
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

NET215

Introducing Amazon VPC Lattice: Simplifying application networking

Justin Davies (he/him)
Principal Product Manager,
EC2 Networking, AWS

Sathya Ramaseshan (he/him)
Principal Product Manager,
EC2 Networking, AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do we make it simple for developers to connect, secure, and monitor their services, without sacrificing the controls admins need to audit and secure their environment?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Need for service-to-service communication

Current solutions: Overview and pain points

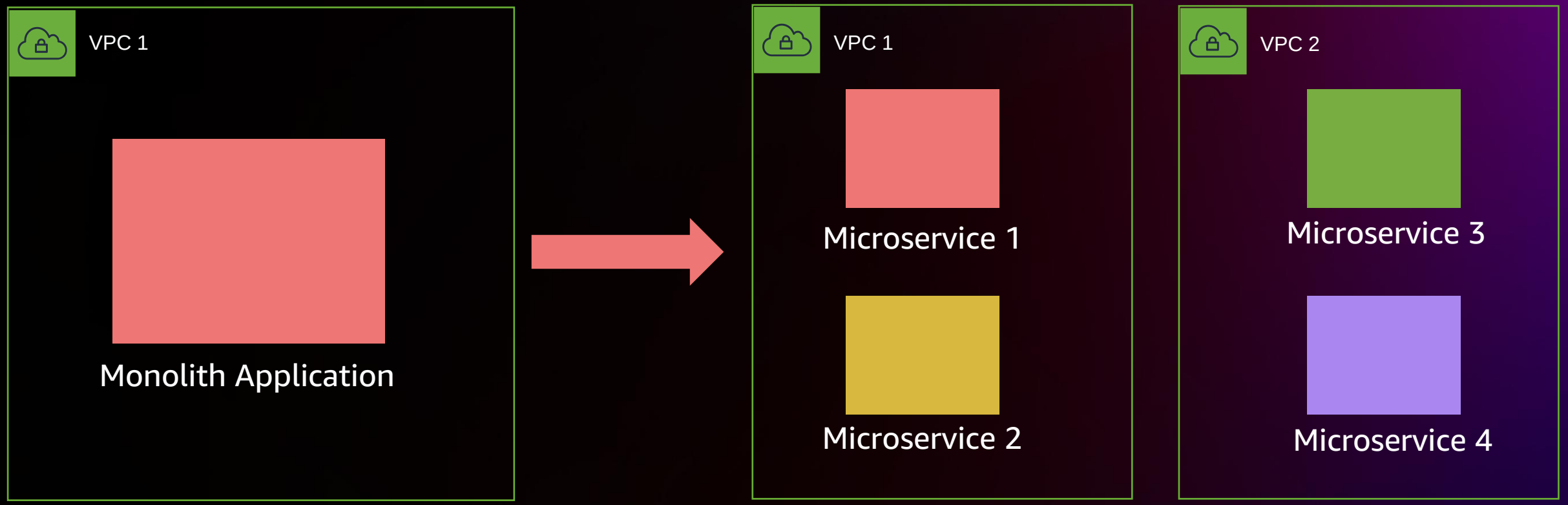
VPC Lattice: Key features and functionality

Use-cases: How Amazon VPC Lattice helps

Next-steps: How to sign up

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

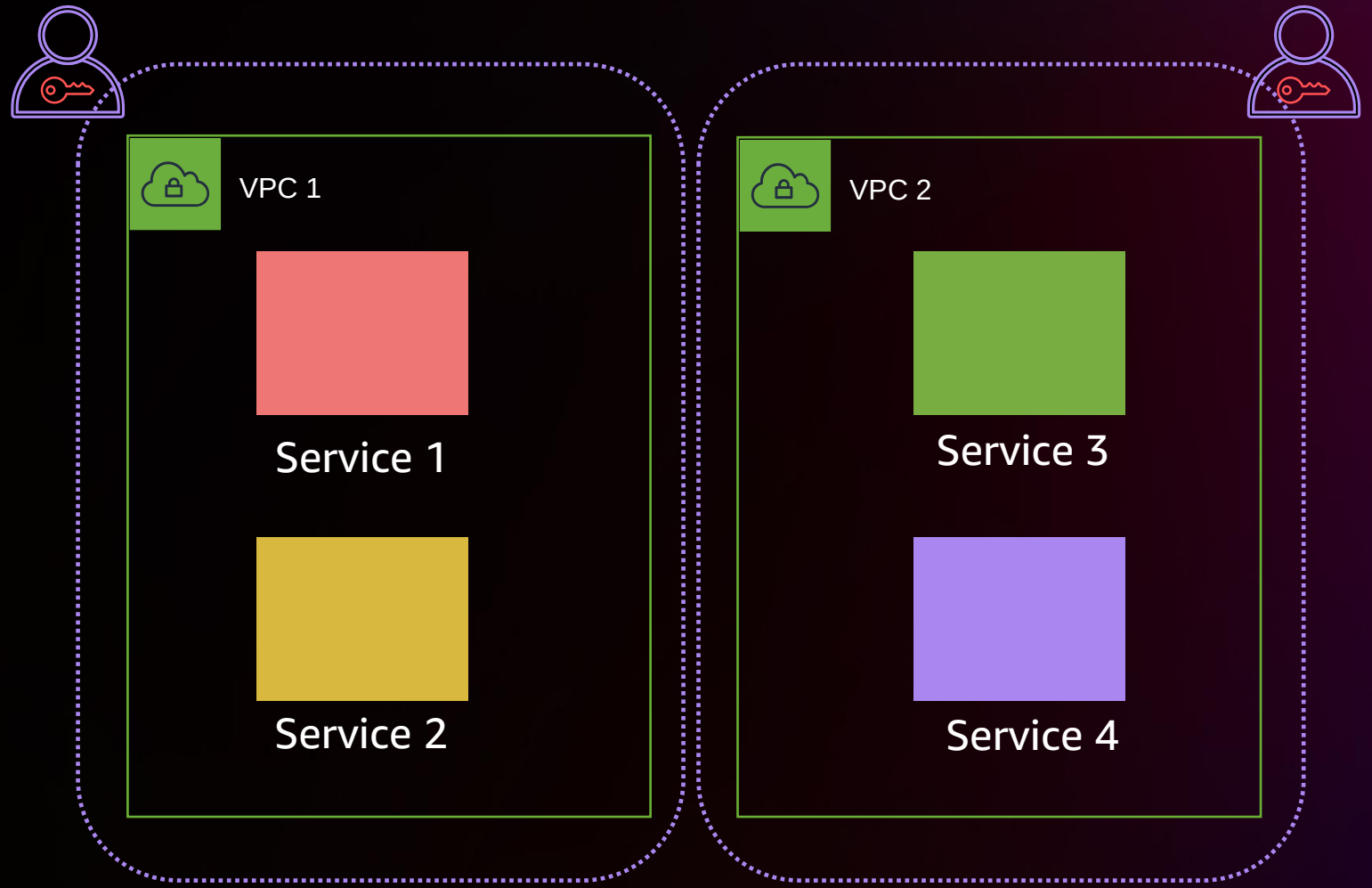
The journey from monolith to microservices



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

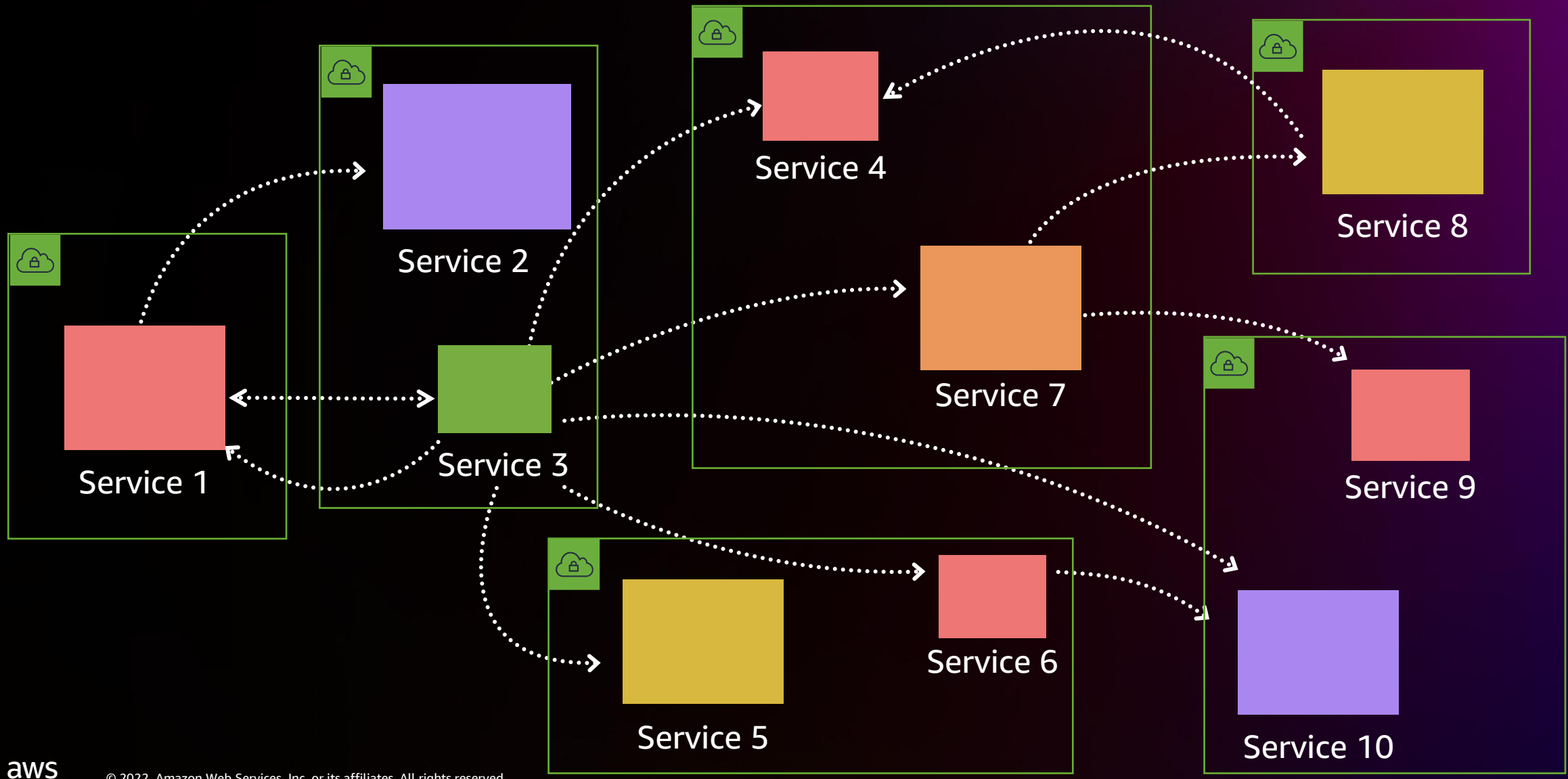
Give service teams their own sandbox

Network and permission boundaries with VPCs and accounts



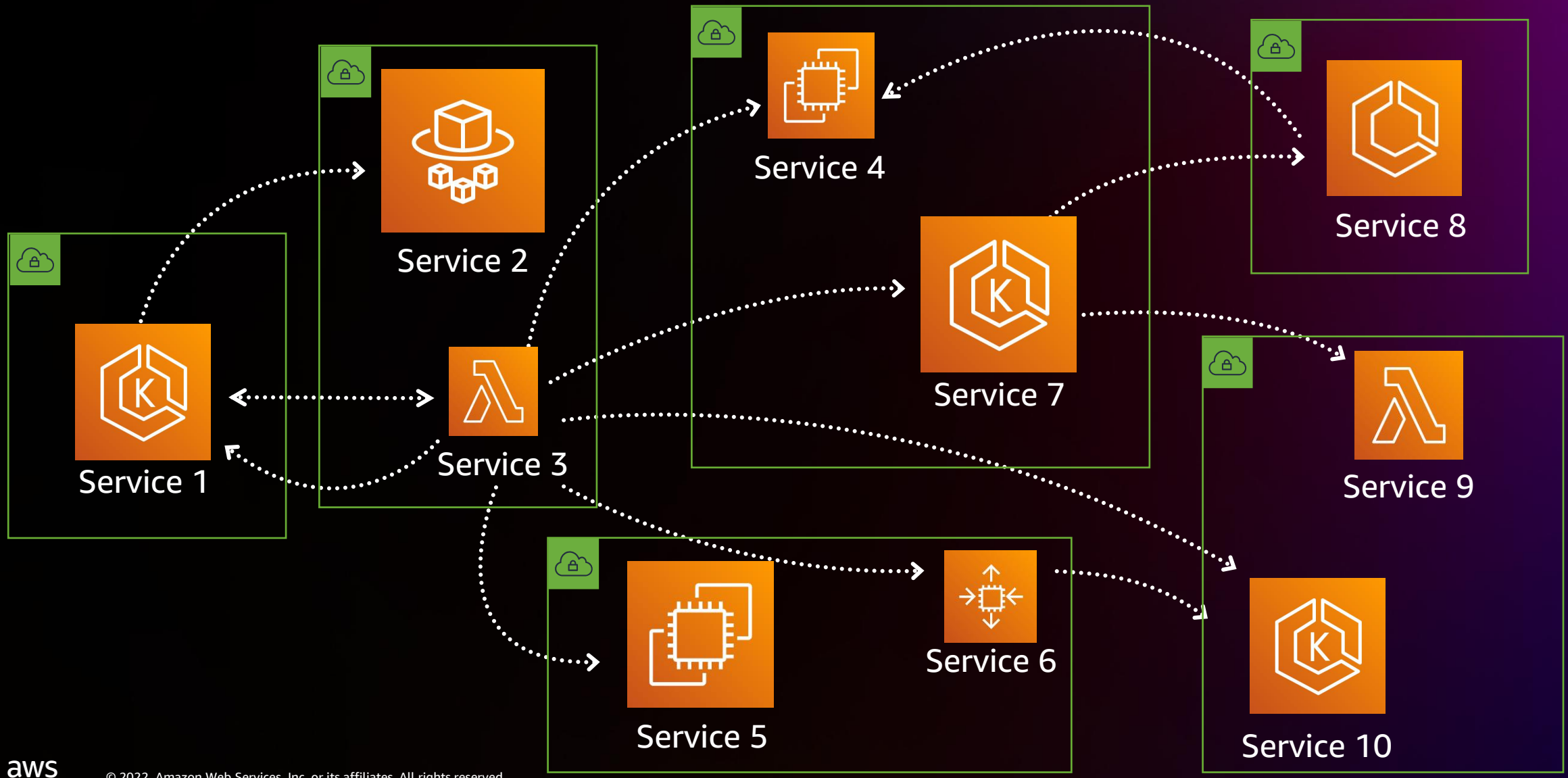
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

But does it match your application boundary?



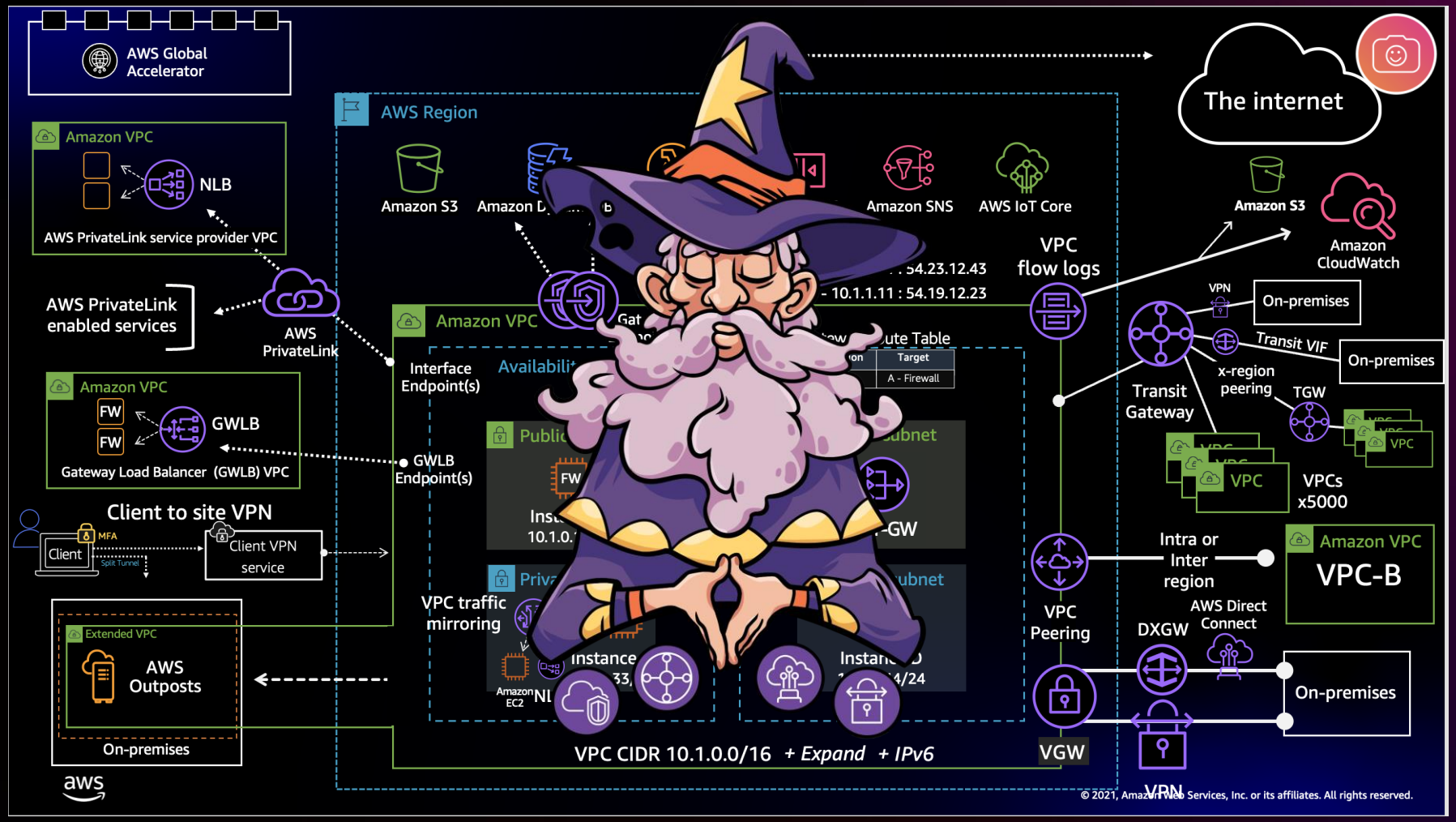
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

But does it match your application boundary?



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Devs shouldn’t need to be network wizards



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Devs shouldn’t need to be network wizards





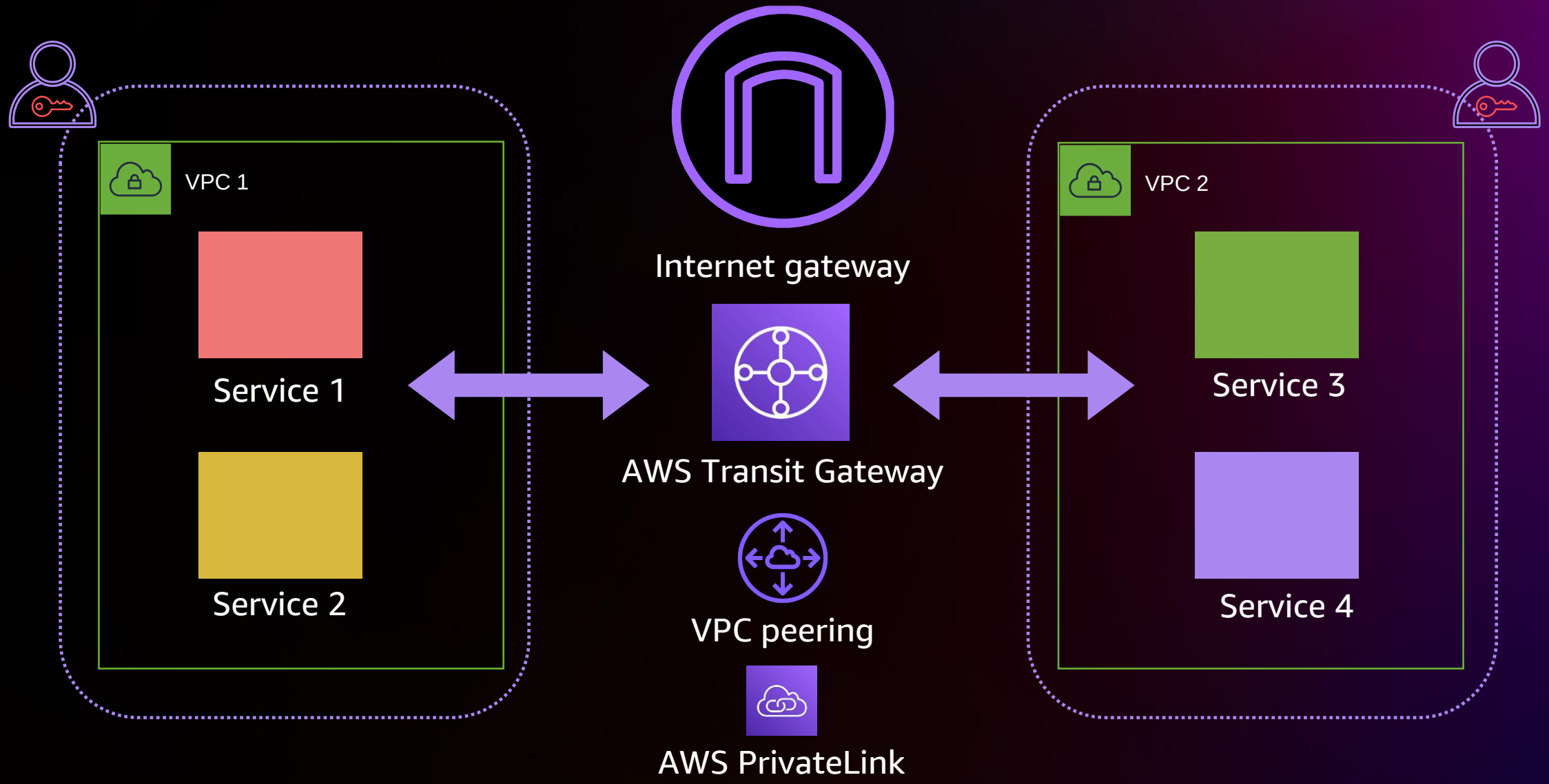
Developer ✗



Admin ✓

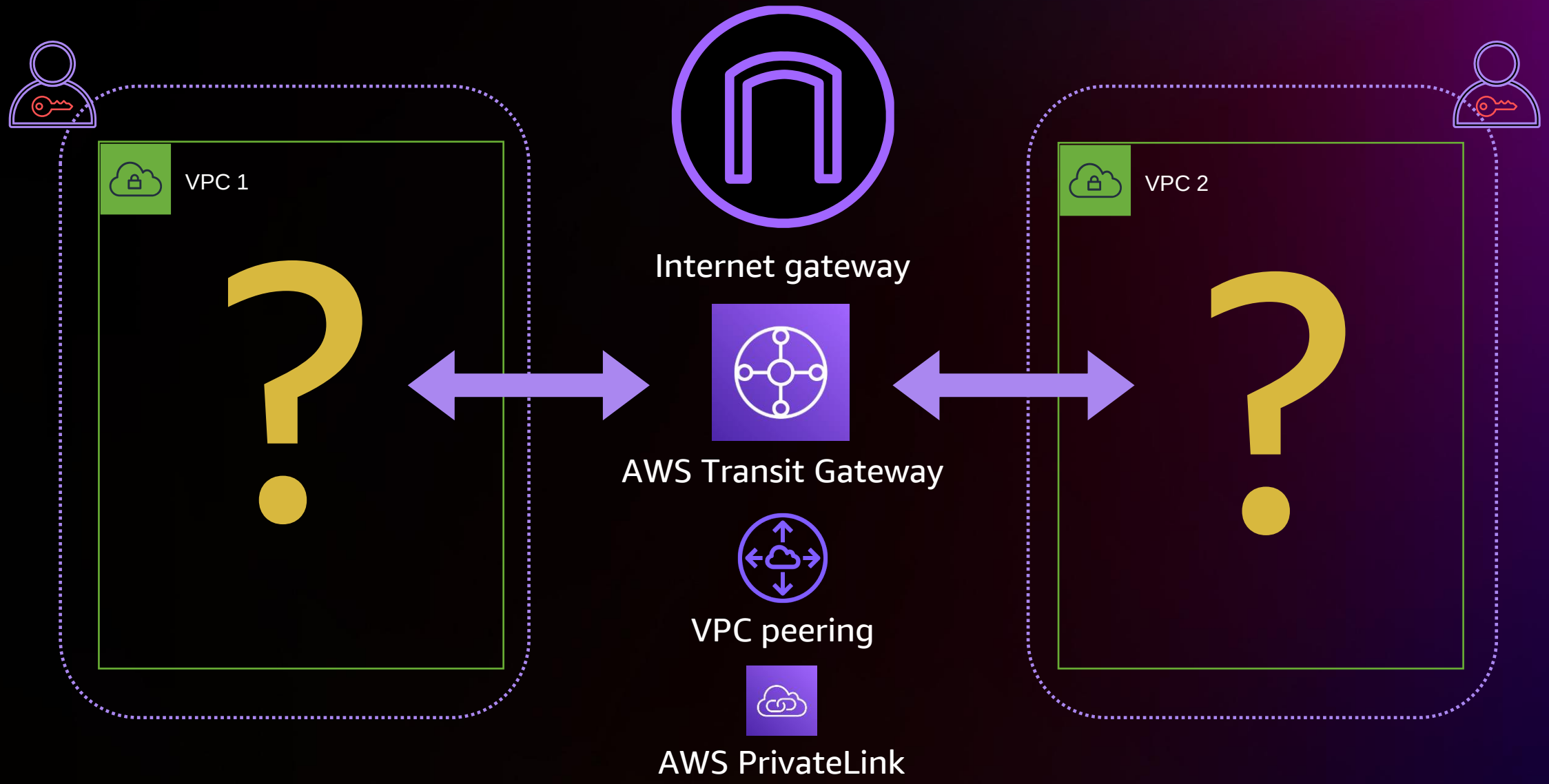
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The network portion...



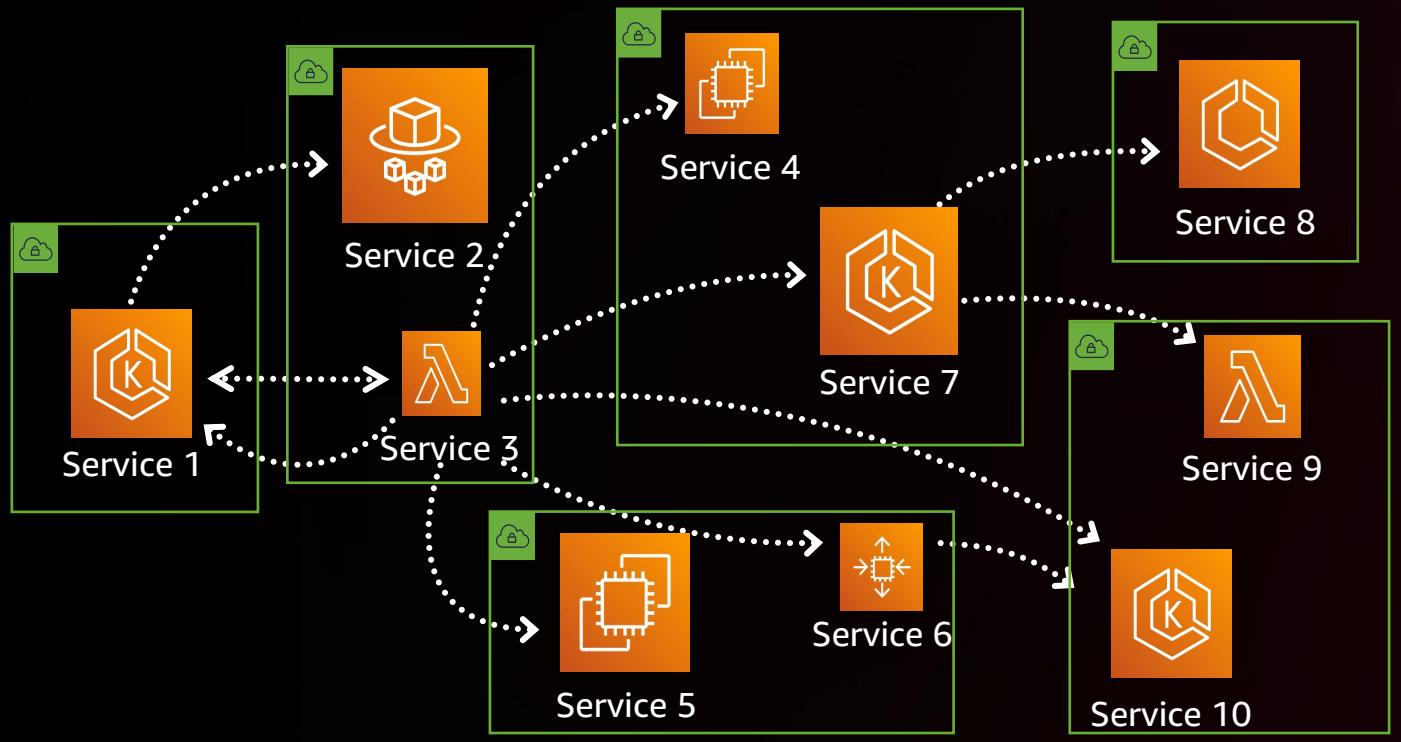
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The network portion...



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do you handle more than network connectivity?



Service discovery

Traffic management

Load balancing

Authentication

Authorization

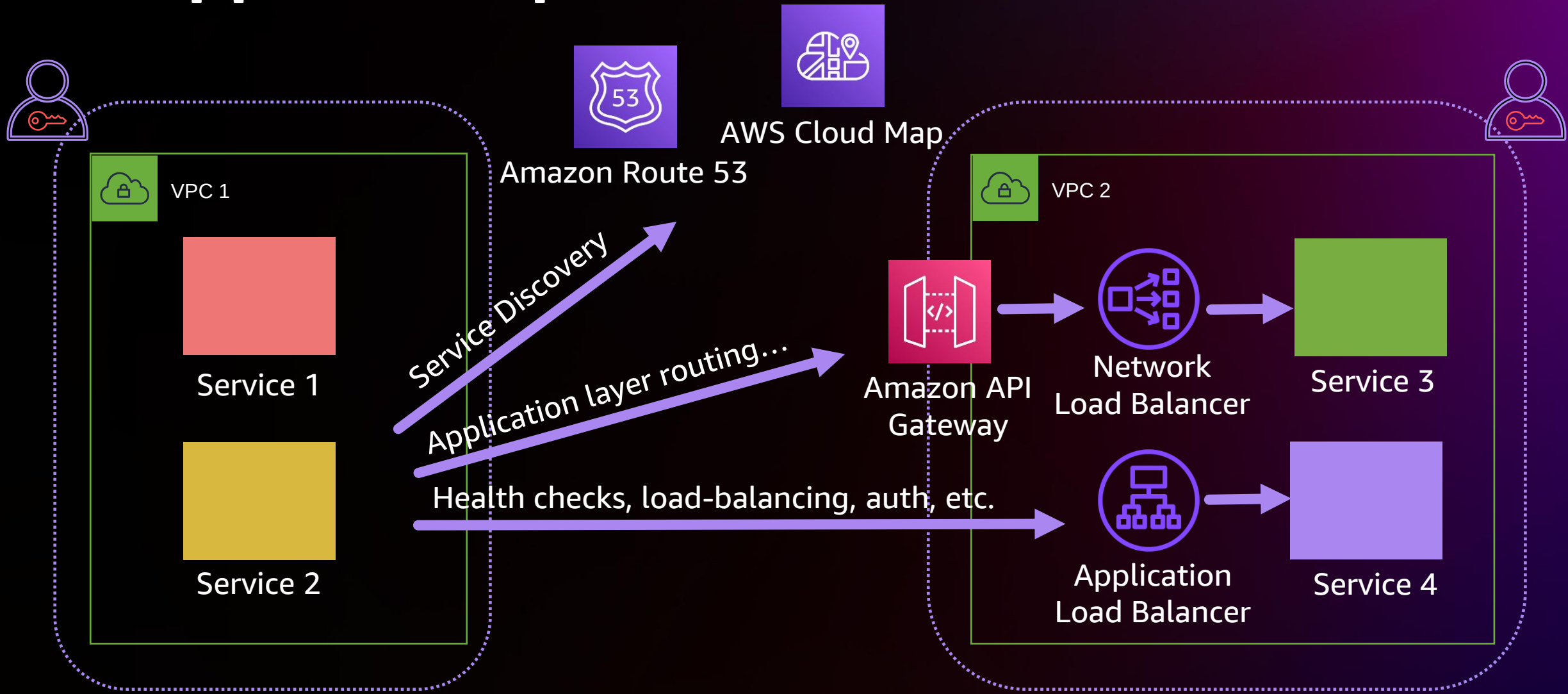
Observability

?

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The application portion…

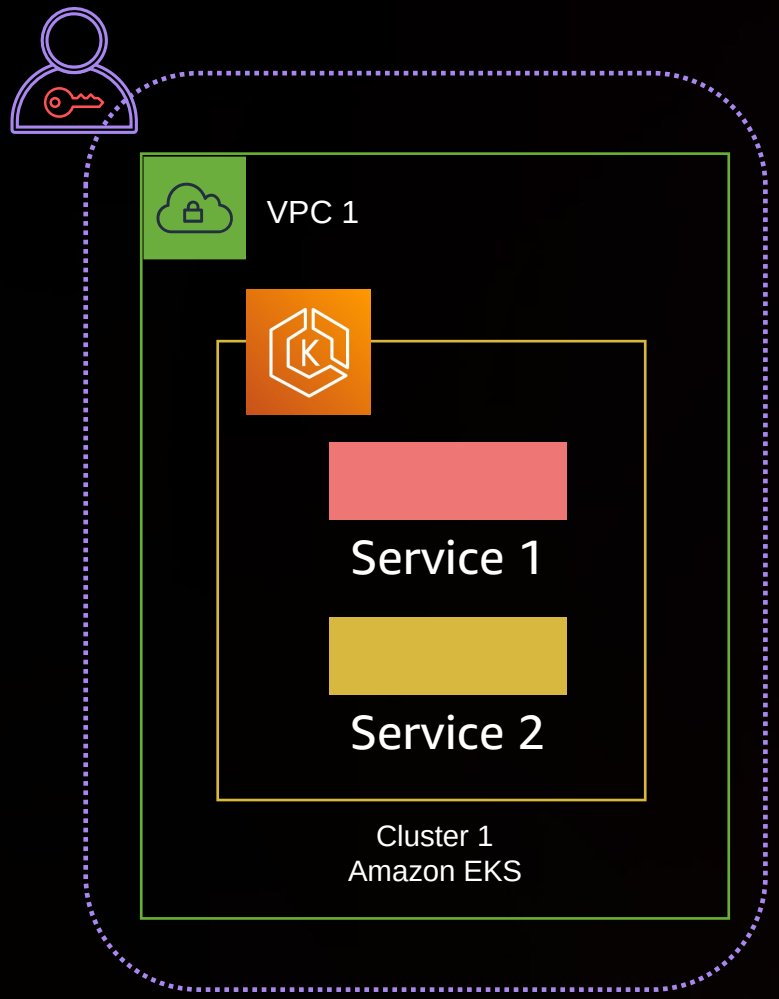


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Note: Don't see your favorite service?
Don't worry. Not an exhaustive list.

Containers:

Basics out of the box…



In VPC network connectivity ✓

Service discovery ✓

Basic round robin load balancing ✓

Traffic management ?

Authentication ?

Authorization ?

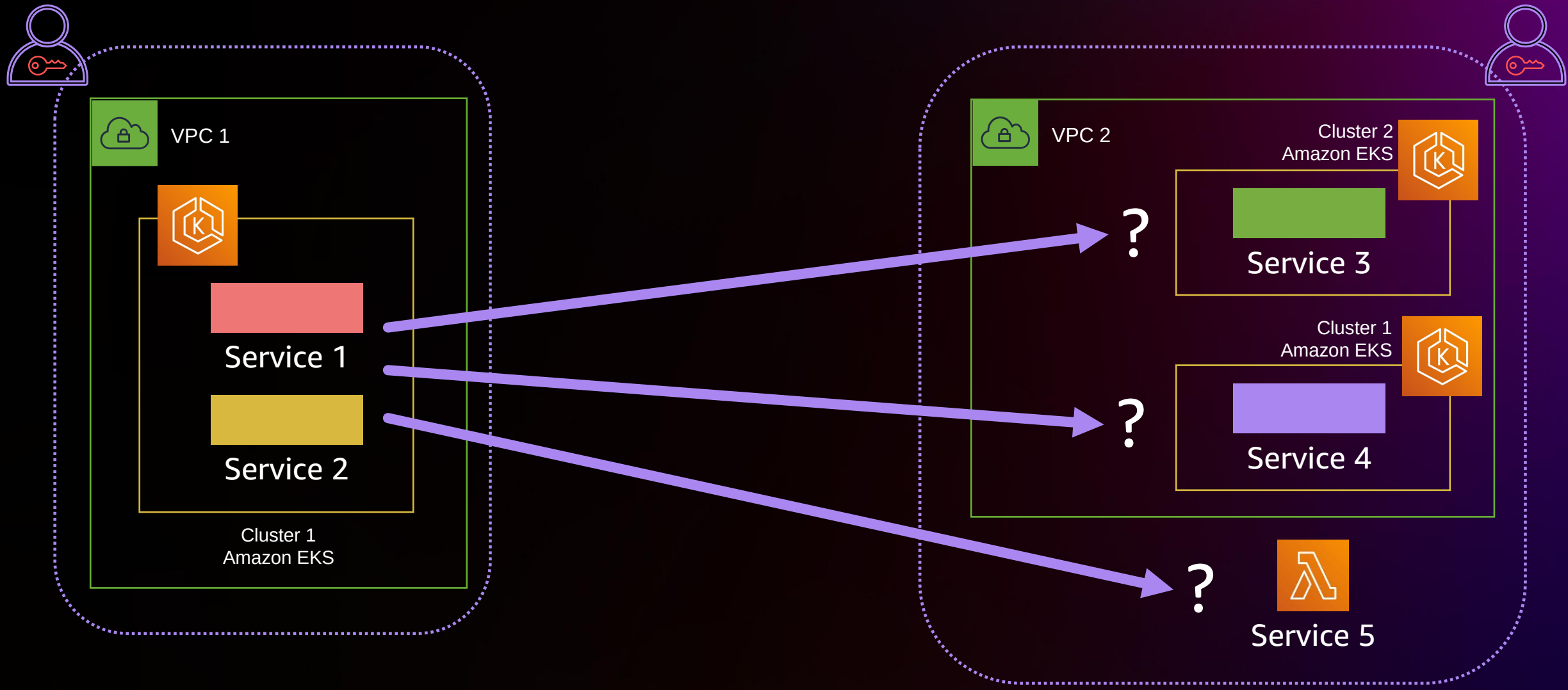
Observability ?

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Containers:

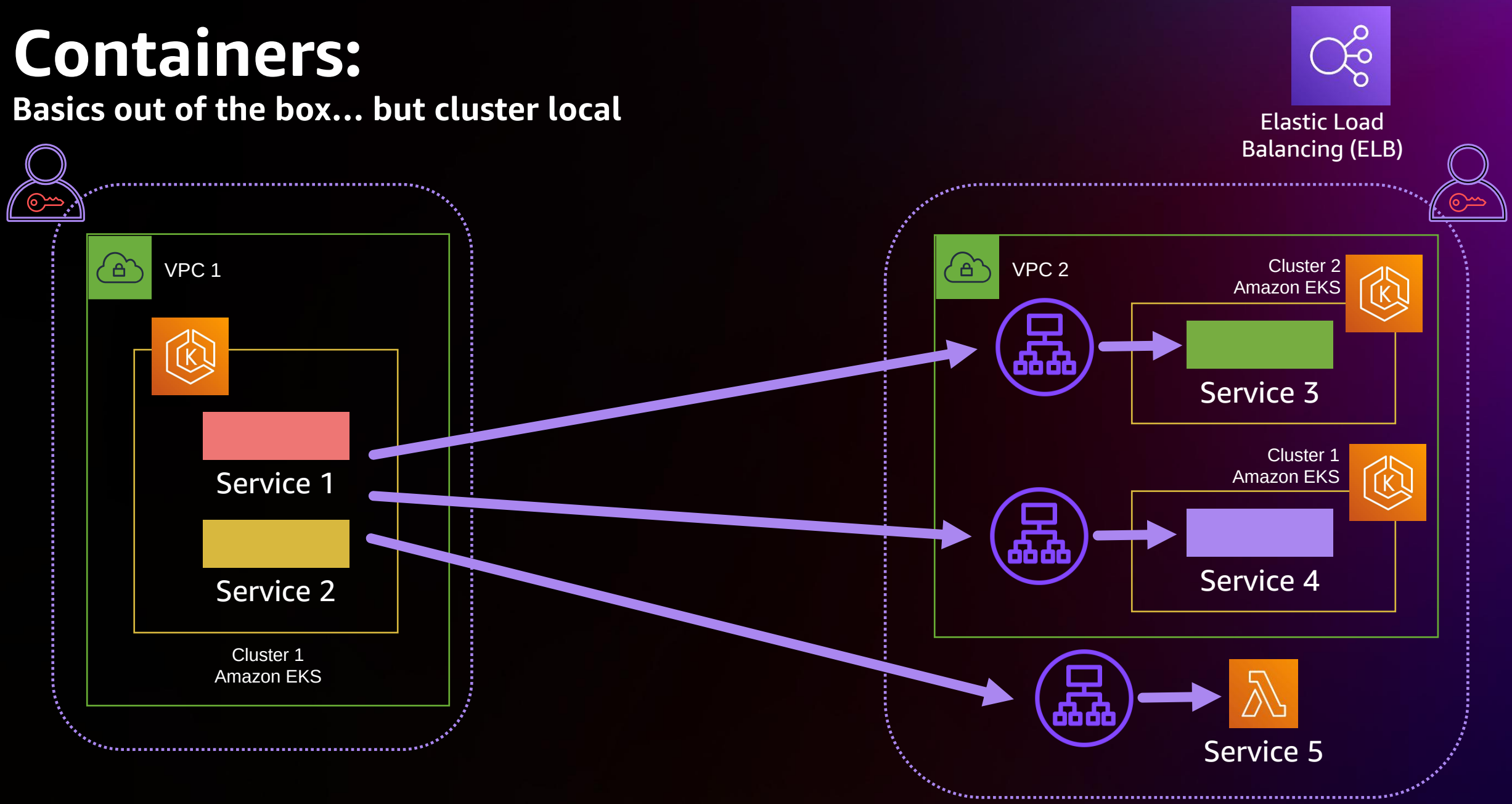
Basics out of the box… but cluster local



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Containers:

Basics out of the box… but cluster local

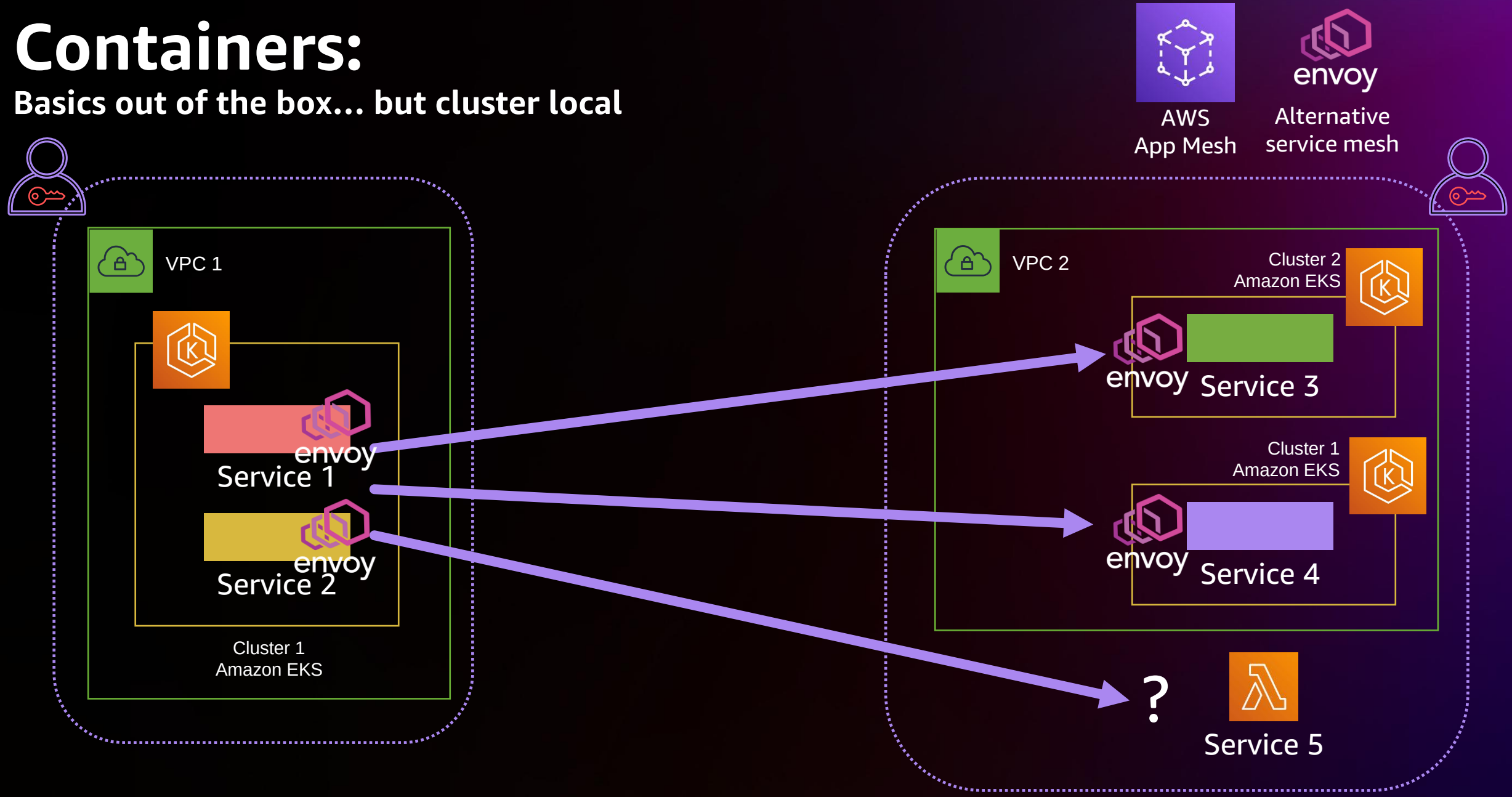


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Note: Don't see your favorite service? Don't worry. Not an exhaustive list.

Containers:

Basics out of the box… but cluster local

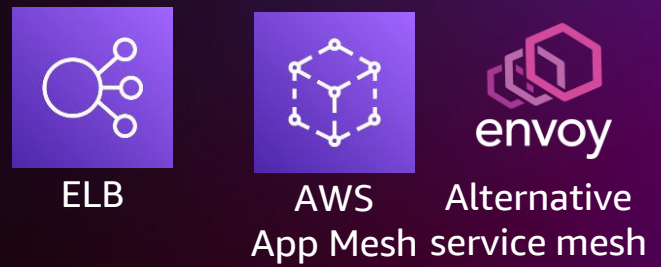


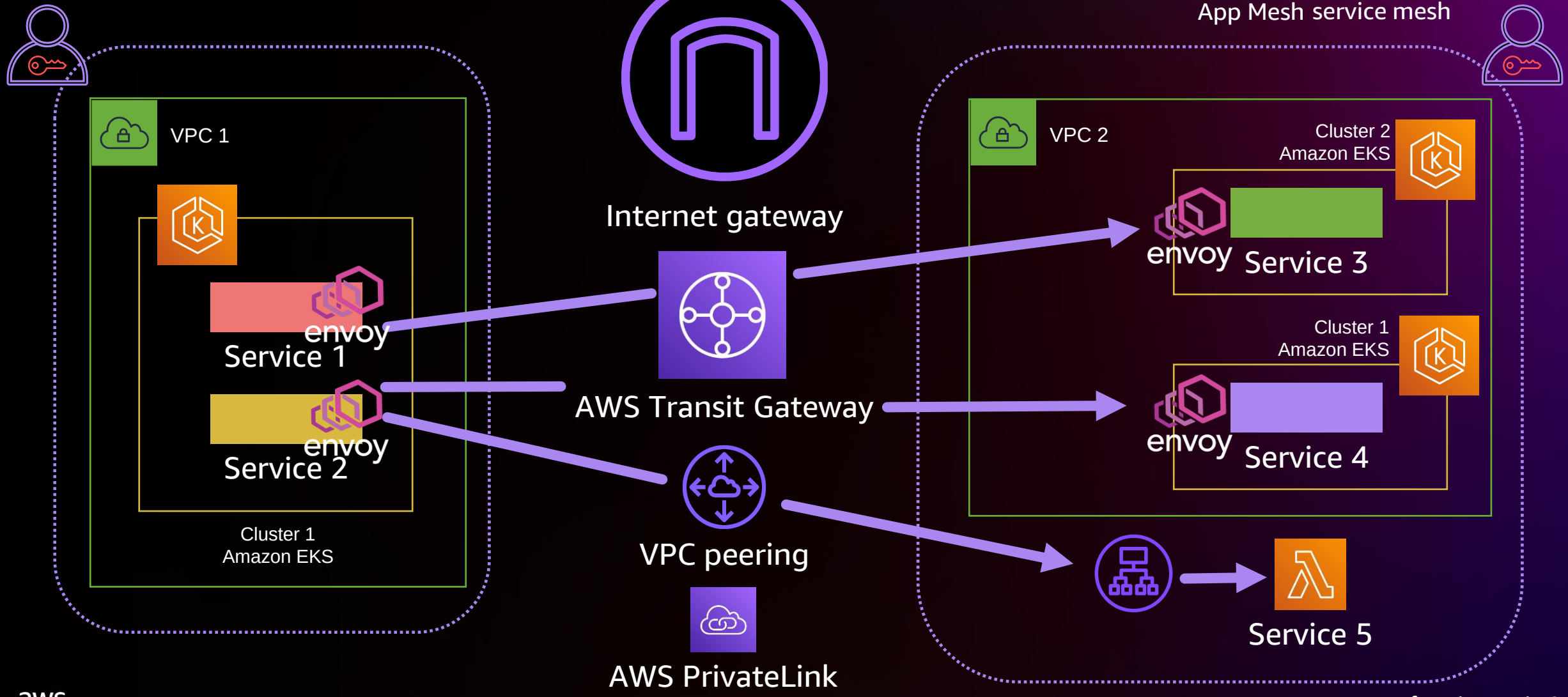
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Note: Don't see your favorite service?
Don't worry. Not an exhaustive list.

Oh yeah...

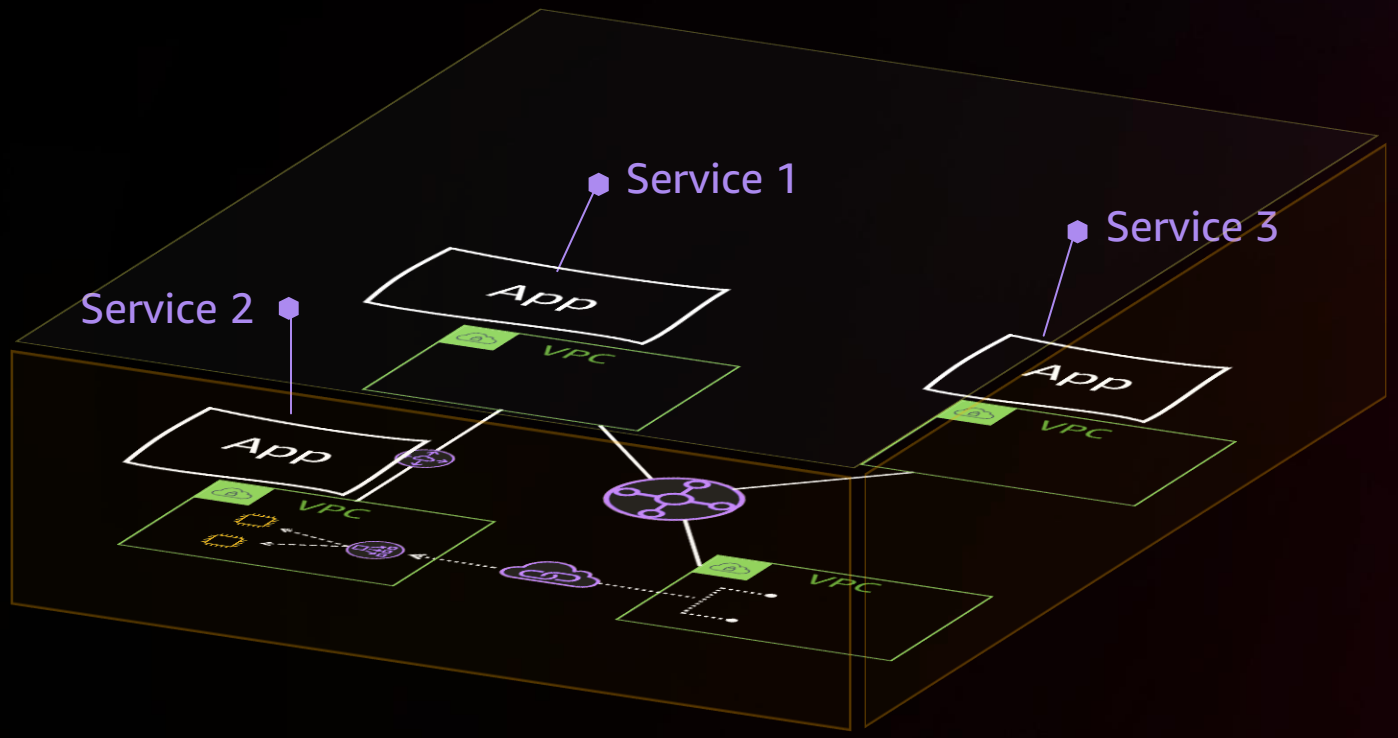
the network is still there!





© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Note: Don't see your favorite service?
Don't worry. Not an exhaustive list.



SECURITY LAYER (Admin/Dev)

Security applies to the complete deployment, often in both application and VPC layers

APPLICATION LAYER (Dev)

Applications deployed across multiple VPCs and Accounts

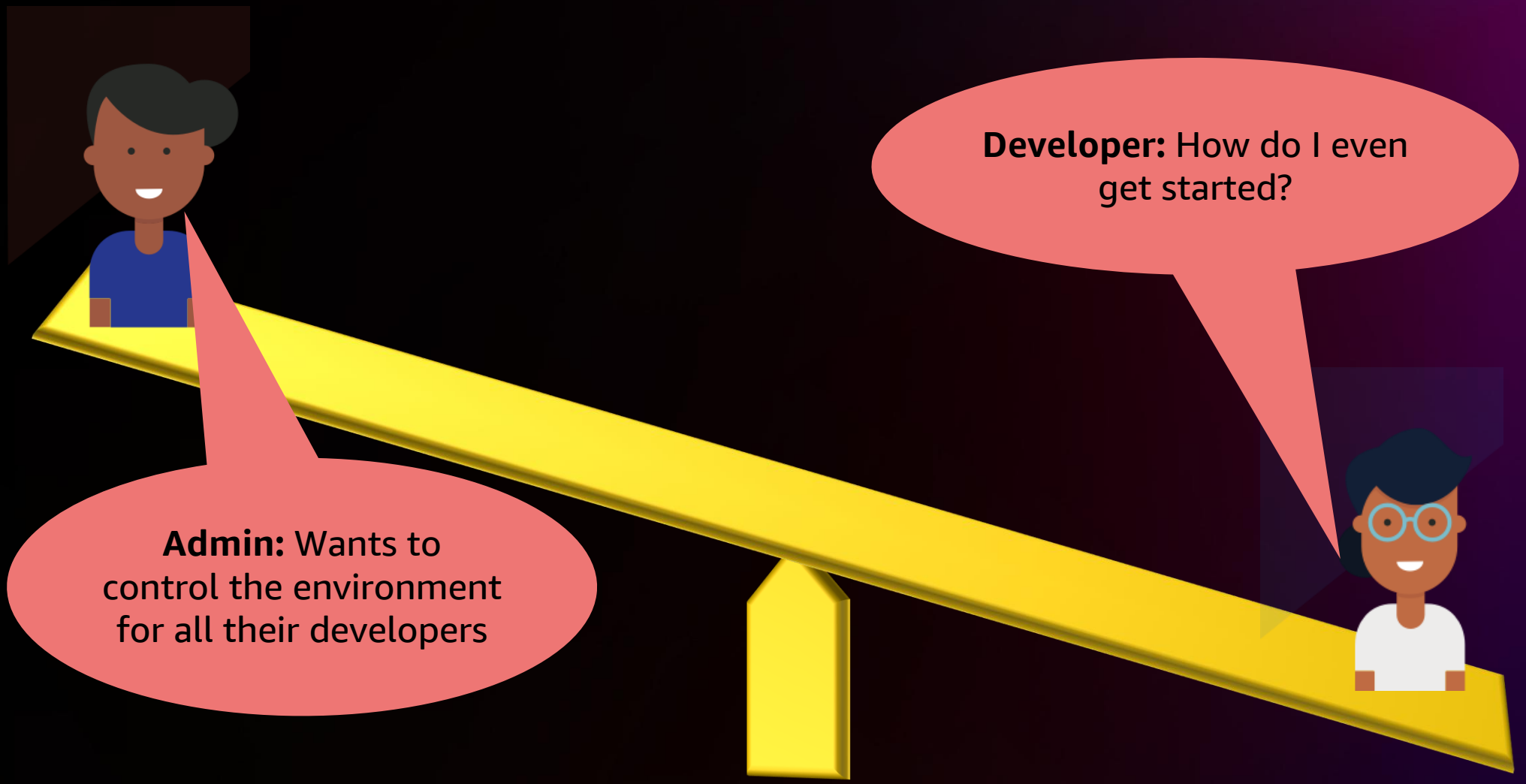
NETWORKING LAYER (Admin)

Provides connectivity between applications throughout the deployment

aws

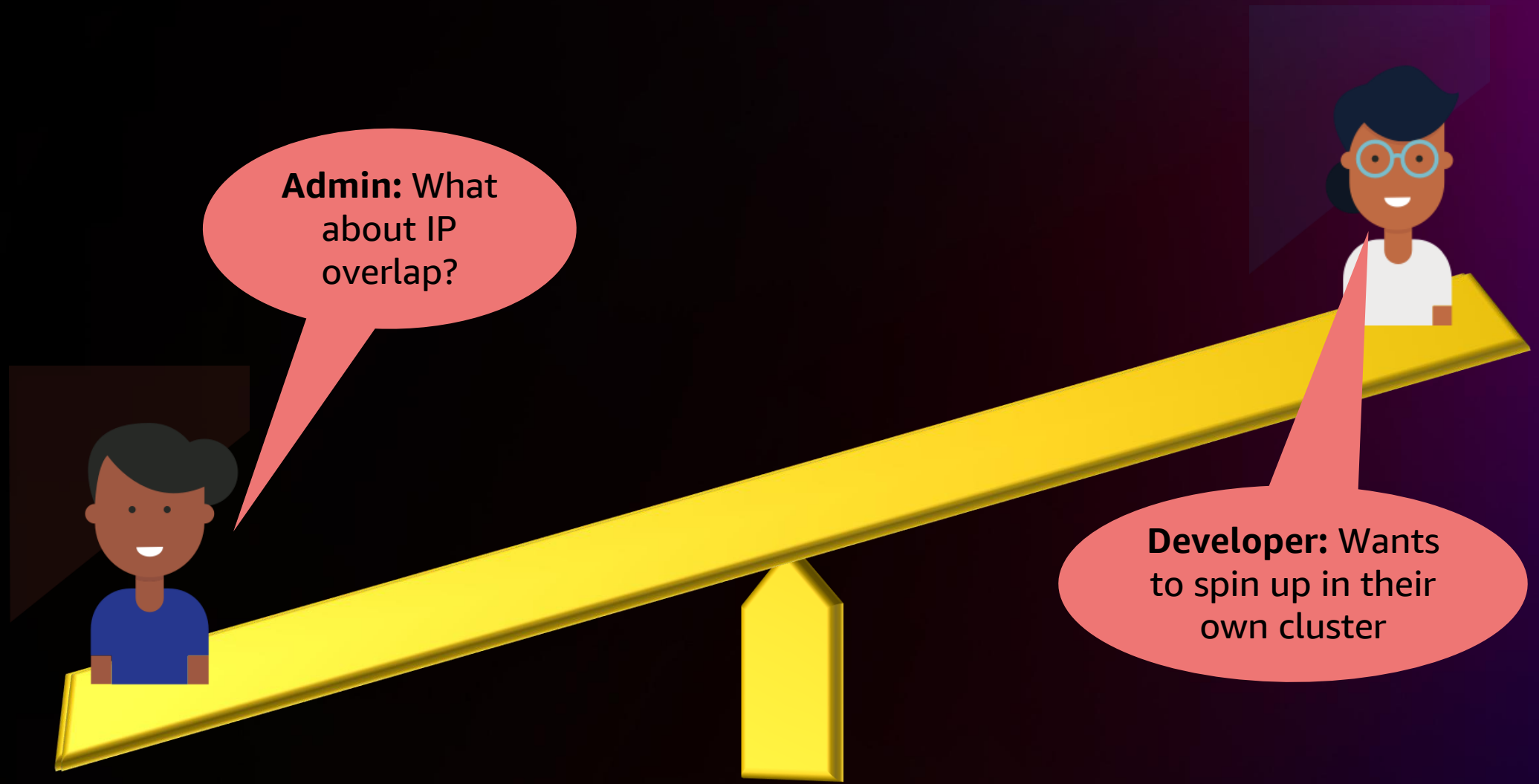
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Connectivity conundrum



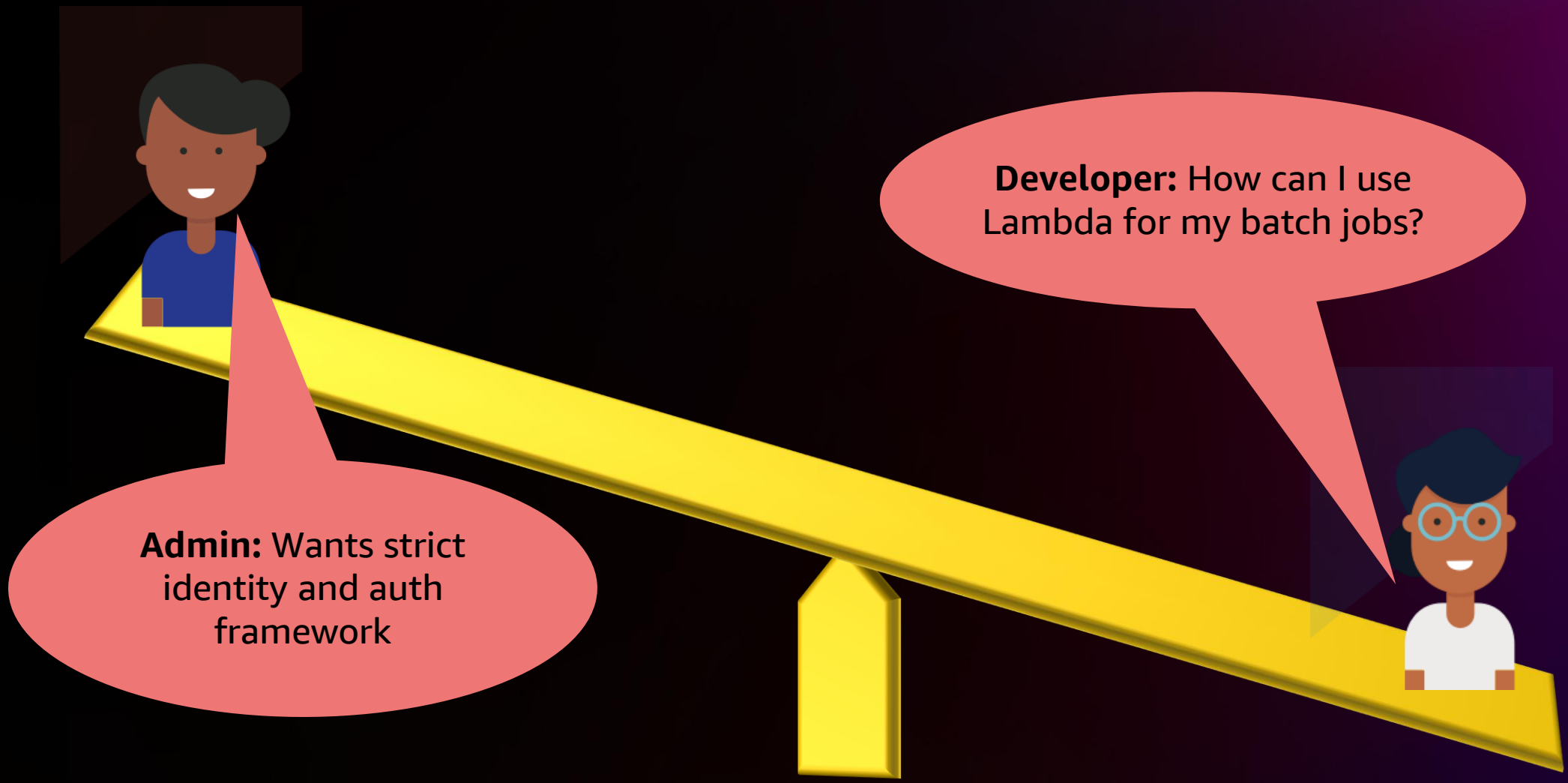
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Connectivity conundrum



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security conundrum



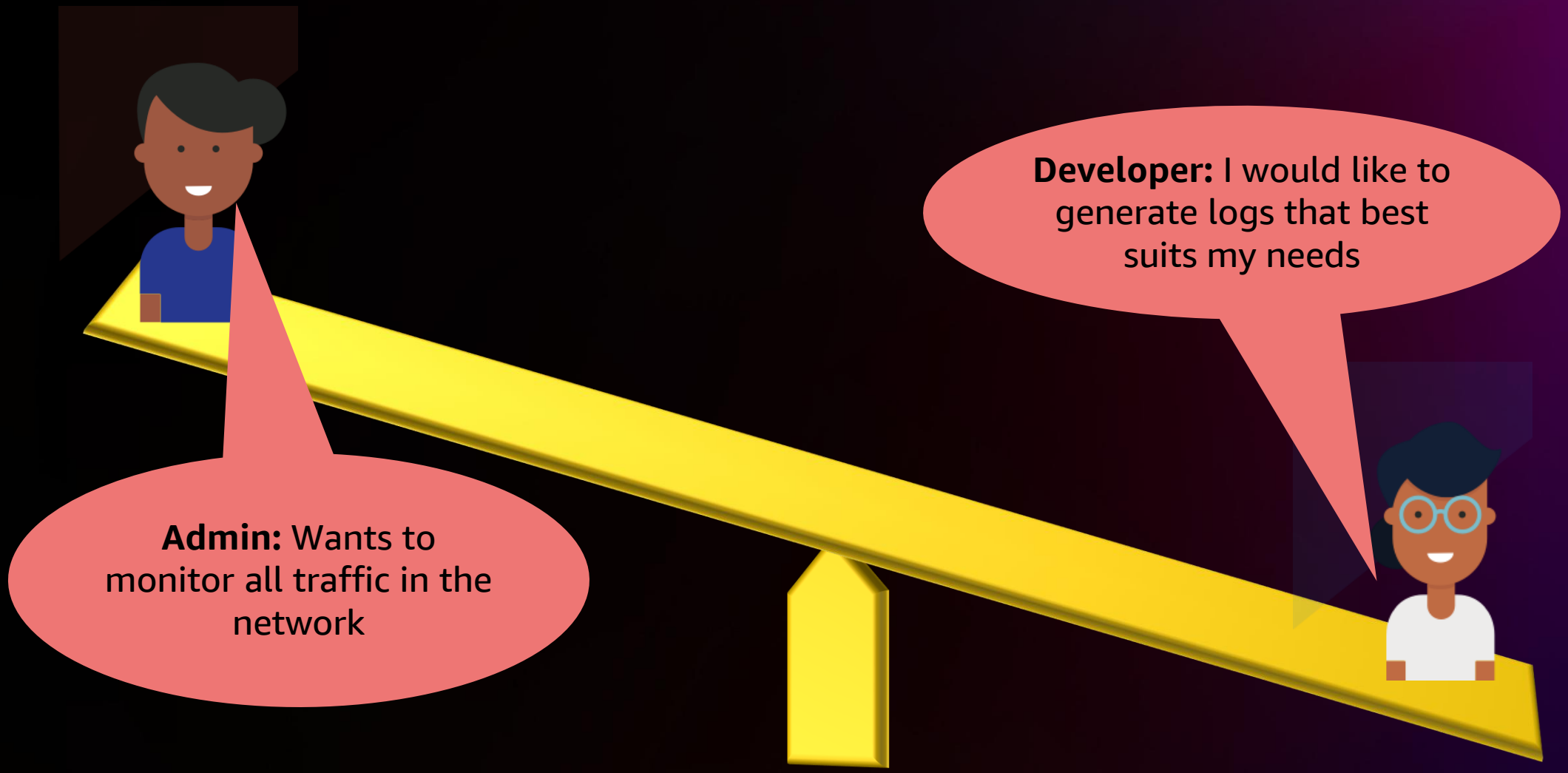
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security conundrum



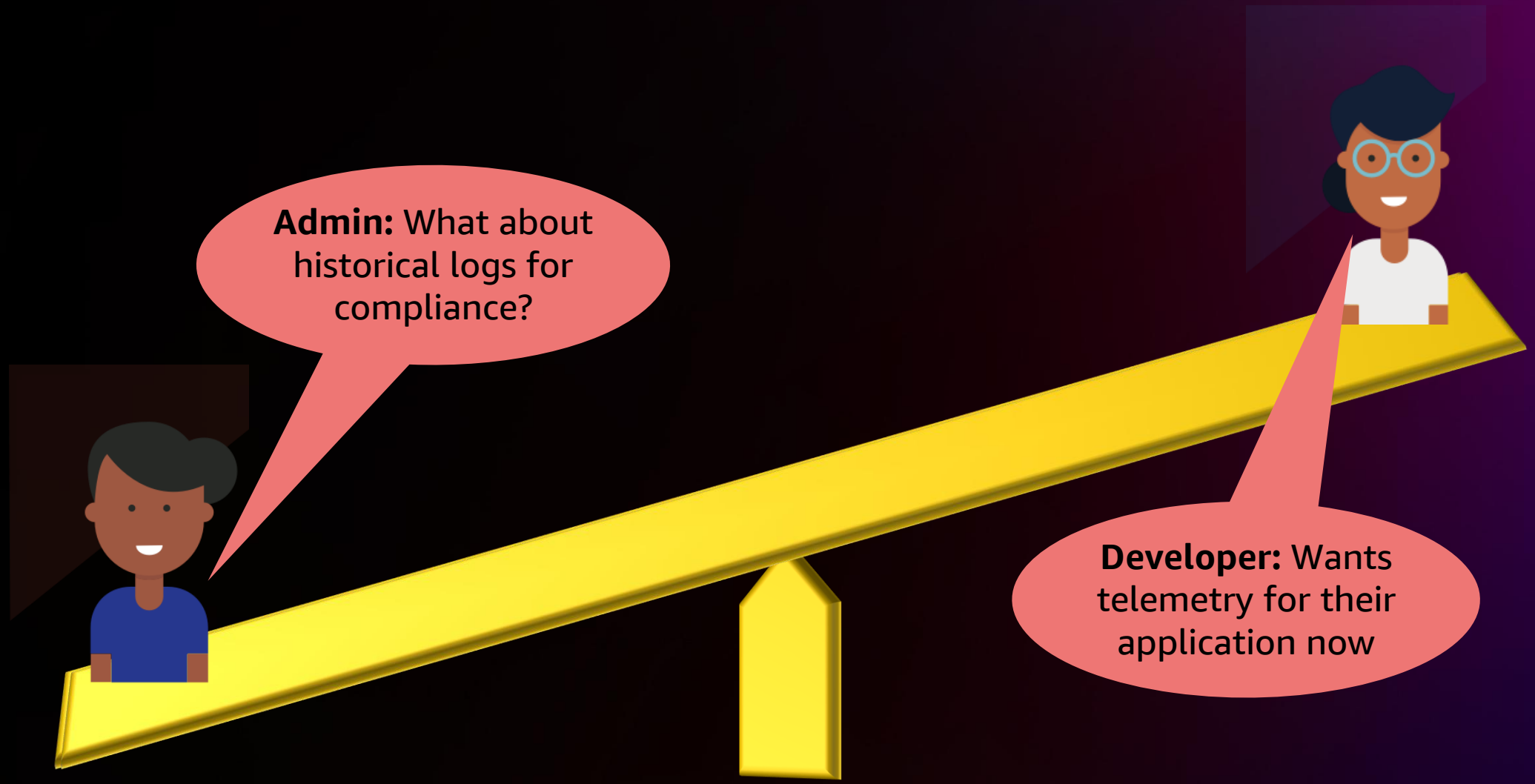
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitoring conundrum



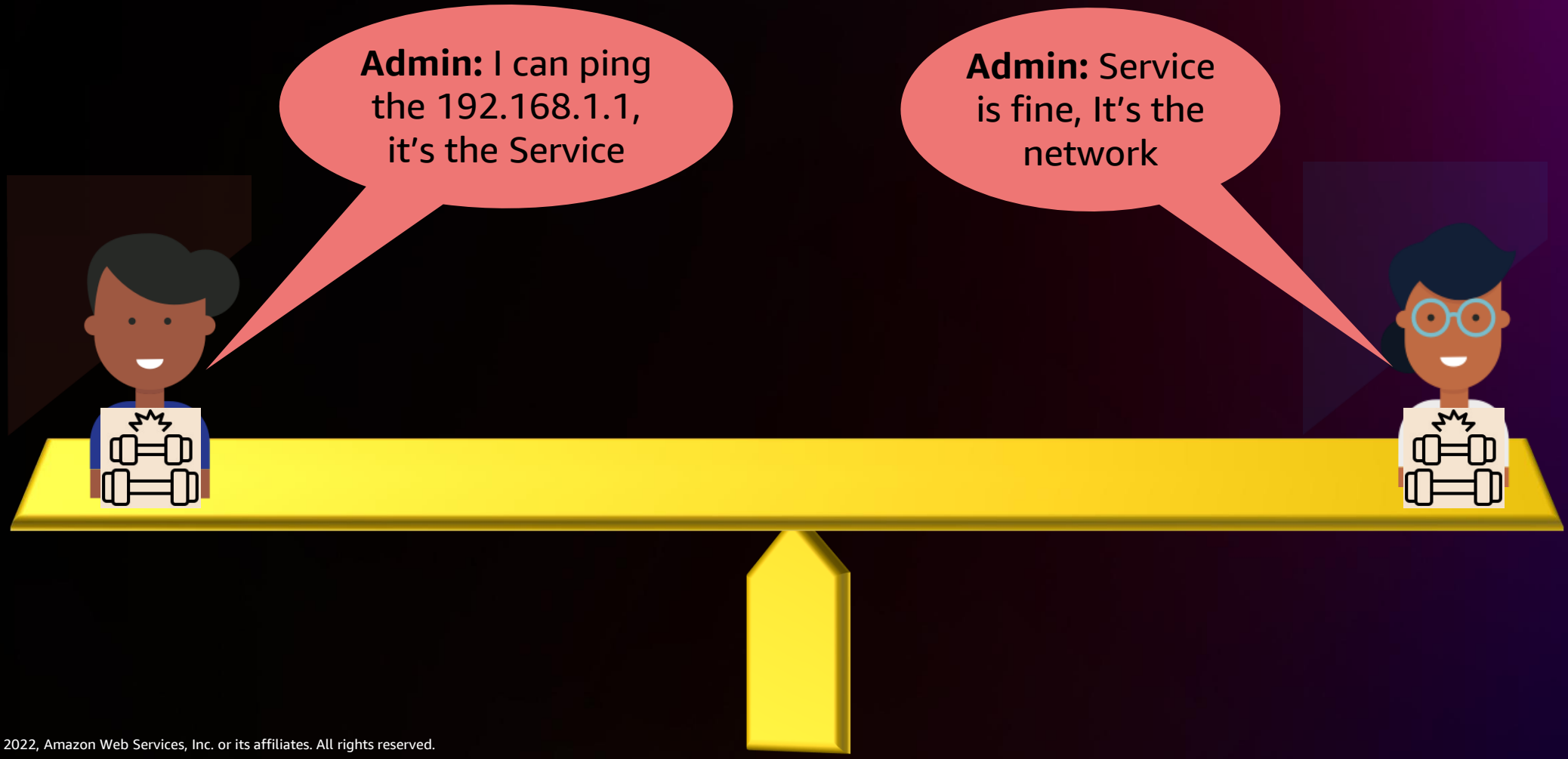
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitoring conundrum



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitoring conundrum



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Persona problem...



Admin*/Cloud, Network, InfoSec

- Wants to empower developers without losing control
- Needs centralized tools to implement and enforce the organization's security posture

"I want to empower service owners to have seamless service-to-service communication, but need the ability to provide oversight and enforce coarse grained access controls. I need observability that is integrated with my developers' systems instead of being disjointed with overlays and today's service mesh implementations."



Developer/Service Owner

- Doesn't want to deal with networks
- Needs advanced telemetry to help optimize and troubleshoot applications

"Service-to-service communication should just work. I want to focus on building business logic into my applications, not learning the… what's it called…OSI Model?"

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NEW

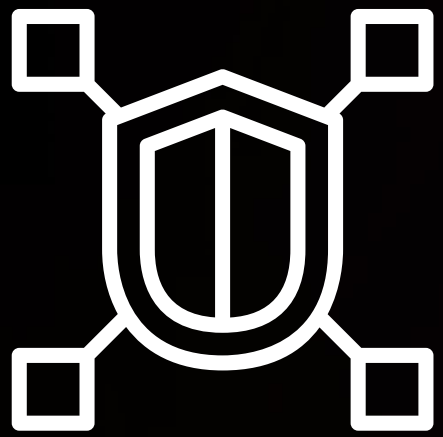
Amazon VPC Lattice

Bridging the gap between admins and developers

IN PREVIEW

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice

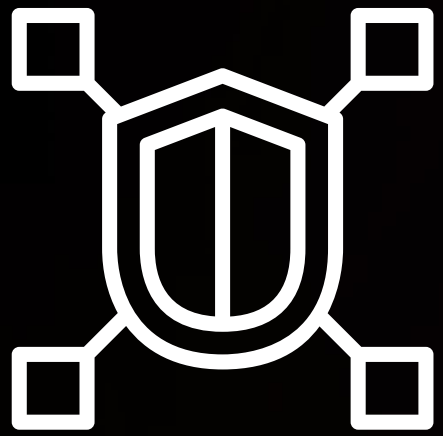


Combines network connectivity with an application layer proxy

- Automatically handles connectivity between VPCs and accounts
- Apply rich traffic control, such as application layer load-balancing and weighted targets to support blue-green deployments

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice



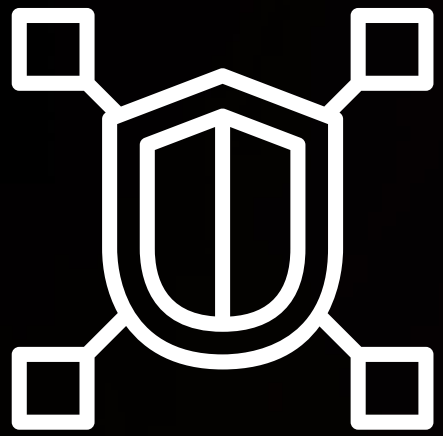
Helps implement zero-trust principles

- Integrated with AWS Identity and Access Management (IAM): Enforce authentication and implement fine-grained authorization for your own service-to-service communication

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice



Consistent experience across instances, containers, and serverless

- Built directly into VPC and natively integrated with AWS services so you can mix and match your compute types to meet the needs of each service

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

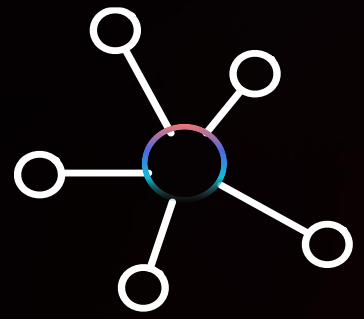
But how?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice



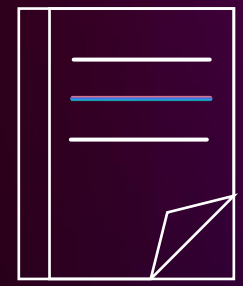
SERVICE



SERVICE NETWORK



AUTH POLICIES



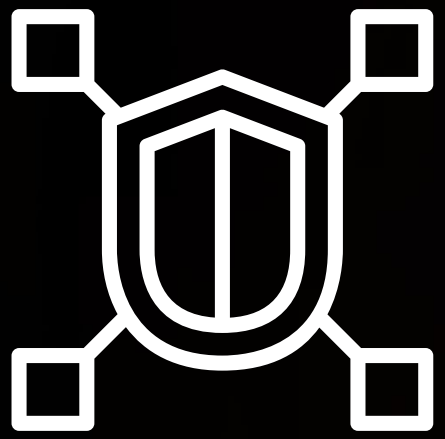
SERVICE DIRECTORY

Key components

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice

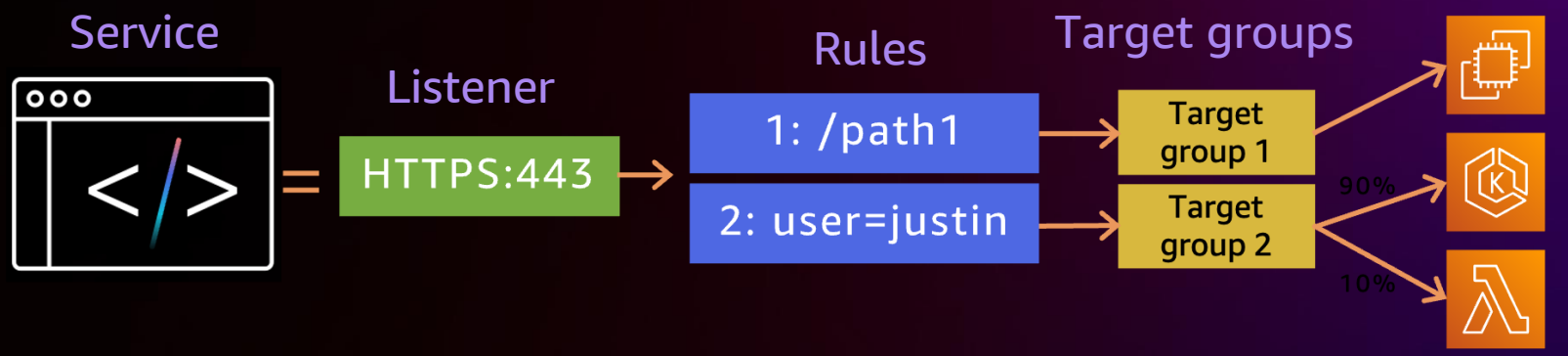


Key components



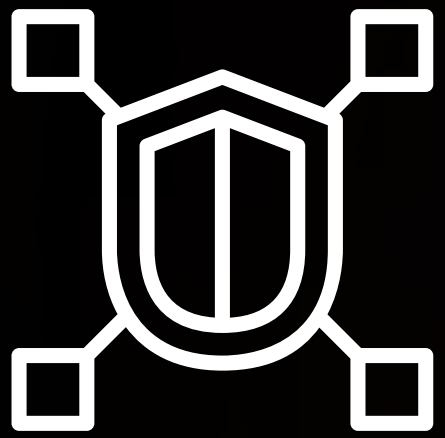
SERVICE

A unit of application running on instances, containers, and serverless and consisting of listeners, rules, and target groups

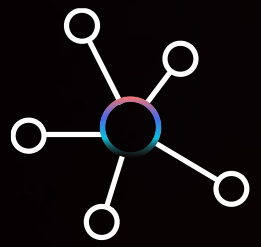


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice

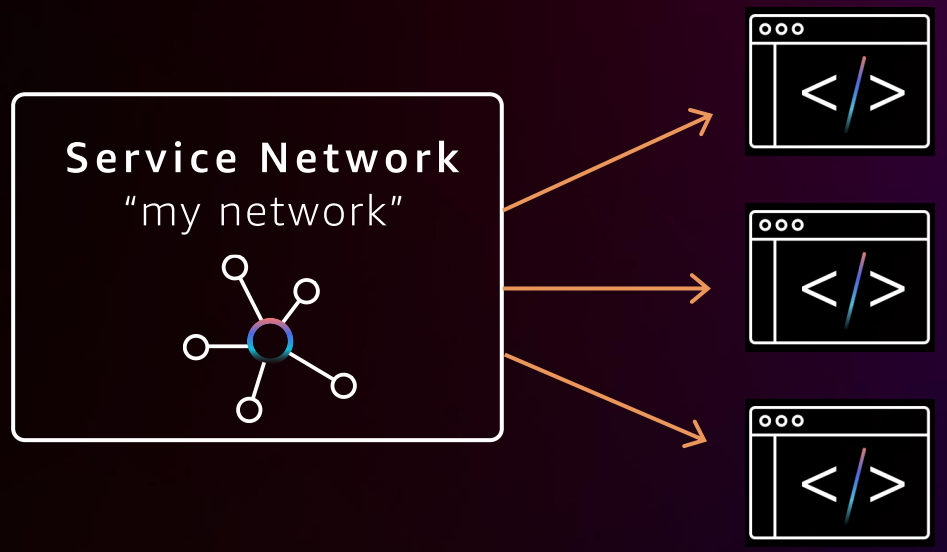


Key components



SERVICE NETWORK

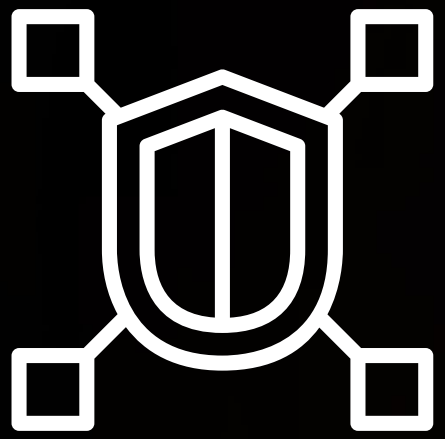
A logical boundary that is used to automatically implement service discovery and connectivity and apply common access and observability policies to a collection of services



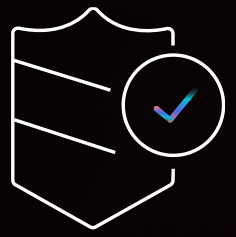
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice

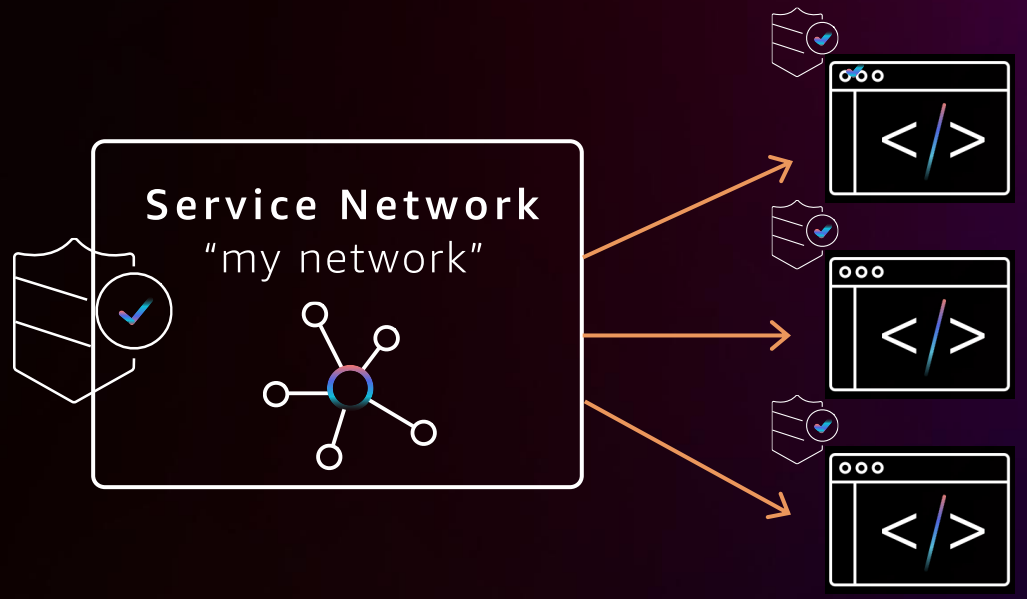


Key components

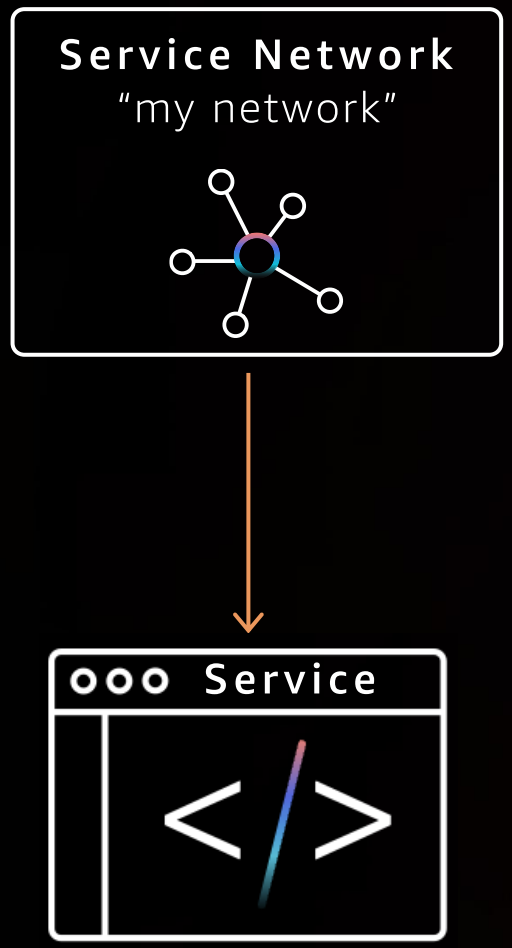


AUTH POLICIES

IAM resource policy that can be associated with a Service Network and individual Services to support request level authentication and context specific authorization



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



ADMIN

```
"Effect": "Allow",
"Principal": "*",
"Action": "vpc-lattice-svcs:Invoke",
"Resource": "*",
"Condition": {
   "StringEquals": {
      "aws:PrincipalOrgID": [
         "o-123456example"
```

AUTH POLICIES

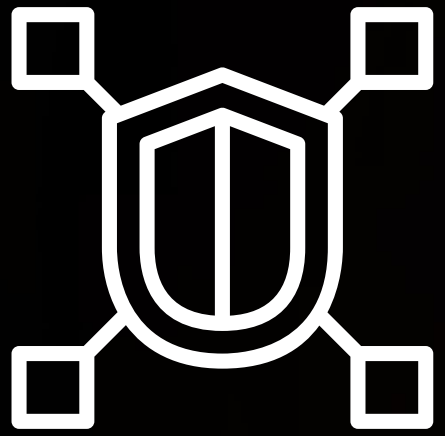


DEVELOPER

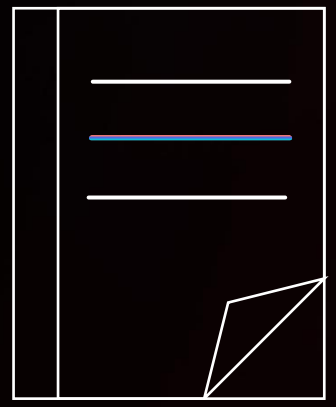
```
"Effect":"Allow",
"Principal":{
   "AWS":[
      "arn:aws:iam::123456789012:role/rates-client",
   ]
},
"Action":"vpc-lattice-svcs:Invoke",
"Resource":[
   "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0"
],
"Condition":{
   "StringEquals": {
      "vpc-lattice-svcs:Method": "GET"
   }
```

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice



Key components



SERVICE DIRECTORY

A centralized view of the services that you own or that have been shared with you through AWS Resource Access Manager (AWS RAM)

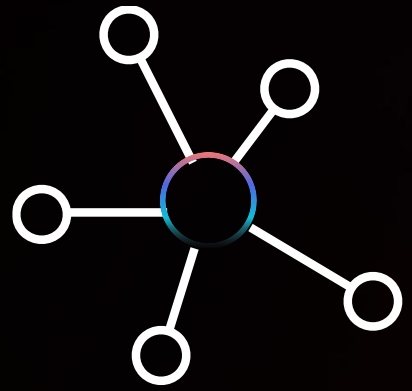
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Who does what?

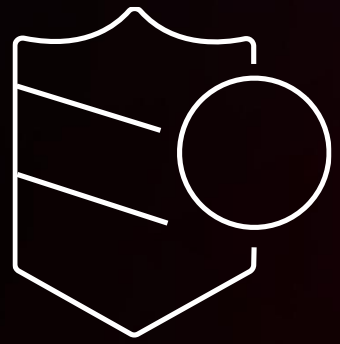
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



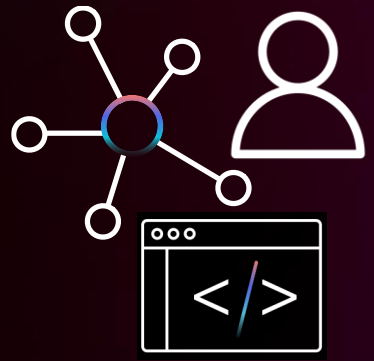
Admin



Create a service network



Define access and monitoring



Associate VPCs and services



Share with other accounts

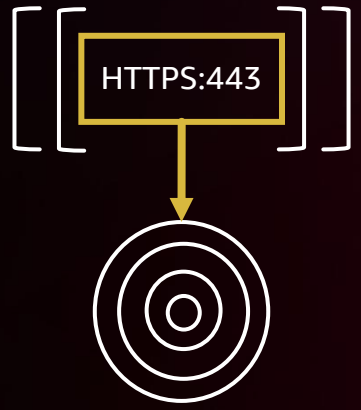
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



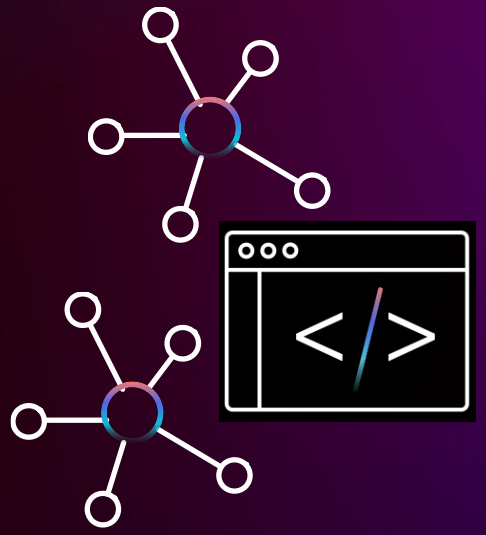
Service owner



Create a service



Define routing and authorization



Associate to service networks

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Something for everyone



Cloud / Network Admin or InfoSec

- Can empower developers without losing control
- Enforce security guardrails
- Centralized tools to monitor service-to-service interactions



Developer / Service Owner

- Simple onboarding – no networking needed
- Compute flexibility to use instances, containers, or serverless
- Request level routing and load balancing to support advanced deployment patterns (blue-green, canary, etc.)
- Fine grained and context specific authorization
- Detailed metrics and access logs for greater visibility

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

But how?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



1. Create service with Amazon VPC Lattice

1.

Service Directory
"my services"

2. Associate service with service network

2.

Service Network
"my network"

AWS account

VPC

my network

VPC

my network

AWS account

VPC

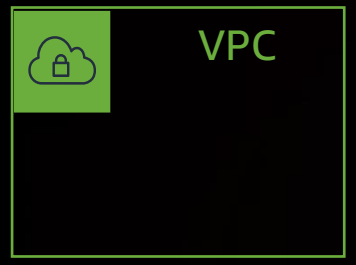
my network

3.

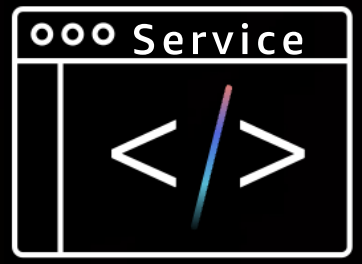
3. Associate service network to VPCs

Configuration

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Each VPC can associate with 1 service network



Each service can associate with many service networks

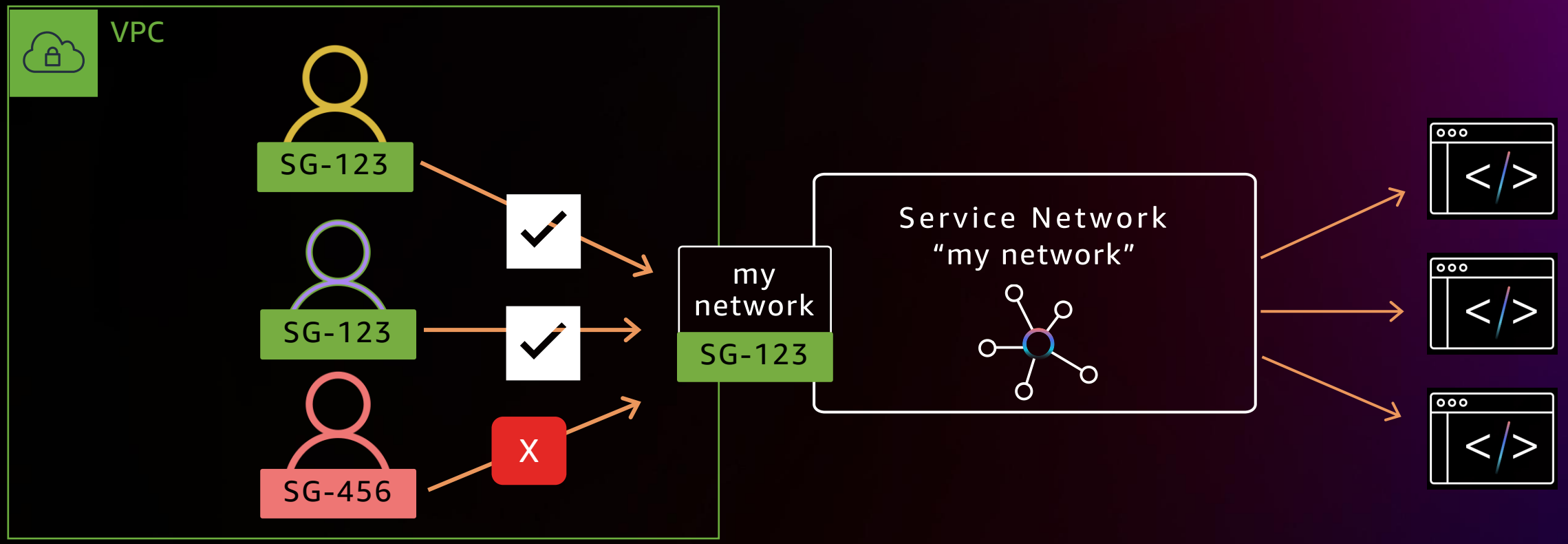
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What about security controls? Defense in depth?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network layer controls

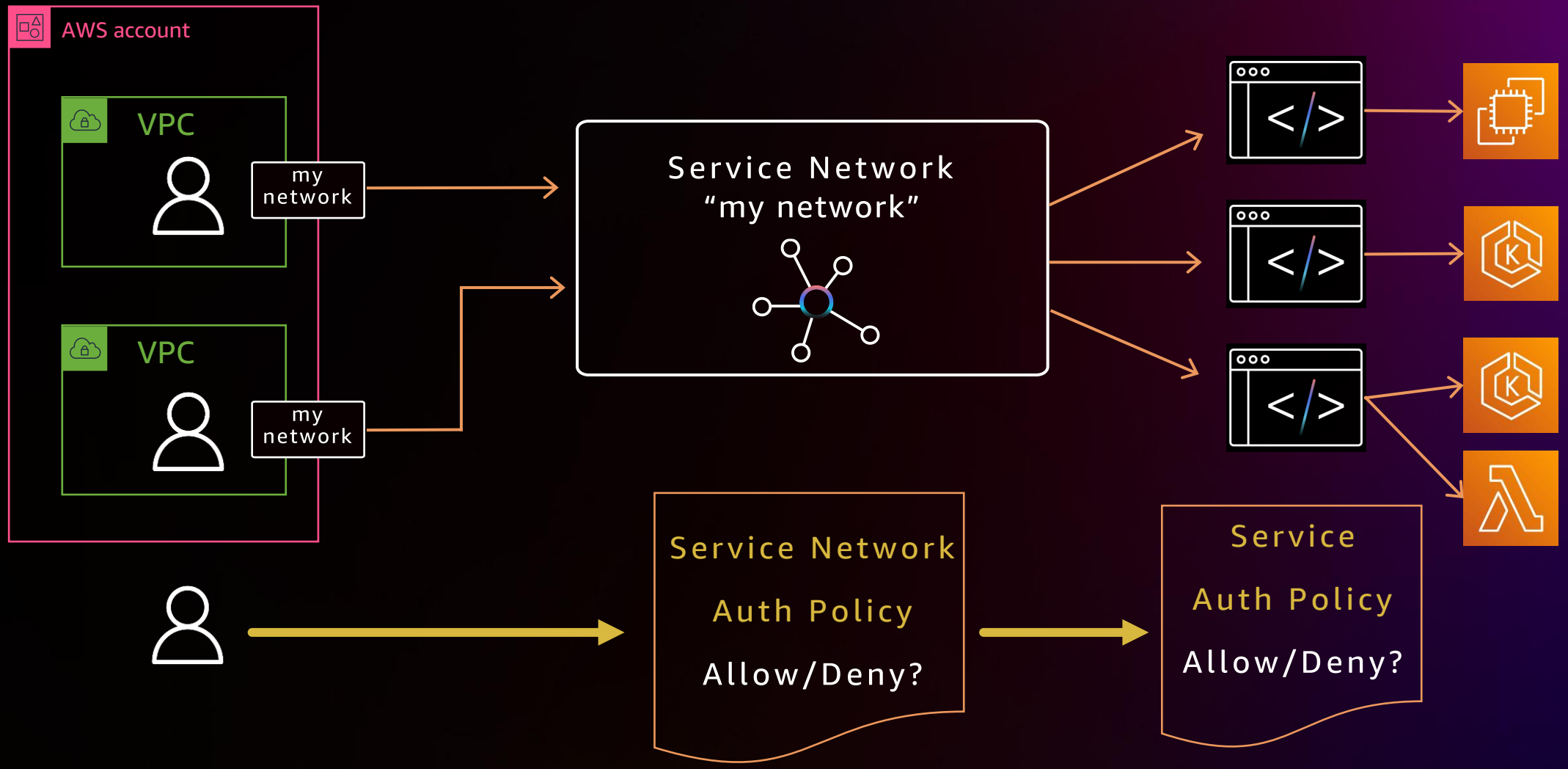
Lock down which resources in a VPC can access the service network with security groups



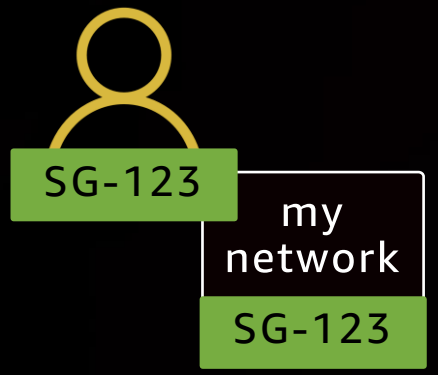
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application layer controls

Apply auth polices at service network and/or service to enforce “AuthNZ”

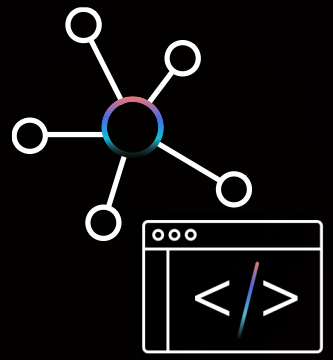


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Network Layer

Security groups can apply network level controls to restrict which resources in a VPC can use the service network



Application Layer

Both services and service networks can have auth policies and be shared with Resource Access Manager

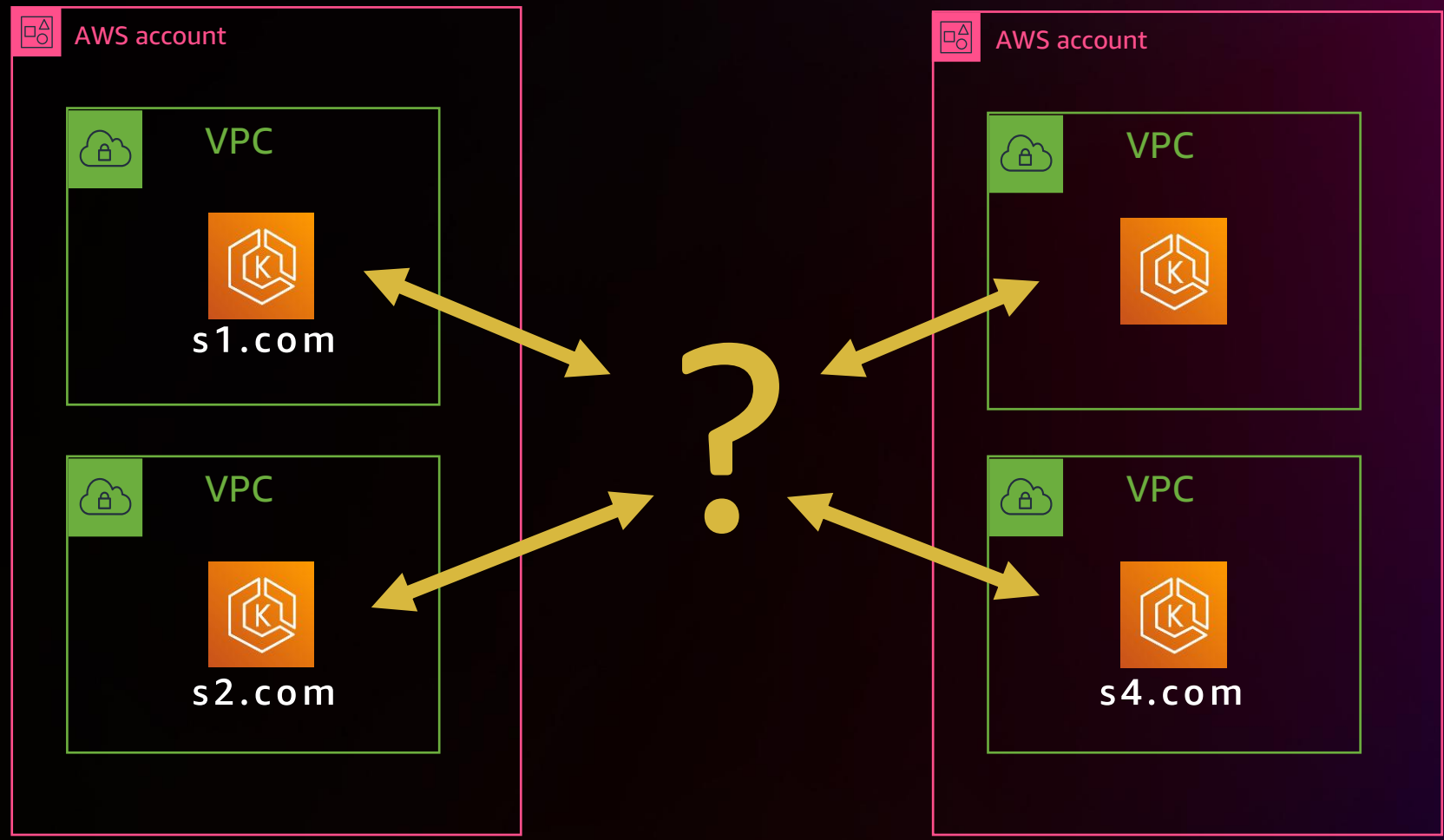
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are some use cases?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

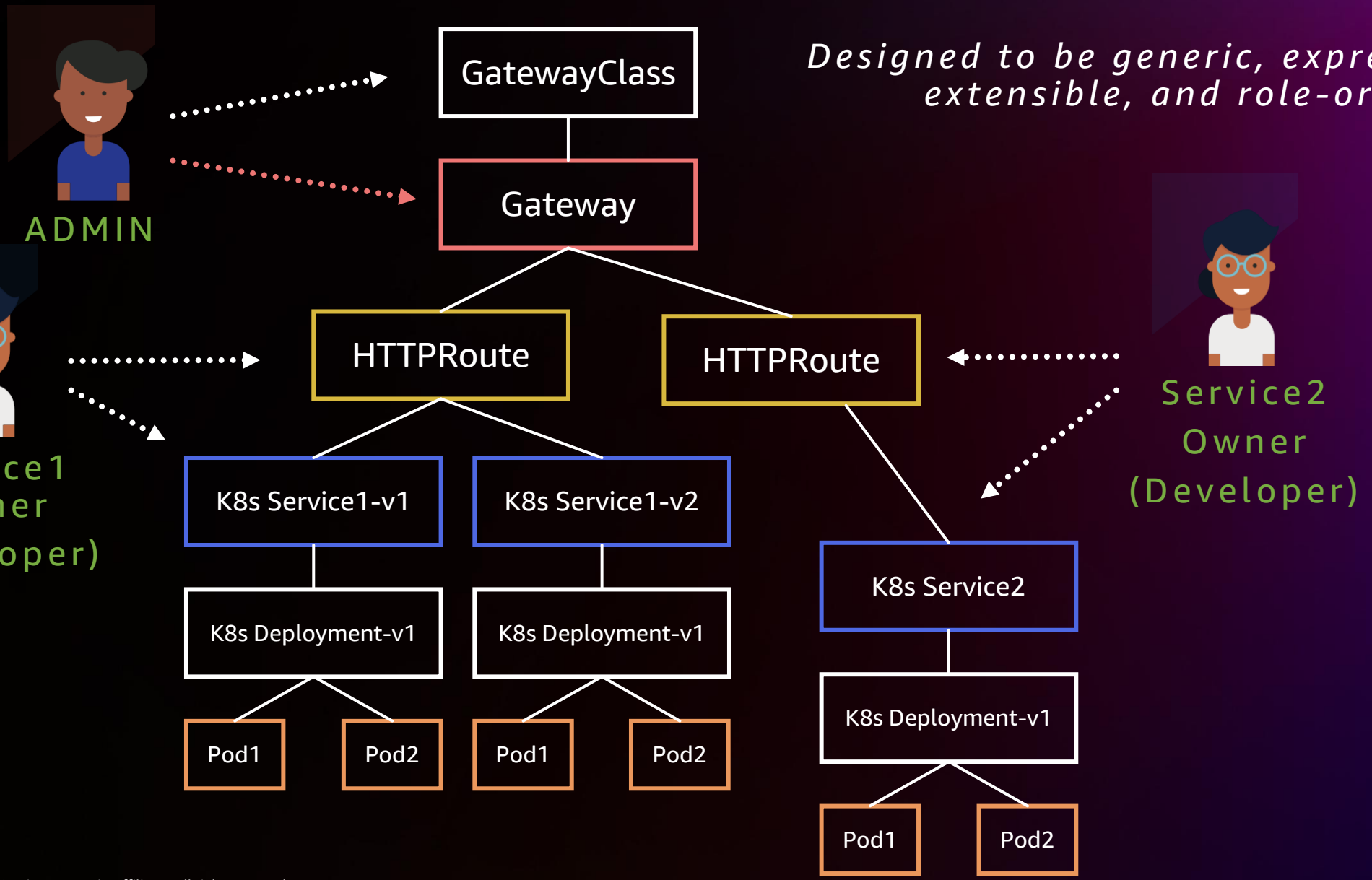
Multi-cluster, multi-VPC K8s



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

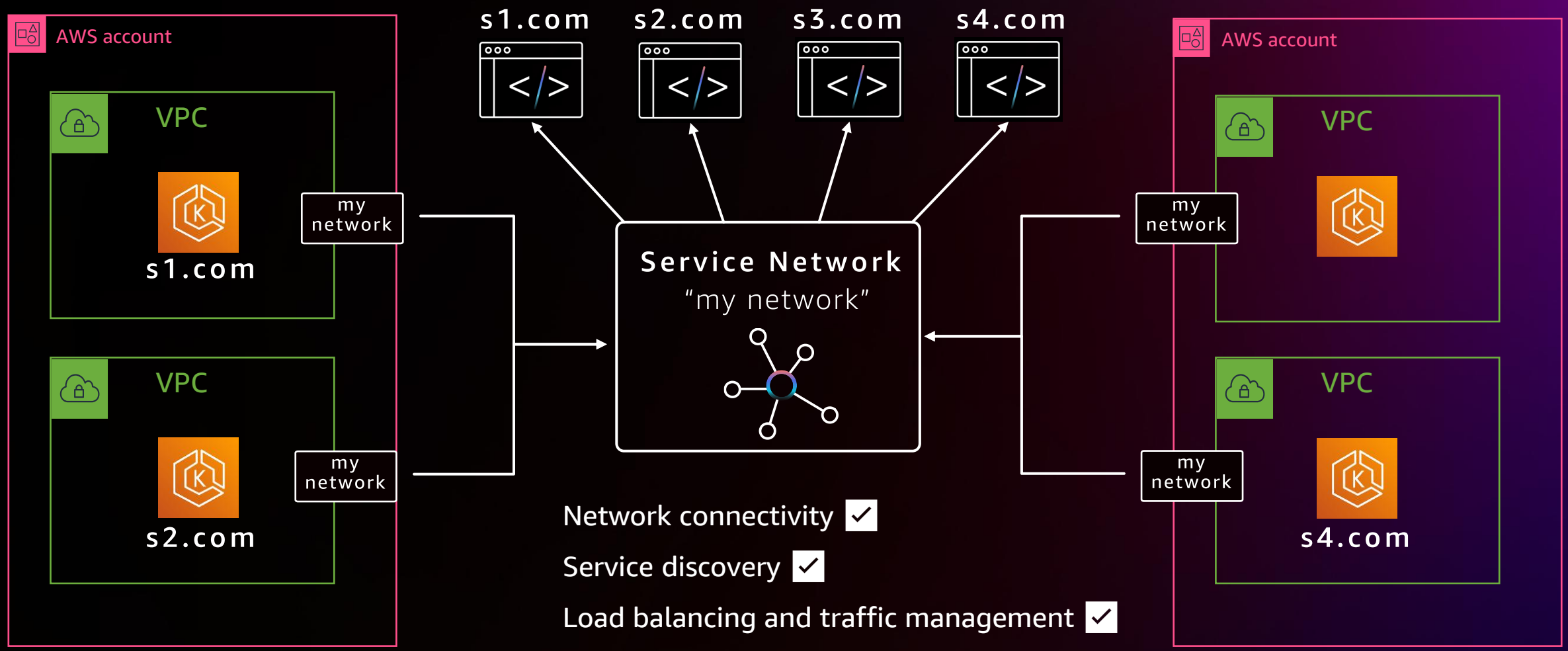
k8 Gateway API: More than an evolution to ingress

Designed to be generic, expressive, extensible, and role-oriented



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-cluster, Multi-VPC K8s



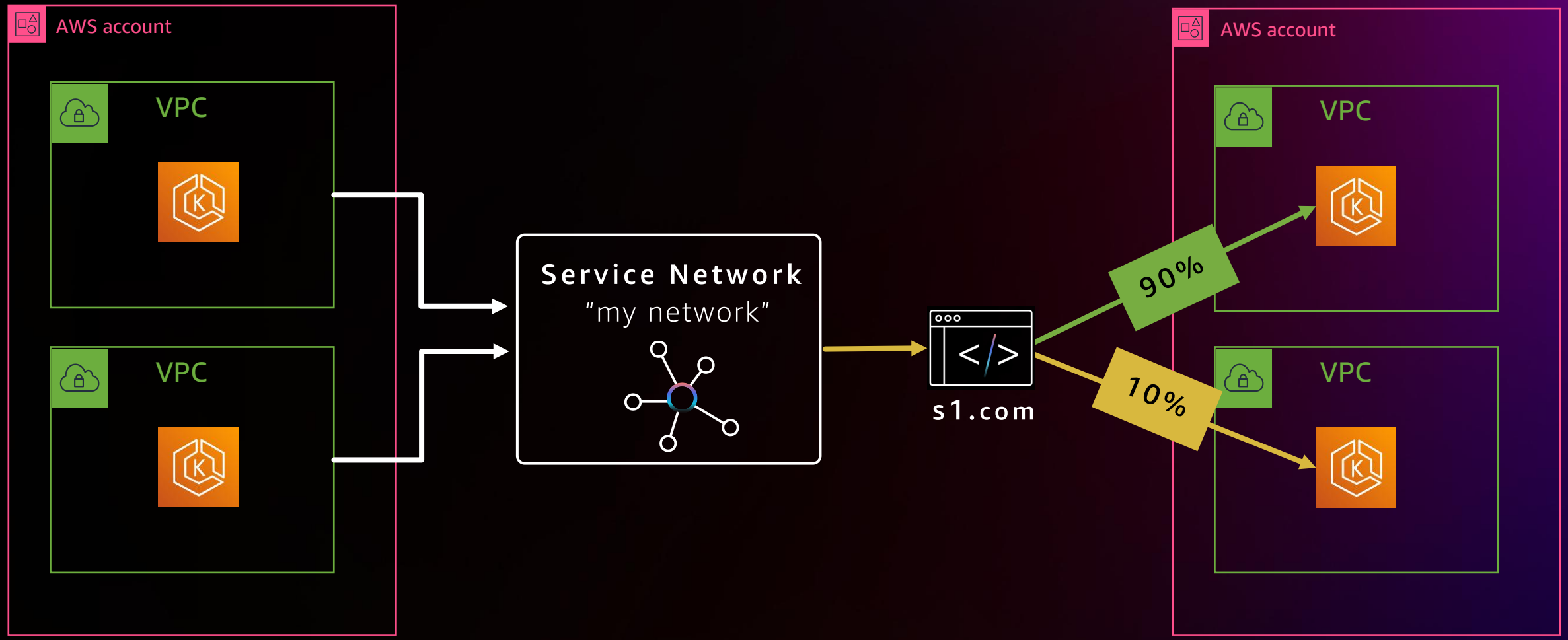
- Network connectivity ✓
- Service discovery ✓
- Load balancing and traffic management ✓
- Authentication and authorization ✓
- Observability ✓

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Can this help with cluster upgrades?
Can I shift traffic between clusters? VPCs?

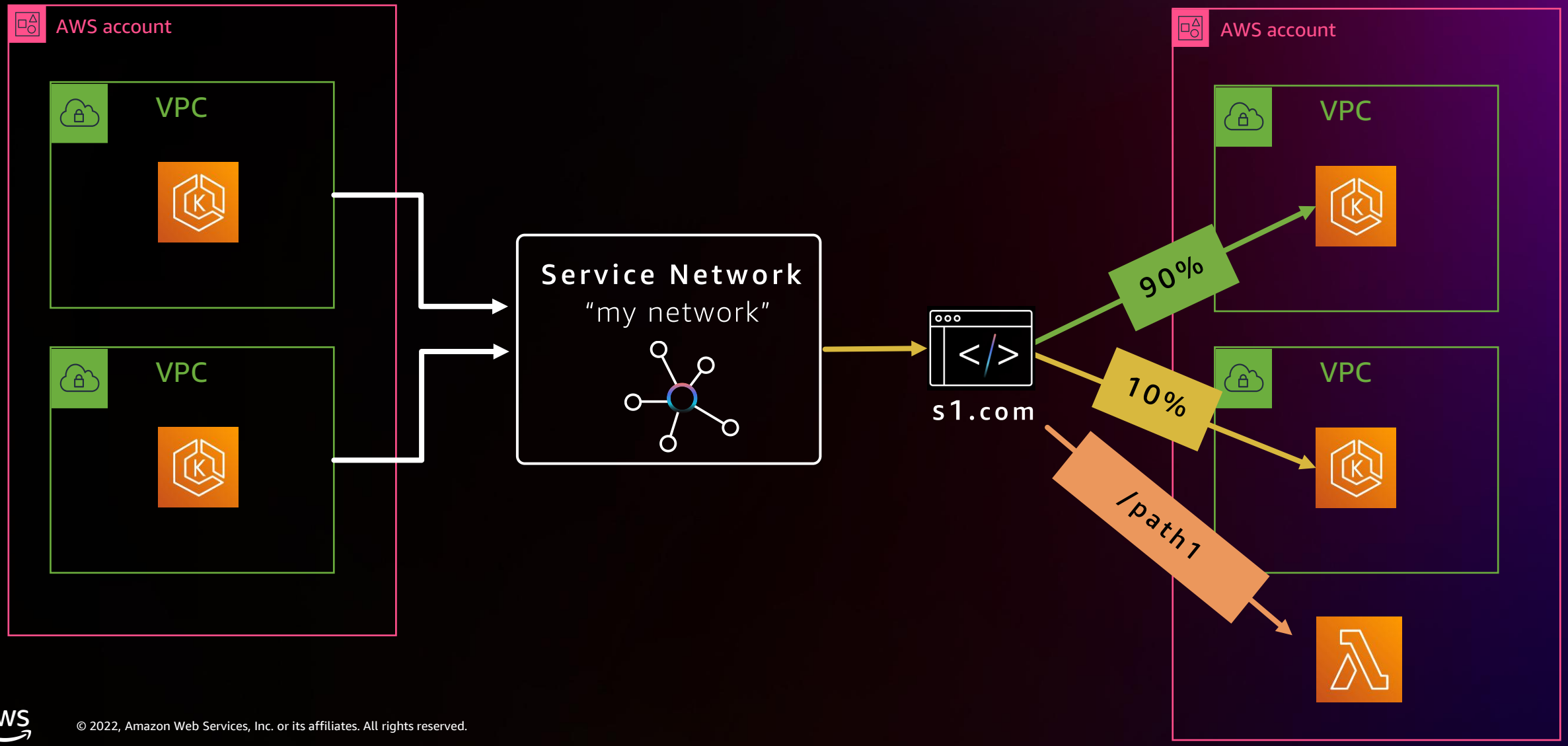
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Weighted routing and load balancing



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mix and match compute targets



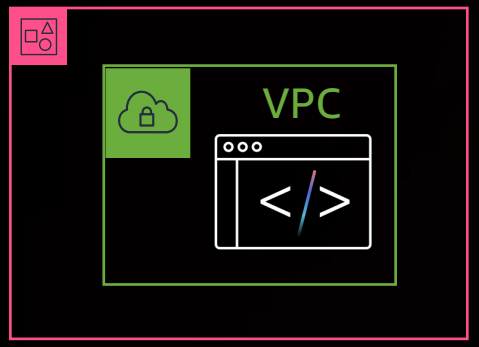
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reduce scope of impact, and limit exposure: “tiny bubbles”

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

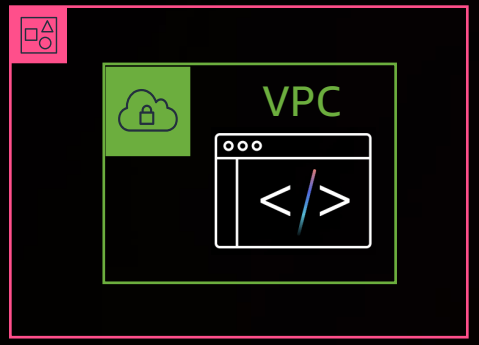


Service 1



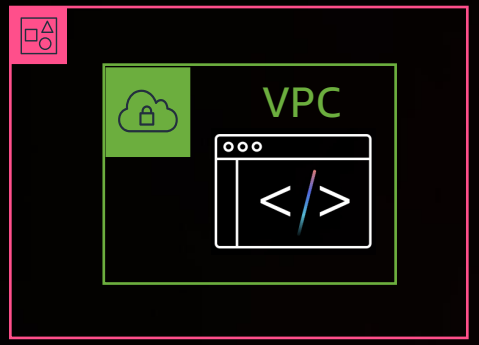


Service 2



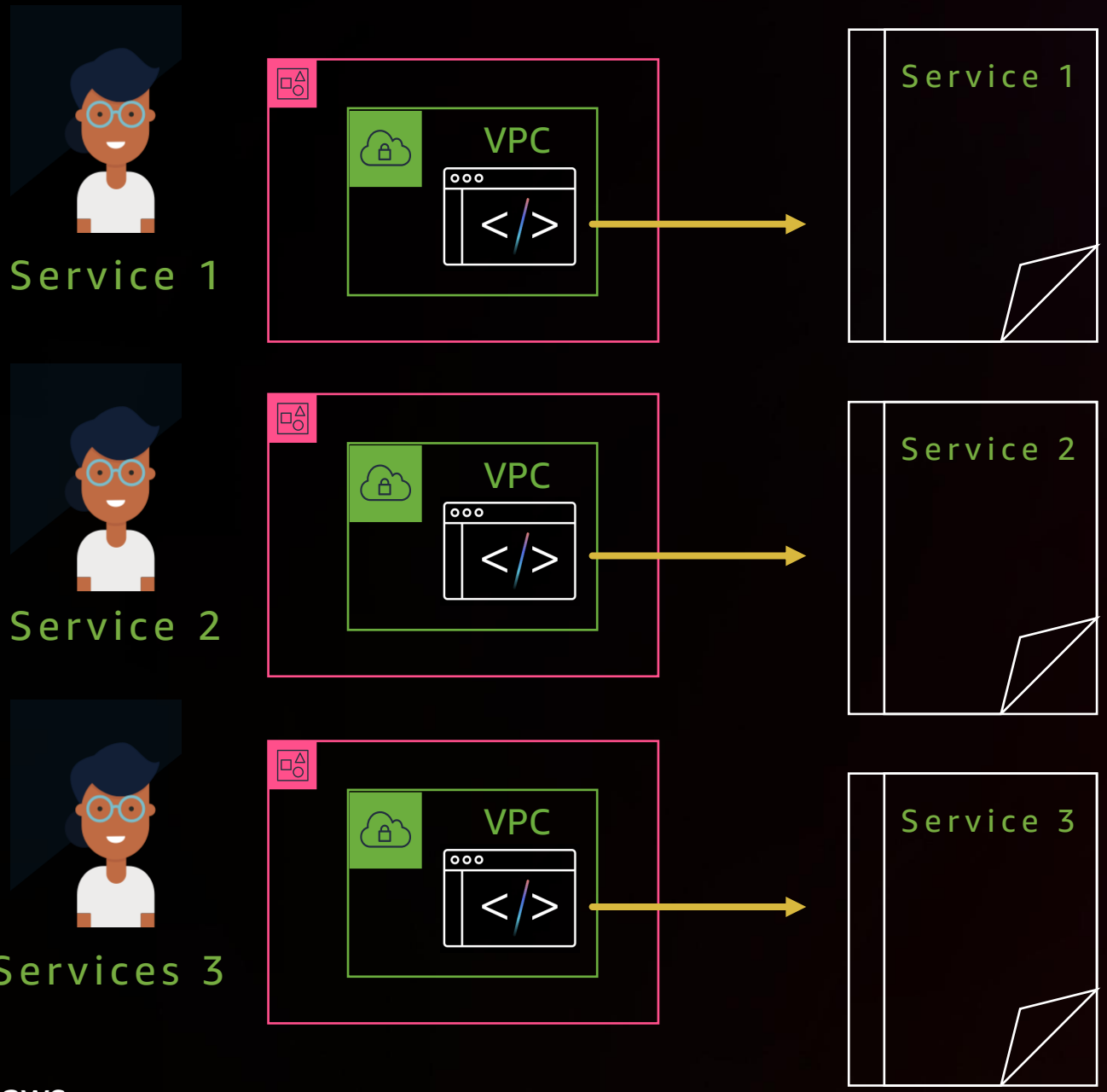


Services 3



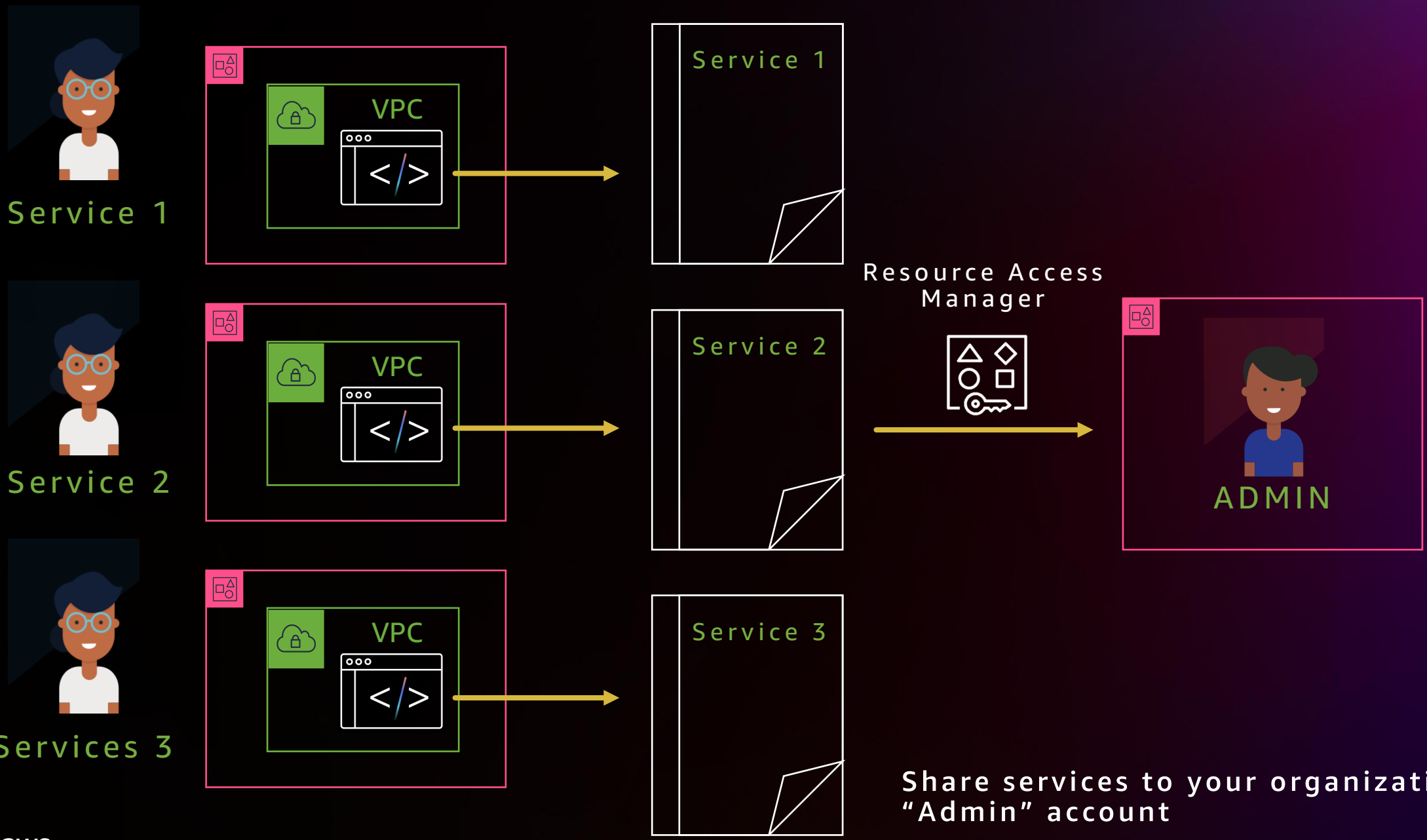
Services get their own VPC/accounts
Nothing gets in or out

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



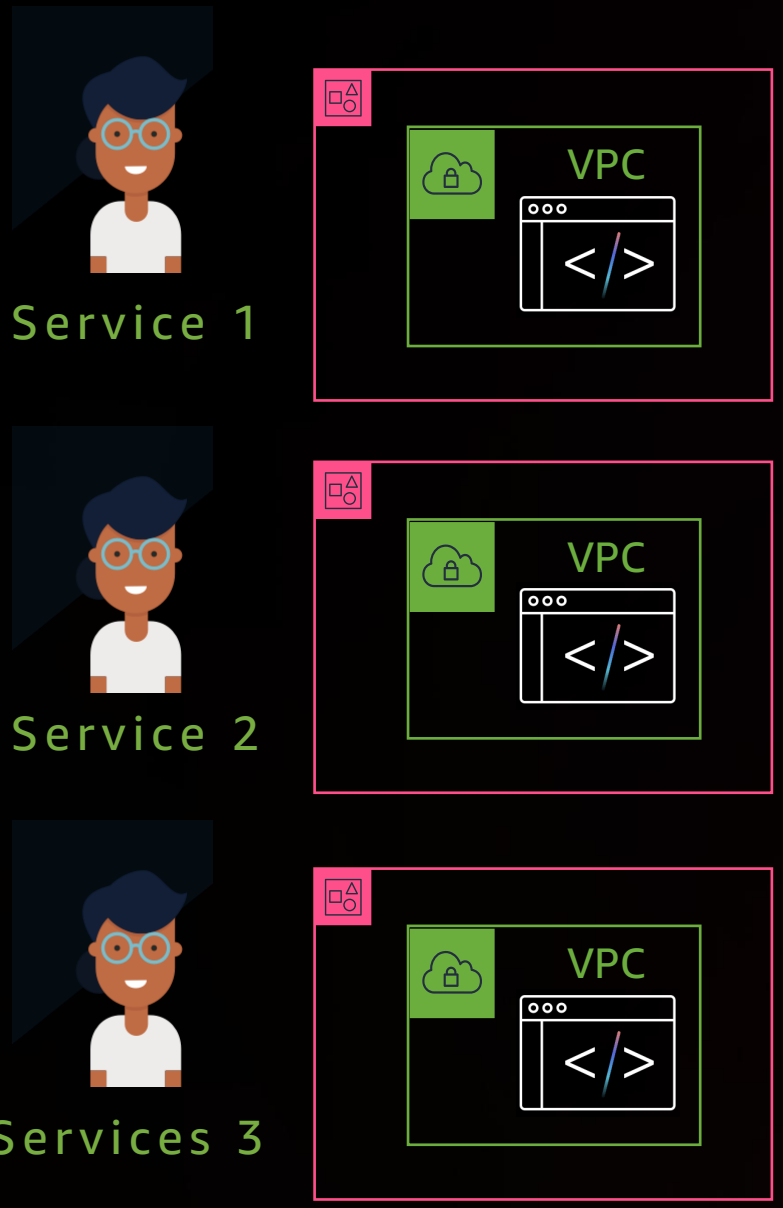
Register the services you want to share

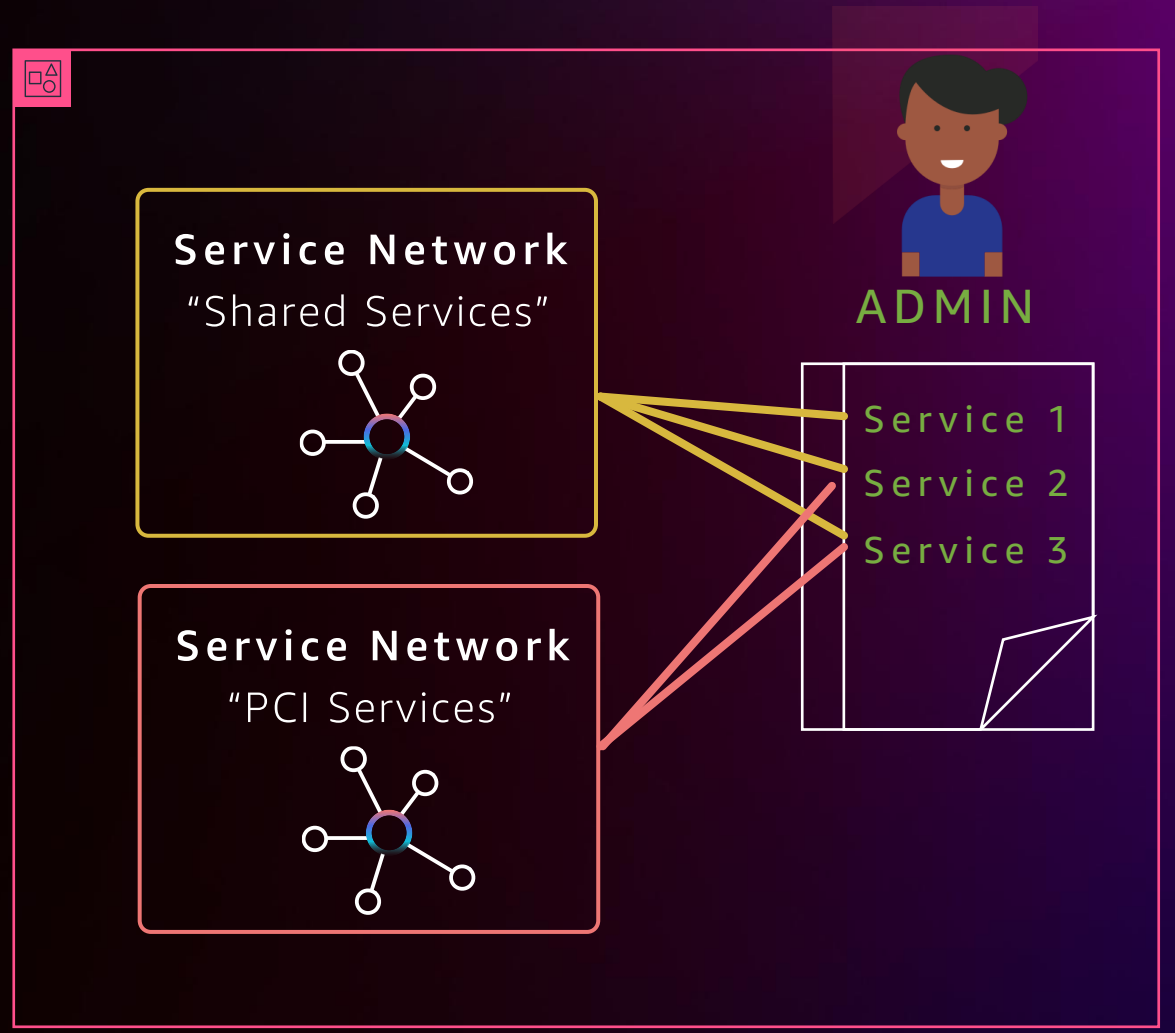
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Share services to your organization or “Admin” account

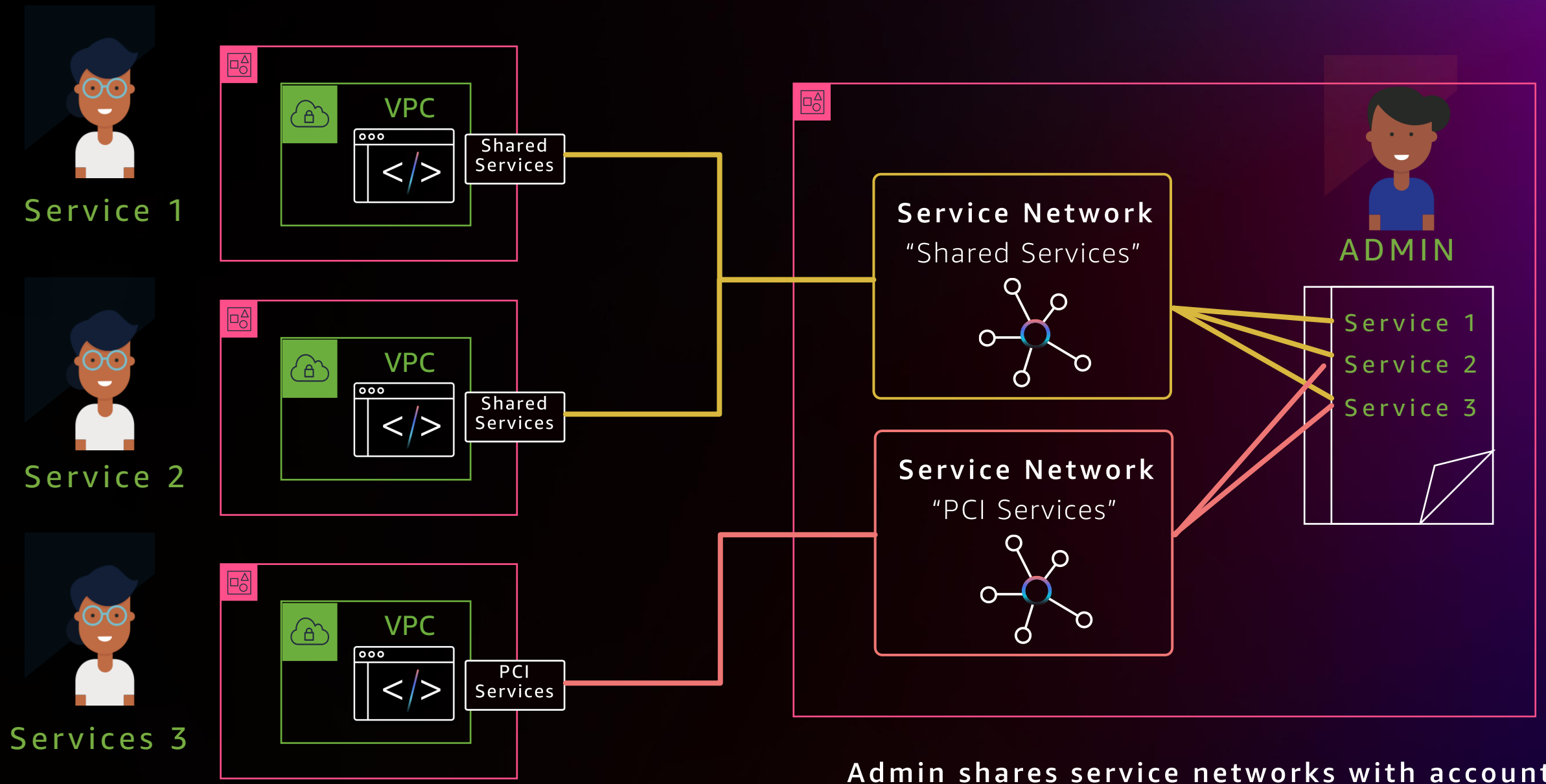
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.





Admin associates services based on common access/permission requirements

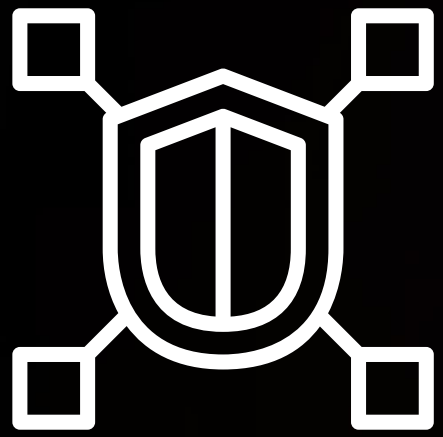
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Admin shares service networks with accounts based on access/permission requirements

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Lattice



Secure by default: Services only have access to the services in their service network

Enforce authentication and authorization on every request to and from your services

Simplified auth policy with proper network scoping

VPCs with unique access requirements can use their own service network

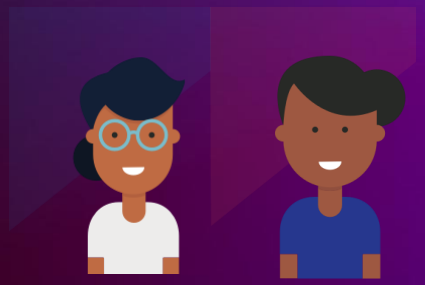
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sign me up!

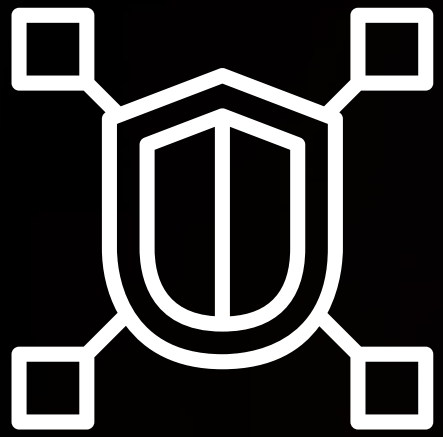
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Preview



For admins and developers

Amazon VPC Lattice



- **Simplify service-to-service connectivity at scale**
- **Enhance application layer security**
- **Implement advanced traffic management**
- **Gain visibility into service-to-service interactions**

Visit: aws.amazon.com/vpc/lattice
to learn more and sign-up

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Justin Davies
daviesju@amazon.com
LinkedIn | Twitter: mrjustind@

Sathya Ramaseshan
sramases@amazon.com
LinkedIn: sathya-ramaseshan@



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.