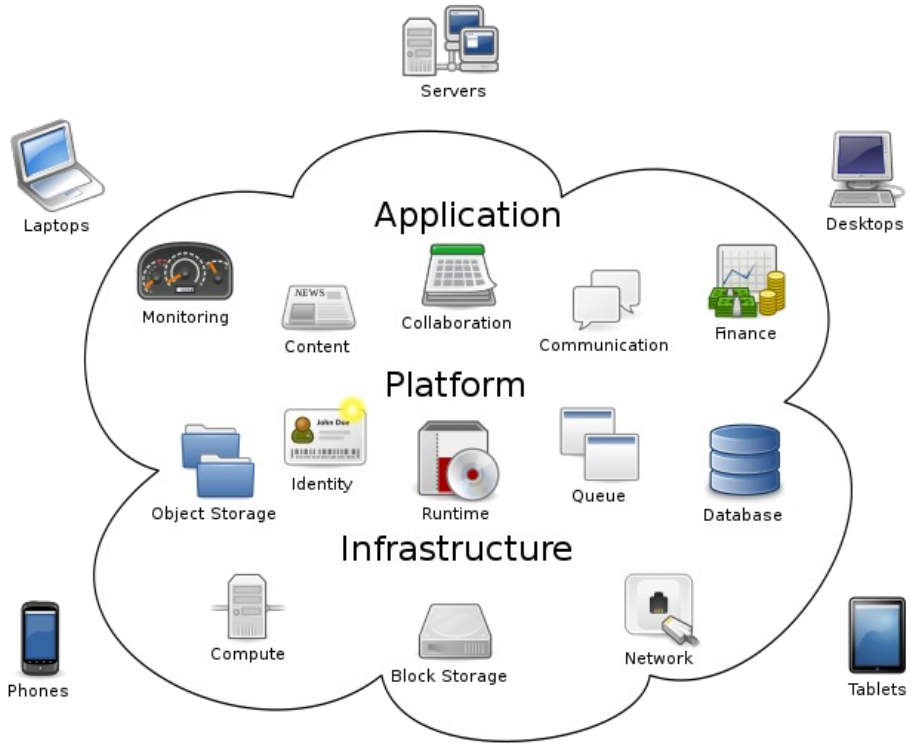


https://commons.wikimedia.org/wiki/File:Cloud_computing.svg

What is *hybrid Cloud?*



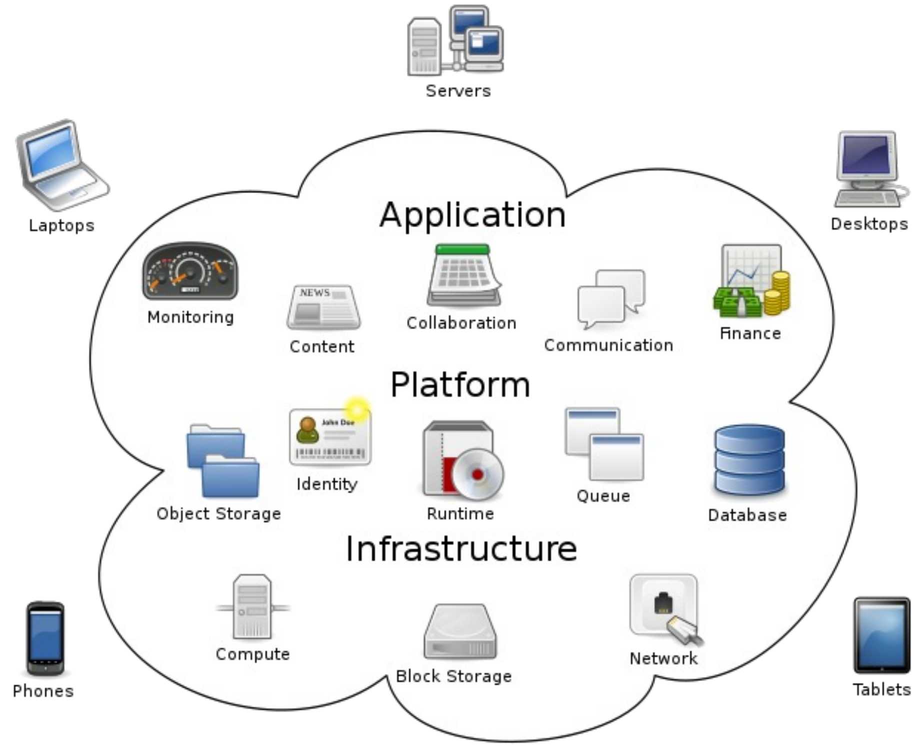
Cloud One



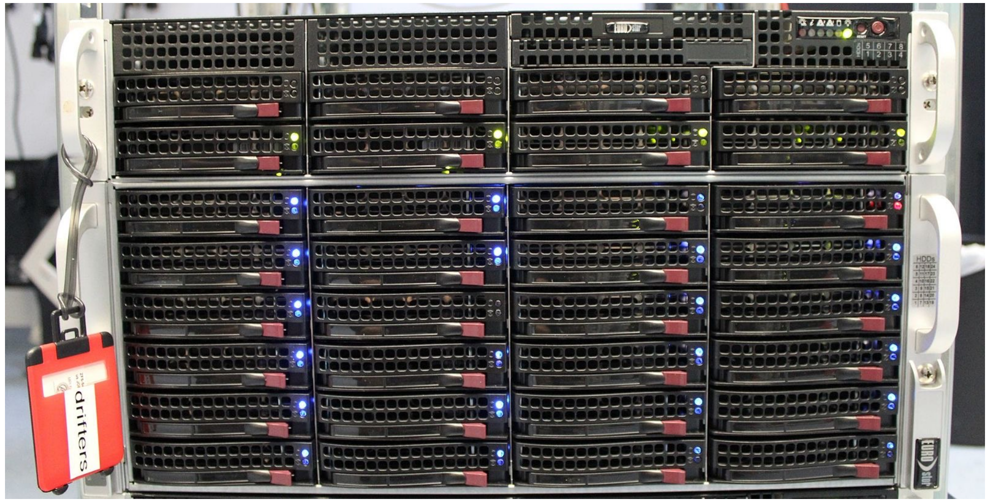
Cloud Two

https://commons.wikimedia.org/wiki/File:Cloud_computing.svg

What else is *hybrid Cloud?*



Cloud

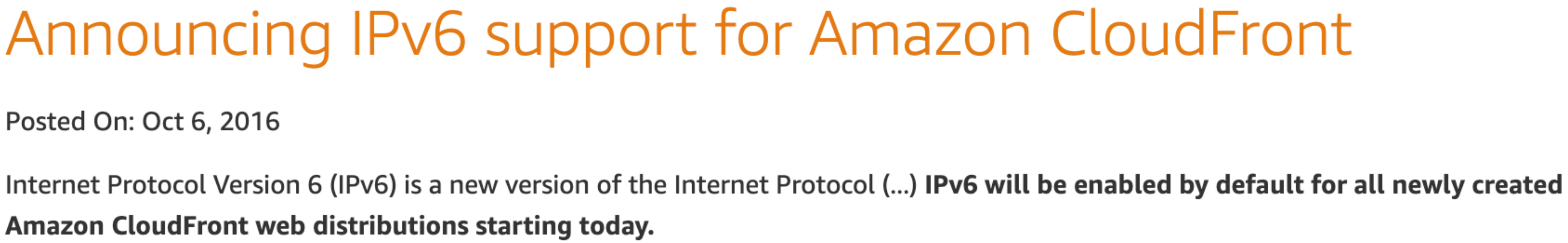


On-prem infra

https://commons.wikimedia.org/wiki/File:ZFS_server_front_26.jpg

Cloud & IPv6: The Edge

CDNs

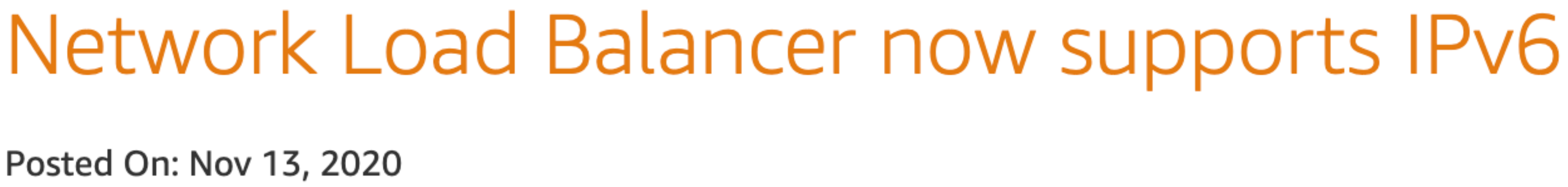


Announcing IPv6 support for Amazon CloudFront

Posted On: Oct 6, 2016

Internet Protocol Version 6 (IPv6) is a new version of the Internet Protocol (...) **IPv6 will be enabled by default for all newly created Amazon CloudFront web distributions starting today.**

Load Balancers



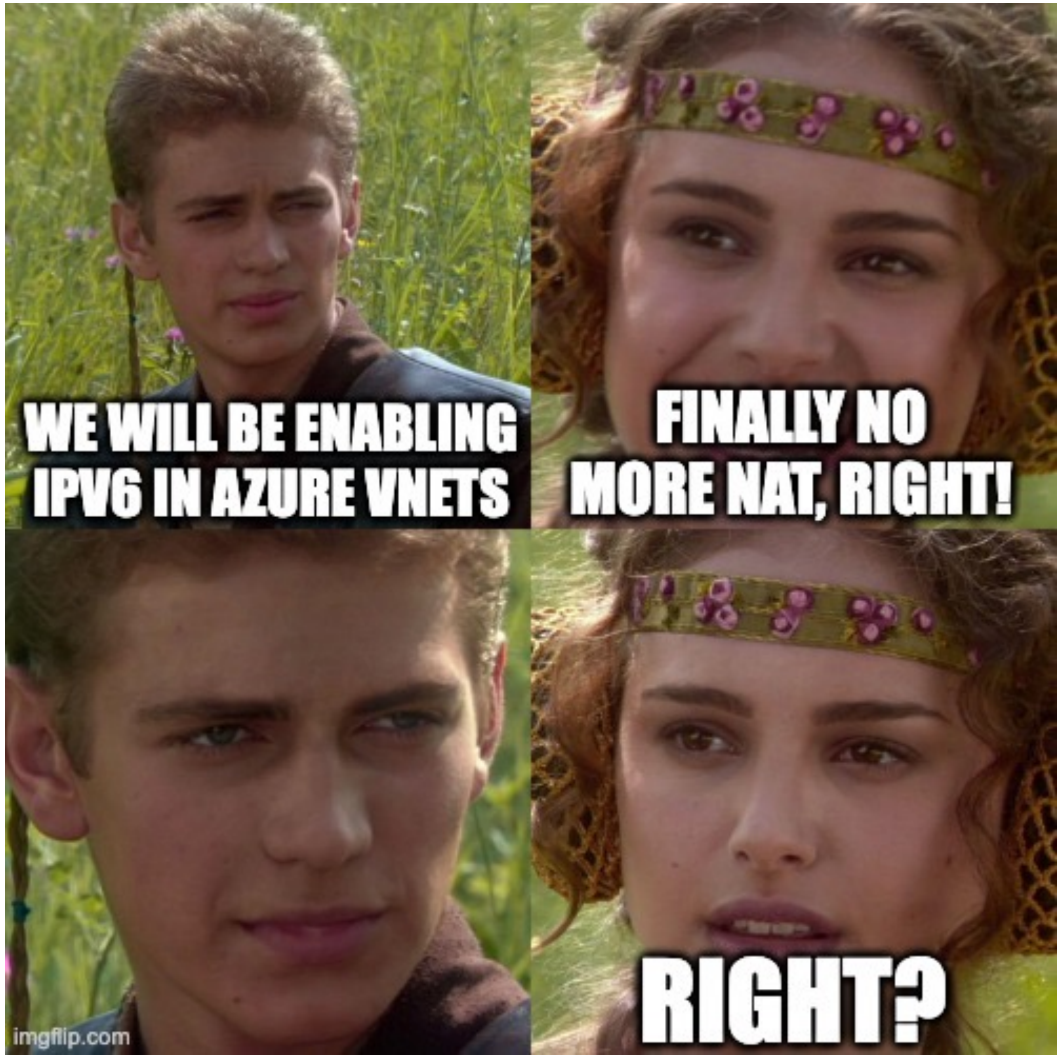
Network Load Balancer now supports IPv6

Posted On: Nov 13, 2020

Cloud & IPv6: Network

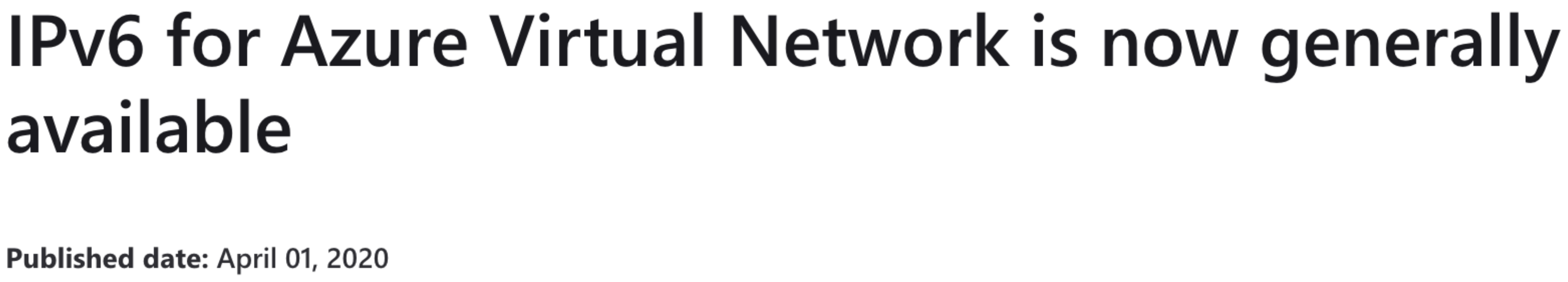
A network like no other

Cloud & IPv6: Network


WE WILL BE ENABLING IPV6 IN AZURE VNETS
FINALLY NO MORE NAT, RIGHT!
RIGHT?
imgflip.com

Cloud & IPv6: Compute

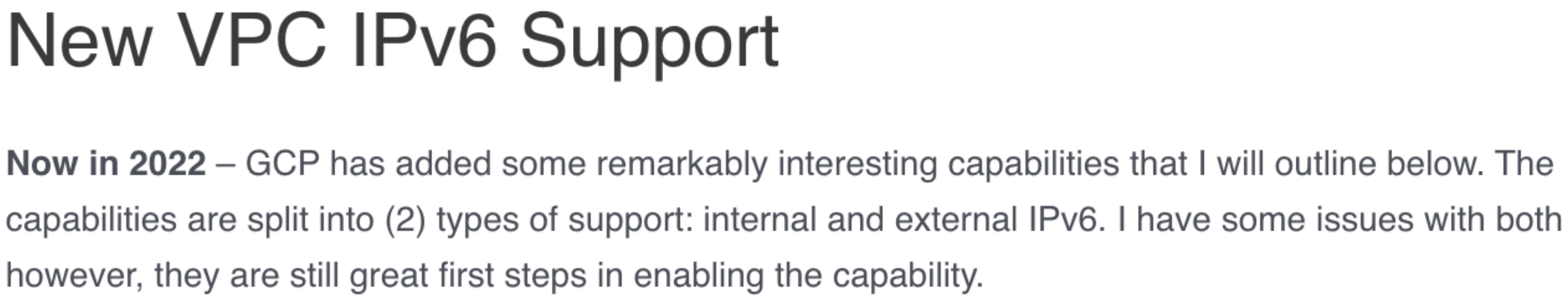
Virtual networks



IPv6 for Azure Virtual Network is now generally available

Published date: April 01, 2020

Compute instances



New VPC IPv6 Support

Now in 2022 – GCP has added some remarkably interesting capabilities that I will outline below. The capabilities are split into (2) types of support: internal and external IPv6. I have some issues with both however, they are still great first steps in enabling the capability.

https://www.tachyondynamics.com/2022/06/06/google-cloud-platform-gcp-and-new-ipv6-support/

Cloud & IPv6: Compute

FULL IPV6 IN THE PUBLIC CLOUD
ME
GOOGLE CLOUD
ME
FULL IPV6 IN THE PUBLIC CLOUD
imgflip.com

Cloud & IPv6: Storage & DB

Object storage*

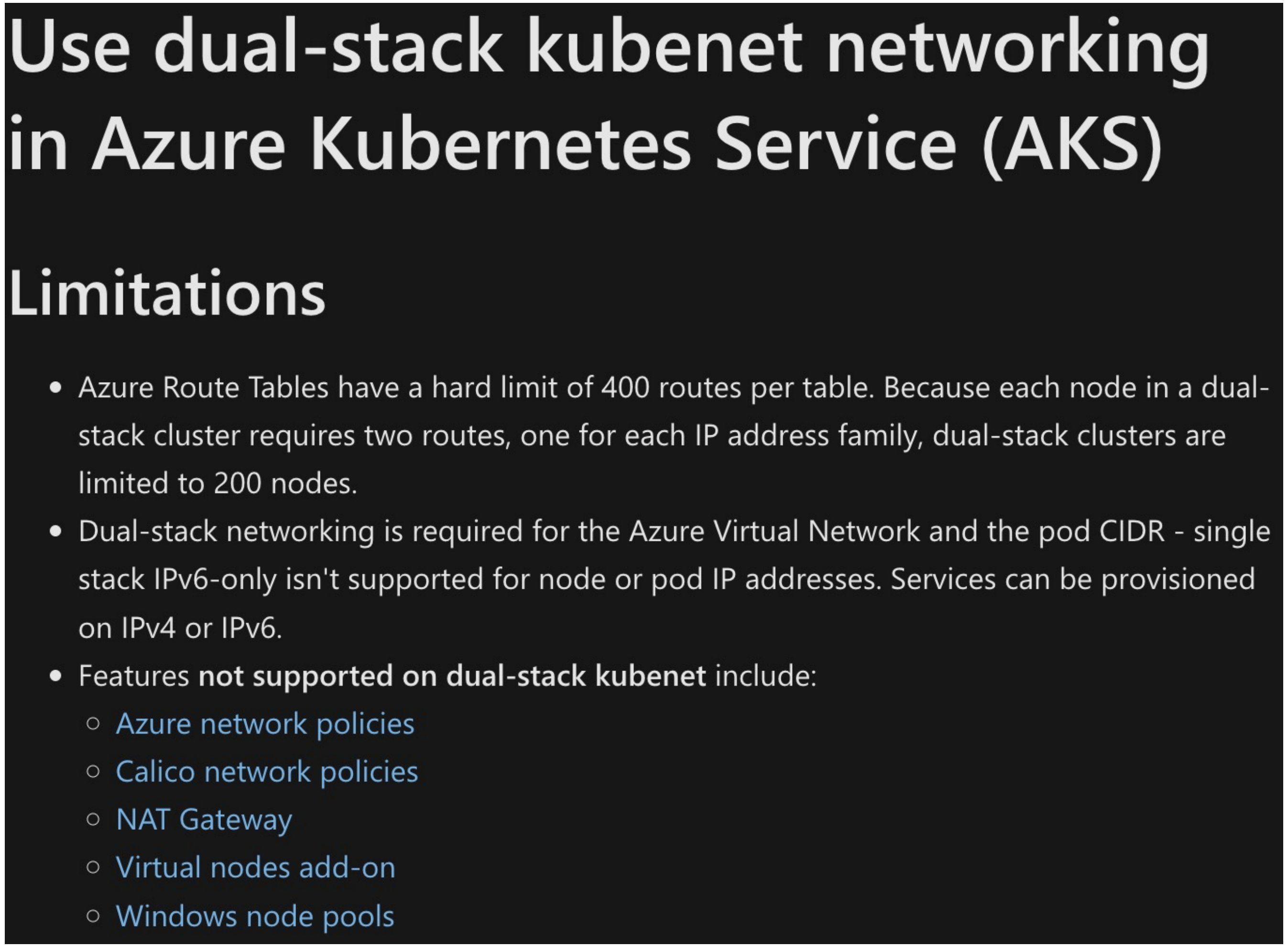
Databases*

~~File storage~~

Cloud & IPv6: Containers

Dual-stack Kubernetes

Cloud & IPv6: Containers

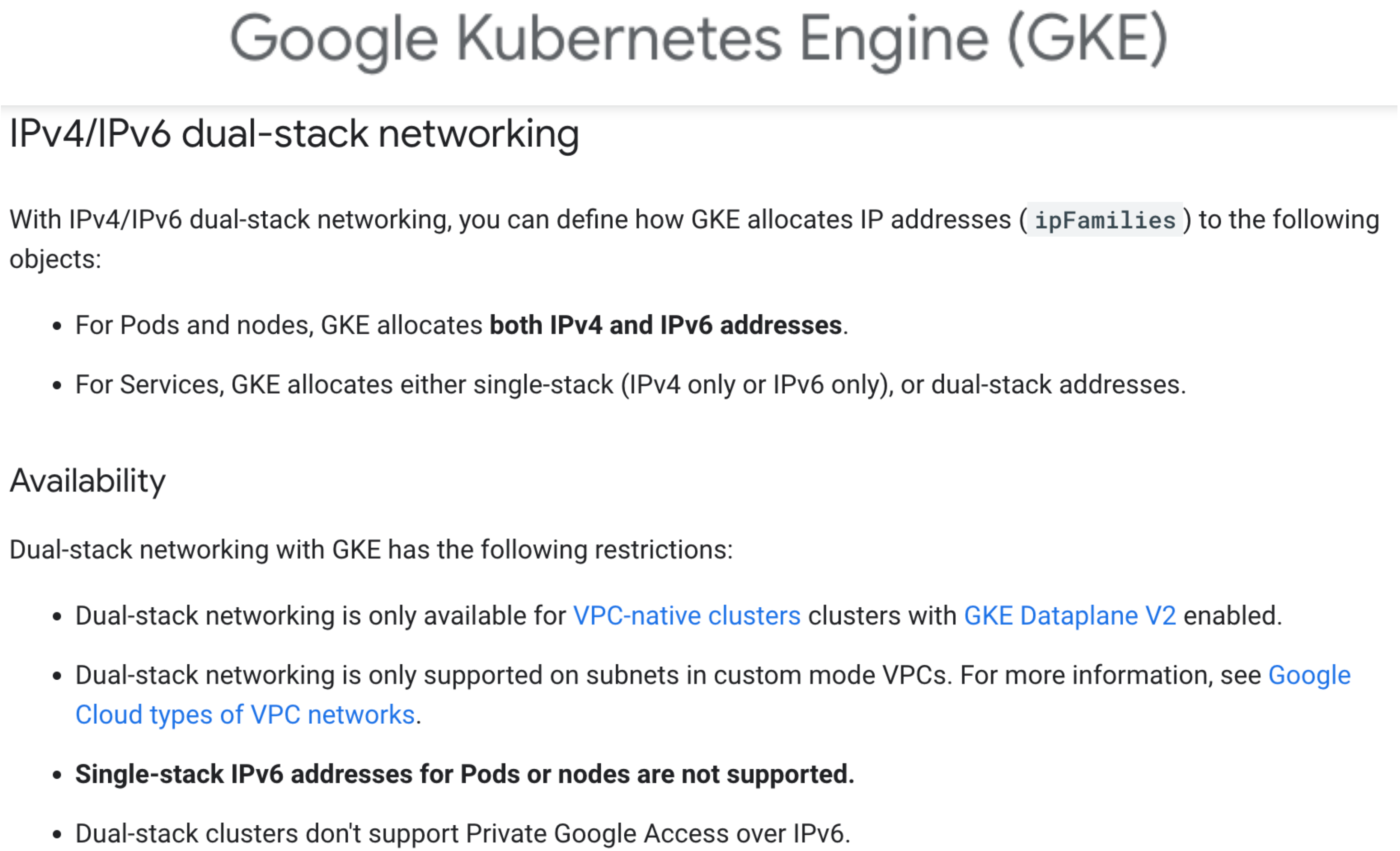


Use dual-stack kubenet networking in Azure Kubernetes Service (AKS)

Limitations

- Azure Route Tables have a hard limit of 400 routes per table. Because each node in a dual-stack cluster requires two routes, one for each IP address family, dual-stack clusters are limited to 200 nodes.
- Dual-stack networking is required for the Azure Virtual Network and the pod CIDR - single stack IPv6-only isn't supported for node or pod IP addresses. Services can be provisioned on IPv4 or IPv6.
- Features **not supported on dual-stack kubenet** include:
    - Azure network policies
    - Calico network policies
    - NAT Gateway
    - Virtual nodes add-on
    - Windows node pools

Cloud & IPv6: Containers



Google Kubernetes Engine (GKE)

IPv4/IPv6 dual-stack networking

With IPv4/IPv6 dual-stack networking, you can define how GKE allocates IP addresses (`ipFamilies`) to the following objects:

- For Pods and nodes, GKE allocates **both IPv4 and IPv6 addresses**.
- For Services, GKE allocates either single-stack (IPv4 only or IPv6 only), or dual-stack addresses.

Availability

Dual-stack networking with GKE has the following restrictions:

- Dual-stack networking is only available for VPC-native clusters clusters with GKE Dataplane V2 enabled.
- Dual-stack networking is only supported on subnets in custom mode VPCs. For more information, see Google Cloud types of VPC networks.
- **Single-stack IPv6 addresses for Pods or nodes are not supported.**
- Dual-stack clusters don't support Private Google Access over IPv6.

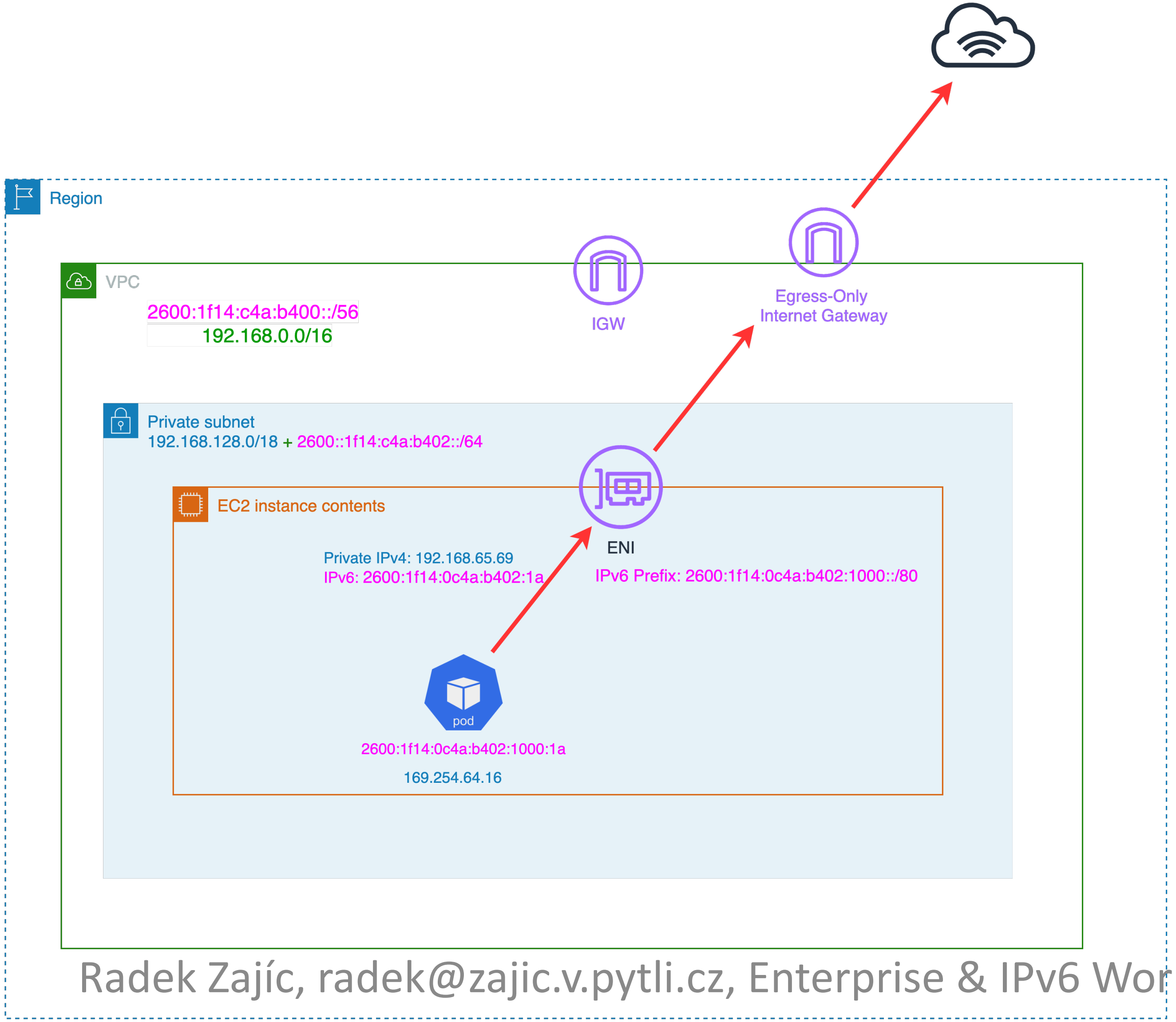
Cloud & IPv6: Containers

Dual-stack Kubernetes

~~IPv6-only Kubernetes~~

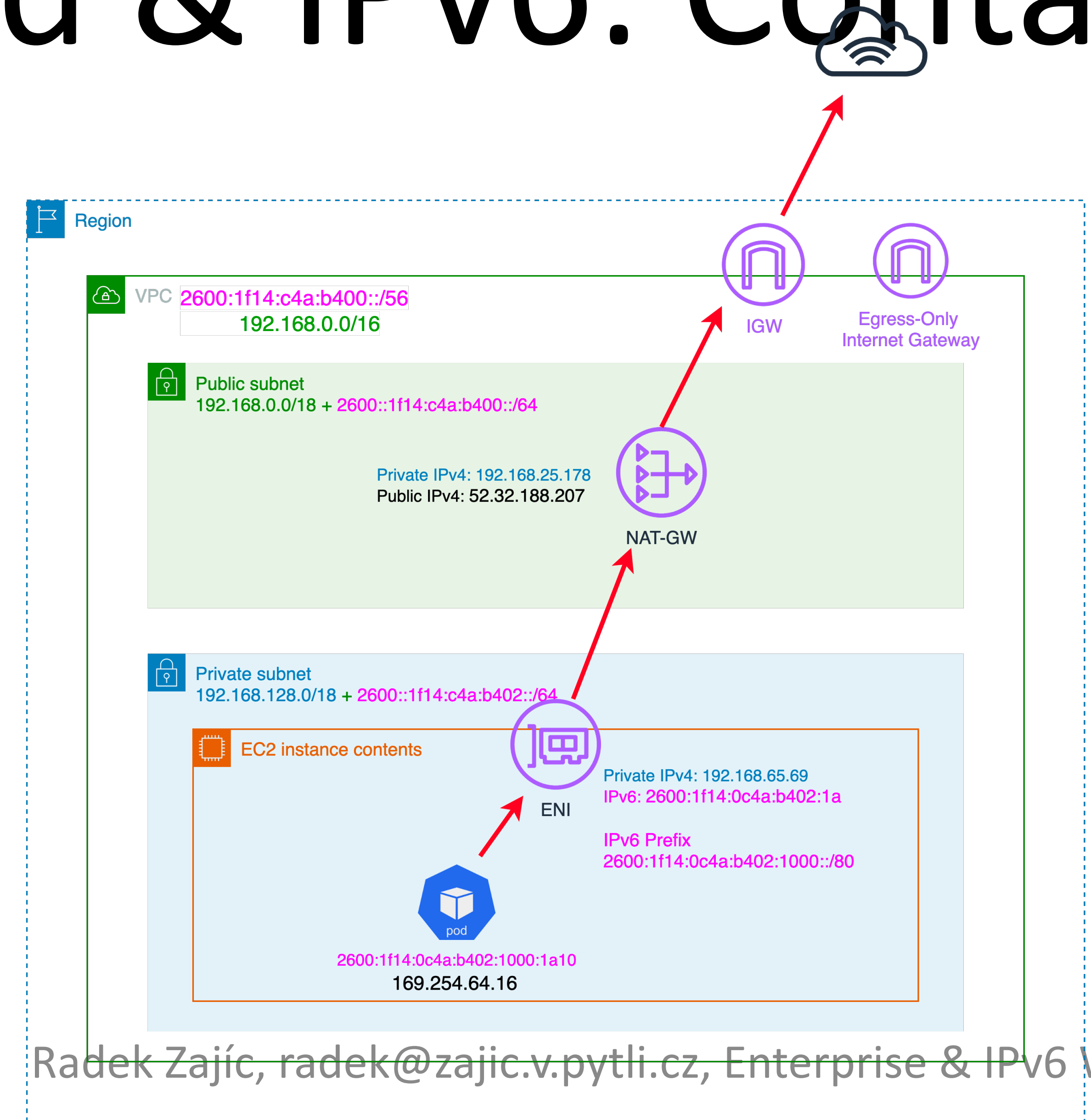
Pseudo-IPv6-only Kubernetes

Cloud & IPv6: Containers


Region
VPC
2600:1f14:c4a:b400::/56
192.168.0.0/16
IGW
Egress-Only
Internet Gateway
Private subnet
192.168.128.0/18 + 2600::1f14:c4a:b402::/64
EC2 instance contents
ENI
Private IPv4: 192.168.65.69
IPv6: 2600:1f14:0c4a:b402:1a
IPv6 Prefix: 2600:1f14:0c4a:b402:1000::/80
pod
2600:1f14:0c4a:b402:1000:1a
169.254.64.16

Amazon
EKS

Cloud & IPv6: Containers


Region
VPC
2600:1f14:c4a:b400::/56
192.168.0.0/16
IGW
Egress-Only
Internet Gateway
Public subnet
192.168.0.0/18 + 2600::1f14:c4a:b400::/64
Private IPv4: 192.168.25.178
Public IPv4: 52.32.188.207
NAT-GW
Private subnet
192.168.128.0/18 + 2600::1f14:c4a:b402::/64
EC2 instance contents
ENI
Private IPv4: 192.168.65.69
IPv6: 2600:1f14:0c4a:b402:1a
IPv6 Prefix
2600:1f14:0c4a:b402:1000::/80
pod
2600:1f14:0c4a:b402:1000:1a10
169.254.64.16

Amazon
EKS

https://aws.amazon.com/blogs/containers/amazon-eks-launches-ipv6-support/

Cloud & IPv6: Serverless

Lambdas

Serverless containers

API gateways, databases, and more

Cloud & IPv6: IPv6-only

Currently only in AWS

IPv6-only networks and compute instances

DNS64 and NAT64

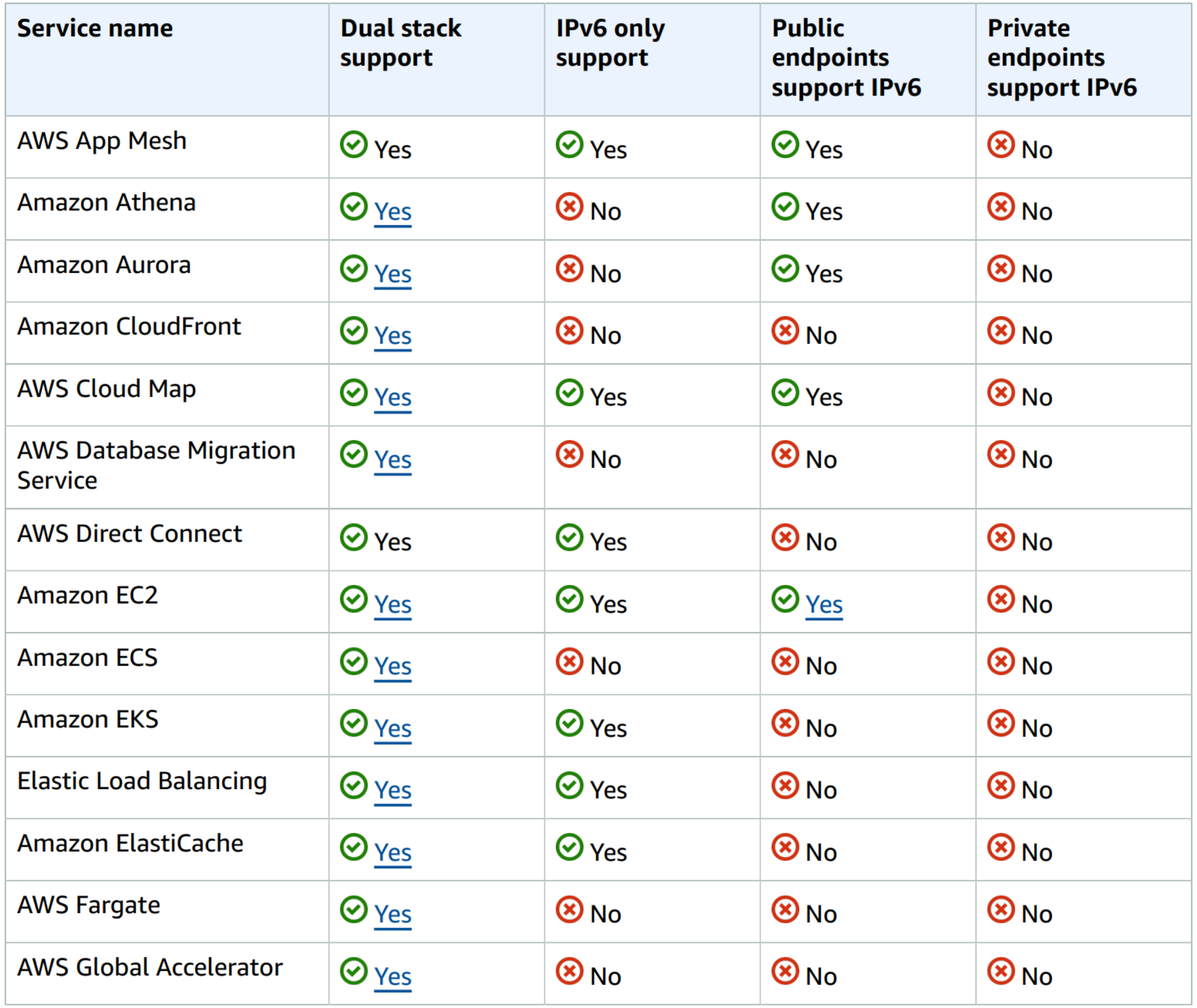
Cloud & IPv6: Enterprise stuff

Cross-connect between on-prem and cloud

Bring Your Own IP(v6)

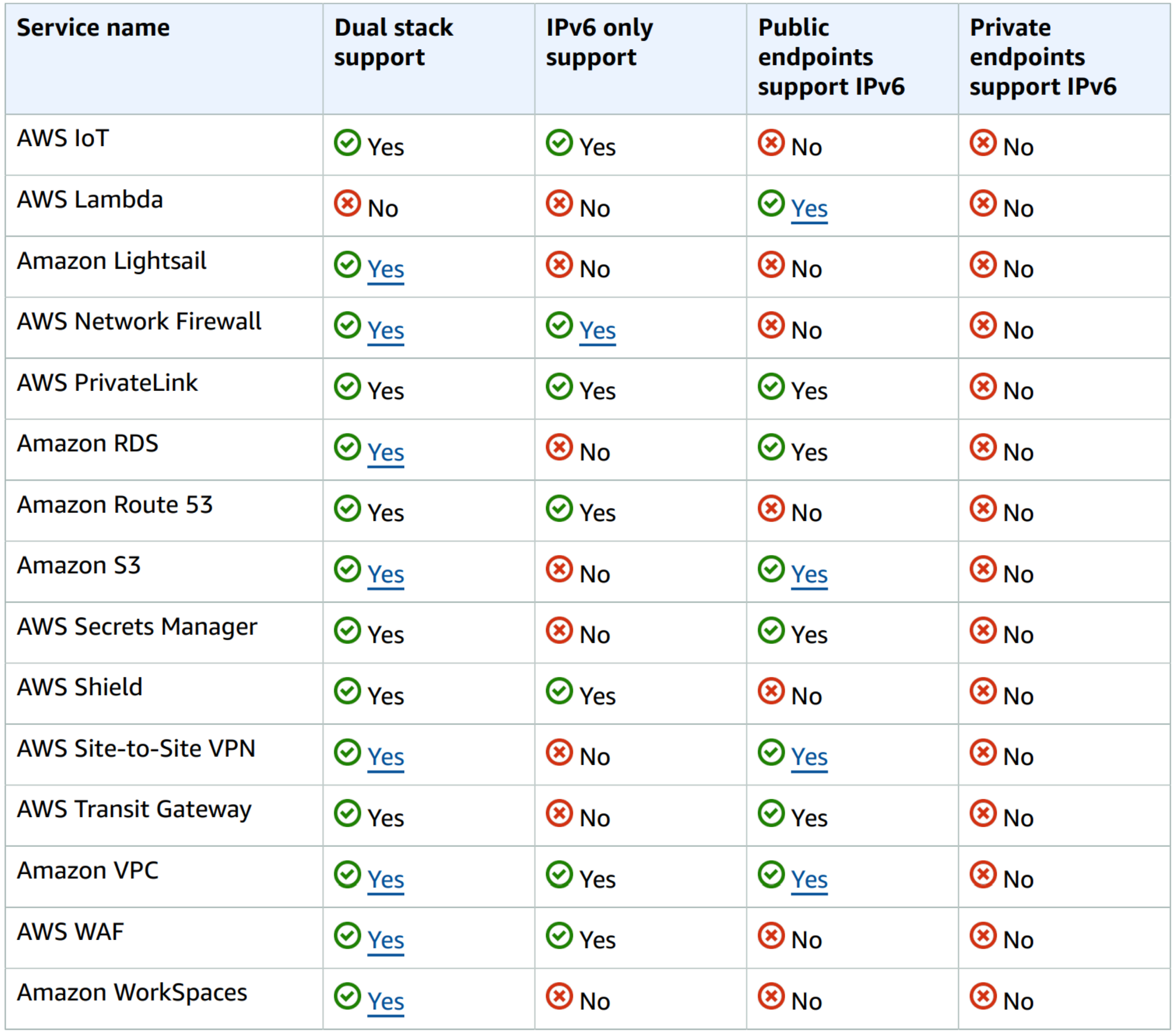
Virtual Desktop Infrastructure

Cloud & IPv6: Managed services



Service name	Dual stack support	IPv6 only support	Public endpoints support IPv6	Private endpoints support IPv6
AWS App Mesh	✓ Yes	✓ Yes	✓ Yes	⊗ No
Amazon Athena	✓ Yes	⊗ No	✓ Yes	⊗ No
Amazon Aurora	✓ Yes	⊗ No	✓ Yes	⊗ No
Amazon CloudFront	✓ Yes	⊗ No	⊗ No	⊗ No
AWS Cloud Map	✓ Yes	✓ Yes	✓ Yes	⊗ No
AWS Database Migration Service	✓ Yes	⊗ No	⊗ No	⊗ No
AWS Direct Connect	✓ Yes	✓ Yes	⊗ No	⊗ No
Amazon EC2	✓ Yes	✓ Yes	✓ Yes	⊗ No
Amazon ECS	✓ Yes	⊗ No	⊗ No	⊗ No
Amazon EKS	✓ Yes	✓ Yes	⊗ No	⊗ No
Elastic Load Balancing	✓ Yes	✓ Yes	⊗ No	⊗ No
Amazon ElastiCache	✓ Yes	✓ Yes	⊗ No	⊗ No
AWS Fargate	✓ Yes	⊗ No	⊗ No	⊗ No
AWS Global Accelerator	✓ Yes	⊗ No	⊗ No	⊗ No

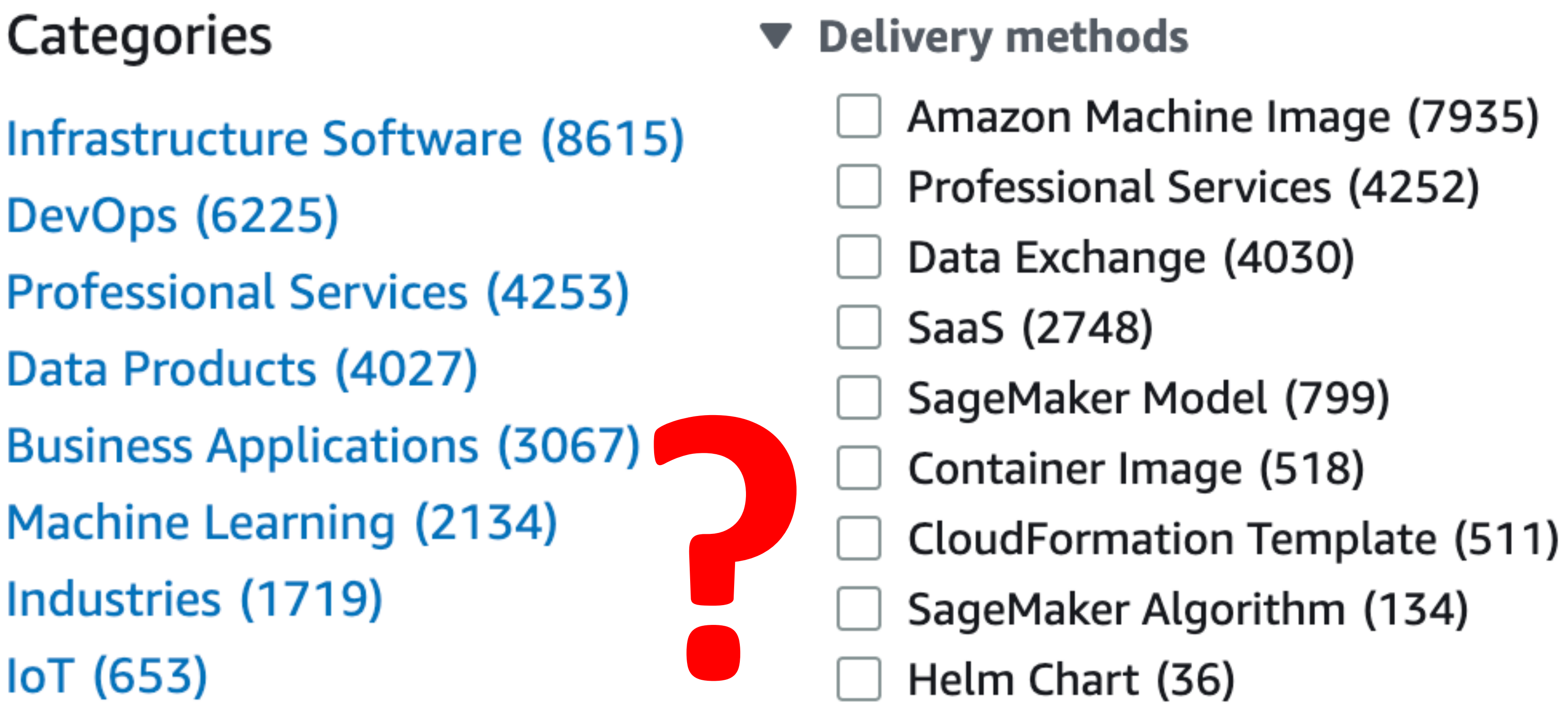
Cloud & IPv6: Managed services



Service name	Dual stack support	IPv6 only support	Public endpoints support IPv6	Private endpoints support IPv6
AWS IoT	✓ Yes	✓ Yes	⊗ No	⊗ No
AWS Lambda	⊗ No	⊗ No	✓ Yes	⊗ No
Amazon Lightsail	✓ Yes	⊗ No	⊗ No	⊗ No
AWS Network Firewall	✓ Yes	✓ Yes	⊗ No	⊗ No
AWS PrivateLink	✓ Yes	✓ Yes	✓ Yes	⊗ No
Amazon RDS	✓ Yes	⊗ No	✓ Yes	⊗ No
Amazon Route 53	✓ Yes	✓ Yes	⊗ No	⊗ No
Amazon S3	✓ Yes	⊗ No	✓ Yes	⊗ No
AWS Secrets Manager	✓ Yes	⊗ No	✓ Yes	⊗ No
AWS Shield	✓ Yes	✓ Yes	⊗ No	⊗ No
AWS Site-to-Site VPN	✓ Yes	⊗ No	✓ Yes	⊗ No
AWS Transit Gateway	✓ Yes	⊗ No	✓ Yes	⊗ No
Amazon VPC	✓ Yes	✓ Yes	✓ Yes	⊗ No
AWS WAF	✓ Yes	✓ Yes	⊗ No	⊗ No
Amazon WorkSpaces	✓ Yes	⊗ No	⊗ No	⊗ No

Cloud & IPv6: SaaS and PaaS

aws marketplace



Categories

Infrastructure Software (8615)
DevOps (6225)
Professional Services (4253)
Data Products (4027)
Business Applications (3067)
Machine Learning (2134)
Industries (1719)
IoT (653)

?

▼ Delivery methods

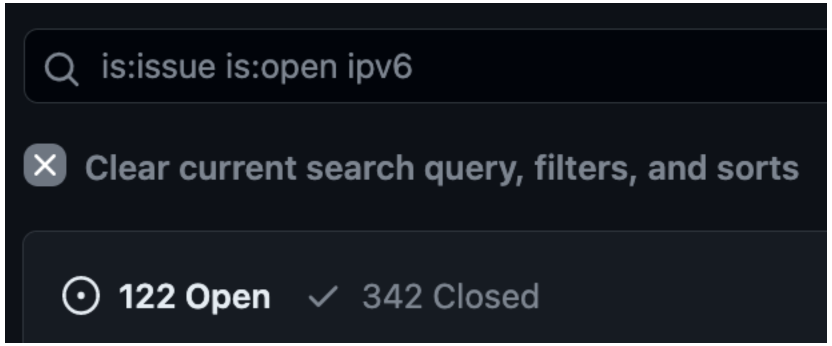
- □ Amazon Machine Image (7935)
- □ Professional Services (4252)
- □ Data Exchange (4030)
- □ SaaS (2748)
- □ SageMaker Model (799)
- □ Container Image (518)
- □ CloudFormation Template (511)
- □ SageMaker Algorithm (134)
- □ Helm Chart (36)

Cloud & IPv6: Automation

HashiCorp Terraform

aws

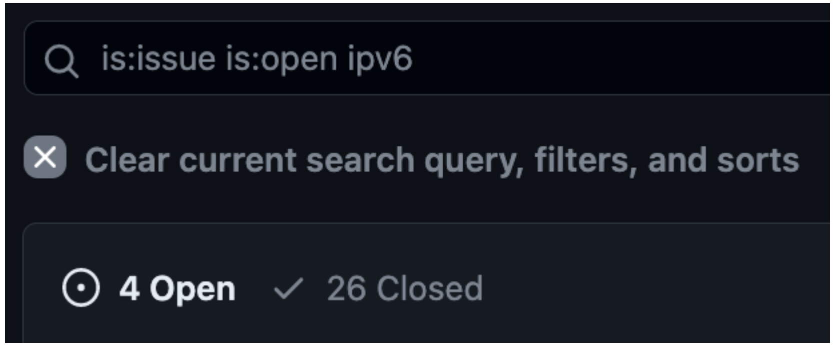
Google Cloud



is:issue is:open ipv6

☒ Clear current search query, filters, and sorts

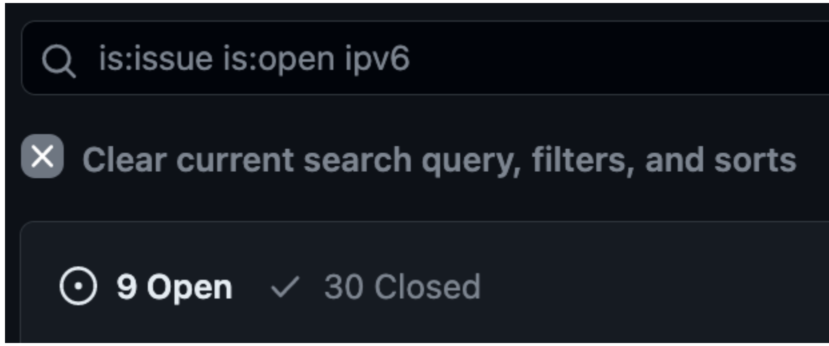
○ 122 Open ✓ 342 Closed



is:issue is:open ipv6

☒ Clear current search query, filters, and sorts

○ 4 Open ✓ 26 Closed



is:issue is:open ipv6

☒ Clear current search query, filters, and sorts

○ 9 Open ✓ 30 Closed

Cloud is not a cure

You create the address plan

You manage the IPv6 transition

You often have to IPv6-enable the services

Cloud is not a cure

IPv4/v6 feature parity is often not there

Some (many?) services lack IPv6 support

Read the fine print!

Why deploy IPv6 in the cloud?

Compliance reasons

Customers (even internal) asking for it

Save some costs

Why deploy IPv6 in the cloud?

Resolve resource exhaustion

Avoid IP address collisions

Experiment with IPv6-only

Examples of limitations

Azure and 1:1 IPv6 NAT

AWS, databases and IPv6(-only)

AWS Client VPN and the IPv6 routing fail

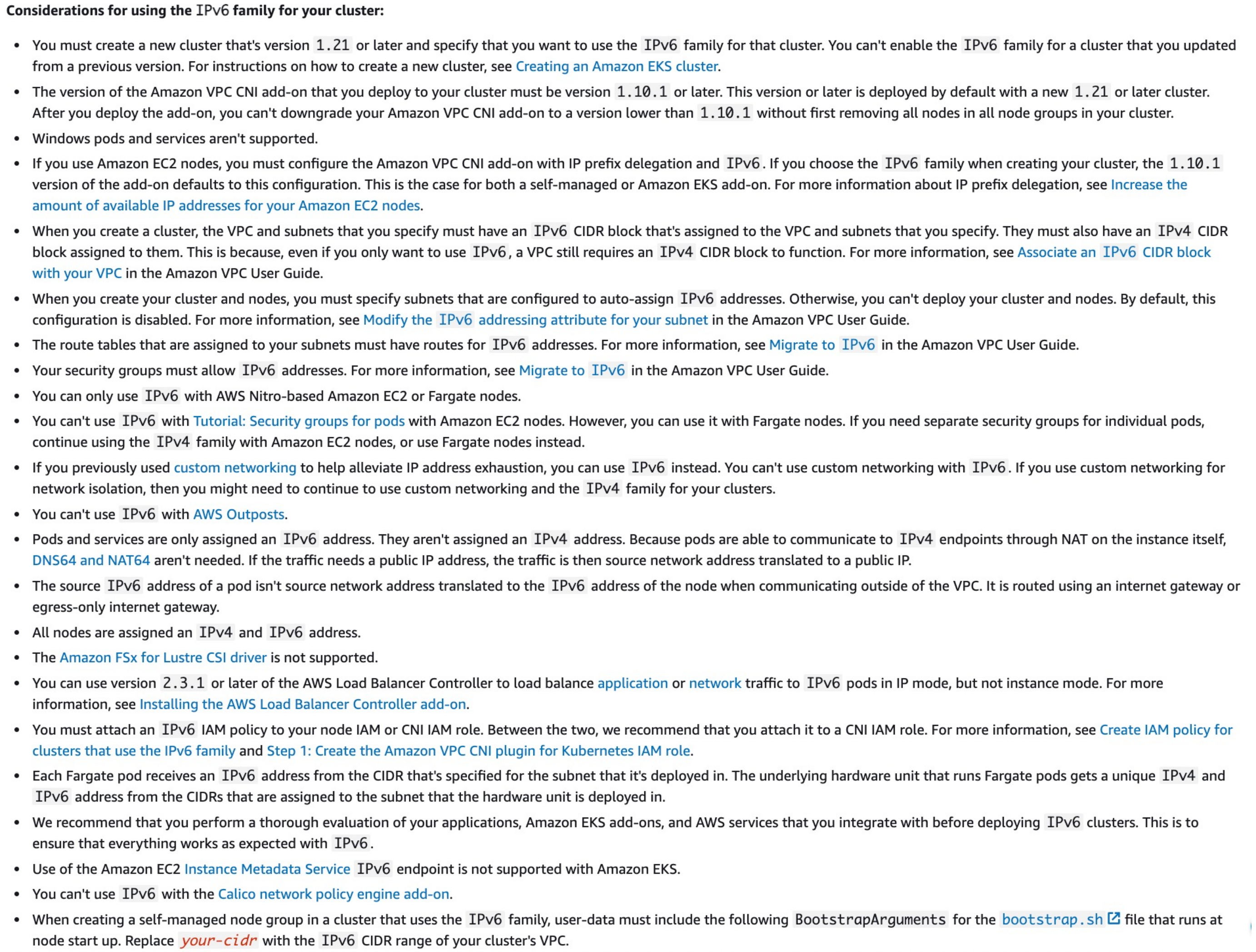
Examples of limitations: Azure FW

“Azure Firewall is a cloud-native and **intelligent** network firewall security service that provides the **best of breed** threat protection for your cloud workloads running in Azure. It's a fully stateful, firewall as a service with built-in high availability and **unrestricted cloud scalability**. It provides both east-west and north-south traffic inspection.”

(…)

“Azure Firewall **doesn't currently support IPv6**. It can **operate in a dual stack VNet** using only IPv4, but the firewall subnet must be IPv4-only.”

Examples of limitations: AWS K8s



Considerations for using the `IPv6` family for your cluster:

- You must create a new cluster that's version `1.21` or later and specify that you want to use the `IPv6` family for that cluster. You can't enable the `IPv6` family for a cluster that you updated from a previous version. For instructions on how to create a new cluster, see Creating an Amazon EKS cluster.
- The version of the Amazon VPC CNI add-on that you deploy to your cluster must be version `1.10.1` or later. This version or later is deployed by default with a new `1.21` or later cluster. After you deploy the add-on, you can't downgrade your Amazon VPC CNI add-on to a version lower than `1.10.1` without first removing all nodes in all node groups in your cluster.
- Windows pods and services aren't supported.
- If you use Amazon EC2 nodes, you must configure the Amazon VPC CNI add-on with IP prefix delegation and `IPv6`. If you choose the `IPv6` family when creating your cluster, the `1.10.1` version of the add-on defaults to this configuration. This is the case for both a self-managed or Amazon EKS add-on. For more information about IP prefix delegation, see Increase the amount of available IP addresses for your Amazon EC2 nodes.
- When you create a cluster, the VPC and subnets that you specify must have an `IPv6` CIDR block that's assigned to the VPC and subnets that you specify. They must also have an `IPv4` CIDR block assigned to them. This is because, even if you only want to use `IPv6`, a VPC still requires an `IPv4` CIDR block to function. For more information, see Associate an `IPv6` CIDR block with your VPC in the Amazon VPC User Guide.
- When you create your cluster and nodes, you must specify subnets that are configured to auto-assign `IPv6` addresses. Otherwise, you can't deploy your cluster and nodes. By default, this configuration is disabled. For more information, see Modify the `IPv6` addressing attribute for your subnet in the Amazon VPC User Guide.
- The route tables that are assigned to your subnets must have routes for `IPv6` addresses. For more information, see Migrate to `IPv6` in the Amazon VPC User Guide.
- Your security groups must allow `IPv6` addresses. For more information, see Migrate to `IPv6` in the Amazon VPC User Guide.
- You can only use `IPv6` with AWS Nitro-based Amazon EC2 or Fargate nodes.
- You can't use `IPv6` with Tutorial: Security groups for pods with Amazon EC2 nodes. However, you can use it with Fargate nodes. If you need separate security groups for individual pods, continue using the `IPv4` family with Amazon EC2 nodes, or use Fargate nodes instead.
- If you previously used custom networking to help alleviate IP address exhaustion, you can use `IPv6` instead. You can't use custom networking with `IPv6`. If you use custom networking for network isolation, then you might need to continue to use custom networking and the `IPv4` family for your clusters.
- You can't use `IPv6` with AWS Outposts.
- Pods and services are only assigned an `IPv6` address. They aren't assigned an `IPv4` address. Because pods are able to communicate to `IPv4` endpoints through NAT on the instance itself, DNS64 and NAT64 aren't needed. If the traffic needs a public IP address, the traffic is then source network address translated to a public IP.
- The source `IPv6` address of a pod isn't source network address translated to the `IPv6` address of the node when communicating outside of the VPC. It is routed using an internet gateway or egress-only internet gateway.
- All nodes are assigned an `IPv4` and `IPv6` address.
- The Amazon FSx for Lustre CSI driver is not supported.
- You can use version `2.3.1` or later of the AWS Load Balancer Controller to load balance application or network traffic to `IPv6` pods in IP mode, but not instance mode. For more information, see Installing the AWS Load Balancer Controller add-on.
- You must attach an `IPv6` IAM policy to your node IAM or CNI IAM role. Between the two, we recommend that you attach it to a CNI IAM role. For more information, see Create IAM policy for clusters that use the IPv6 family and Step 1: Create the Amazon VPC CNI plugin for Kubernetes IAM role.
- Each Fargate pod receives an `IPv6` address from the CIDR that's specified for the subnet that it's deployed in. The underlying hardware unit that runs Fargate pods gets a unique `IPv4` and `IPv6` address from the CIDRs that are assigned to the subnet that the hardware unit is deployed in.
- We recommend that you perform a thorough evaluation of your applications, Amazon EKS add-ons, and AWS services that you integrate with before deploying `IPv6` clusters. This is to ensure that everything works as expected with `IPv6`.
- Use of the Amazon EC2 Instance Metadata Service `IPv6` endpoint is not supported with Amazon EKS.
- You can't use `IPv6` with the Calico network policy engine add-on.
- When creating a self-managed node group in a cluster that uses the `IPv6` family, user-data must include the following `BootstrapArguments` for the `bootstrap.sh` ↗ file that runs at node start up. Replace *`your-cidr`* with the `IPv6` CIDR range of your cluster's VPC.

https://docs.aws.amazon.com/eks/latest/userguide/cni-ipv6.html

Multi-cloud and IPv6

So you want to use multiple clouds and IPv6…

…are you sure?

Cloud surprises

IPv6 support in Azure Active Directory – What's changing?

Our **service endpoint URLs will now resolve to return both IPv4 and IPv6 addresses.** (...)

When will IPv6 be supported in Azure AD?

We'll begin introducing IPv6 support to Azure AD in **April 2023**.

We know that IPv6 support is a significant change for some organizations. We're publishing this information now so that customers can make plans to ensure readiness.

What does my organization have to do?

If you have public IPv6 addresses representing your network, **take the actions that are described in the following sections as soon as possible.**

If customers don't update their named locations with these IPv6 addresses, their users will be blocked.

https://learn.microsoft.com/en-us/troubleshoot/azure/active-directory/azure-ad-ipv6-support

Enterprise IPv6 deployment

Geolocation

External blocklists

Internal/external firewall rules

Dual-stack application support

Train your developers

Provide your developers with IPv6 nets

Build IPv6-enabled apps

Test in an IPv6-only dev environment

You are the customer of The Cloud

Prepare yourself to avoid surprises

Build your lab, start early

Ask for feature parity

Ask for IPv6 on by default

Don’t forget about security

IPv6 & the big clouds: resources

AWS (announcements)

Google Cloud (announcements)

Azure VNET (announcements)

Eyal Estrin: Is the public cloud ready for IPv6?

Q & A

Thank you

linkedin.com/in/radek-zajic/

@zajDee