AWS re:Invent

NET321

AWS PrivateLink deployments: DNS mechanisms for routing & resiliency

James Devine

Senior Specialist Solutions Architect – Networking and VMware
Amazon Web Services

AWS re:Invent

aws

What to expect from this session

300-level session – you should have at least a basic understanding of PrivateLink and DNS

Deep dive into architectures and best practices

You don’t need to be a networking guru, PrivateLink is actually pretty simple and DNS just resolves names to IPs!

Agenda

PrivateLink overview (and updates!)

HA by design: Hyperplane

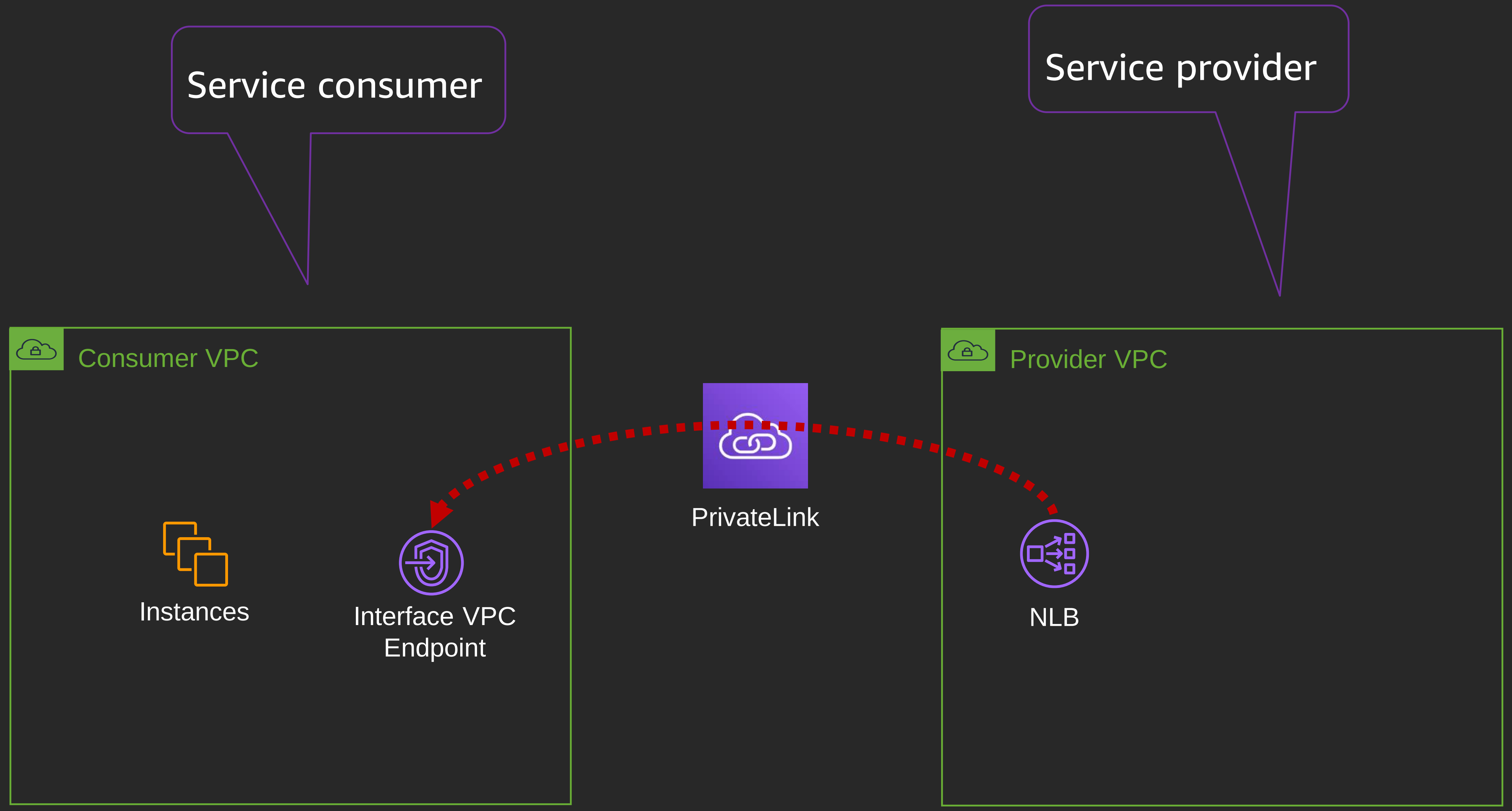
Amazon Route 53 Overview

Architectures

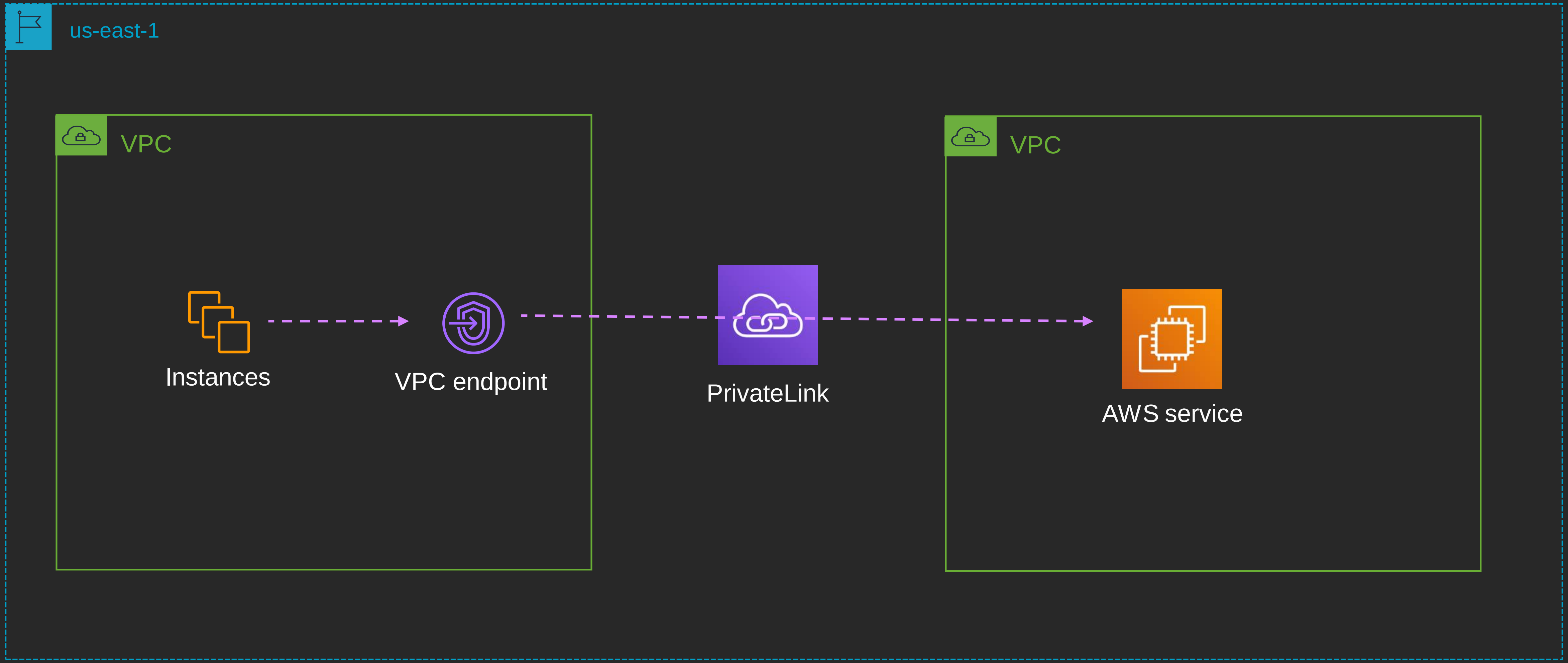
Best practices

PrivateLink overview (and updates!)

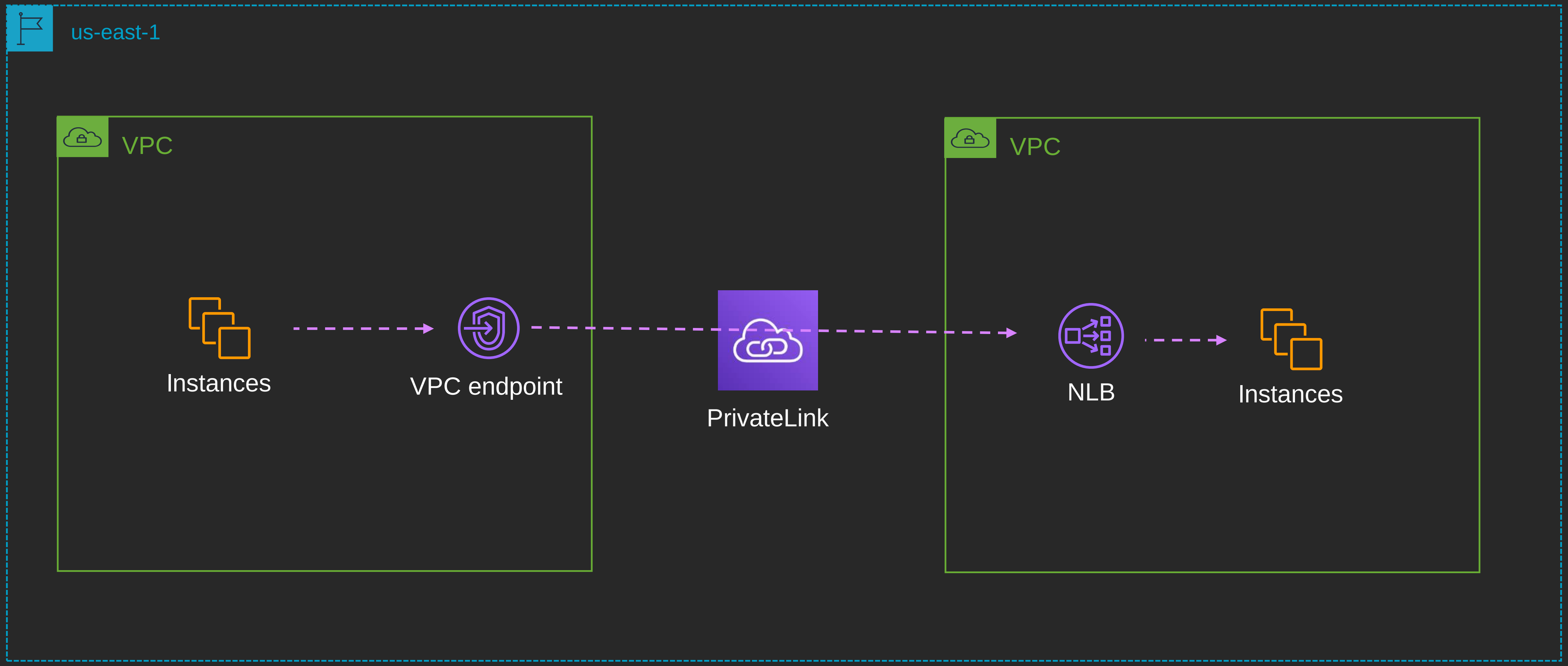
PrivateLink quick overview



PrivateLink Interface Endpoints – AWS Services

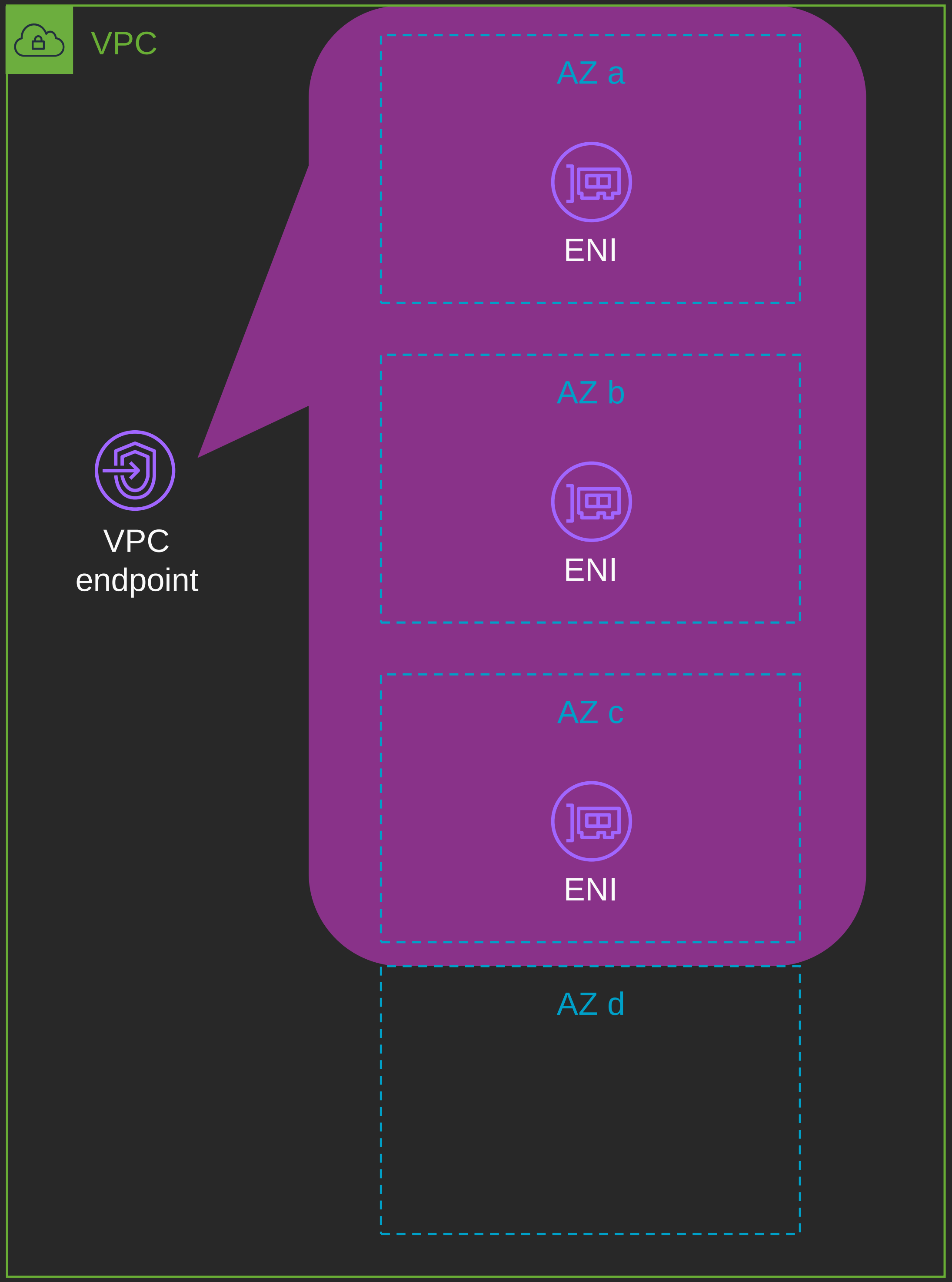


PrivateLink interface endpoints – endpoint services and SaaS

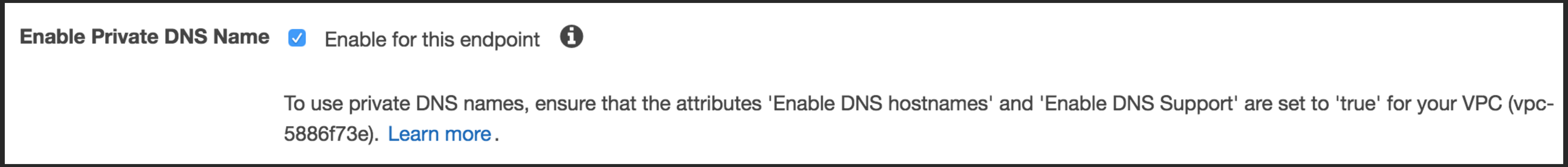


VPC endpoints and ENIs

- A VPC endpoint is a collection of ENIs spanning subnets
- Within a subnet, a VPCE is represented as an ENI
    - At most one ENI per AZ
    - An ENI is used to connect to a PrivateLink enabled service

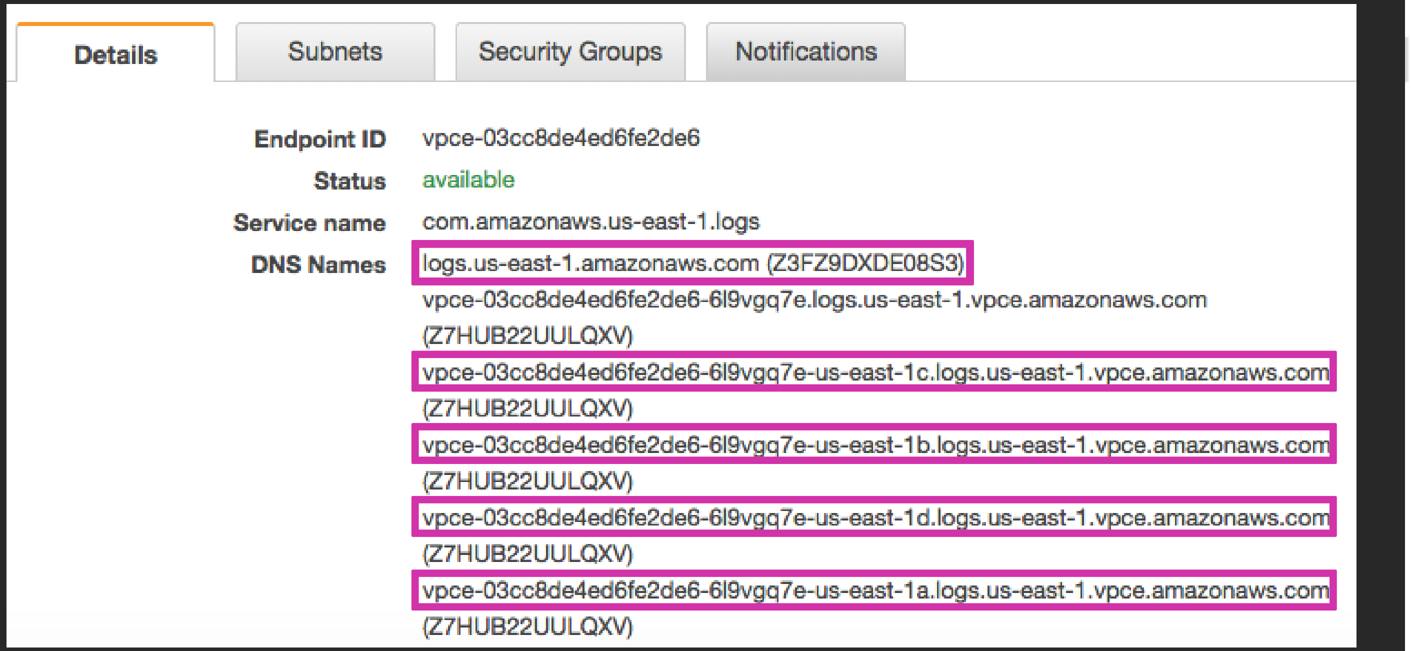


Interface endpoints Private DNS

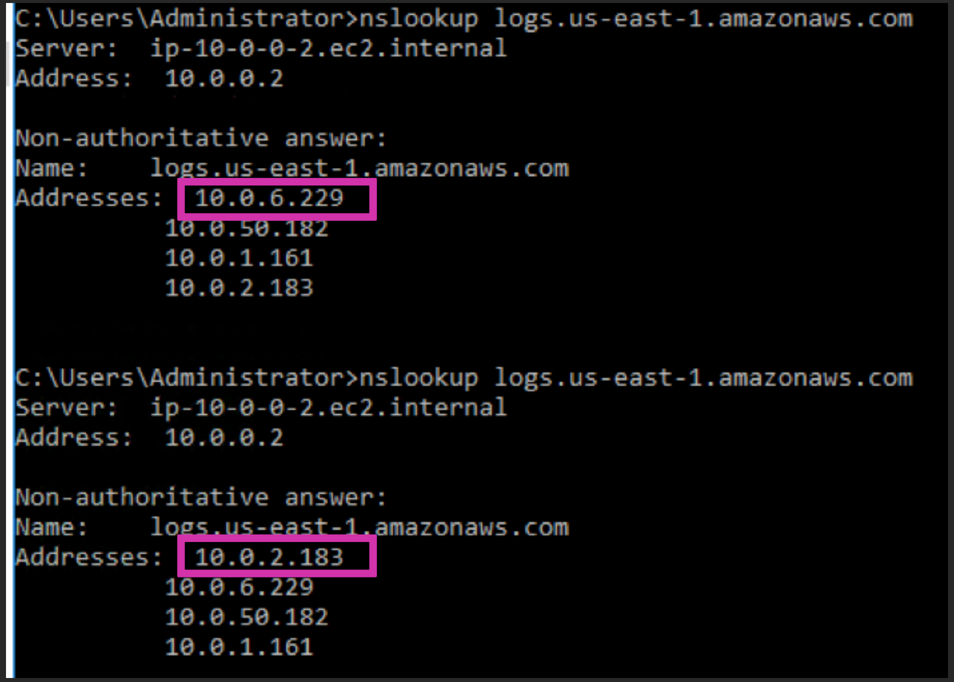


Enable Private DNS Name ☑ Enable for this endpoint ℹ

To use private DNS names, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS Support' are set to 'true' for your VPC (vpc-5886f73e). Learn more.

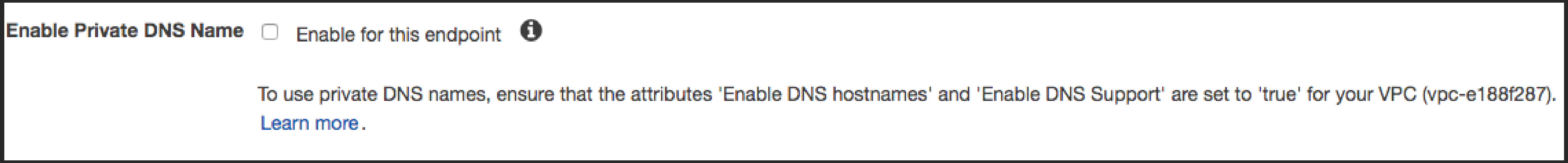


Endpoint ID	vpce-03cc8de4ed6fe2de6
Status	available
Service name	com.amazonaws.us-east-1.logs
DNS Names	logs.us-east-1.amazonaws.com (Z3FZ9DXDE08S3) vpce-03cc8de4ed6fe2de6-6l9vgq7e.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV) vpce-03cc8de4ed6fe2de6-6l9vgq7e-us-east-1c.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV) vpce-03cc8de4ed6fe2de6-6l9vgq7e-us-east-1b.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV) vpce-03cc8de4ed6fe2de6-6l9vgq7e-us-east-1d.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV) vpce-03cc8de4ed6fe2de6-6l9vgq7e-us-east-1a.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV)



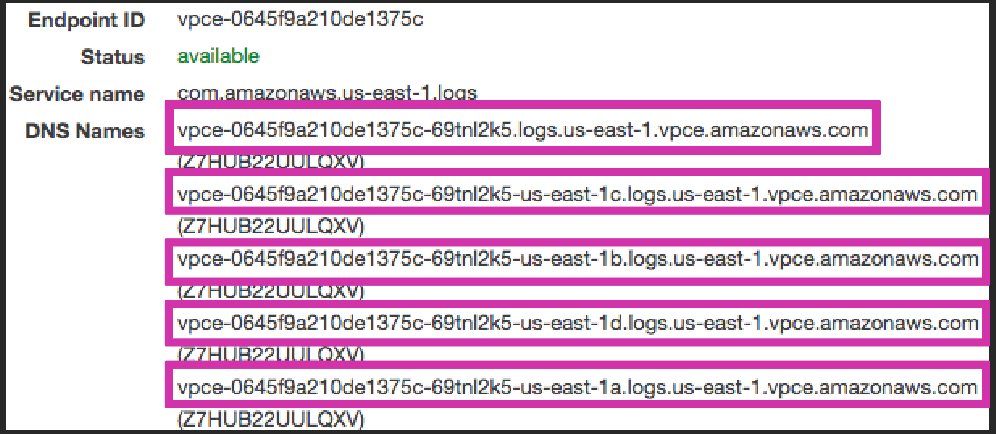
```
C:\Users\Administrator>nslookup logs.us-east-1.amazonaws.com
Server:  ip-10-0-0-2.ec2.internal
Address:  10.0.0.2

Non-authoritative answer:
Name:    logs.us-east-1.amazonaws.com
Addresses:  10.0.6.229
          10.0.50.182
          10.0.1.161
          10.0.2.183


C:\Users\Administrator>nslookup logs.us-east-1.amazonaws.com
Server:  ip-10-0-0-2.ec2.internal
Address:  10.0.0.2

Non-authoritative answer:
Name:    logs.us-east-1.amazonaws.com
Addresses:  10.0.2.183
          10.0.6.229
          10.0.50.182
          10.0.1.161
```

Interface endpoints Public DNS

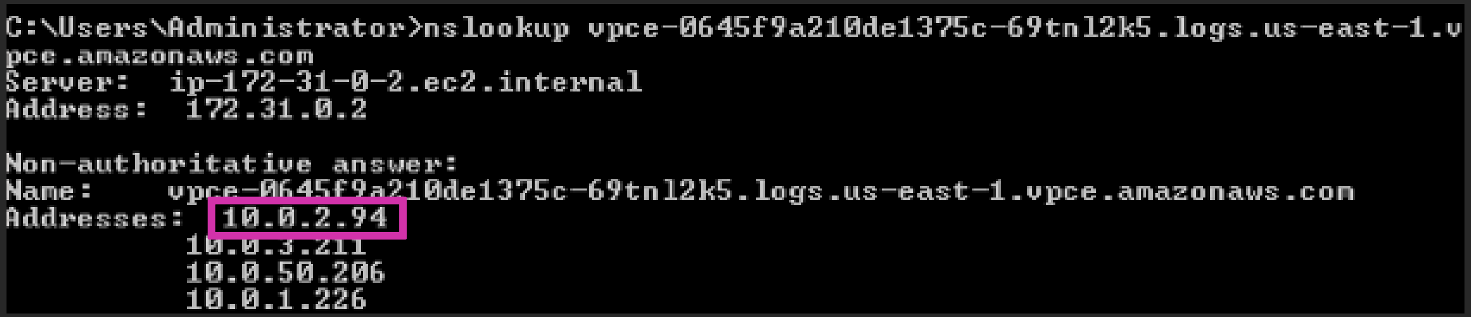


Enable Private DNS Name ☐ Enable for this endpoint

To use private DNS names, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS Support' are set to 'true' for your VPC (vpc-e188f287). Learn more.

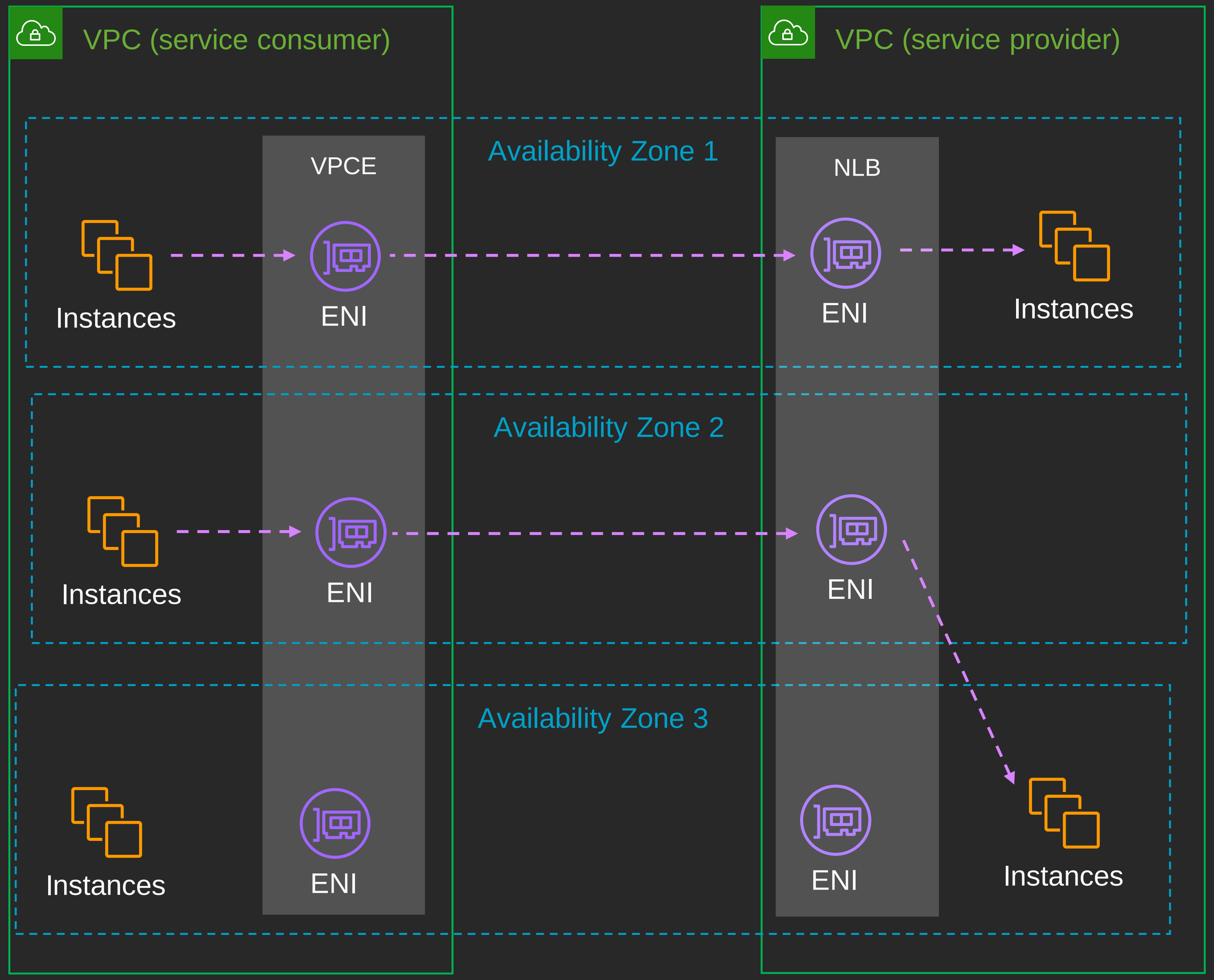


Endpoint ID	vpce-0645f9a210de1375c
Status	available
Service name	com.amazonaws.us-east-1.logs
DNS Names	vpce-0645f9a210de1375c-69tnl2k5.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV) vpce-0645f9a210de1375c-69tnl2k5-us-east-1c.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV) vpce-0645f9a210de1375c-69tnl2k5-us-east-1b.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV) vpce-0645f9a210de1375c-69tnl2k5-us-east-1d.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV) vpce-0645f9a210de1375c-69tnl2k5-us-east-1a.logs.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV)



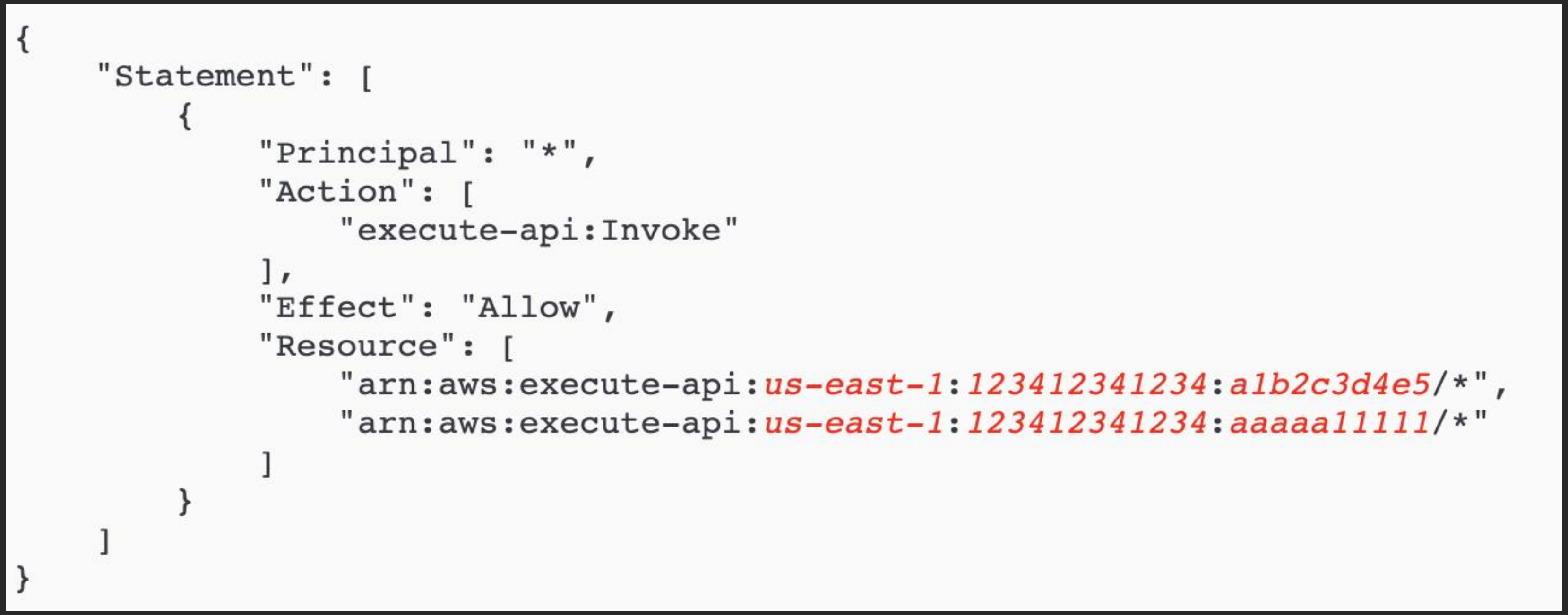
```
C:\Users\Administrator>nslookup vpce-0645f9a210de1375c-69tnl2k5.logs.us-east-1.v
pce.amazonaws.com
Server:  ip-172-31-0-2.ec2.internal
Address:  172.31.0.2

Non-authoritative answer:
Name:    vpce-0645f9a210de1375c-69tnl2k5.logs.us-east-1.vpce.amazonaws.com
Addresses:  10.0.2.94
          10.0.3.211
          10.0.50.206
          10.0.1.226
```

Cross-zone load balancing

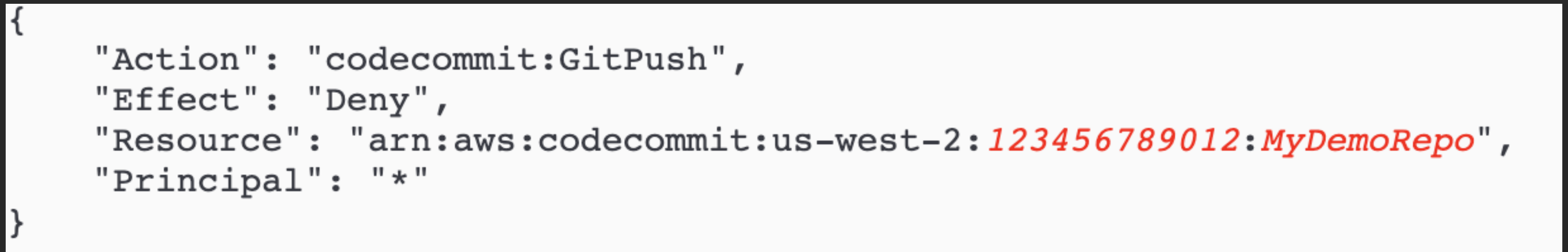


Endpoint policies

- IAM policy for all endpoints
- Growing number of AWS services support endpoint policies
  - Granular control over access to the service



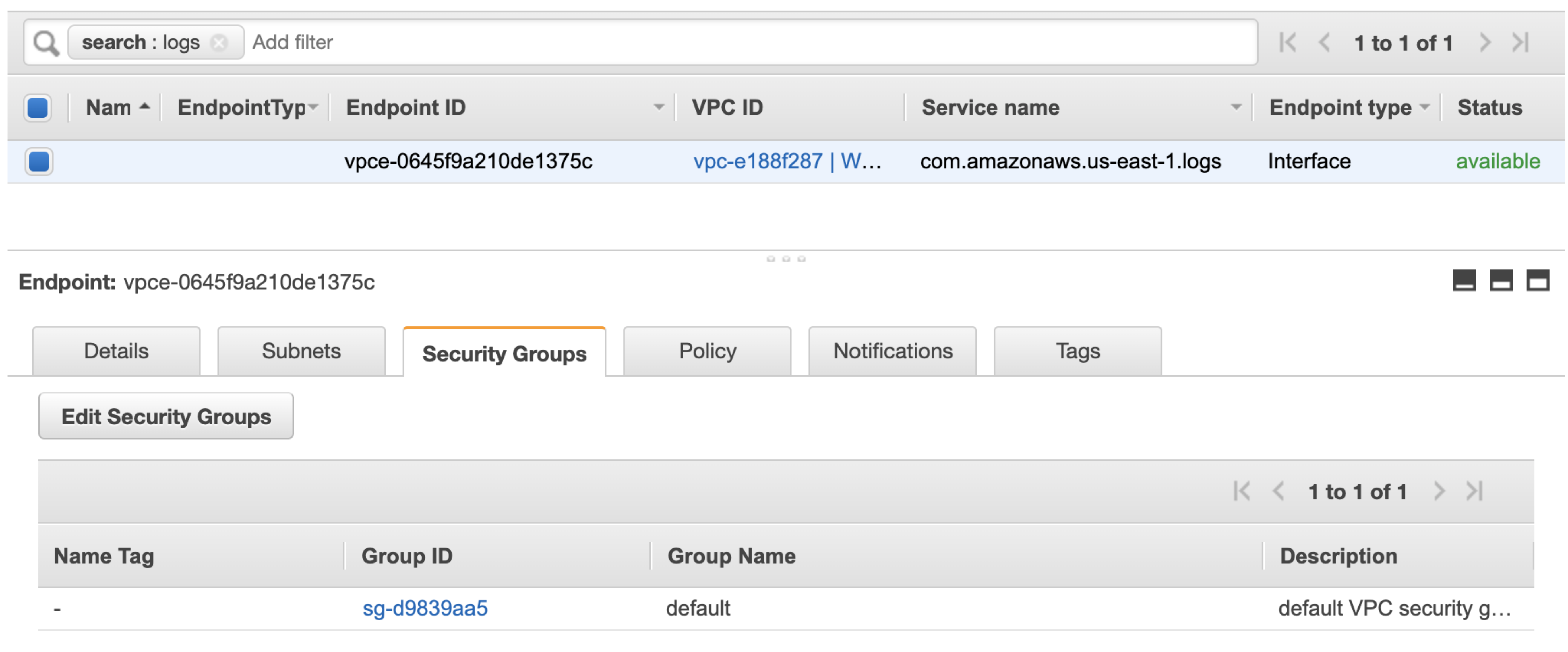
```
{
    "Statement": [
        {
            "Principal": "*",
            "Action": [
                "execute-api:Invoke"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:execute-api:us-east-1:123412341234:a1b2c3d4e5/*",
                "arn:aws:execute-api:us-east-1:123412341234:aaaaa11111/*"
            ]
        }
    ]
}
```



```
{
    "Action": "codecommit:GitPush",
    "Effect": "Deny",
    "Resource": "arn:aws:codecommit:us-west-2:123456789012:MyDemoRepo",
    "Principal": "*"
}
```

Security groups

Control traffic to a VPCE



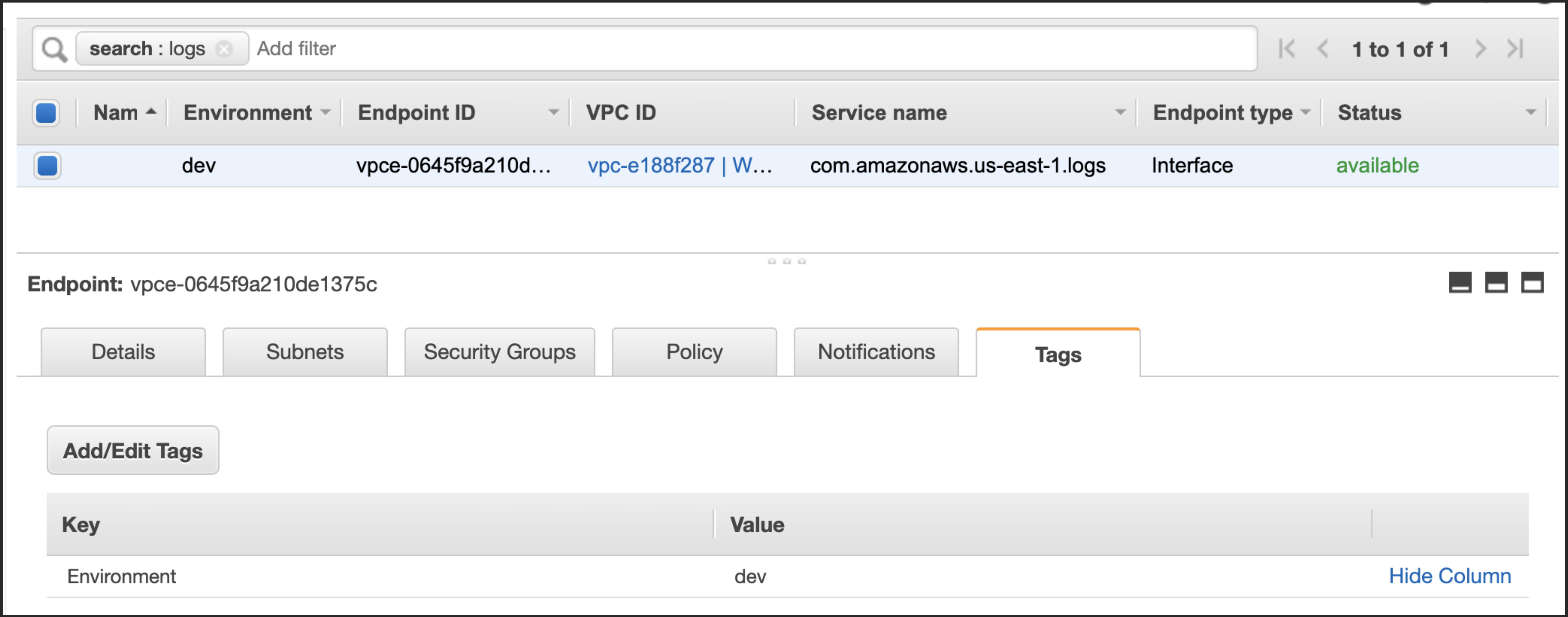
☐	Nam	EndpointTyp	Endpoint ID	VPC ID	Service name	Endpoint type	Status
☐			vpce-0645f9a210de1375c	vpc-e188f287 | W...	com.amazonaws.us-east-1.logs	Interface	available

Endpoint: vpce-0645f9a210de1375c

Name Tag	Group ID	Group Name	Description
-	sg-d9839aa5	default	default VPC security g...

Tagging

Manage access and endpoint management



	Nam	Environment	Endpoint ID	VPC ID	Service name	Endpoint type	Status
■		dev	vpce-0645f9a210d…	vpc-e188f287 | W…	com.amazonaws.us-east-1.logs	Interface	available

Endpoint: vpce-0645f9a210de1375c

Key	Value	
Environment	dev	Hide Column

“Everything fails all the time”

Werner Vogels

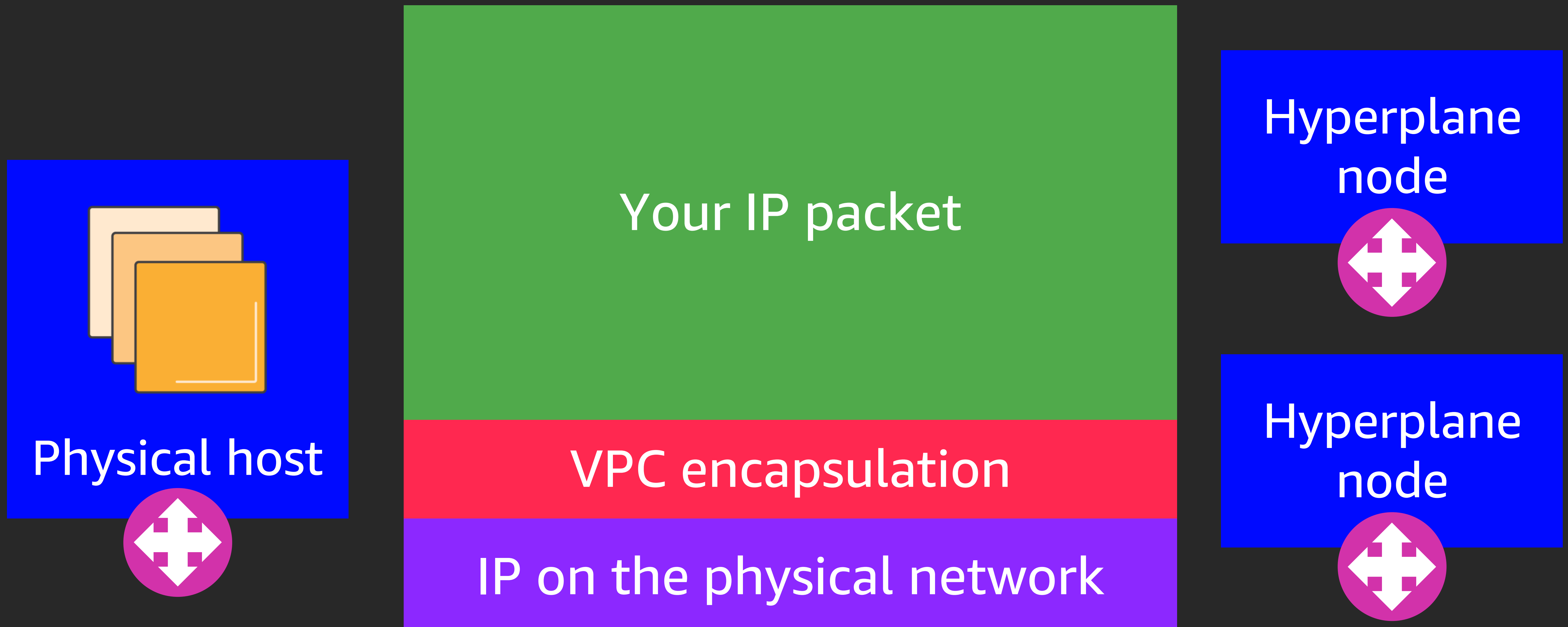
Chief Technology Officer
Amazon.com

AWS re:Invent

aws

HA by design: Hyperplane

Hyperplane



Physical host

Your IP packet

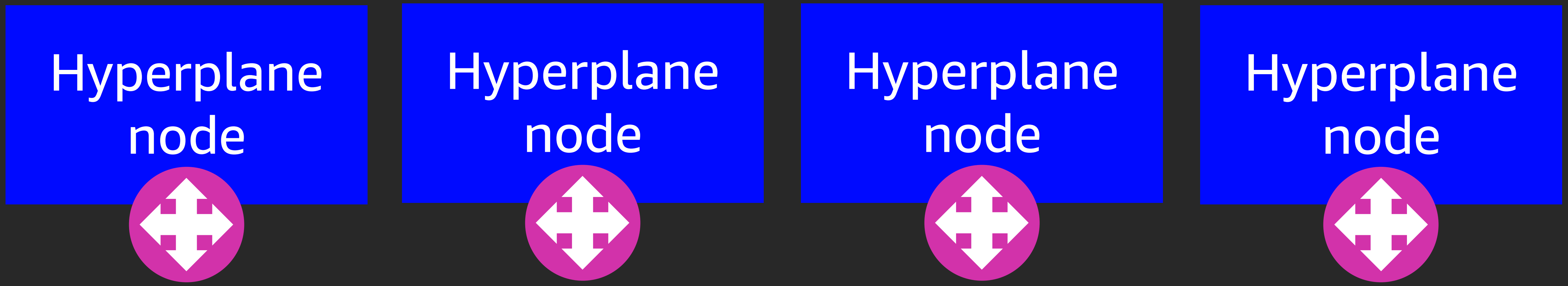
VPC encapsulation

IP on the physical network

Hyperplane node

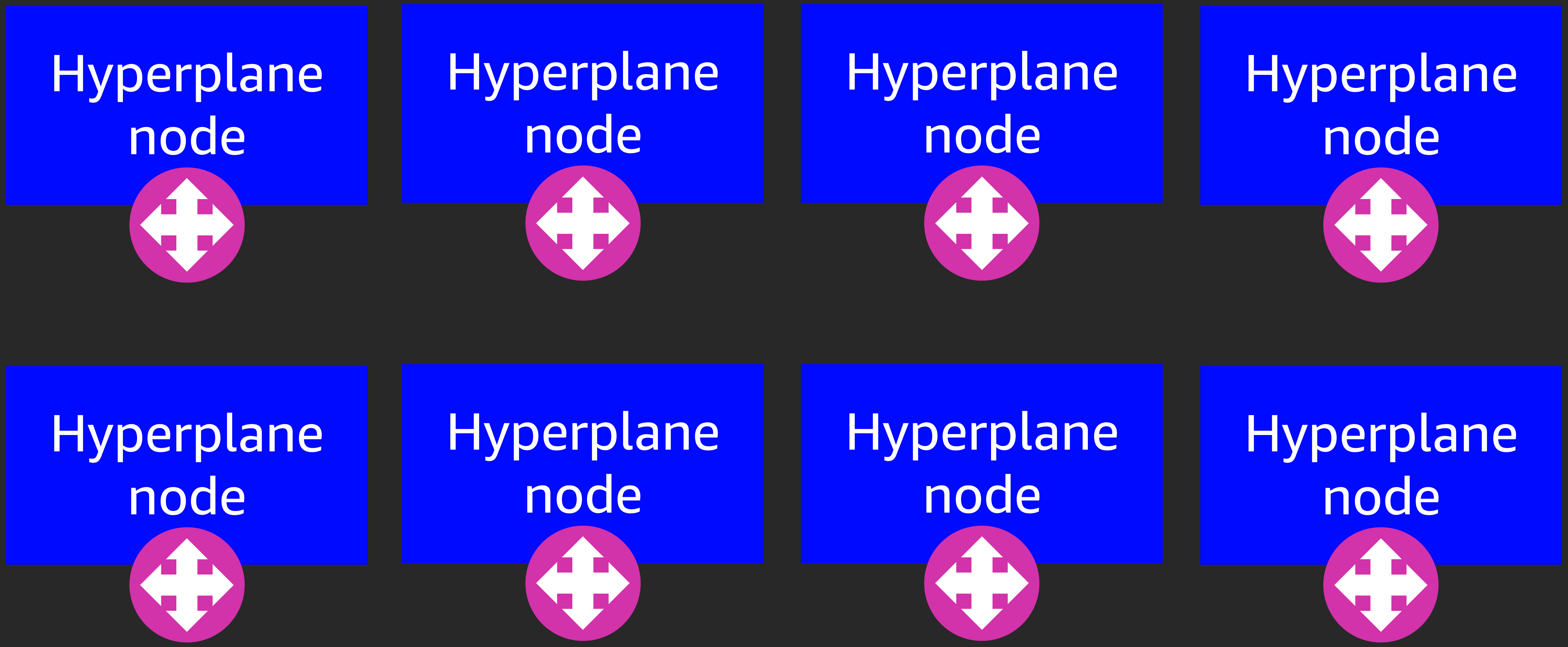
Hyperplane node

Hyperplane



Hyperplane nodes make transactional decisions and share state in tens of microseconds

Hyperplane shuffle sharding



Hyperplane node

Hyperplane node

Hyperplane node

Hyperplane node

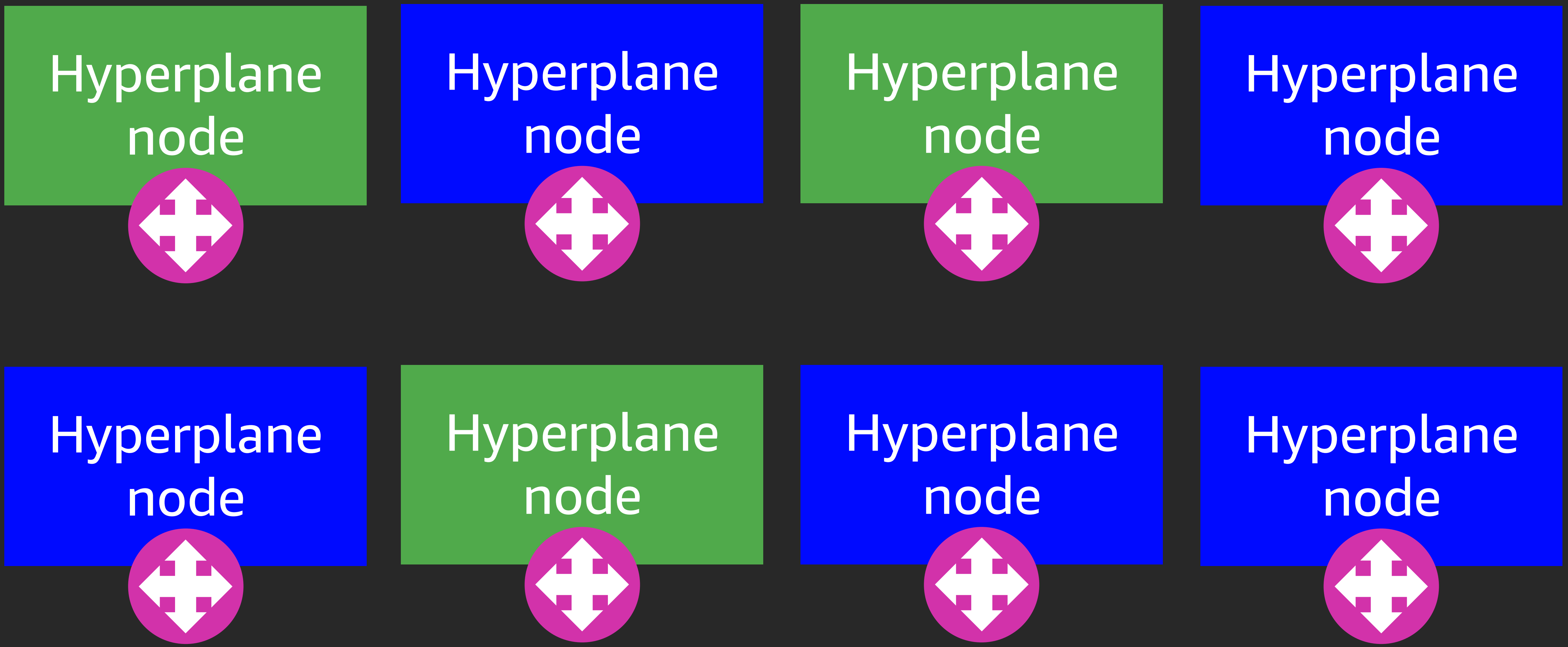
Hyperplane node

Hyperplane node

Hyperplane node

Hyperplane node

Hyperplane shuffle sharding



Hyperplane node

Hyperplane node

Hyperplane node

Hyperplane node

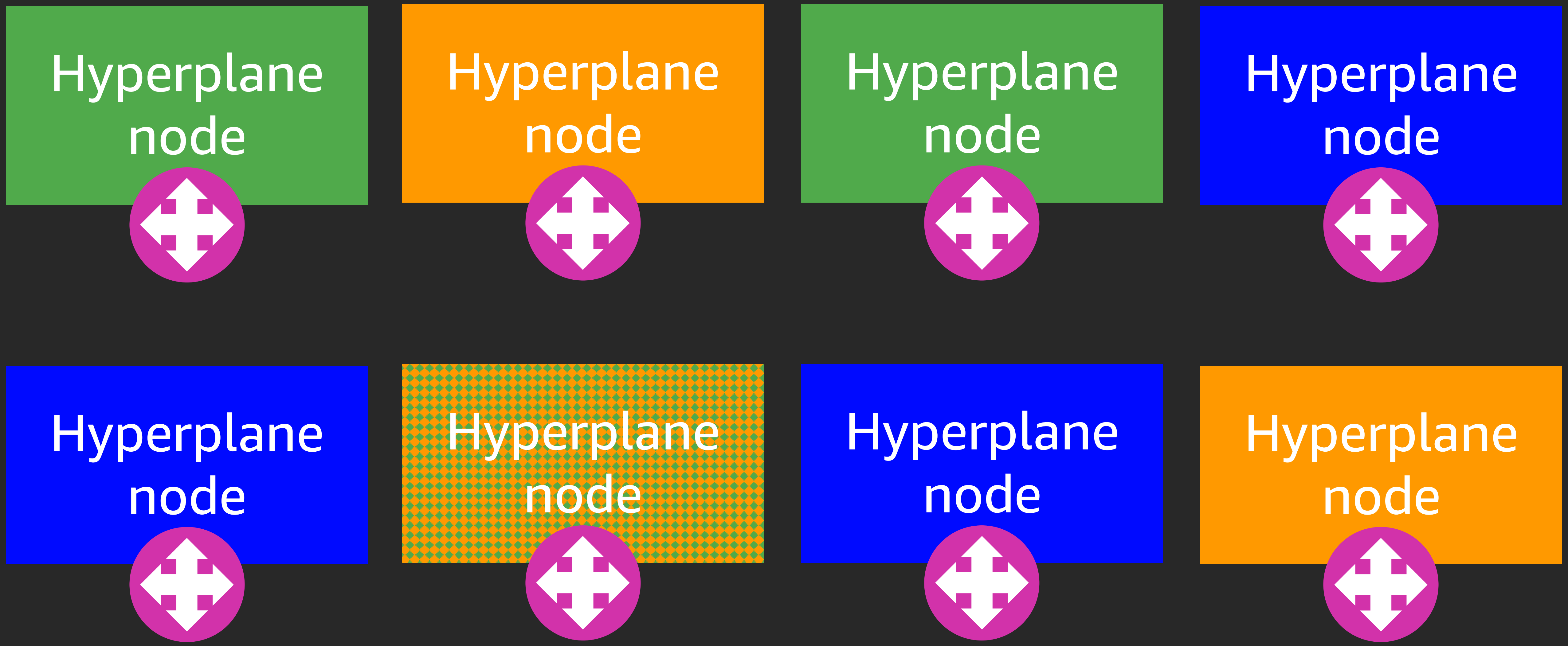
Hyperplane node

Hyperplane node

Hyperplane node

Hyperplane node

Hyperplane shuffle sharding



Hyperplane node

Hyperplane node

Hyperplane node

Hyperplane node

Hyperplane node

Hyperplane node

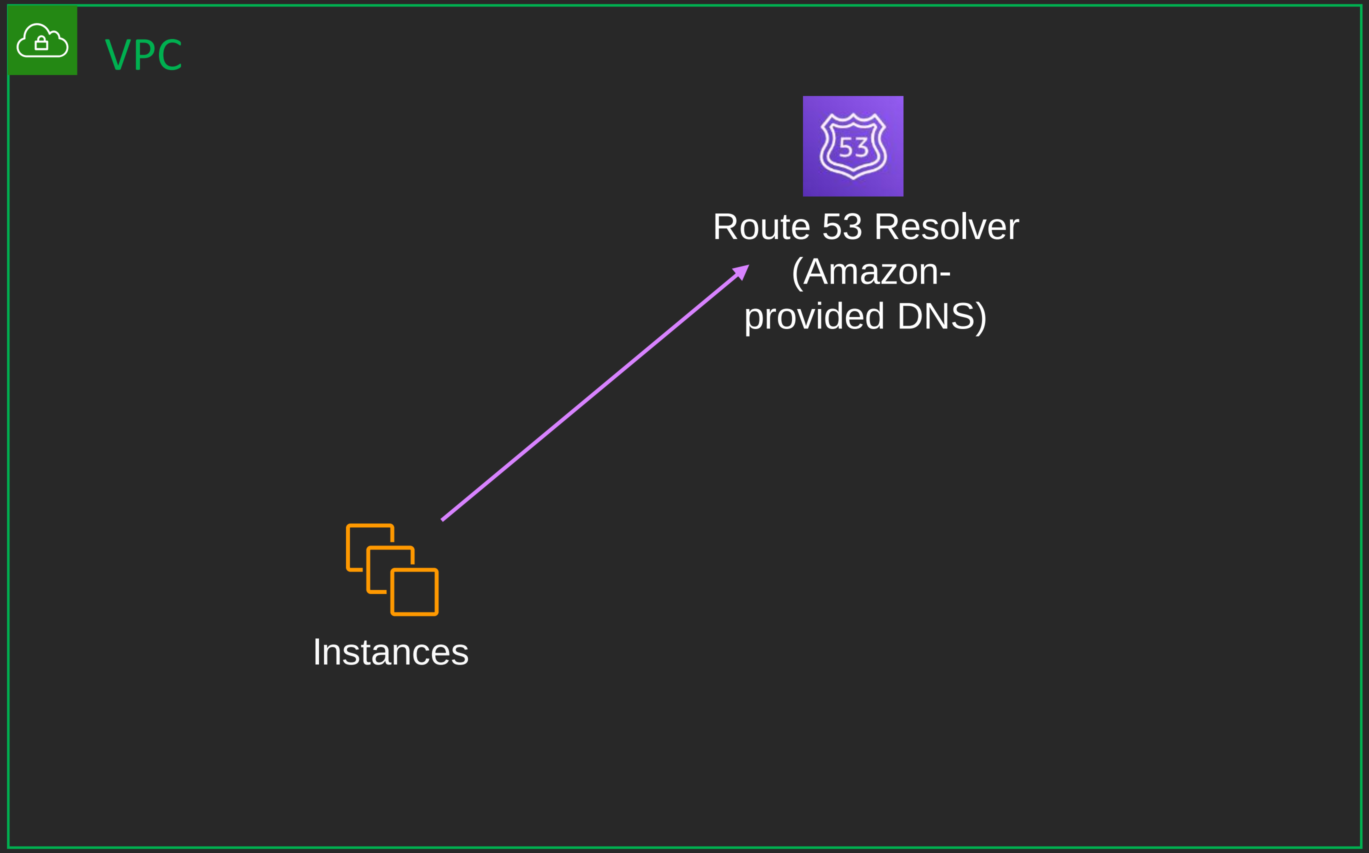
Hyperplane node

Hyperplane node

Route 53 overview

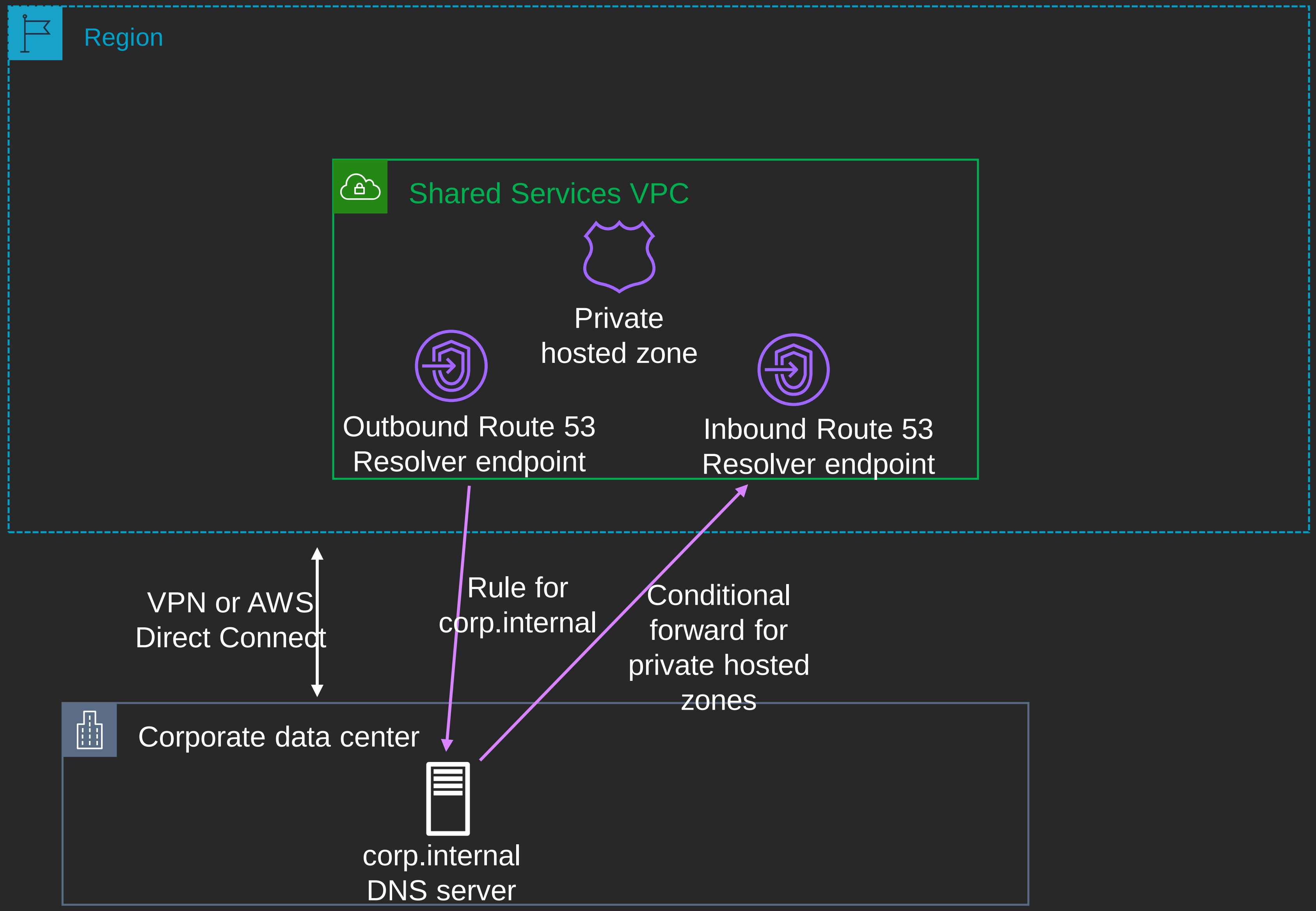
Route 53 Resolver – VPC view

- Recursive DNS server
- +2 IPs from VPC CIDR
- Built-in redundancy

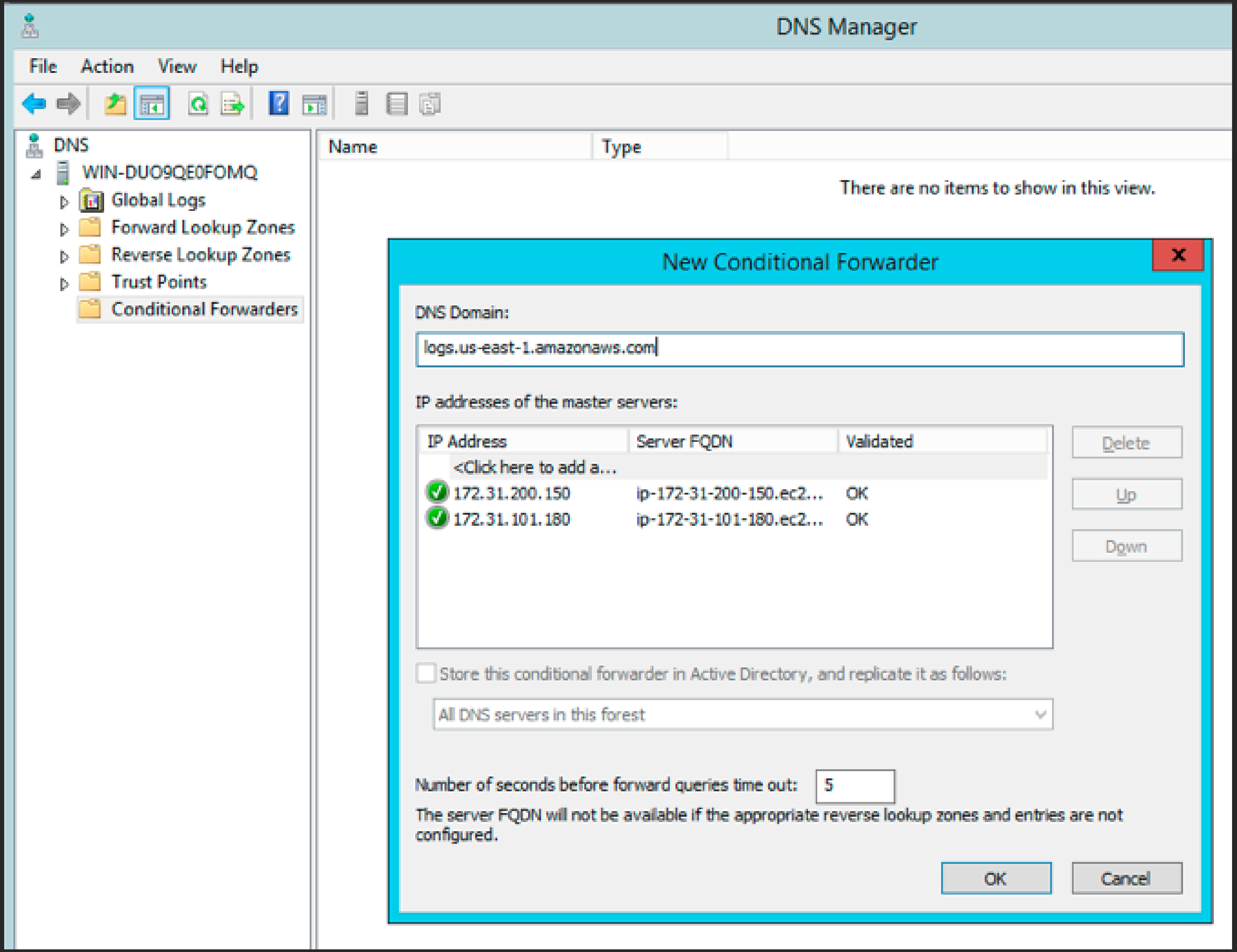


Route 53 Resolver endpoints – hybrid DNS

- Inbound endpoint: share VPC DNS view
- Built-in redundancy


Region
Shared Services VPC
Private hosted zone
Outbound Route 53 Resolver endpoint
Inbound Route 53 Resolver endpoint
VPN or AWS Direct Connect
Rule for corp.internal
Conditional forward for private hosted zones
Corporate data center
corp.internal DNS server

Conditional forwarding – examples



There are no items to show in this view.

DNS Domain: logs.us-east-1.amazonaws.com

IP addresses of the master servers:

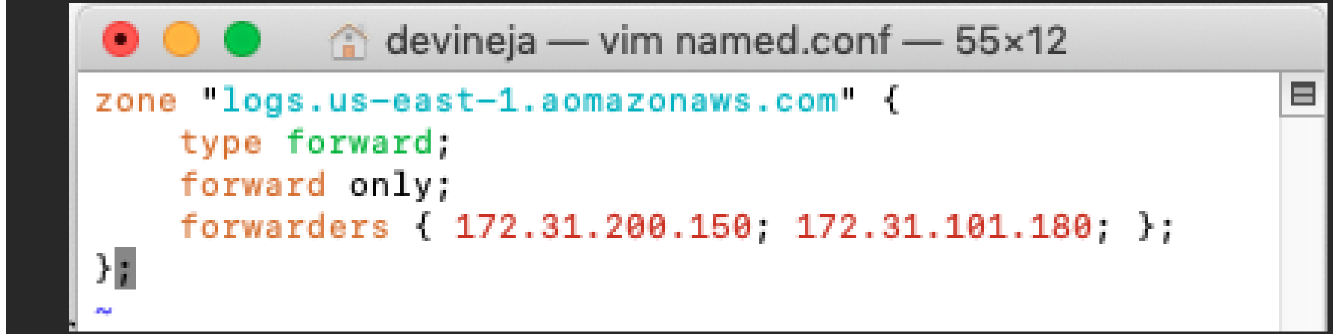
IP Address	Server FQDN	Validated
<Click here to add a...		
✓ 172.31.200.150	ip-172-31-200-150.ec2...	OK
✓ 172.31.101.180	ip-172-31-101-180.ec2...	OK

☐ Store this conditional forwarder in Active Directory, and replicate it as follows:

All DNS servers in this forest

Number of seconds before forward queries time out: 5

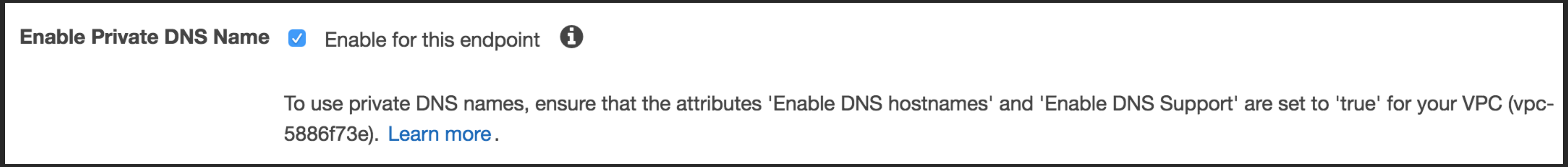
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.



```
zone "logs.us-east-1.aomazonaws.com" {
    type forward;
    forward only;
    forwarders { 172.31.200.150; 172.31.101.180; };
};
~
```

Private hosted zones for AWS services

Private DNS option only applies to VPC (and inbound endpoint) name resolution

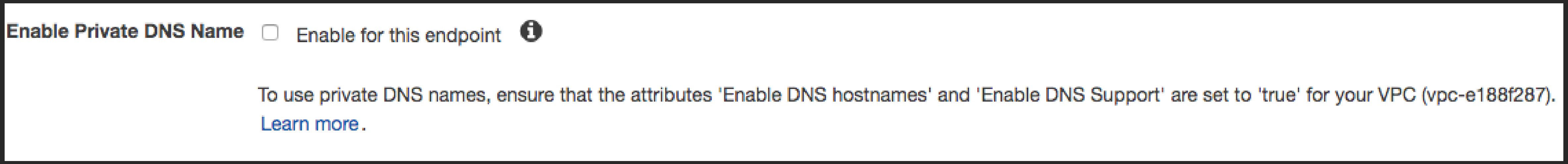


Enable Private DNS Name ☑ Enable for this endpoint ℹ

To use private DNS names, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS Support' are set to 'true' for your VPC (vpc-5886f73e). Learn more.

Doesn't work VPC-to-VPC (peering, AWS Transit Gateway, etc.)

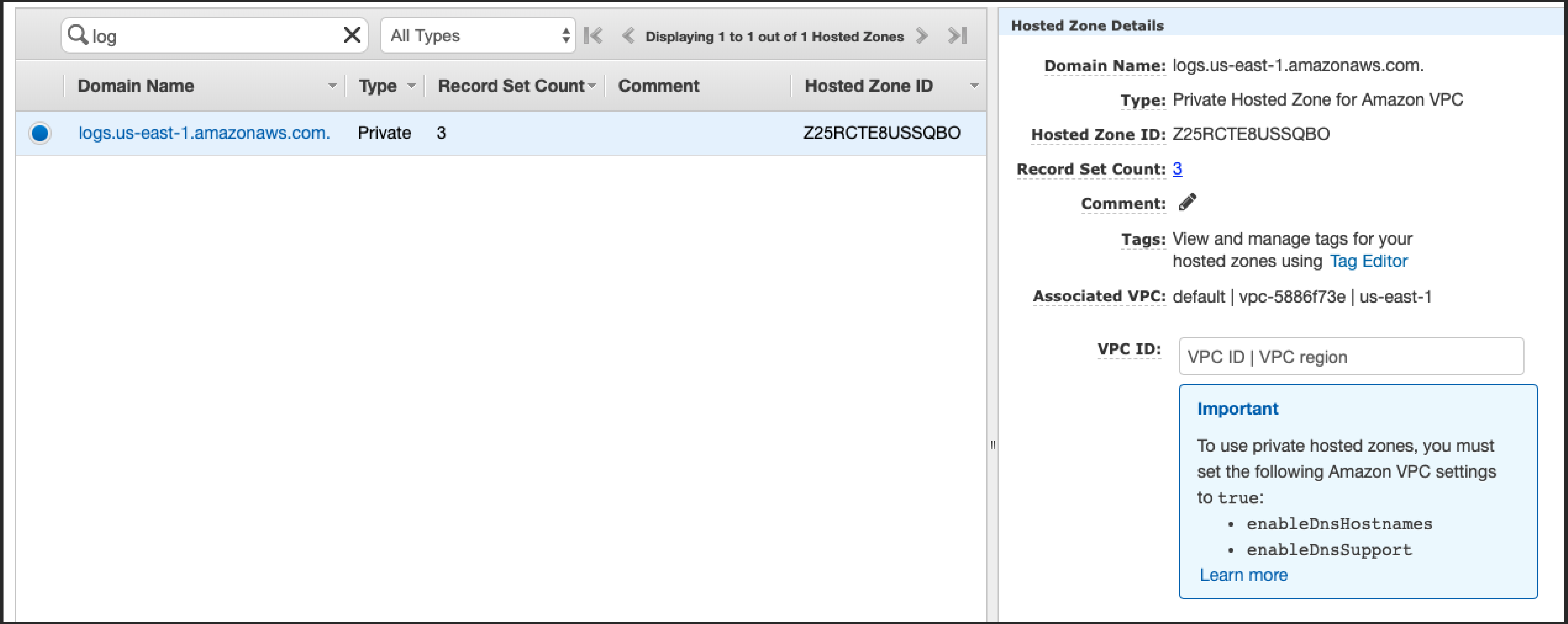
Can disable and create a private hosted zone



Enable Private DNS Name □ Enable for this endpoint ℹ

To use private DNS names, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS Support' are set to 'true' for your VPC (vpc-e188f287). Learn more.

Private hosted zones for AWS services



	Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
●	logs.us-east-1.amazonaws.com.	Private	3		Z25RCTE8USSQBO

Hosted Zone Details

Domain Name: logs.us-east-1.amazonaws.com.

Type: Private Hosted Zone for Amazon VPC

Hosted Zone ID: Z25RCTE8USSQBO

Record Set Count: 3

Comment:

Tags: View and manage tags for your hosted zones using Tag Editor

Associated VPC: default | vpc-5886f73e | us-east-1

VPC ID: VPC ID | VPC region

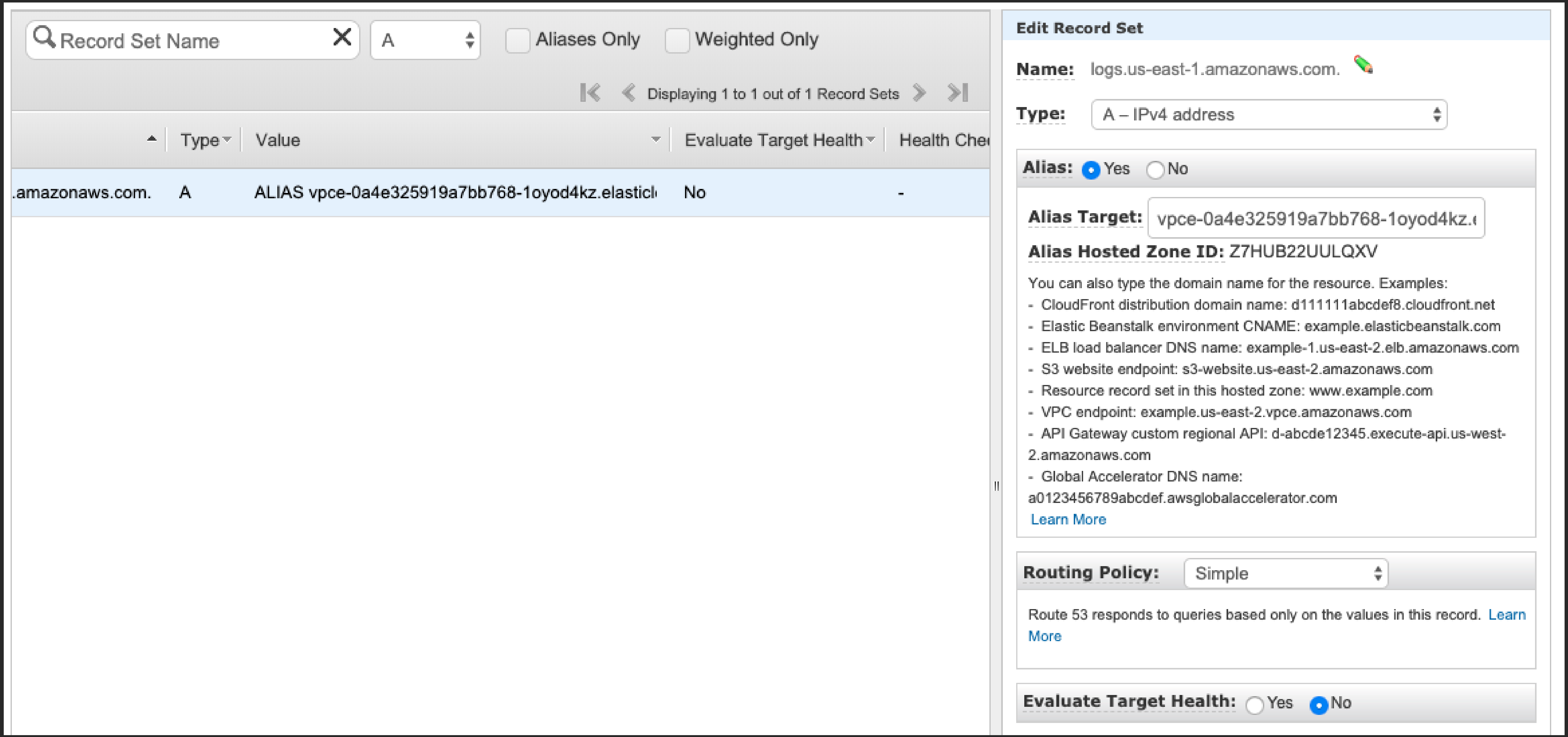
Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Learn more

Private hosted zones for AWS services



Record Set Name | A | □ Aliases Only | □ Weighted Only

Displaying 1 to 1 out of 1 Record Sets

	Type	Value	Evaluate Target Health	Health Che
.amazonaws.com.	A	ALIAS vpce-0a4e325919a7bb768-1oyod4kz.elasticl	No	-

Edit Record Set

Name: logs.us-east-1.amazonaws.com.

Type: A – IPv4 address

Alias: ● Yes ○ No

Alias Target: vpce-0a4e325919a7bb768-1oyod4kz.e

Alias Hosted Zone ID: Z7HUB22UULQXV

You can also type the domain name for the resource. Examples:

- CloudFront distribution domain name: d111111abcdef8.cloudfront.net
- Elastic Beanstalk environment CNAME: example.elasticbeanstalk.com
- ELB load balancer DNS name: example-1.us-east-2.elb.amazonaws.com
- S3 website endpoint: s3-website.us-east-2.amazonaws.com
- Resource record set in this hosted zone: www.example.com
- VPC endpoint: example.us-east-2.vpce.amazonaws.com
- API Gateway custom regional API: d-abcde12345.execute-api.us-west-2.amazonaws.com
- Global Accelerator DNS name: a0123456789abcdef.awsglobalaccelerator.com

Learn More

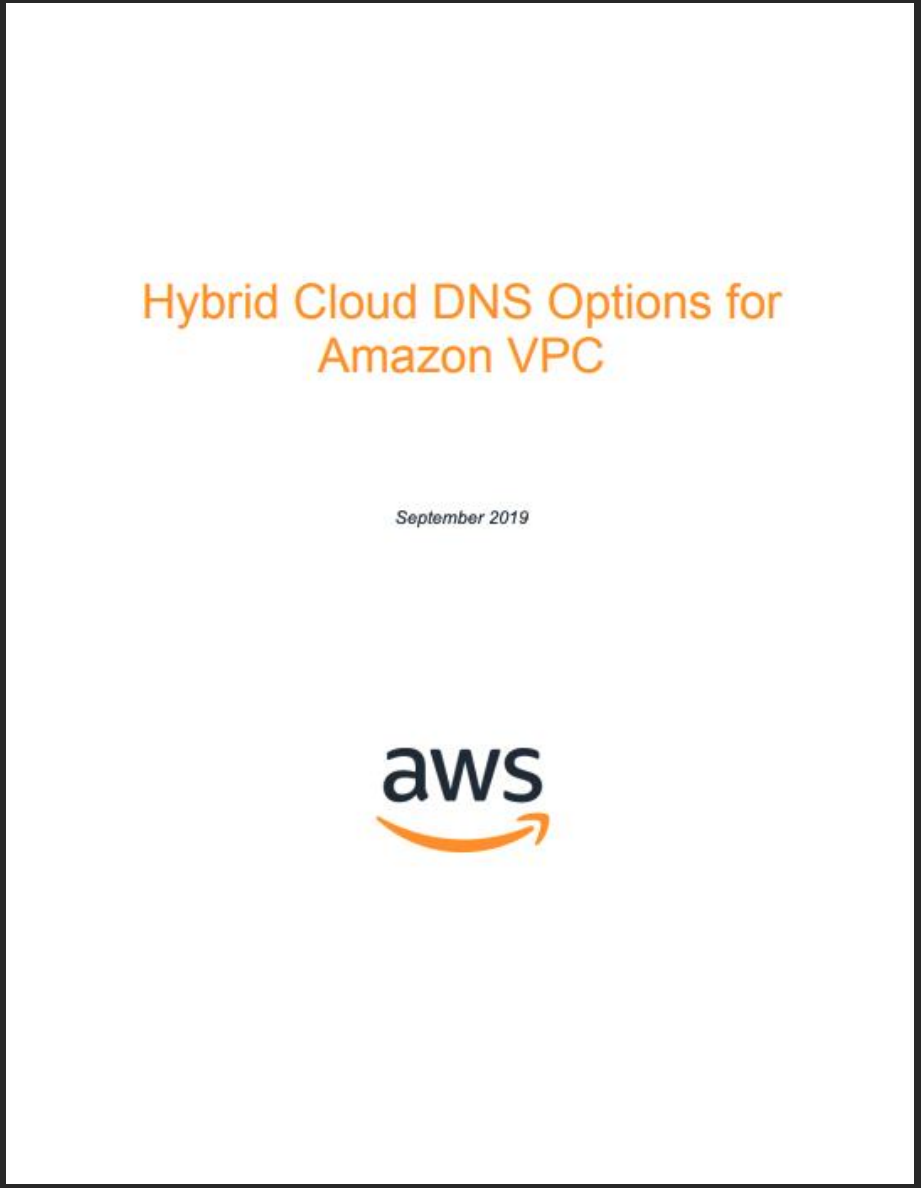
Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. Learn More

Evaluate Target Health: ○ Yes ● No

Hybrid DNS whitepaper

https://d1.awsstatic.com/whitepapers/hybrid-cloud-dns-options-for-vpc.pdf

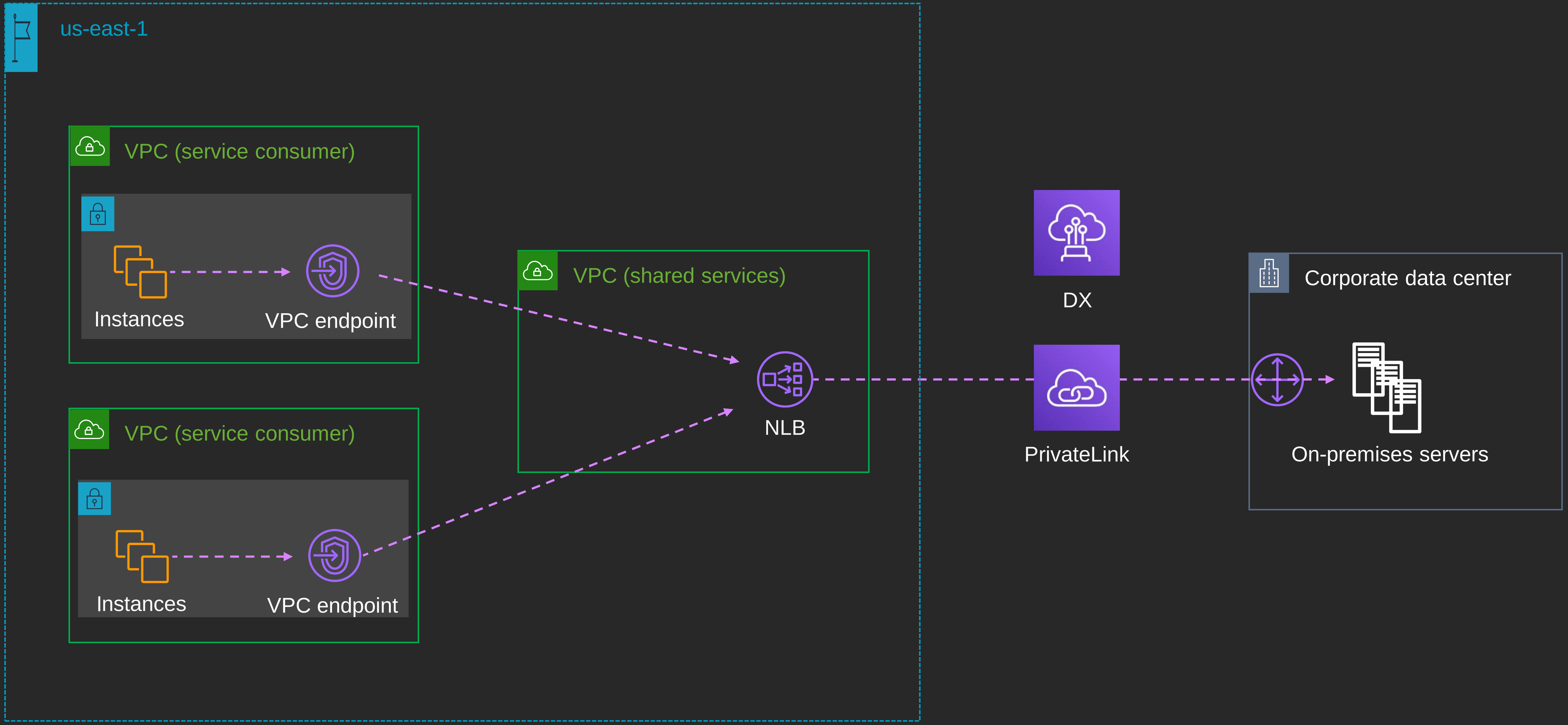


Hybrid Cloud DNS Options for Amazon VPC

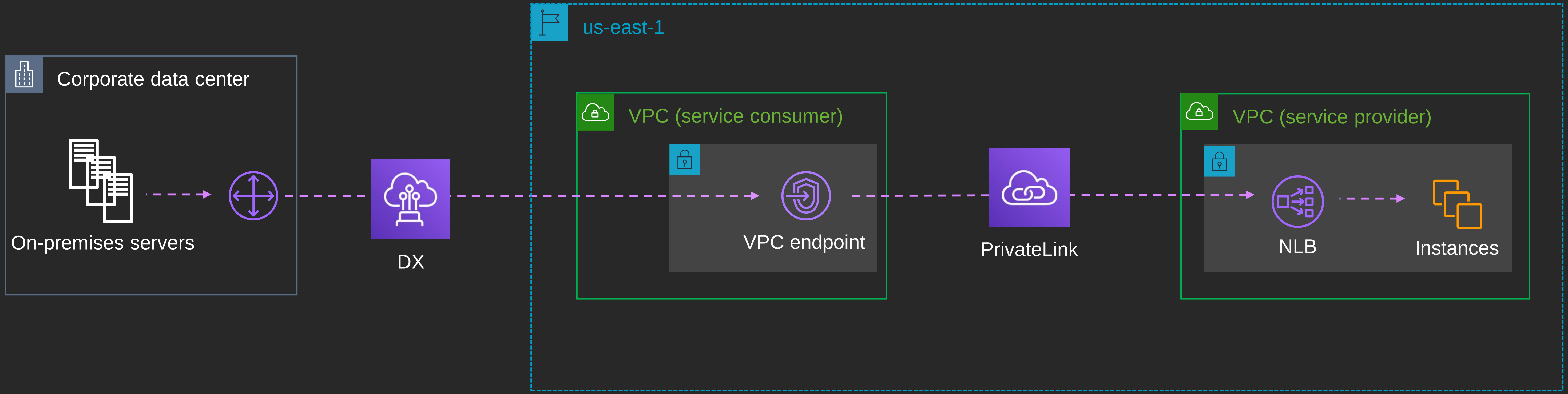
September 2019

Architecture

On-premises service providers

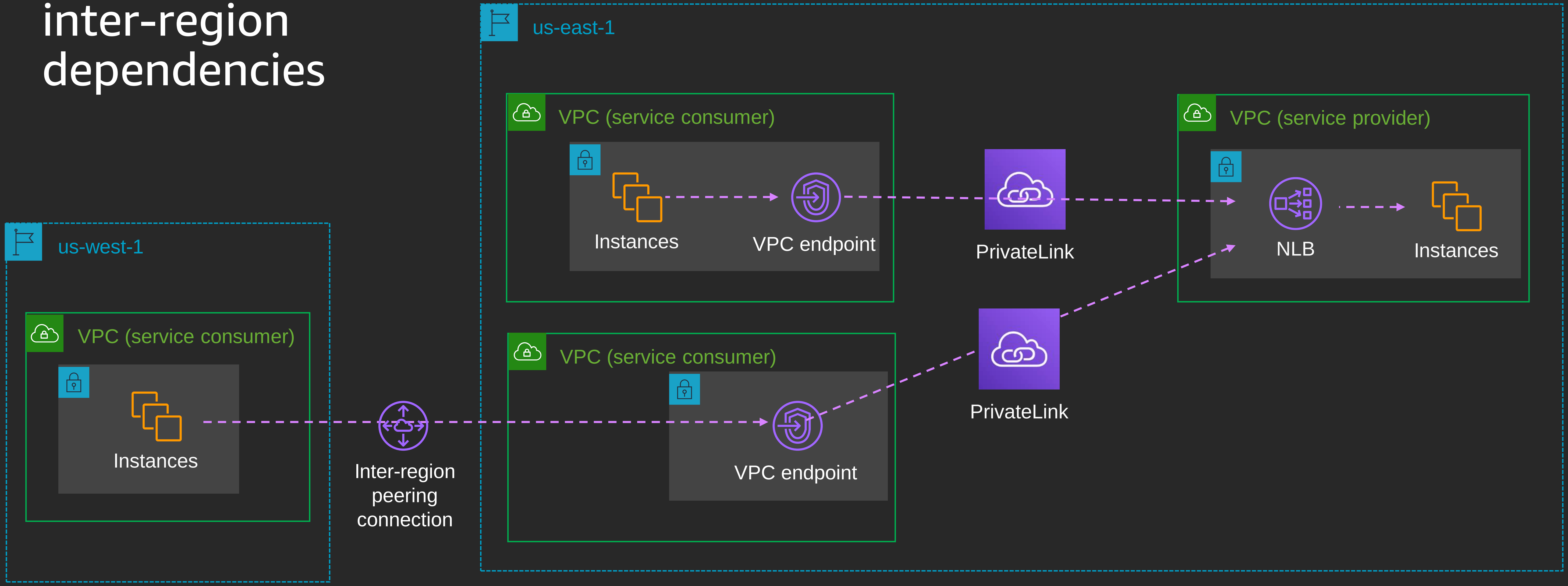


On-premises service consumers



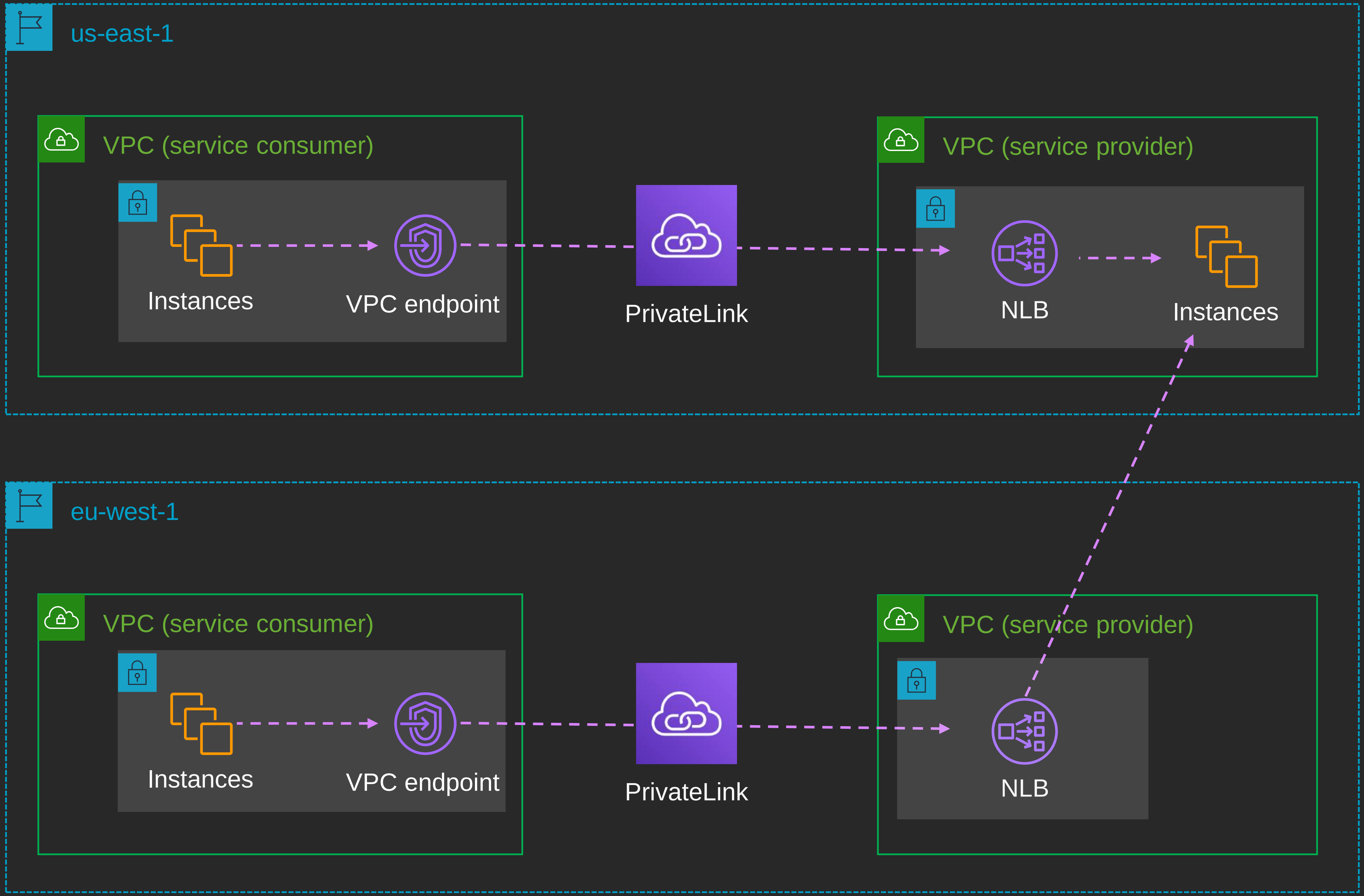
Cross-region connectivity to services

Note: Avoid inter-region dependencies

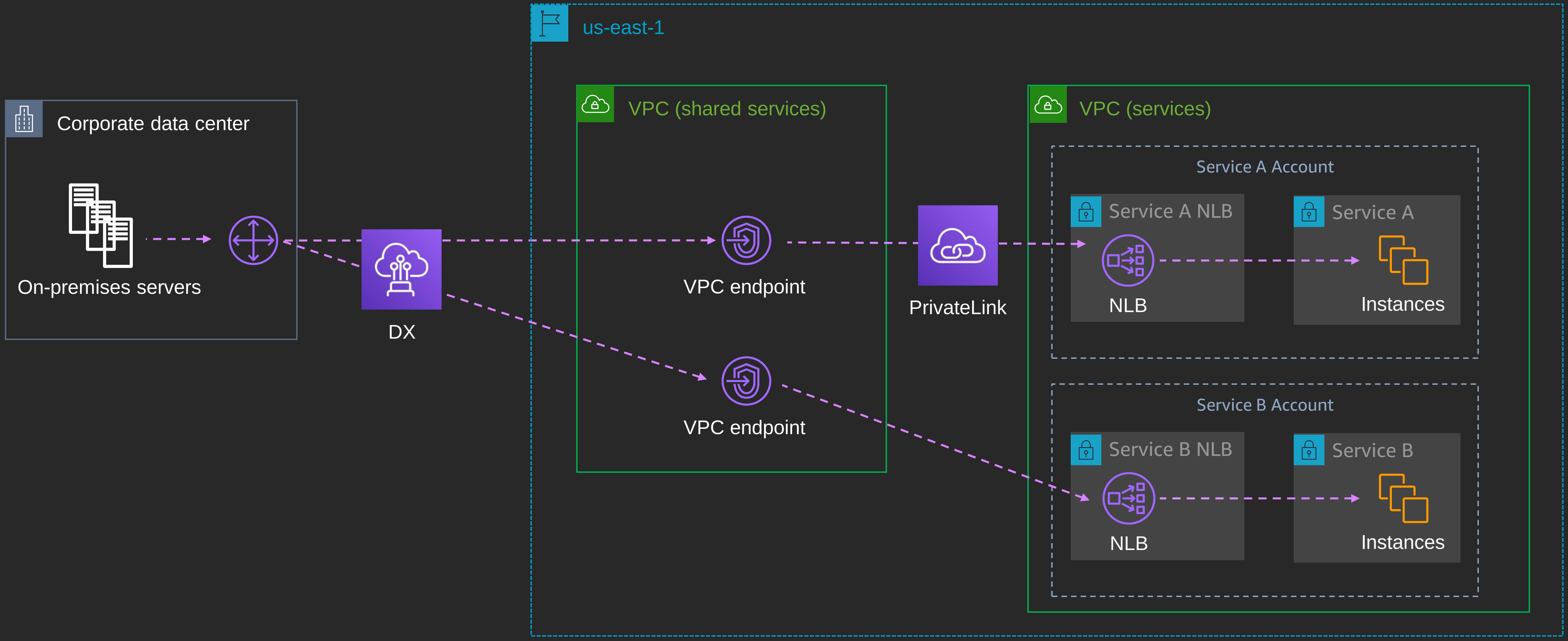


Presenting services in another region

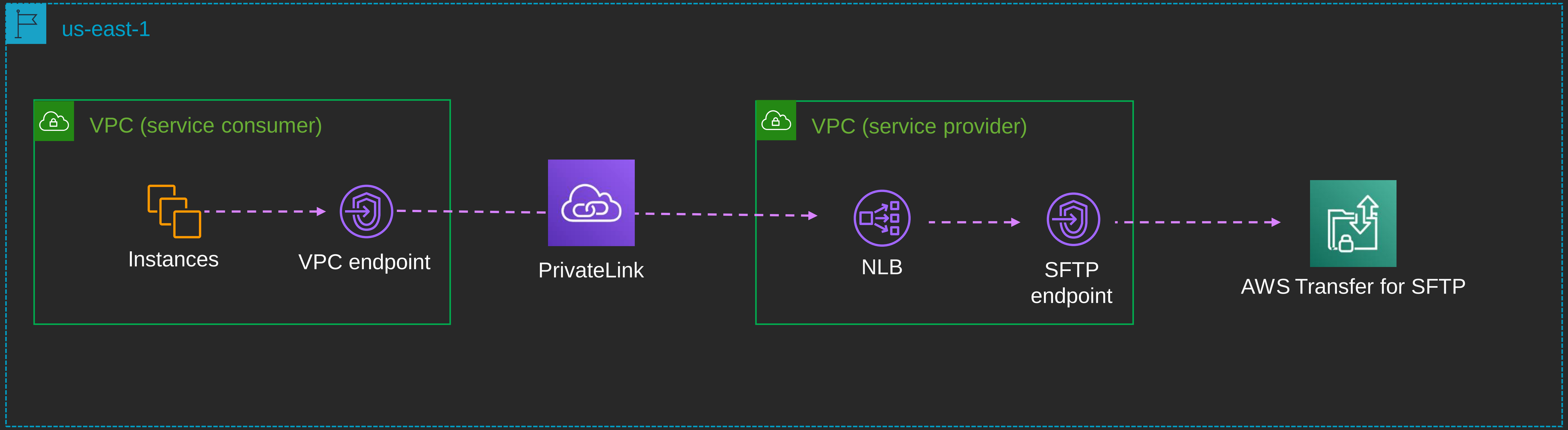
Note: Avoid inter-region dependencies



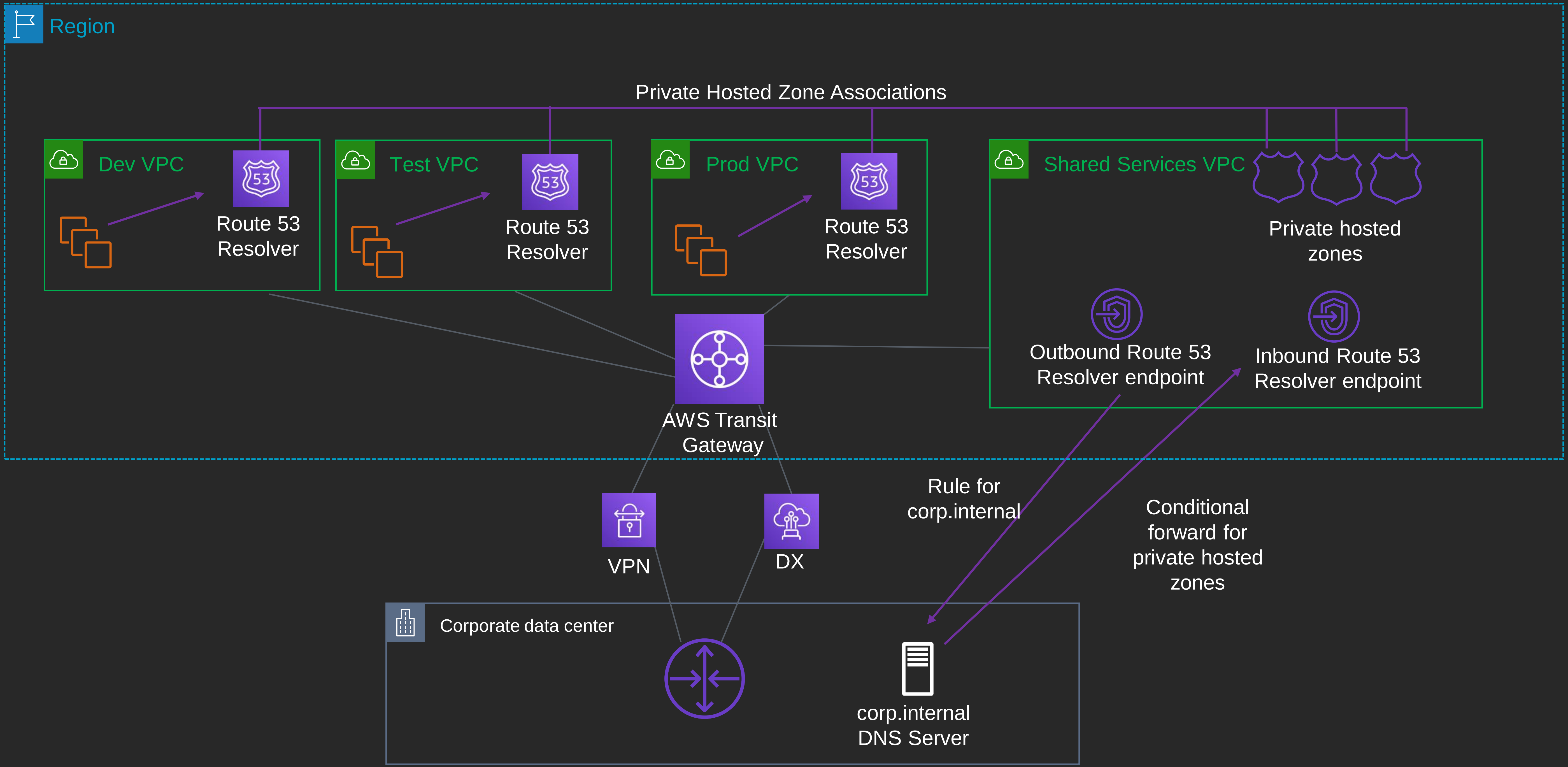
Shared VPC services



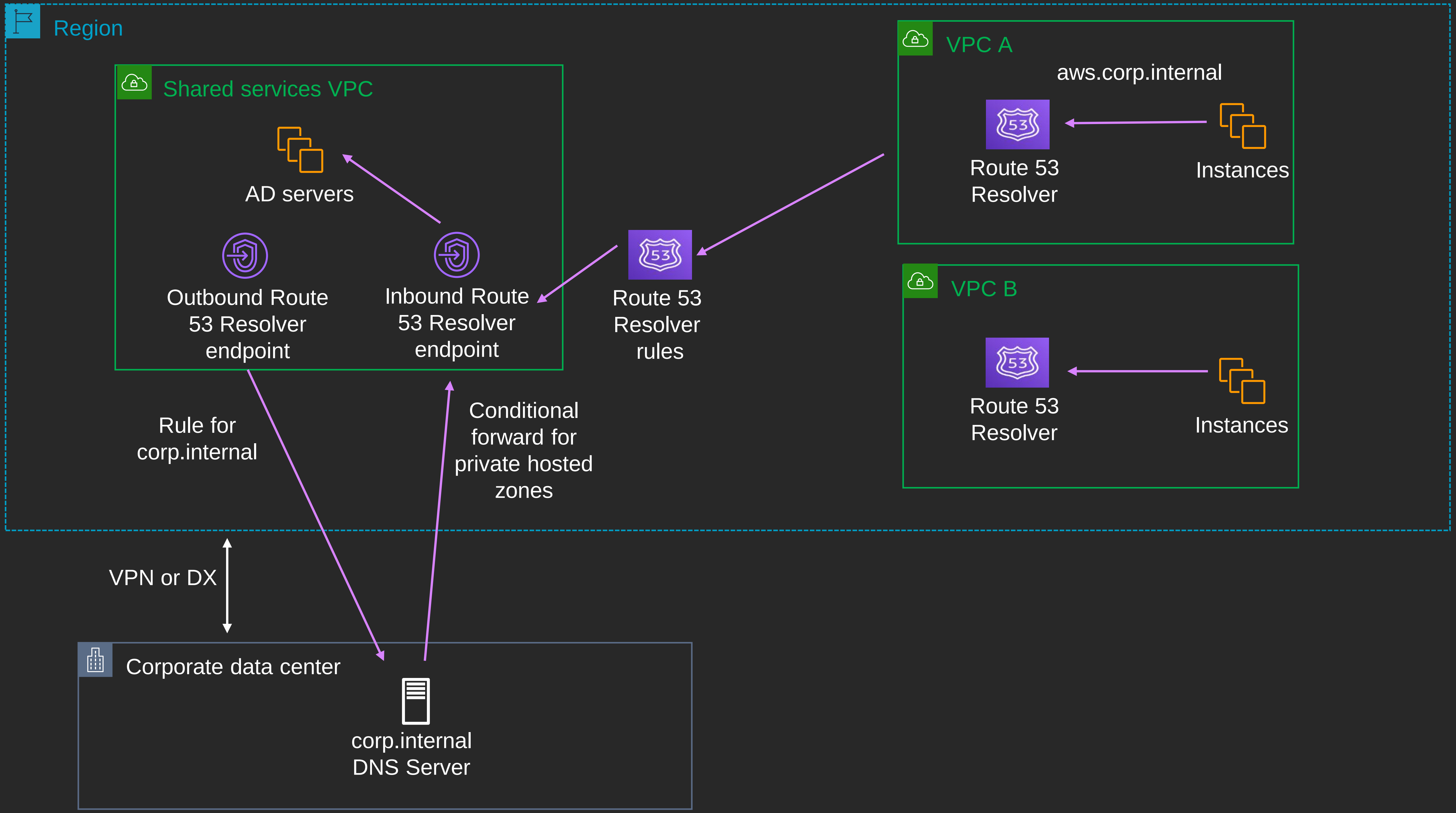
Extending endpoint behind an endpoint



Sharing VPC endpoints



Active Directory hybrid DNS



Best practices

PrivateLink

- Use at least two ENIs per VPCE
- Consider DNS infrastructure to meet your needs
- Ensure service provider NLB has ENI in each AZ
  - Cross-zone load balancing if don’t have service in each AZ
- Avoid building inter-region dependencies

Route 53

- Within a VPC use the “.2” Route 53 Resolver
- Avoid pointing outbound endpoints at inbound endpoints
- Use conditional forwarding for on-premises
- Avoid A records to VPCE ENIs
  - Alias record or CNAME

Takeaways

- PrivateLink endpoints are highly available
- Route 53 is highly available and fault tolerant
- PrivateLink and Route 53 allow you to create novel data flows

Related sessions

NET336 - Amazon Route 53 Resolver: Centralized DNS management of hybrid cloud

NET410 - Deep dive on DNS in the hybrid cloud

NET411 - Managing DNS across hundreds of VPCs

SEC347 - DNS across a multi-account environment

Questions?

Learn networking with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate networking skills

Free digital courses cover topics related to networking and content delivery, including Introduction to Amazon CloudFront and Introduction to Amazon VPC

Validate expertise with the
AWS Certified Advanced Networking - Specialty exam

Visit aws.amazon.com/training/paths-specialty

Thank you!

James Devine
devineja@amazon.com

Please complete the session survey in the mobile app.