AWS re:Invent

DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

API313-NEW

Private API integration for Amazon EventBridge and AWS Step Functions

Uma Ramadoss
Principal Solutions Architect
AWS

Justin Callison
Director, Application Integration
AWS

Michael Gasch
Senior Product Manager
AWS

Agenda

Application **modernization** with Amazon EventBridge and AWS Step Functions

EventBridge and Step Functions with **public and private APIs**

Private APIs **deep dive**

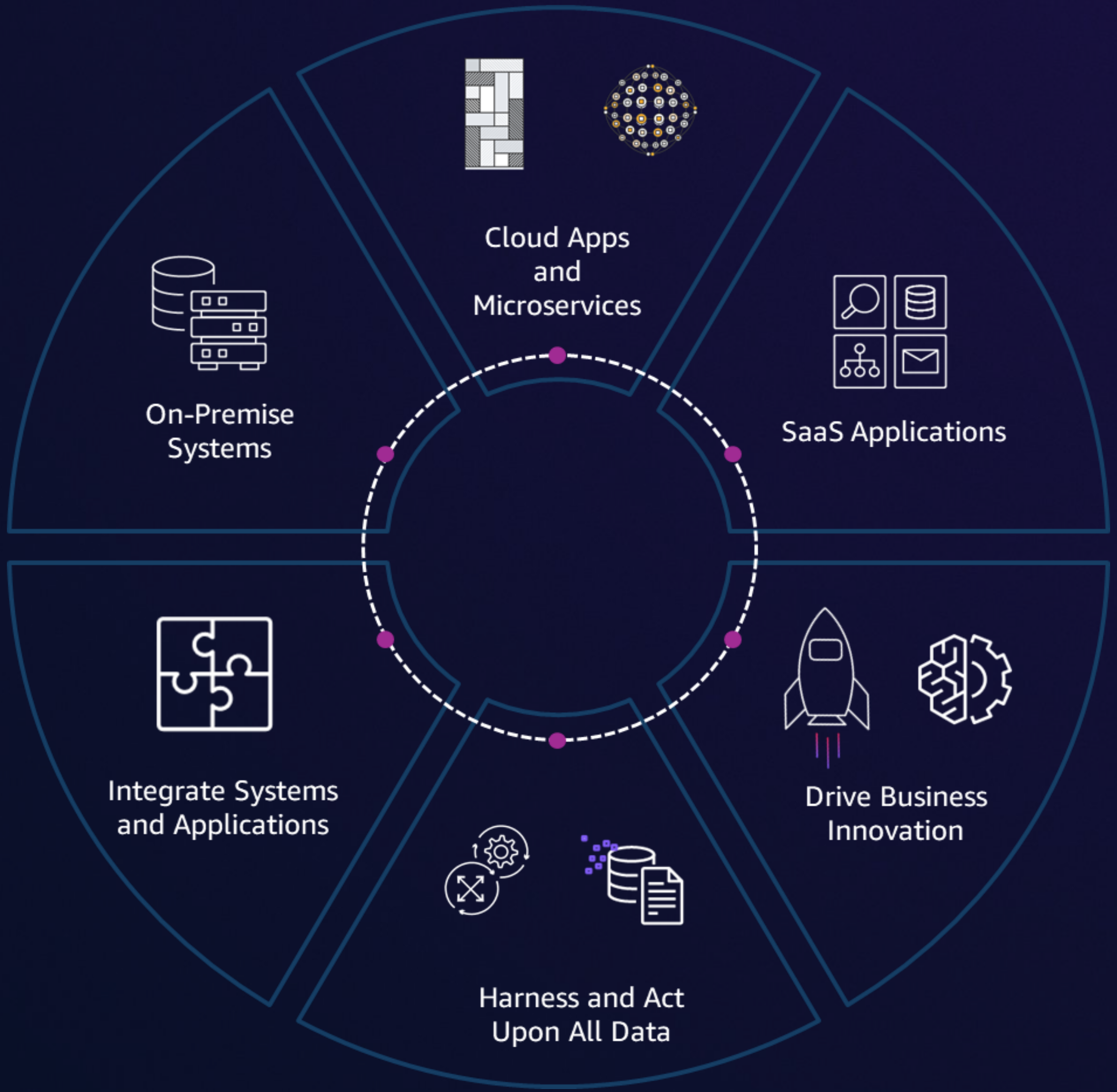
Wrap up

Application modernization with EventBridge and Step Functions

Businesses must adapt to new technologies and market shifts

“Organizations today use over 1,000 applications – but 70% remain disconnected from one another and the core business.”

- Salesforce 2024 Connectivity Benchmark Report


Cloud Apps and Microservices
SaaS Applications
Drive Business Innovation
Harness and Act Upon All Data
Integrate Systems and Applications
On-Premise Systems

EventBridge and Step Functions

Amazon EventBridge

Amazon EventBridge is a **serverless** service that uses events to connect application components together, making it easier for you to build scalable event-driven applications.

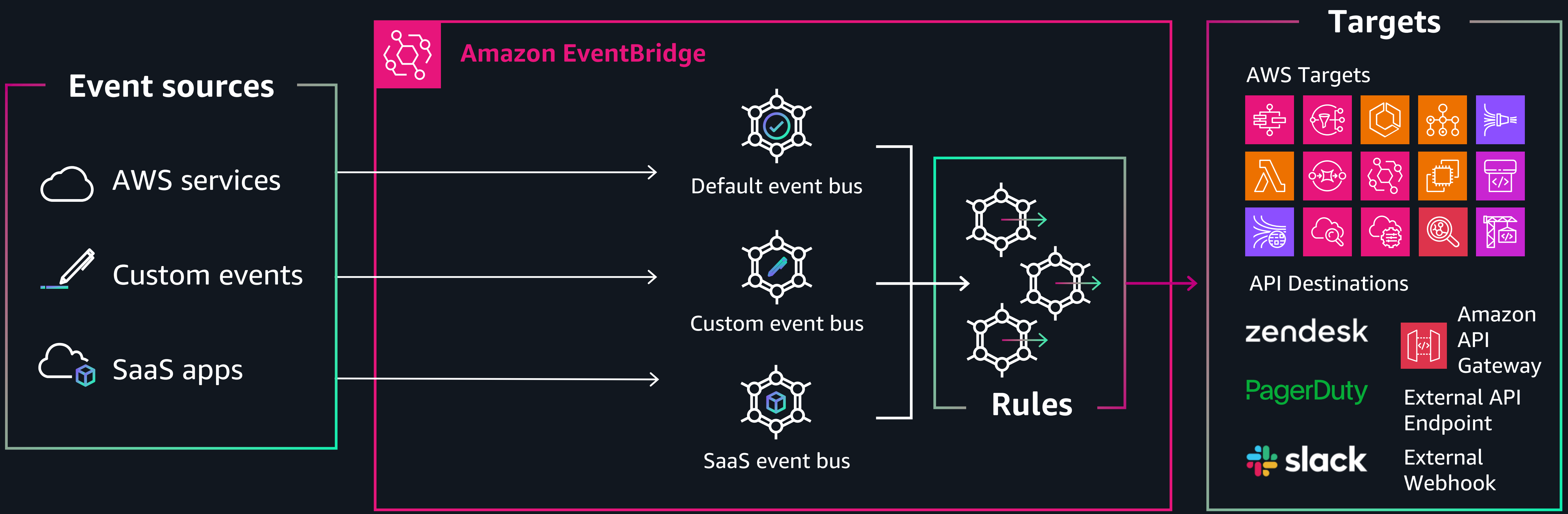
You can use EventBridge to route events from sources such as home-grown applications, AWS services, and third-party software to consumer applications across your organization.

Event bus

Pipes

Scheduler

EventBridge Event Bus



EventBridge Event Bus features

Archive and replay

Easily recover from issues and hydrate new services

Dead-letter queues

Increased resilience and error handling

API destinations

Deliver API requests to any publicly available API, with support for OAuth, header auth (e.g., API key), and basic auth. Includes rate control to ensure downstream APIs aren't overwhelmed

Schema registry and automatic discovery

Keep track of events across your organization. Automatic code bindings speed up development

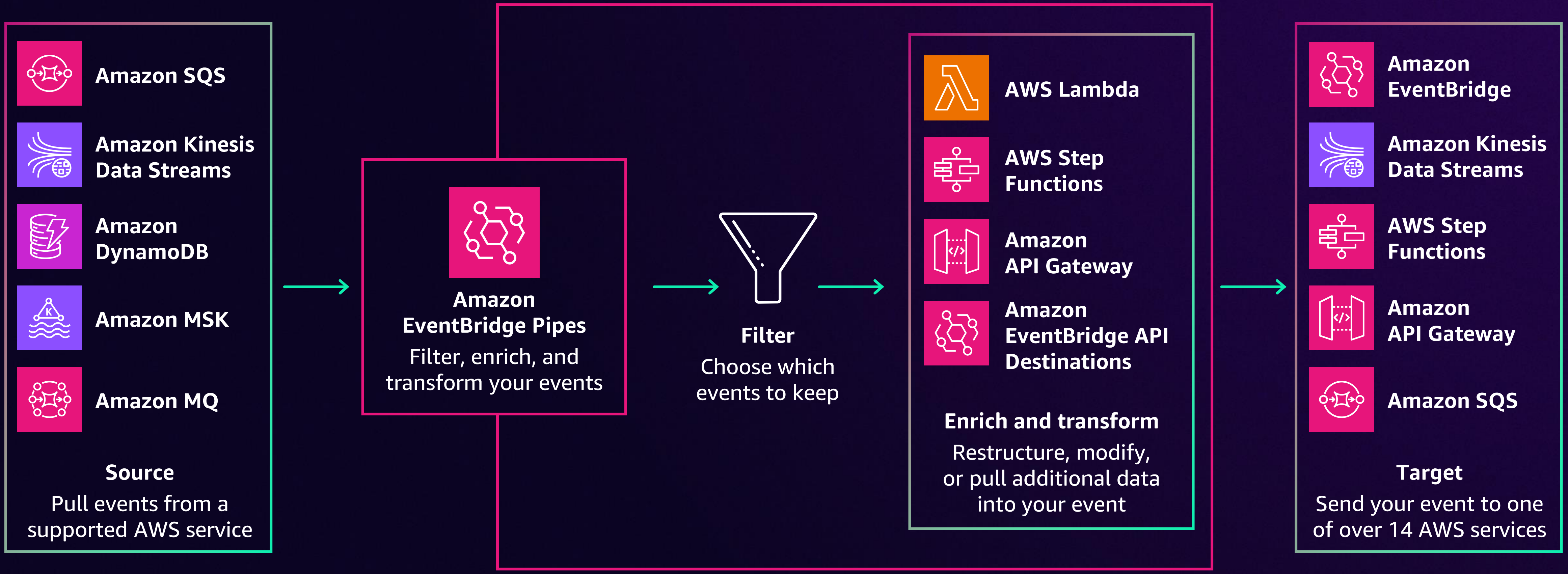
Global endpoints and cross-region event delivery

Automated failover and recovery. Simplify multi-Region availability and disaster recovery strategy

Cross-account delivery

Send or receive events between accounts within same or different Region

EventBridge Pipes connects building blocks



Amazon SQS

Amazon Kinesis Data Streams

Amazon DynamoDB

Amazon MSK

Amazon MQ

Source

Pull events from a supported AWS service

Amazon EventBridge Pipes

Filter, enrich, and transform your events

Filter

Choose which events to keep

AWS Lambda

AWS Step Functions

Amazon API Gateway

Amazon EventBridge API Destinations

Enrich and transform

Restructure, modify, or pull additional data into your event

Amazon EventBridge

Amazon Kinesis Data Streams

AWS Step Functions

Amazon API Gateway

Amazon SQS

Target

Send your event to one of over 14 AWS services

EventBridge Scheduler is flexible and scalable

Time zone schedules

One-time schedules

Millions of schedules

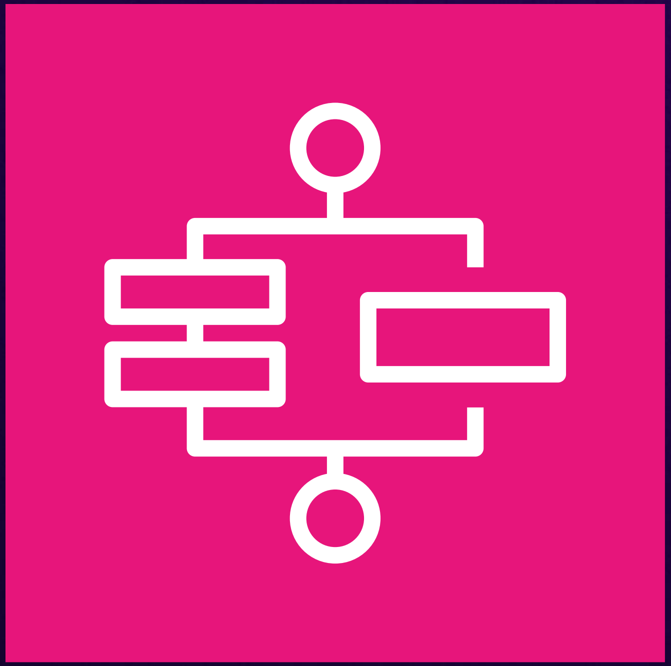
Target over **270 services** and **6000 APIs**

AWS Step Functions

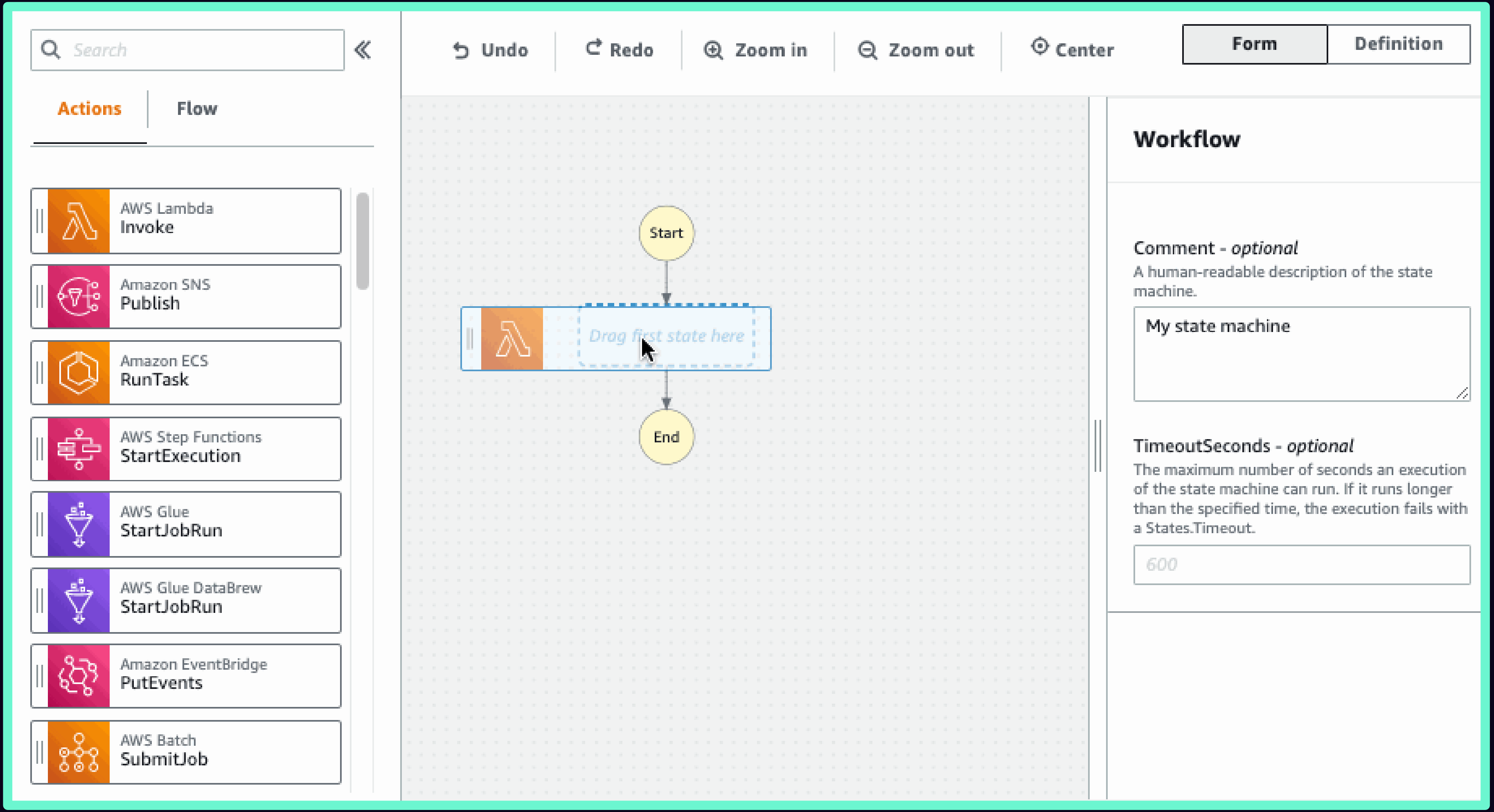
AWS Step Functions provides **serverless orchestration** that helps you build distributed applications, automate processes, orchestrate microservices, and create data and machine learning (ML) pipelines.

You can define and manage the workflow of your application independently from its business logic.

Step Functions frees your functions and containers from excess code, so your applications are faster to write, more resilient, and easier to maintain.



Workflow Studio: Visual designer



Workflow

Comment - *optional*
A human-readable description of the state machine.
My state machine

TimeoutSeconds - *optional*
The maximum number of seconds an execution of the state machine can run. If it runs longer than the specified time, the execution fails with a States.Timeout.
600

Workflow Studio is a drag-and-drop visual builder.

It reduces the time to build a first workflow for new developers.

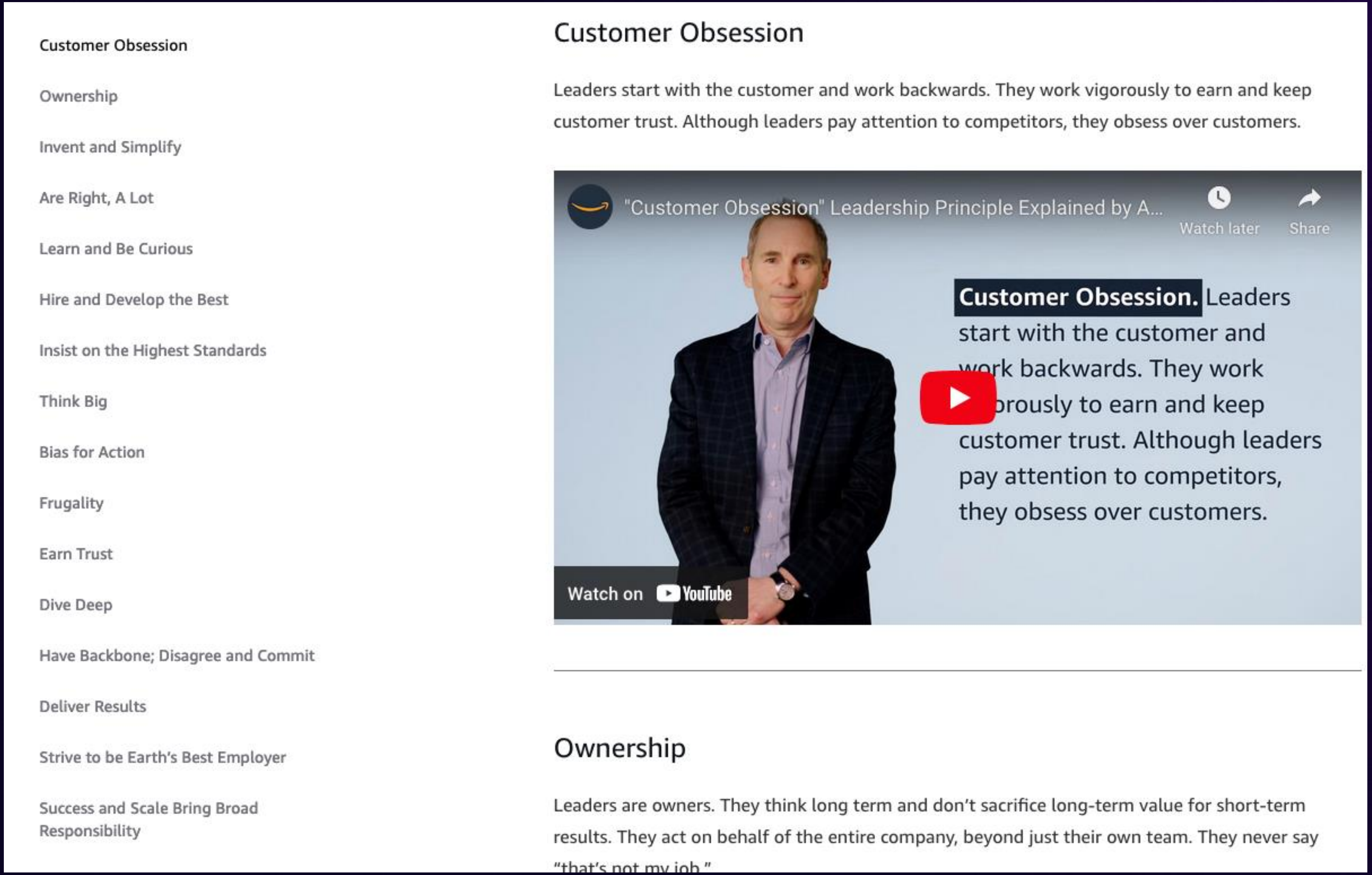
Experienced developers can use it to build and share prototypes with stackholders faster.

Improved workflow visualization using AWS service icons, automatic workflow layouts, and visual cues from workflow definition.

Directly compose applications from over 220 AWS services and 14,000 API actions

An aside on culture and how we work @ AWS

Leadership principles



Customer Obsession

Ownership

Invent and Simplify

Are Right, A Lot

Learn and Be Curious

Hire and Develop the Best

Insist on the Highest Standards

Think Big

Bias for Action

Frugality

Earn Trust

Dive Deep

Have Backbone; Disagree and Commit

Deliver Results

Strive to be Earth's Best Employer

Success and Scale Bring Broad Responsibility

Customer Obsession

Leaders start with the customer and work backwards. They work vigorously to earn and keep customer trust. Although leaders pay attention to competitors, they obsess over customers.

"Customer Obsession" Leadership Principle Explained by A...

Customer Obsession. Leaders start with the customer and work backwards. They work vigorously to earn and keep customer trust. Although leaders pay attention to competitors, they obsess over customers.

Ownership

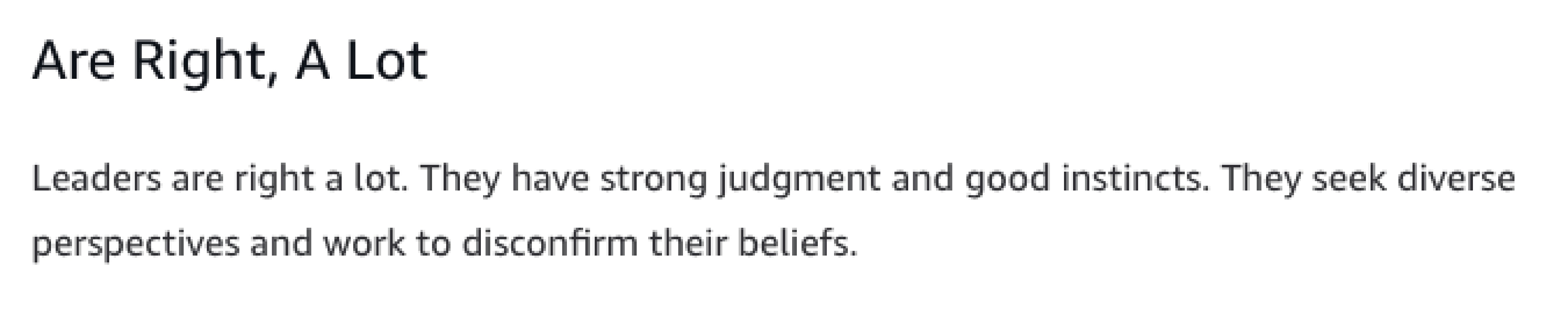
Leaders are owners. They think long term and don't sacrifice long-term value for short-term results. They act on behalf of the entire company, beyond just their own team. They never say "that's not my job."

https://www.aboutamazon.com/about-us/leadership-principles

Our Leadership Principles describe how Amazon does business, how leaders lead, and how we keep the customer at the center of our decisions

Leadership Principles form the fabric of our culture at AWS

Are Right A Lot



Are Right, A Lot

Leaders are right a lot. They have strong judgment and good instincts. They seek diverse perspectives and work to disconfirm their beliefs.

Secret: Are Right, A Lot is really about *how* you make decisions

Tenets

A tenet is a principle or belief that helps teams align and bring everyone into an agreement around critical questions

At Amazon, tenets play a big role in helping us *Be Right, A Lot*

https://aws.amazon.com/blogs/enterprise-strategy/tenets-supercharging-decision-making/

Private APIs integration tenets

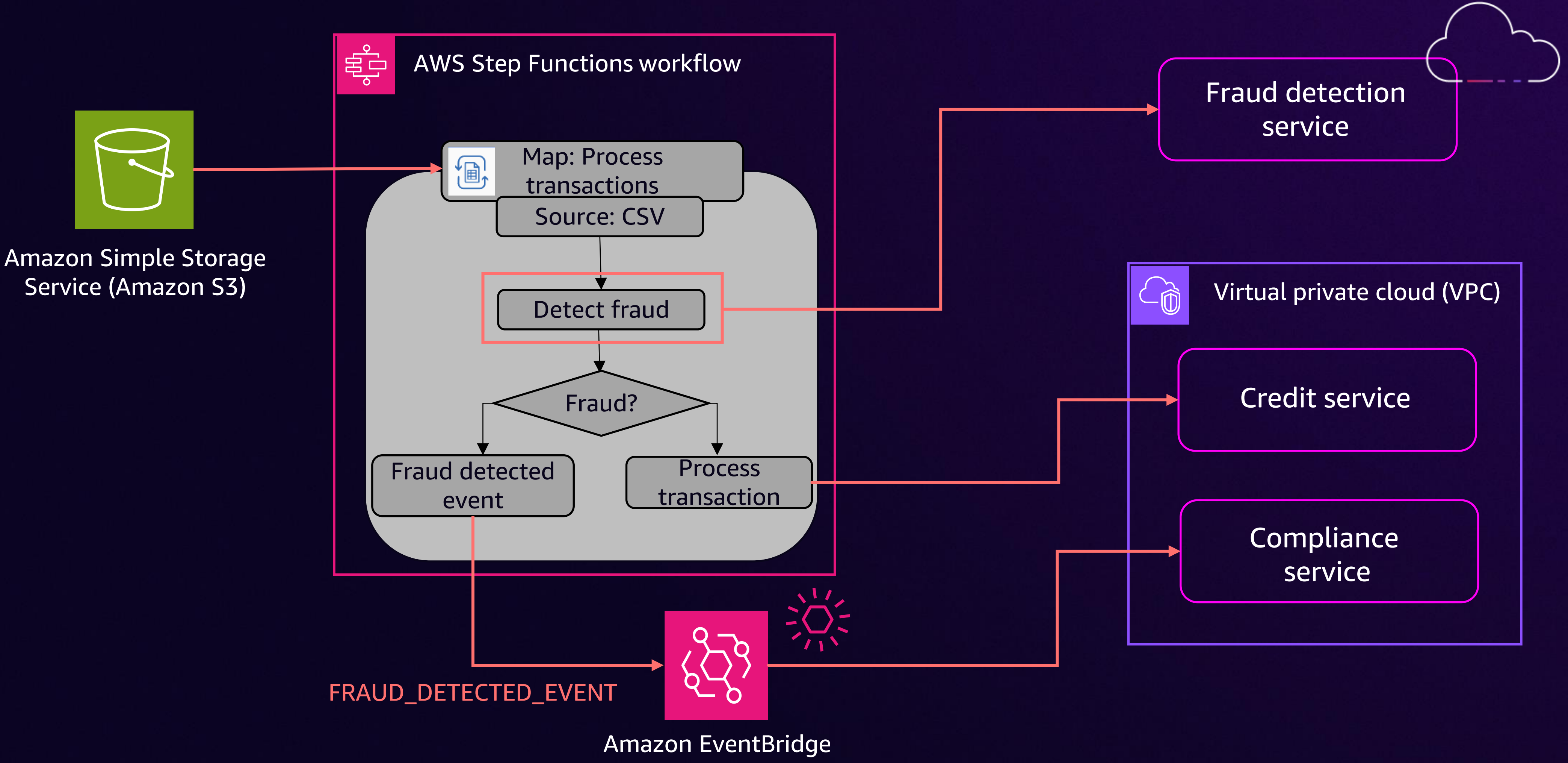
Simple
Developer
Experience

Secure by
Design

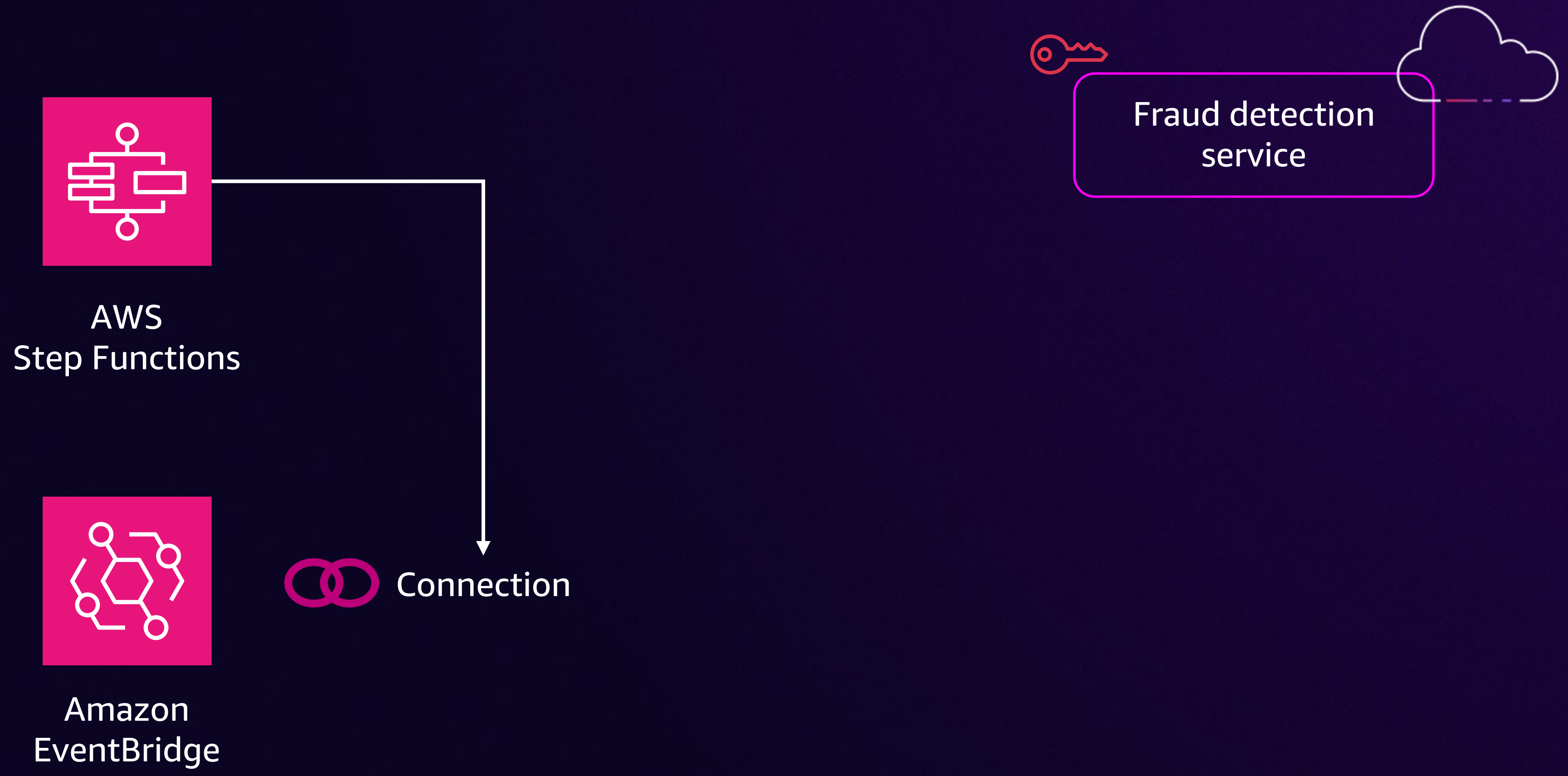
Reliable
integration

EventBridge and Step Functions with public and private APIs

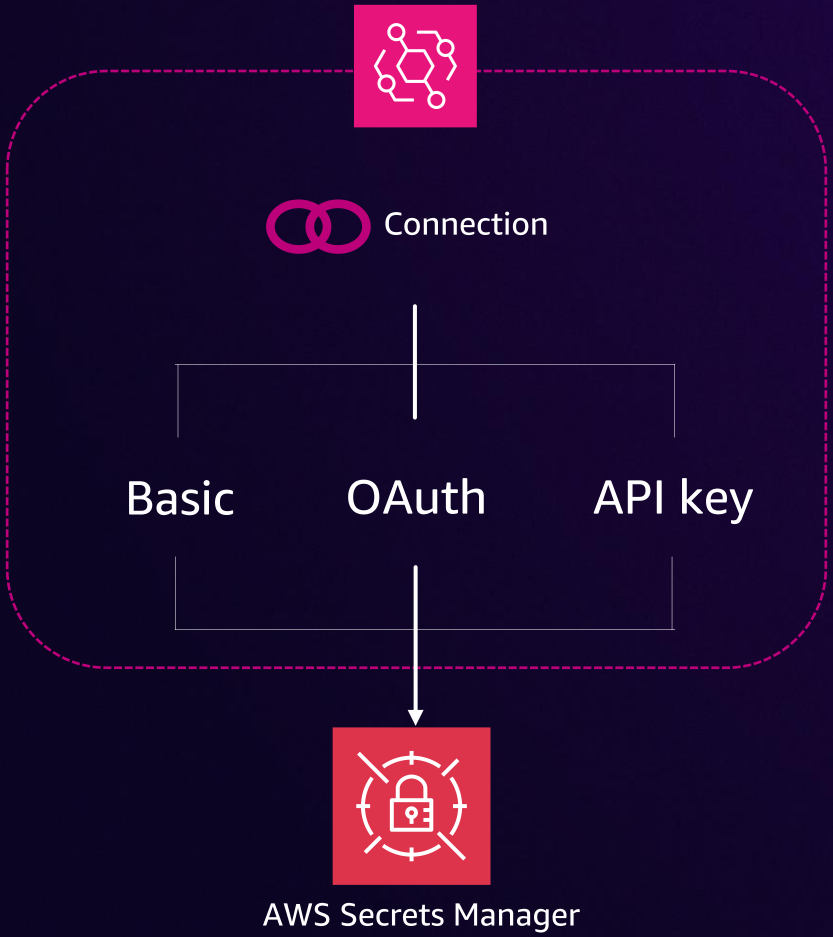
Example use case – Fraud detection



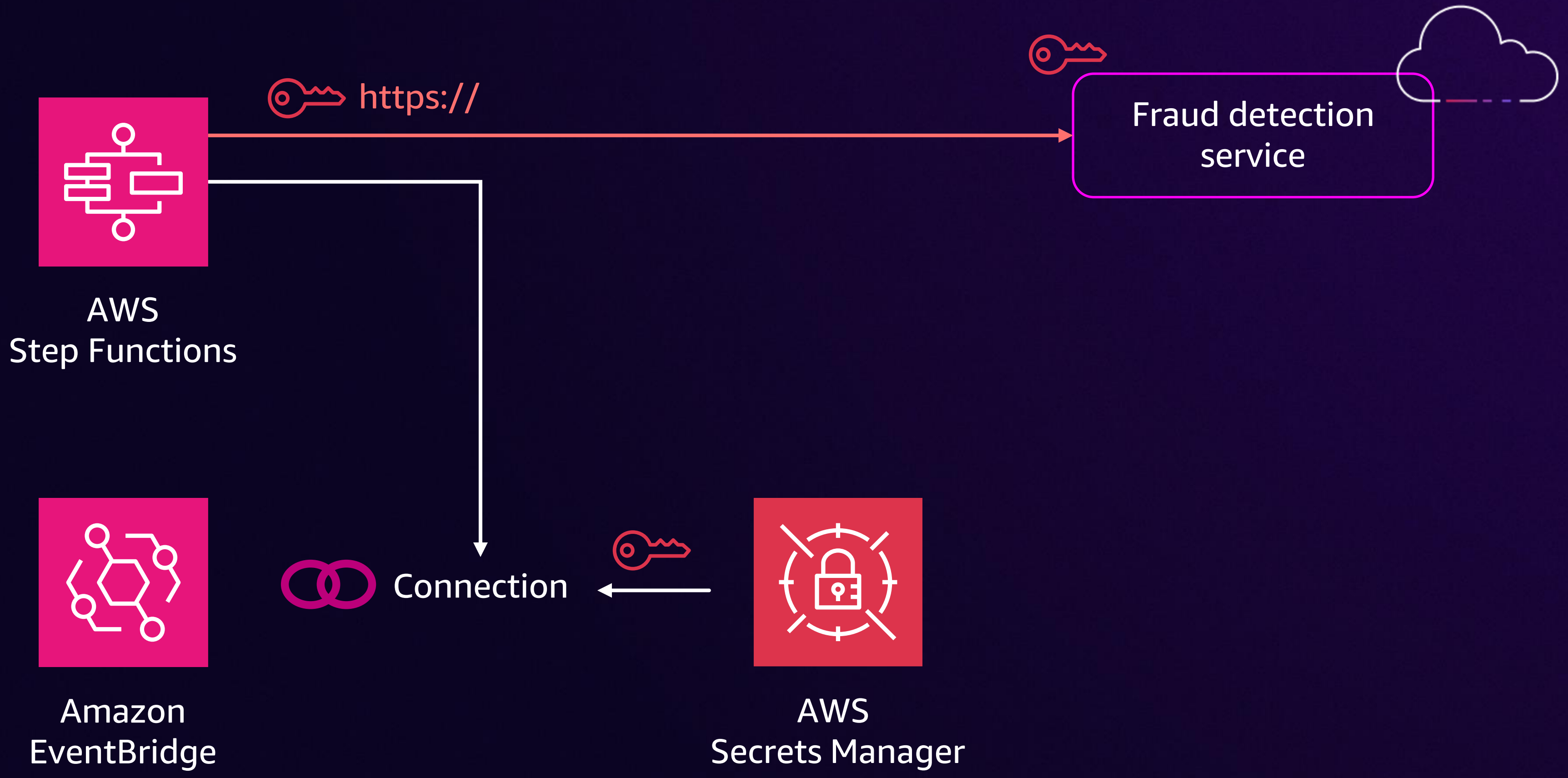
Public API integration with Step Functions



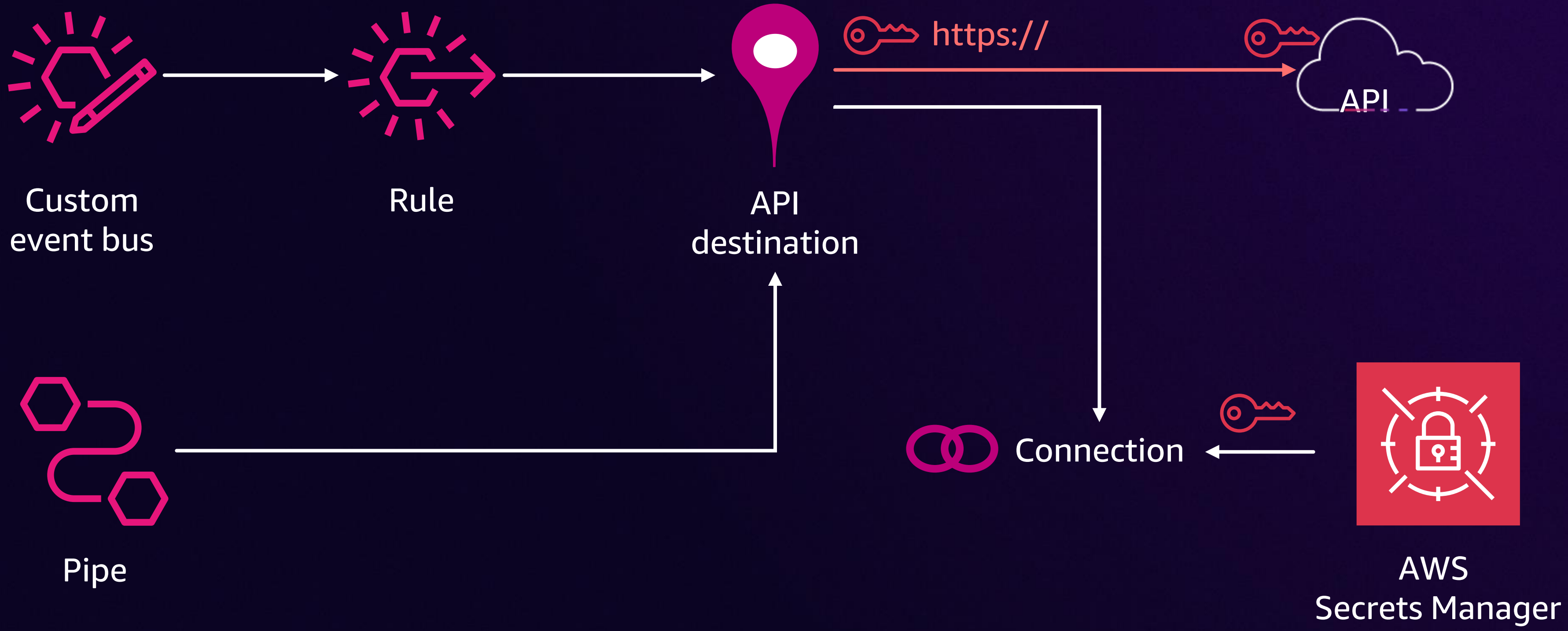
Authorization options



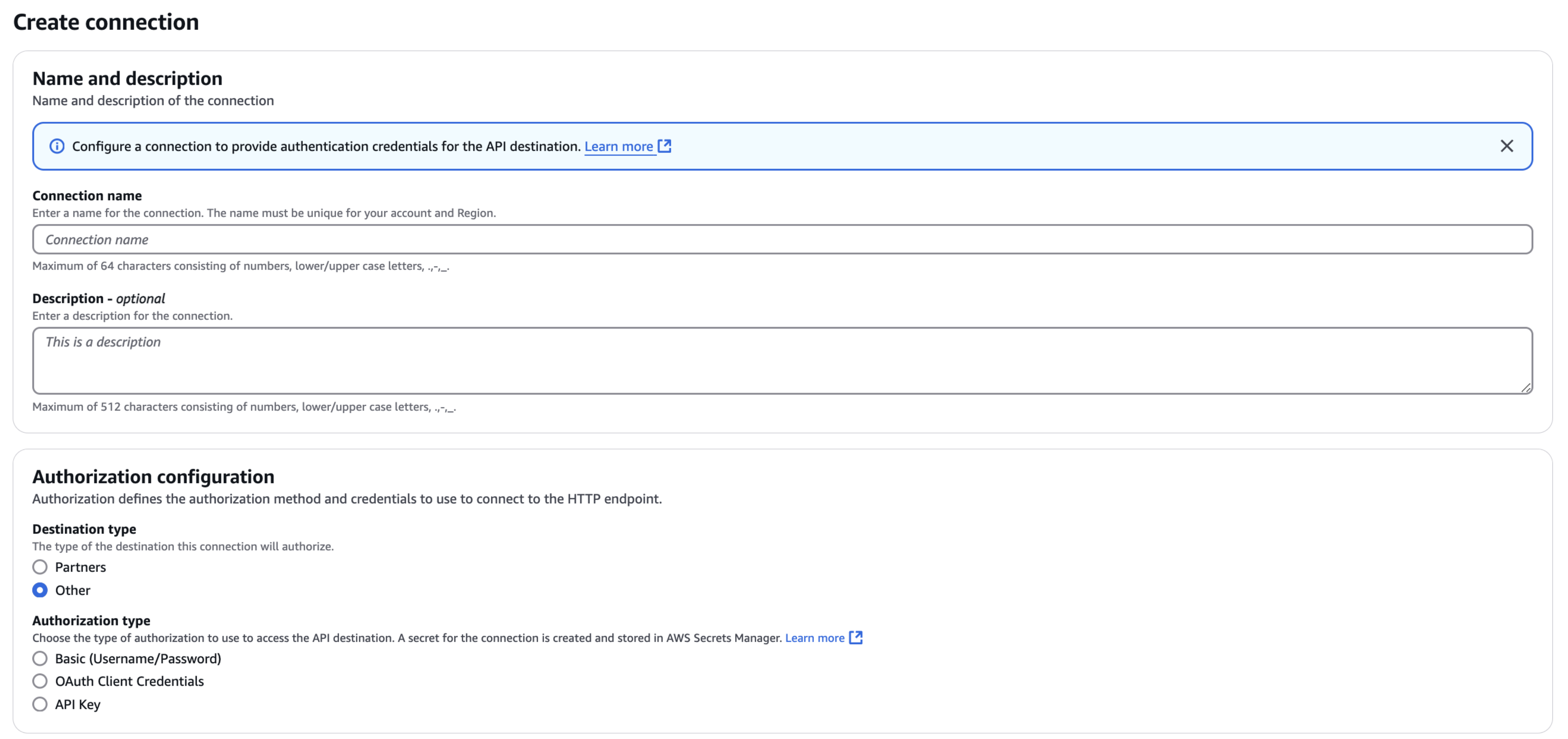
Public API integration with Step Functions



Public API integration with EventBridge



Creating a connection



Create connection

Name and description

Name and description of the connection

ⓘ Configure a connection to provide authentication credentials for the API destination. Learn more ↗ ✕

Connection name

Enter a name for the connection. The name must be unique for your account and Region.

Connection name

Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.

Description - *optional*

Enter a description for the connection.

This is a description

Maximum of 512 characters consisting of numbers, lower/upper case letters, .,-,_.

Authorization configuration

Authorization defines the authorization method and credentials to use to connect to the HTTP endpoint.

Destination type

The type of the destination this connection will authorize.

○ Partners

● Other

Authorization type

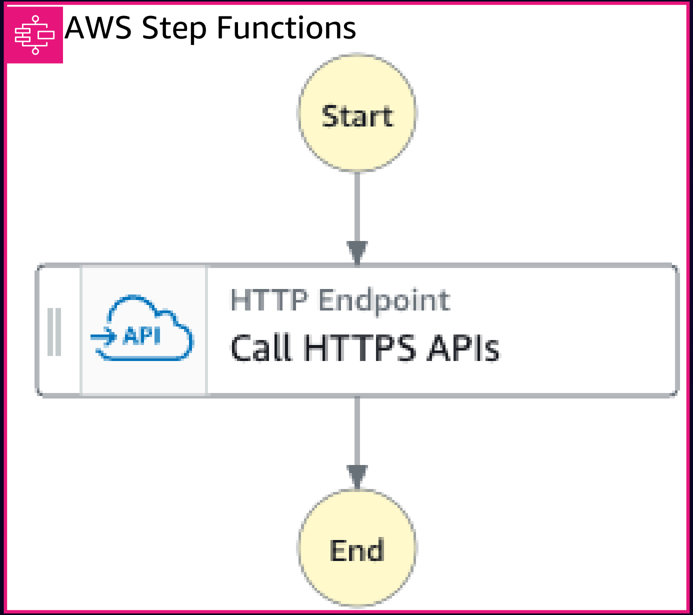
Choose the type of authorization to use to access the API destination. A secret for the connection is created and stored in AWS Secrets Manager. Learn more ↗

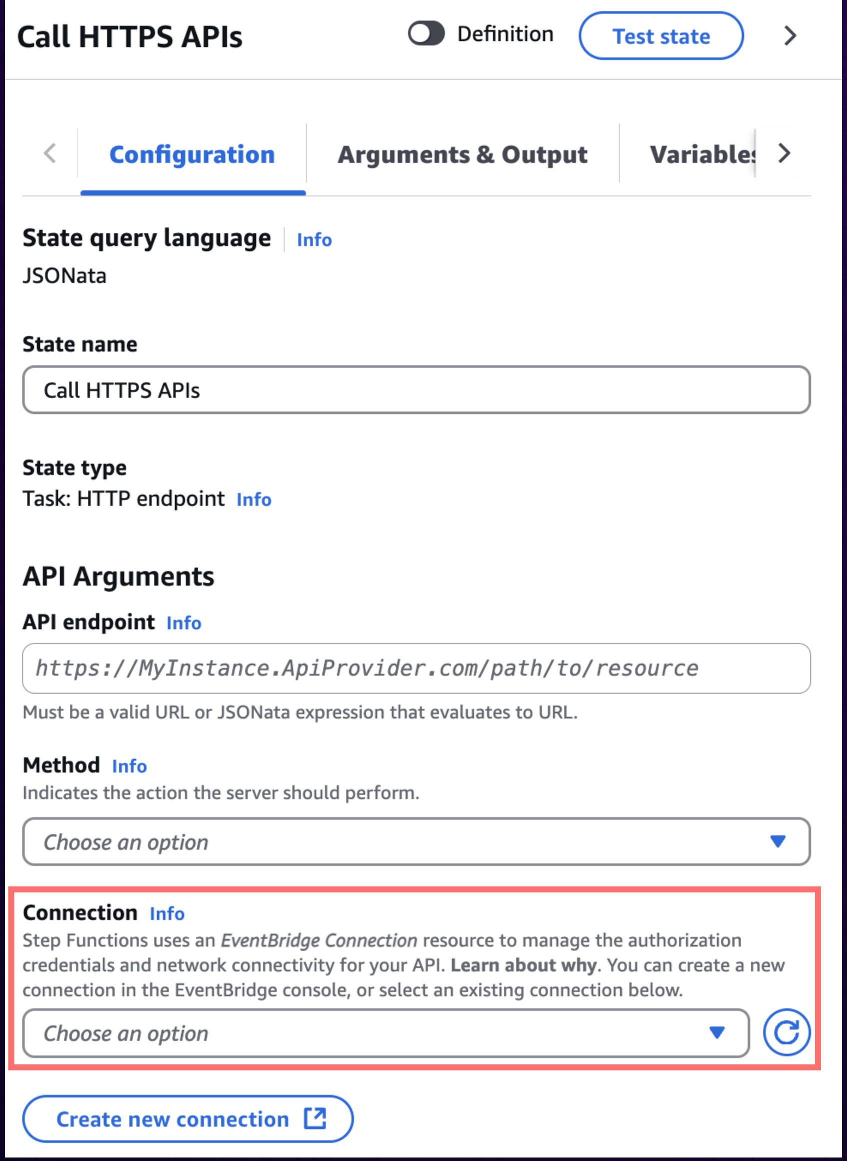
○ Basic (Username/Password)

○ OAuth Client Credentials

○ API Key

Using a connection in Step Functions





State query language Info
JSONata

State name
Call HTTPS APIs

State type
Task: HTTP endpoint Info

API Arguments

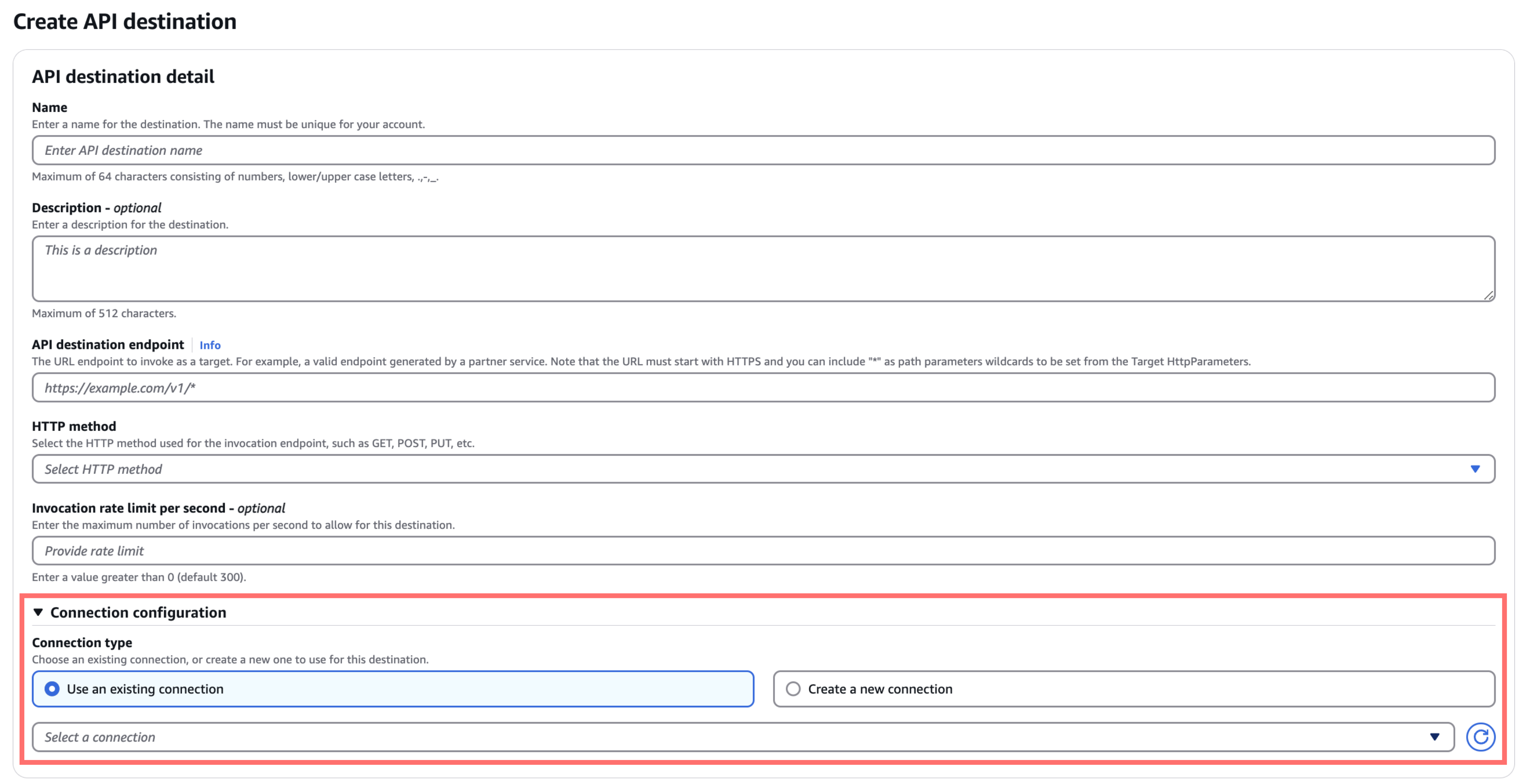
API endpoint Info
https://MyInstance.ApiProvider.com/path/to/resource
Must be a valid URL or JSONata expression that evaluates to URL.

Method Info
Indicates the action the server should perform.
Choose an option ▼

Connection Info
Step Functions uses an *EventBridge Connection* resource to manage the authorization credentials and network connectivity for your API. **Learn about why**. You can create a new connection in the EventBridge console, or select an existing connection below.
Choose an option ▼

Create new connection

Using a connection in EventBridge



Create API destination

API destination detail

Name
Enter a name for the destination. The name must be unique for your account.

Enter API destination name

Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.

Description - *optional*
Enter a description for the destination.

This is a description

Maximum of 512 characters.

API destination endpoint | Info
The URL endpoint to invoke as a target. For example, a valid endpoint generated by a partner service. Note that the URL must start with HTTPS and you can include "*" as path parameters wildcards to be set from the Target HttpParameters.

*https://example.com/v1/**

HTTP method
Select the HTTP method used for the invocation endpoint, such as GET, POST, PUT, etc.

Select HTTP method ▼

Invocation rate limit per second - *optional*
Enter the maximum number of invocations per second to allow for this destination.

Provide rate limit

Enter a value greater than 0 (default 300).

▼ Connection configuration

Connection type
Choose an existing connection, or create a new one to use for this destination.

● Use an existing connection ○ Create a new connection

Select a connection ▼

Benefits of native API integrations

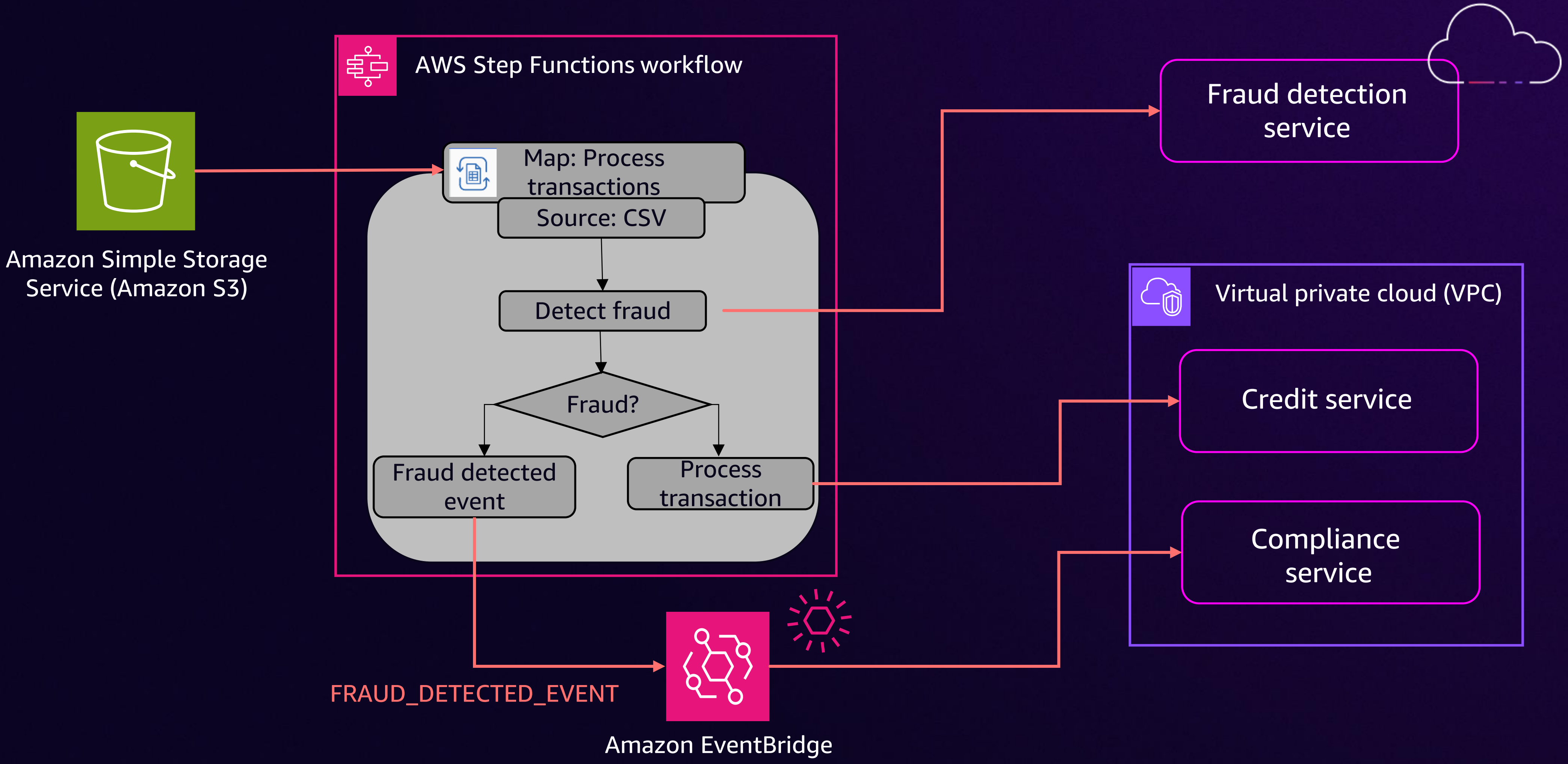
Reduce application footprint

Built-in error handling

Managed security

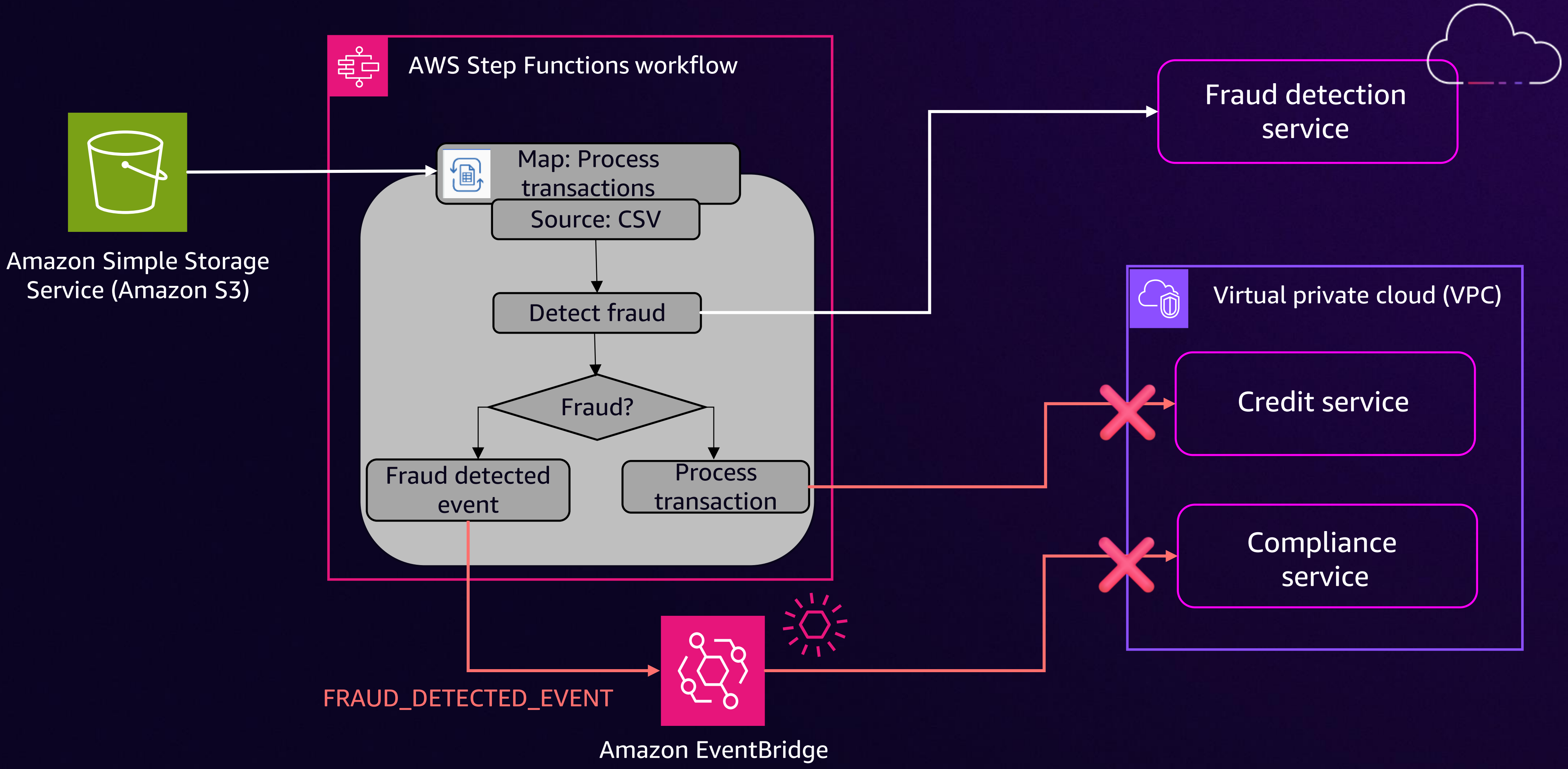
Build EDA easily

Example use case – Fraud detection



What’s the challenge with connecting to private APIs?

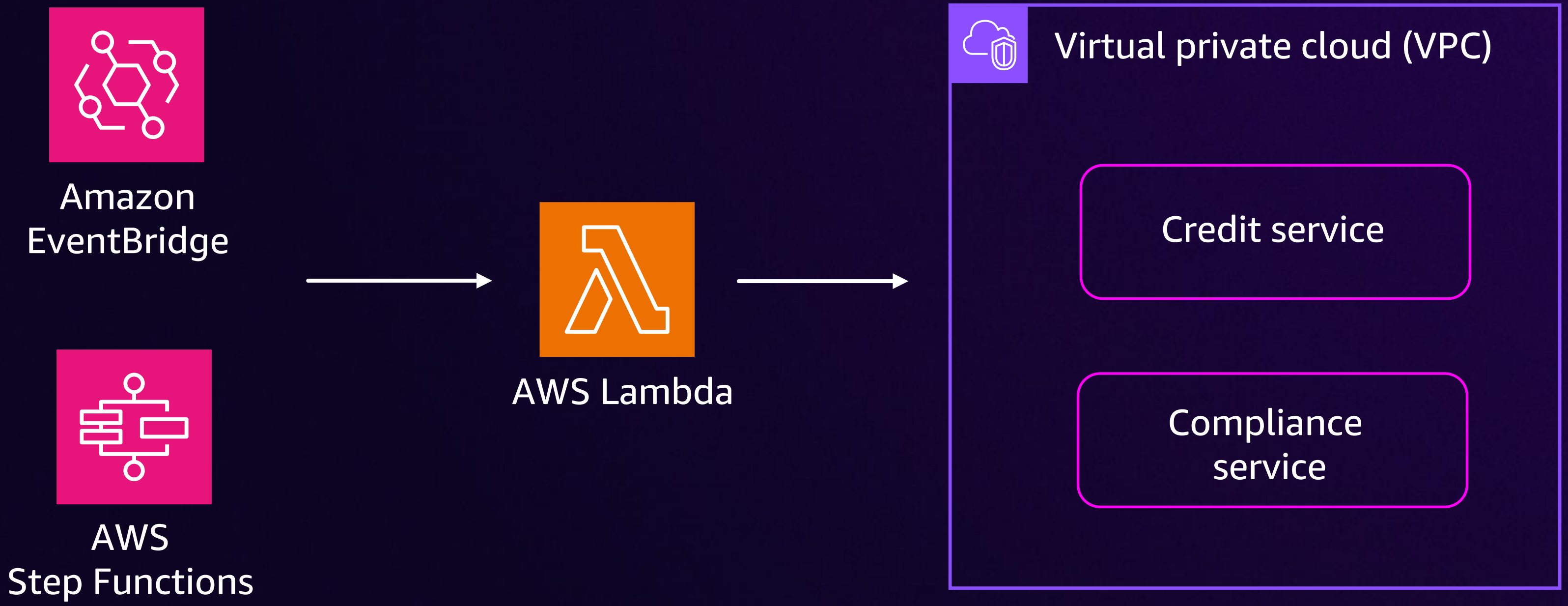
Example use case – Fraud detection



Challenges integrating with private APIs

- Common workarounds
  - Make API public
  - Use VPC-attached AWS Lambda functions
  - Use intermediary Amazon SQS queues (poll from VPC)
- Write and maintain undifferentiated code

Integrating with private APIs before



Integrating with private APIs now

Accelerate innovation and simplify modernization of distributed applications with seamless integration across private and public networks

SIMPLIFY MODERNIZATION

ACHIEVE FASTER TIME TO MARKET

DRIVE HIGHER SECURITY AND COMPLIANCE

Private API integration use cases

Build EDAs with containers

Orchestrate business-critical workflows across VPCs

Deliver AWS service events to services inside VPC

Modernize on-premises applications

Private APIs deep dive

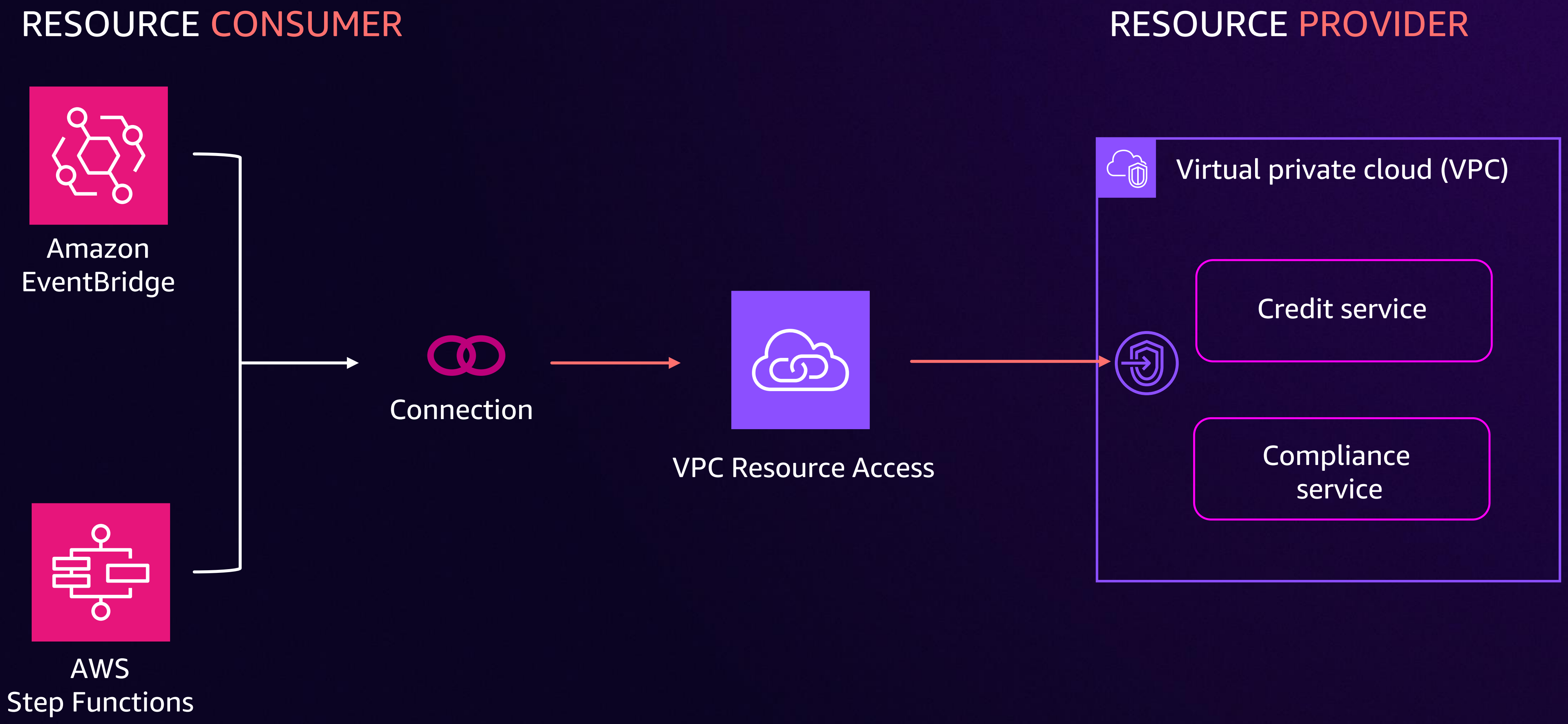
Private APIs integration tenets

Simple developer experience

Secure by design

Reliable integration

Integrating with private APIs now



VPC Resource Access (NEW)

Benefits of VPC Resource Access

VPC Lattice

AWS PrivateLink

Integrated in AWS PrivateLink and VPC Lattice

Sharing with AWS Resource Access Manager (AWS RAM)

One-to-many access

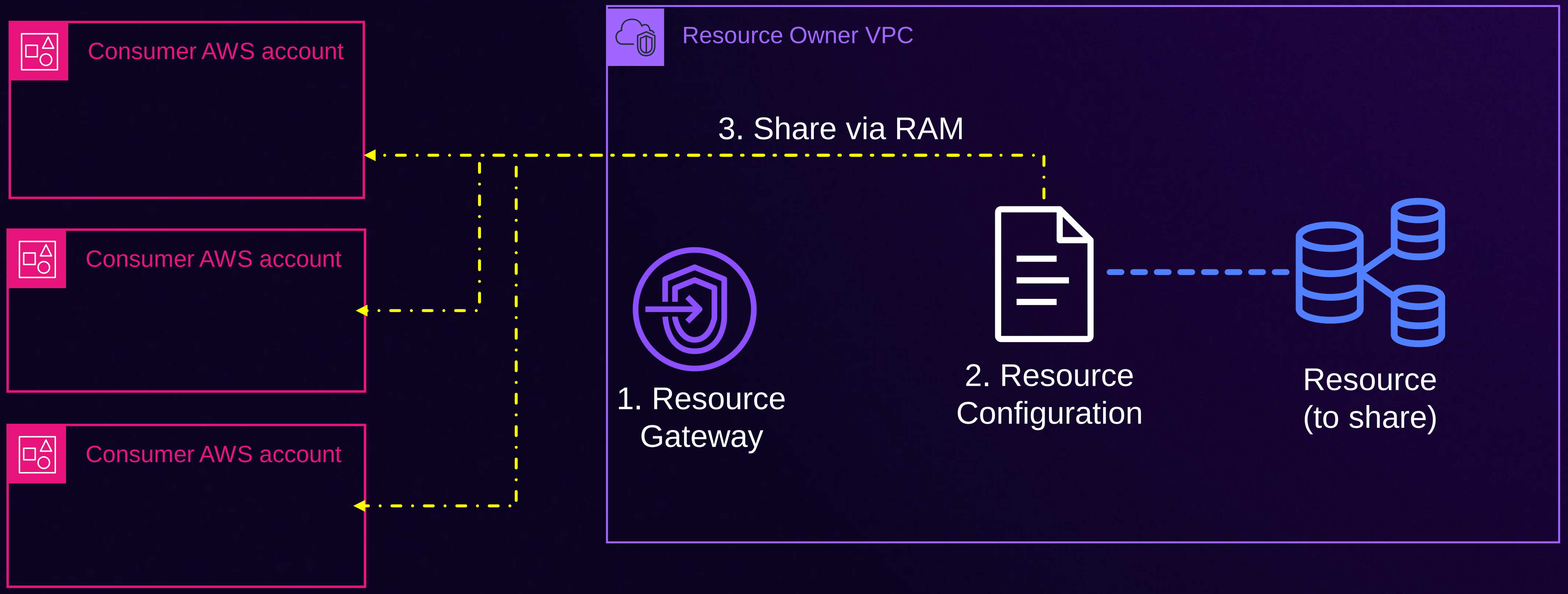
Accessible from on-premises

Resource Provider Experience

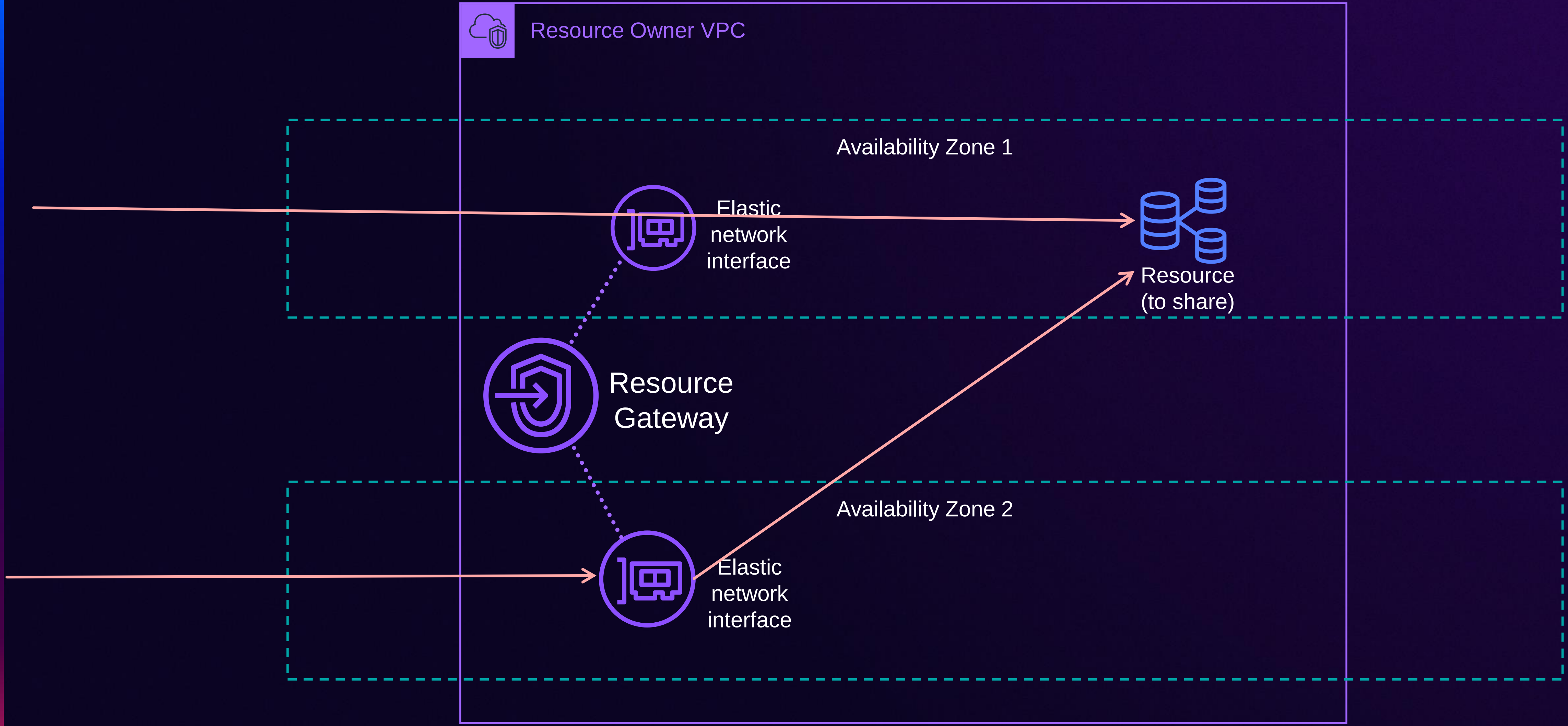
Step 1 (one-time): Create a Resource Gateway

Step 2: Create a *Resource Configuration* for the resource you want to share

Step 3: Share Resource Configuration with consumer via RAM



What is a Resource Gateway ?



What is a Resource Configuration ?

Resource Configuration

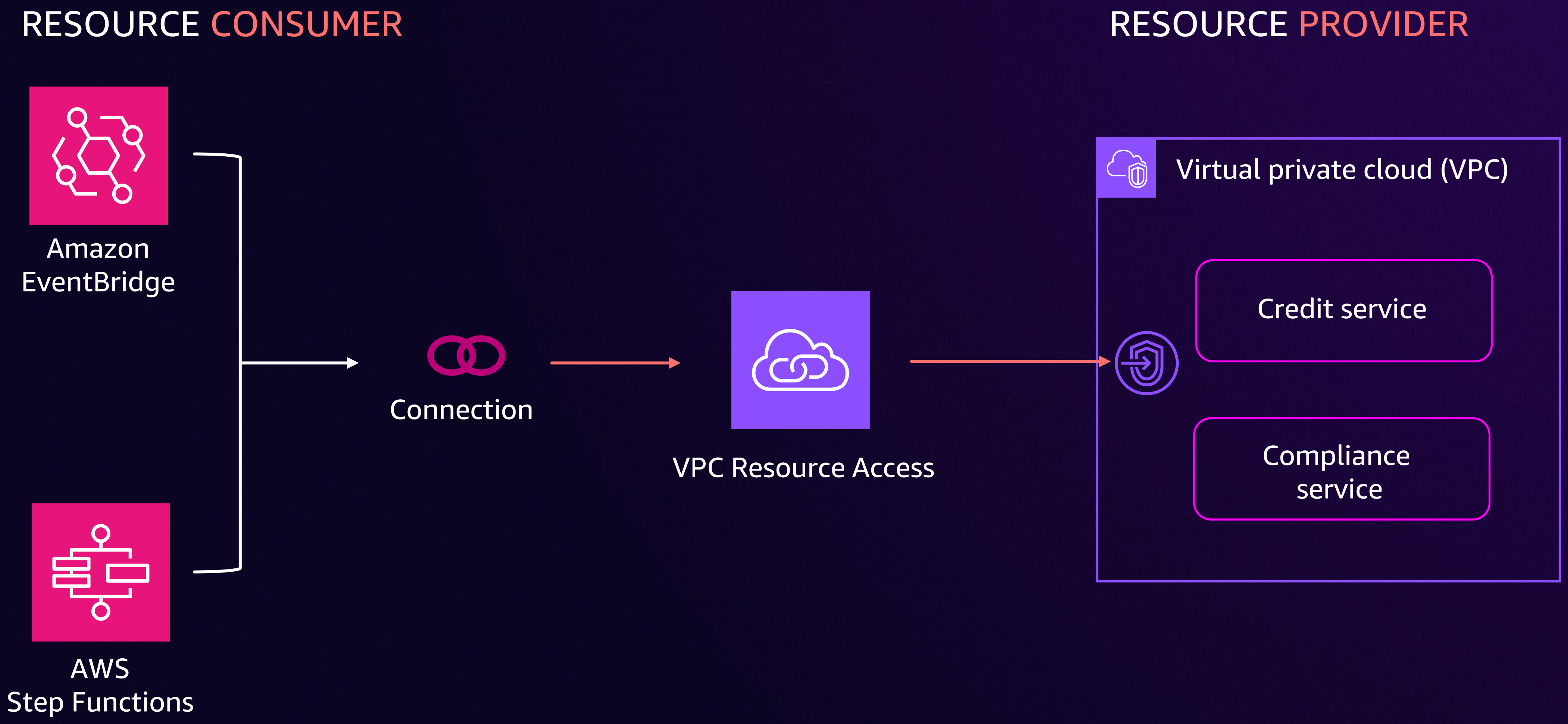
Represents a resource or group of resources that you want to share

IP Address
e.g. 10.6.1.2

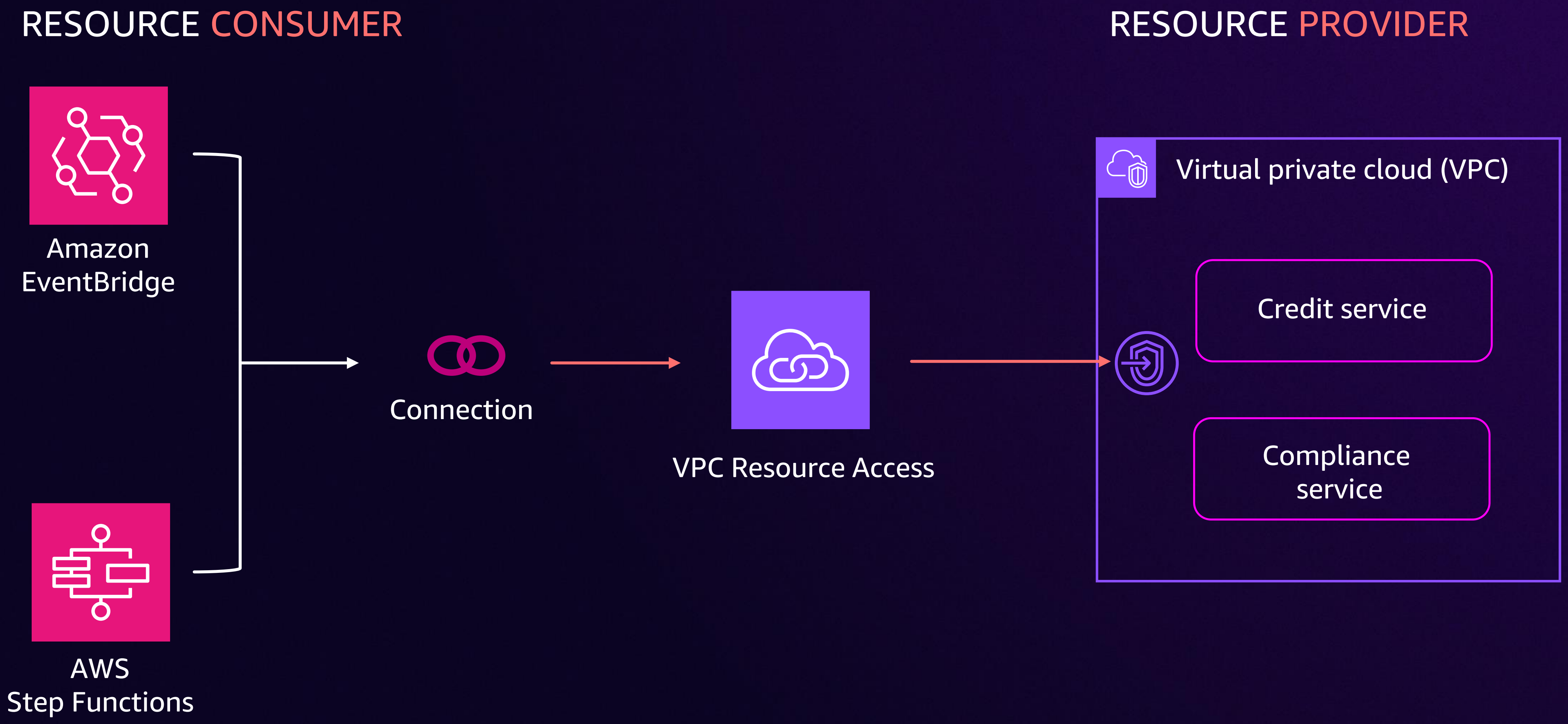
Domain Name
e.g. abc.example.com

ARN
e.g. arn:aws:rds:us-west-2:
123456789012:cluster:db1

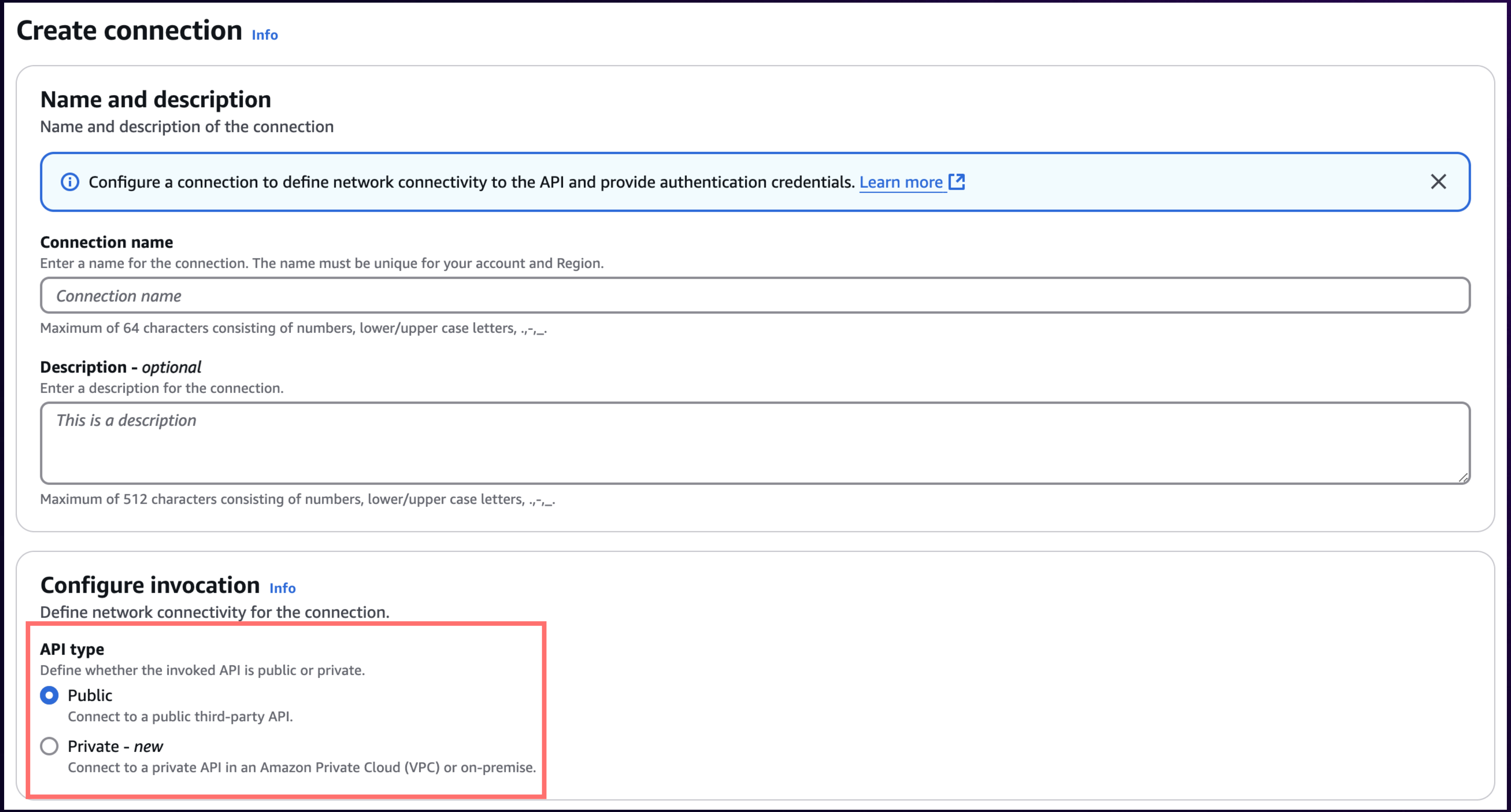
Integrating with private APIs now



Integrating with private APIs now



Resource Consumer Experience



Create connection Info

Name and description

Name and description of the connection

ⓘ Configure a connection to define network connectivity to the API and provide authentication credentials. Learn more ✕

Connection name

Enter a name for the connection. The name must be unique for your account and Region.

Connection name

Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.

Description - *optional*

Enter a description for the connection.

This is a description

Maximum of 512 characters consisting of numbers, lower/upper case letters, .,-,_.

Configure invocation Info

Define network connectivity for the connection.

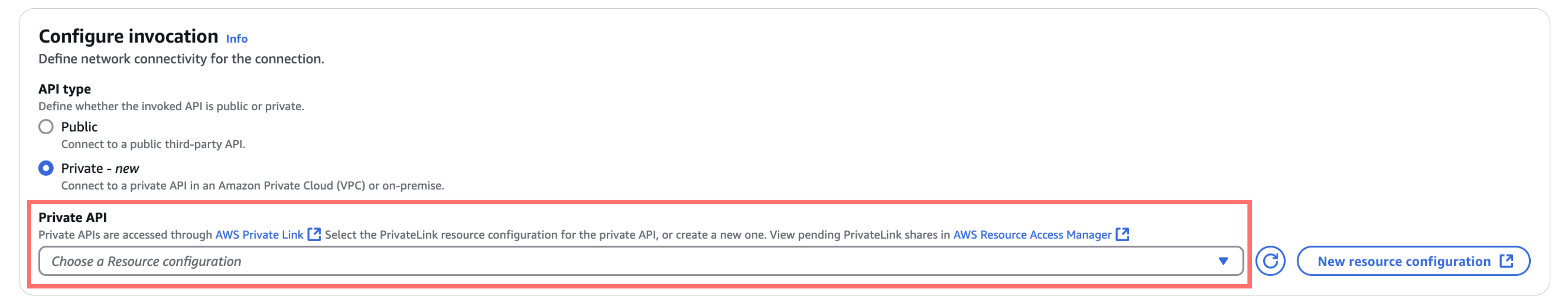
API type

Define whether the invoked API is public or private.

● Public
Connect to a public third-party API.

○ Private - *new*
Connect to a private API in an Amazon Private Cloud (VPC) or on-premise.

Resource Consumer Experience



Configure invocation Info

Define network connectivity for the connection.

API type

Define whether the invoked API is public or private.

○ Public

Connect to a public third-party API.

● Private - *new*

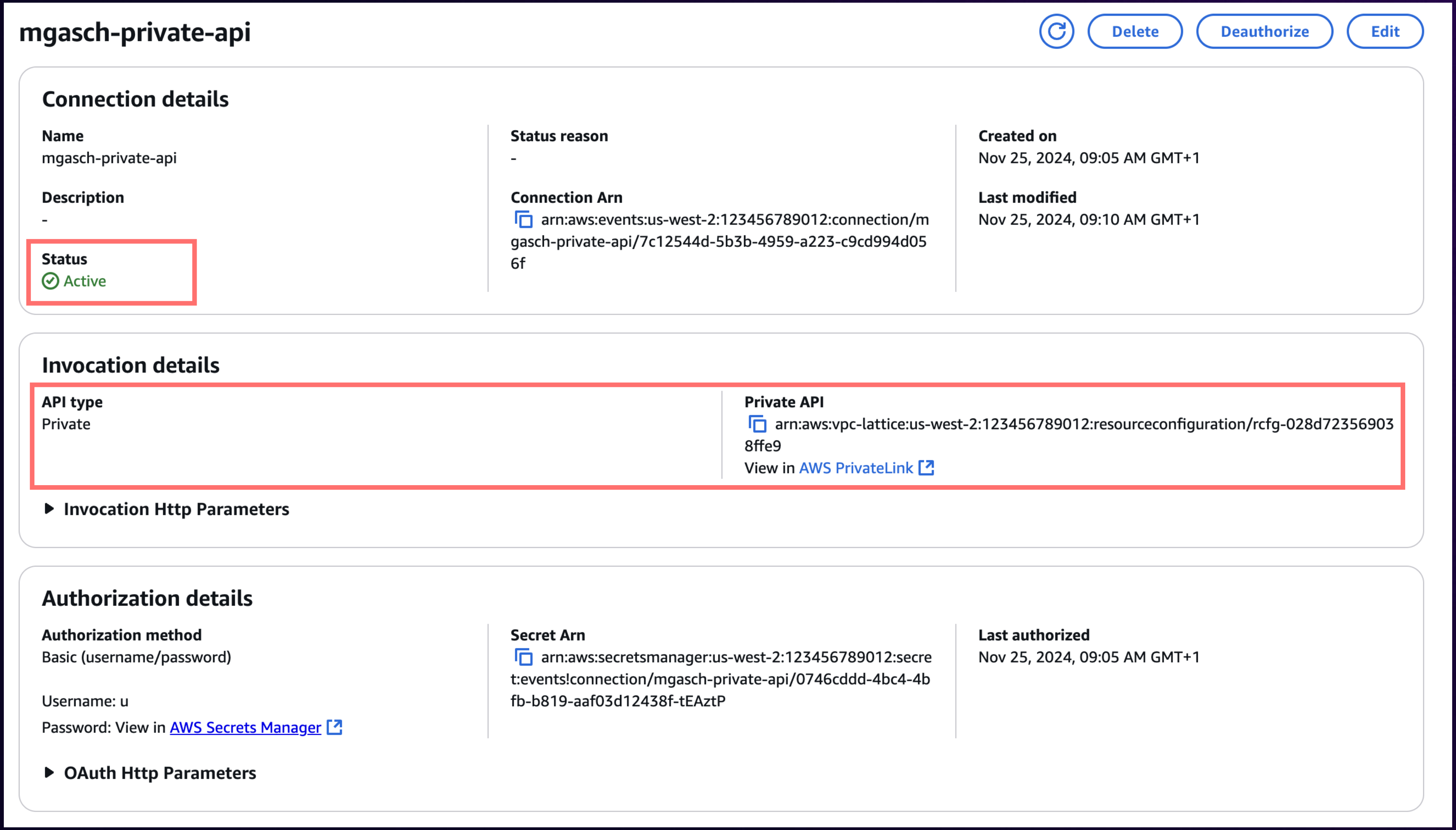
Connect to a private API in an Amazon Private Cloud (VPC) or on-premise.

Private API

Private APIs are accessed through AWS Private Link Select the PrivateLink resource configuration for the private API, or create a new one. View pending PrivateLink shares in AWS Resource Access Manager

Choose a Resource configuration ▼

Resource Consumer Experience



mgasch-private-api

Connection details

Name
mgasch-private-api

Description
-

Status
✓ Active

Status reason
-

Connection Arn
arn:aws:events:us-west-2:123456789012:connection/mgasch-private-api/7c12544d-5b3b-4959-a223-c9cd994d056f

Created on
Nov 25, 2024, 09:05 AM GMT+1

Last modified
Nov 25, 2024, 09:10 AM GMT+1

Invocation details

API type
Private

Private API
arn:aws:vpc-lattice:us-west-2:123456789012:resourceconfiguration/rcfg-028d723569038ffe9
View in AWS PrivateLink

▶ **Invocation Http Parameters**

Authorization details

Authorization method
Basic (username/password)

Username: u
Password: View in AWS Secrets Manager

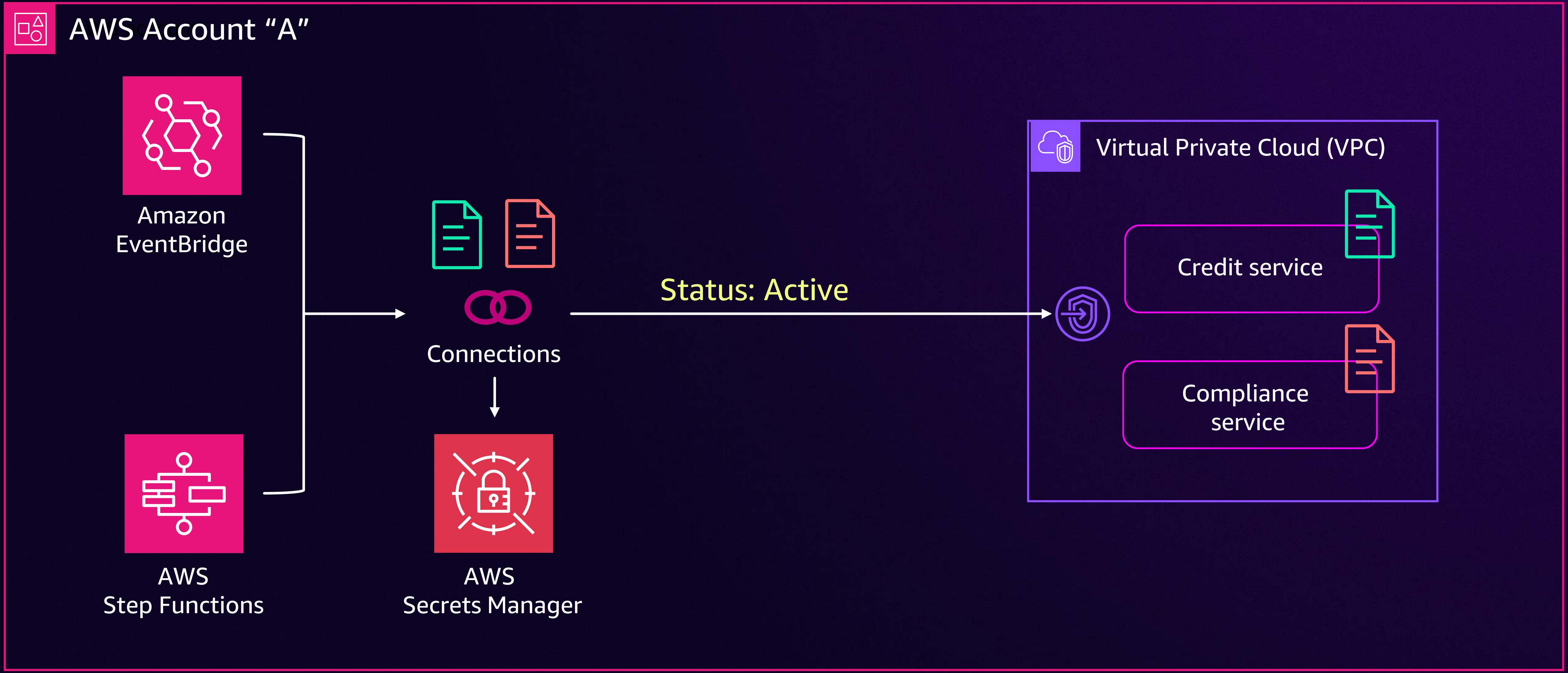
Secret Arn
arn:aws:secretsmanager:us-west-2:123456789012:secret:events!connection/mgasch-private-api/0746cddd-4bc4-4bfb-b819-aaf03d12438f-tEAztP

Last authorized
Nov 25, 2024, 09:05 AM GMT+1

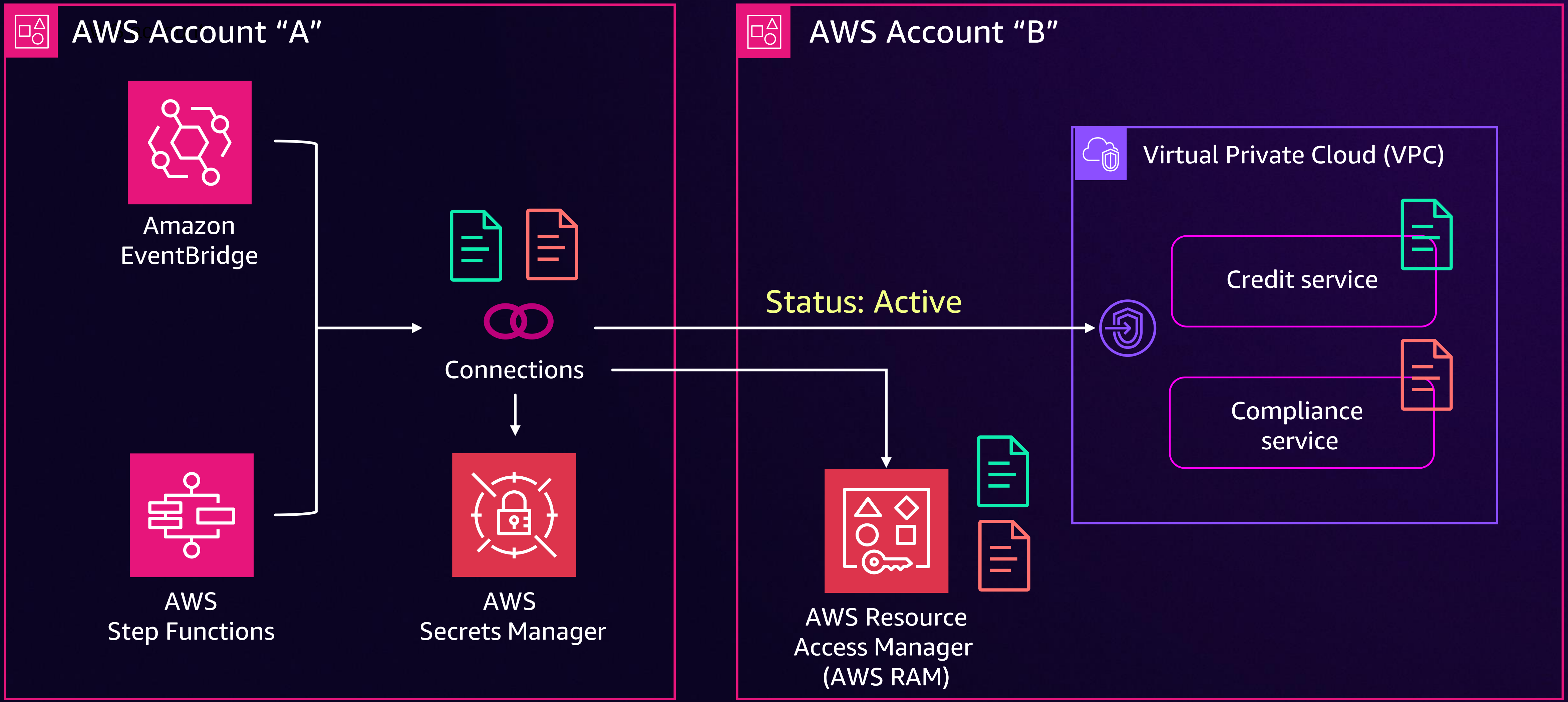
▶ **OAuth Http Parameters**

Single and cross-account Scenarios

Private APIs integration: Same account



Private APIs integration across accounts



Security Controls

Private APIs integration tenets

Simple developer experience

Secure by design

Reliable integration

Security Controls for Providers

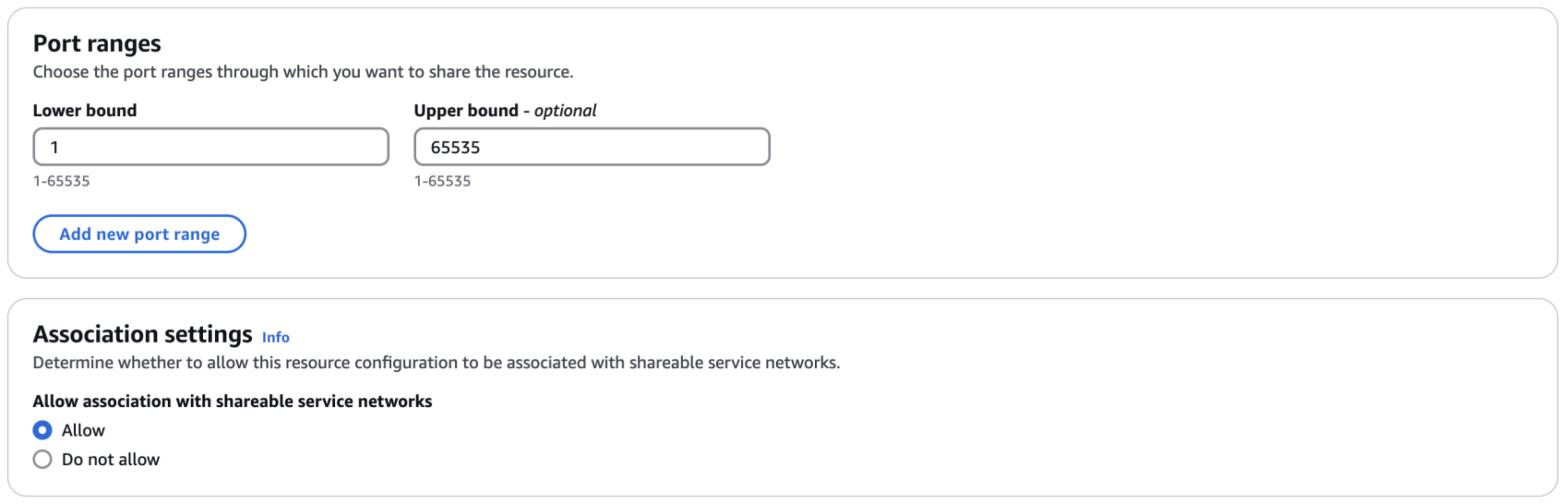
Security controls for providers

API AUTHORIZATION OPTIONS

- Authorization enforced by the target (HTTPS API)
- Supported authorization **options**
  - Basic auth
  - API key (token)
  - OAuth with public and **private** OAuth endpoint
- TLS encrypted

Security controls for providers

- Port ranges and association settings



Port ranges

Choose the port ranges through which you want to share the resource.

Lower bound	Upper bound - *optional*
1	65535
1-65535	1-65535

Association settings

Determine whether to allow this resource configuration to be associated with shareable service networks.

Allow association with shareable service networks

● Allow

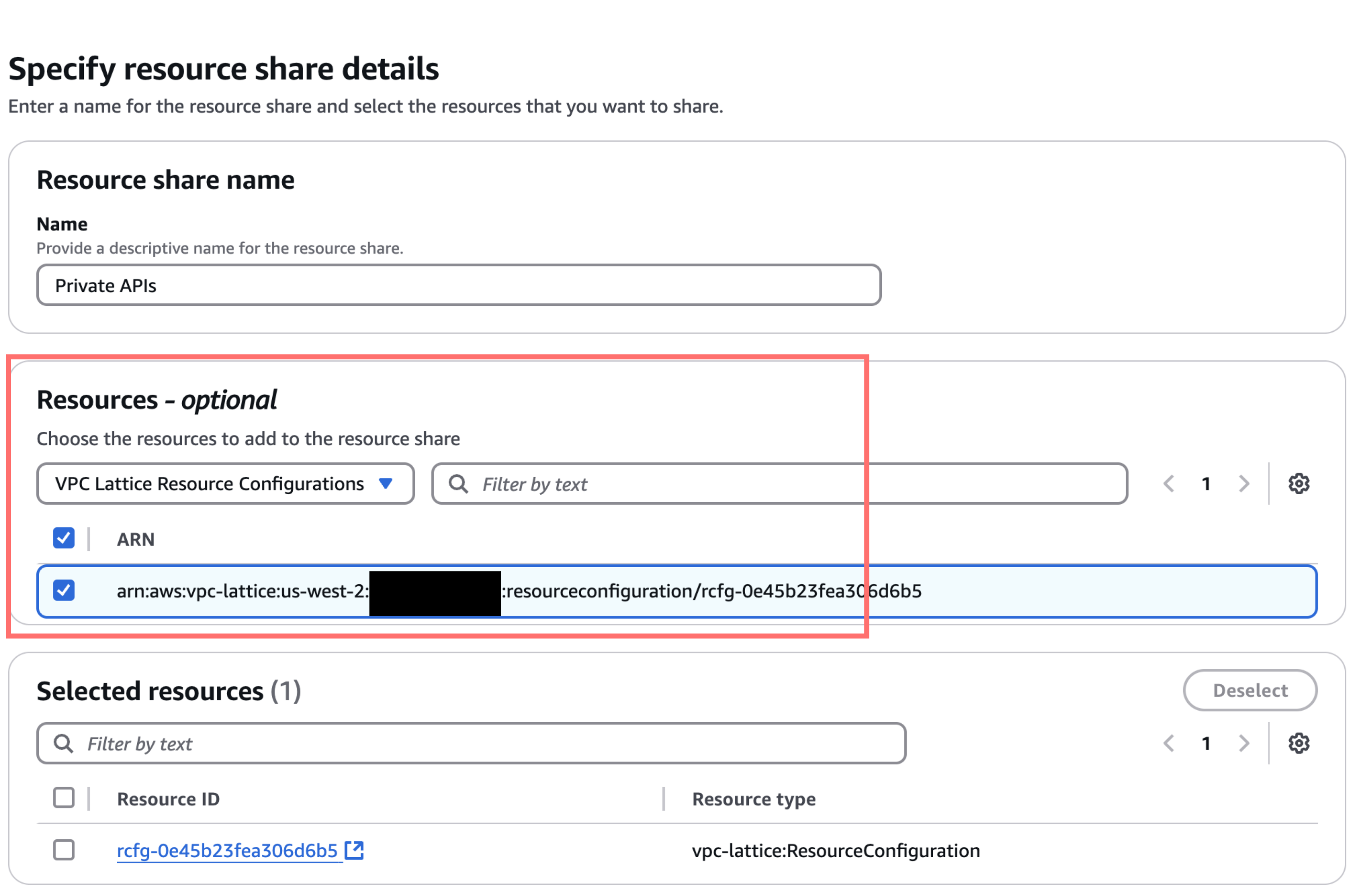
○ Do not allow

Security controls for providers

- Port ranges and association settings
- Fine-grained AWS RAM access controls

Security controls for providers

FINE-GRAINED AWS RAM ACCESS CONTROLS



Specify resource share details

Enter a name for the resource share and select the resources that you want to share.

Resource share name

Name

Provide a descriptive name for the resource share.

Private APIs

Resources - *optional*

Choose the resources to add to the resource share

VPC Lattice Resource Configurations ▼ | Filter by text | ‹ 1 › ⚙

☑	ARN
☑	arn:aws:vpc-lattice:us-west-2:[redacted]:resourceconfiguration/rcfg-0e45b23fea306d6b5

Selected resources (1)

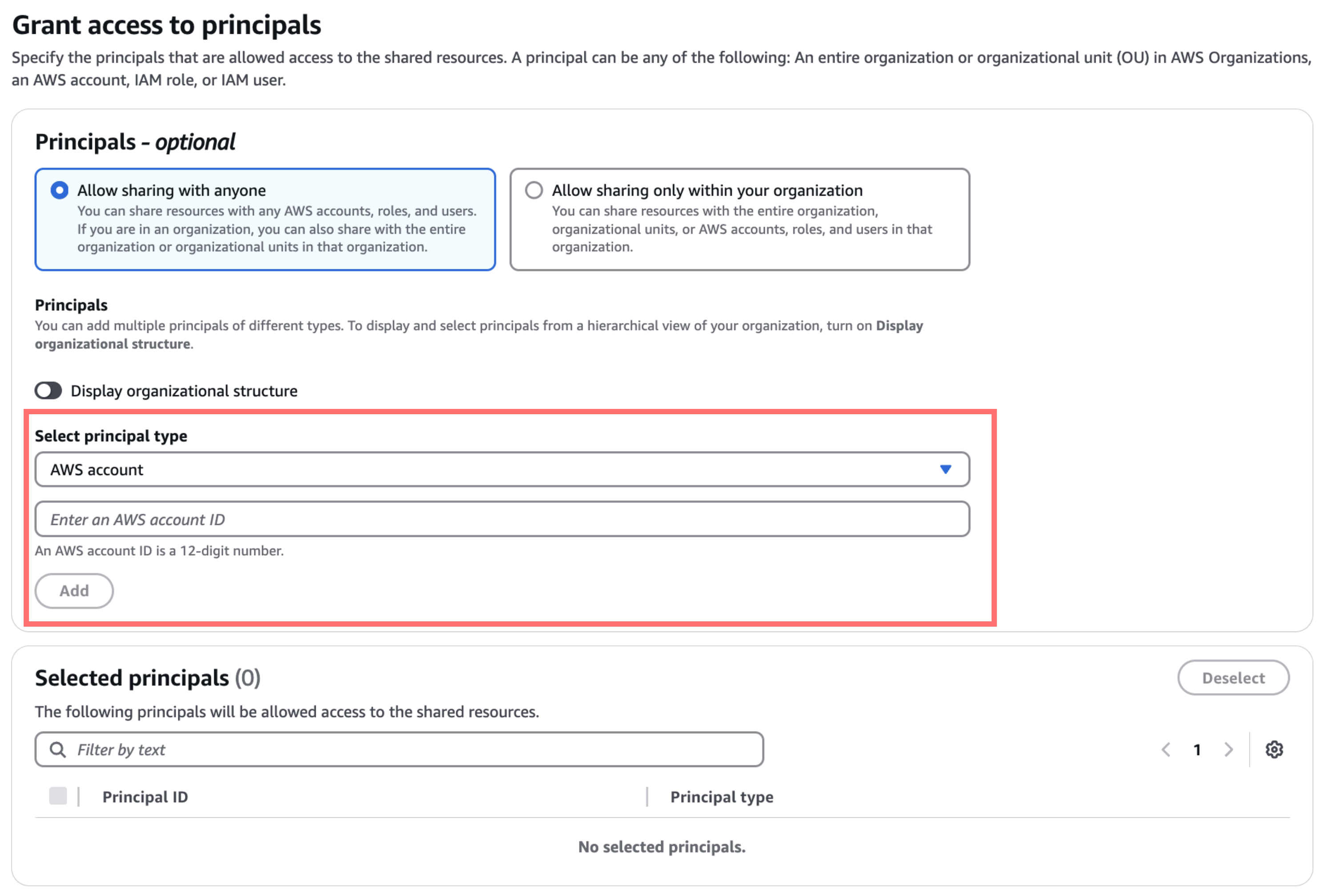
Deselect

Filter by text | ‹ 1 › ⚙

□	Resource ID	Resource type
□	rcfg-0e45b23fea306d6b5	vpc-lattice:ResourceConfiguration

Security controls for providers

FINE-GRAINED AWS RAM ACCESS CONTROLS



Grant access to principals

Specify the principals that are allowed access to the shared resources. A principal can be any of the following: An entire organization or organizational unit (OU) in AWS Organizations, an AWS account, IAM role, or IAM user.

Principals - *optional*

● Allow sharing with anyone
You can share resources with any AWS accounts, roles, and users. If you are in an organization, you can also share with the entire organization or organizational units in that organization.

○ Allow sharing only within your organization
You can share resources with the entire organization, organizational units, or AWS accounts, roles, and users in that organization.

Principals
You can add multiple principals of different types. To display and select principals from a hierarchical view of your organization, turn on **Display organizational structure**.

Display organizational structure

Select principal type
AWS account

Enter an AWS account ID
An AWS account ID is a 12-digit number.

Selected principals (0)

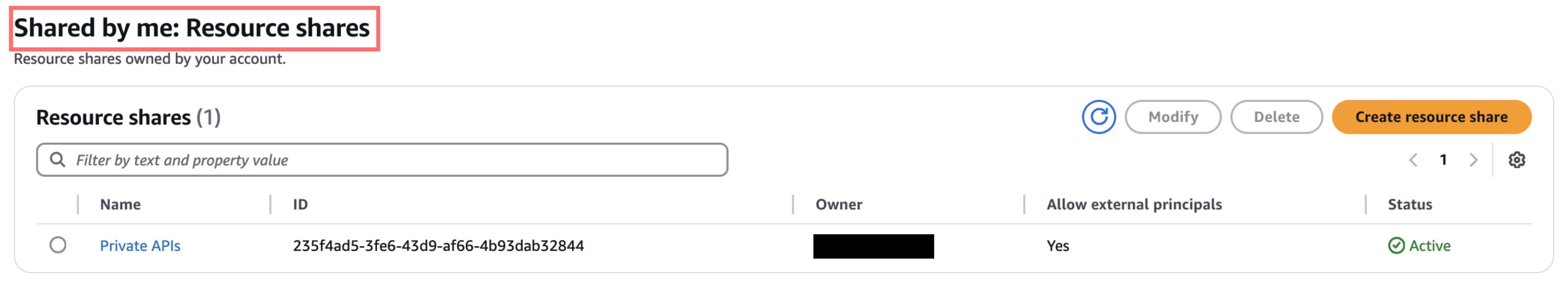
The following principals will be allowed access to the shared resources.

Principal ID	Principal type

No selected principals.

Security controls for providers

FINE-GRAINED AWS RAM ACCESS CONTROLS



Shared by me: Resource shares

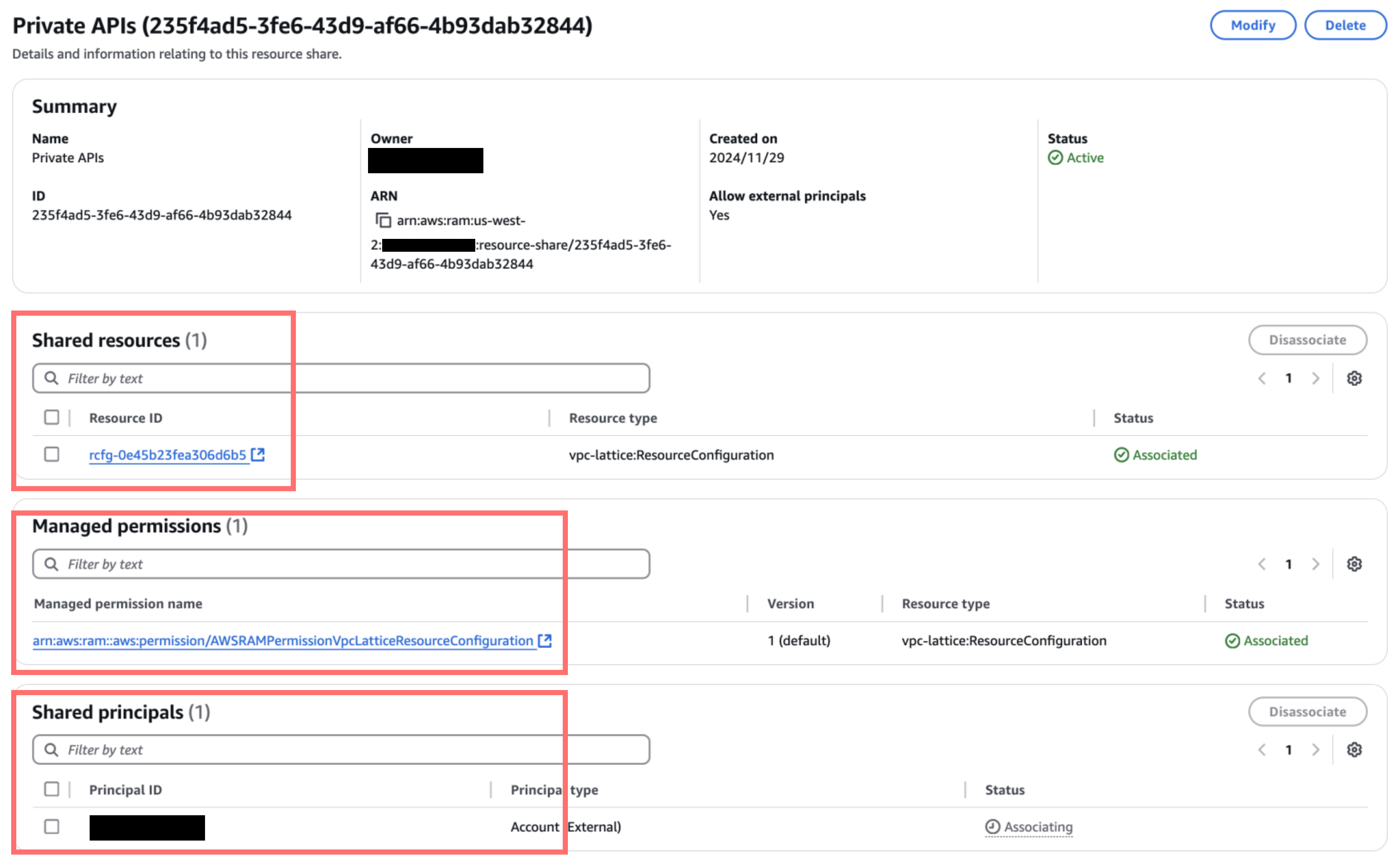
Resource shares owned by your account.

Resource shares (1)

	Name	ID	Owner	Allow external principals	Status
○	Private APIs	235f4ad5-3fe6-43d9-af66-4b93dab32844	[redacted]	Yes	✓ Active

Security controls for providers

FINE-GRAINED AWS RAM ACCESS CONTROLS



Private APIs (235f4ad5-3fe6-43d9-af66-4b93dab32844)

Details and information relating to this resource share.

Summary

Name
Private APIs

ID
235f4ad5-3fe6-43d9-af66-4b93dab32844

Owner
[redacted]

ARN
arn:aws:ram:us-west-2:[redacted]:resource-share/235f4ad5-3fe6-43d9-af66-4b93dab32844

Created on
2024/11/29

Allow external principals
Yes

Status
✓ Active

Shared resources (1)

□ Resource ID	Resource type	Status
□ rcfg-0e45b23fea306d6b5	vpc-lattice:ResourceConfiguration	✓ Associated

Managed permissions (1)

Managed permission name	Version	Resource type	Status
arn:aws:ram::aws:permission/AWSRAMPermissionVpcLatticeResourceConfiguration	1 (default)	vpc-lattice:ResourceConfiguration	✓ Associated

Shared principals (1)

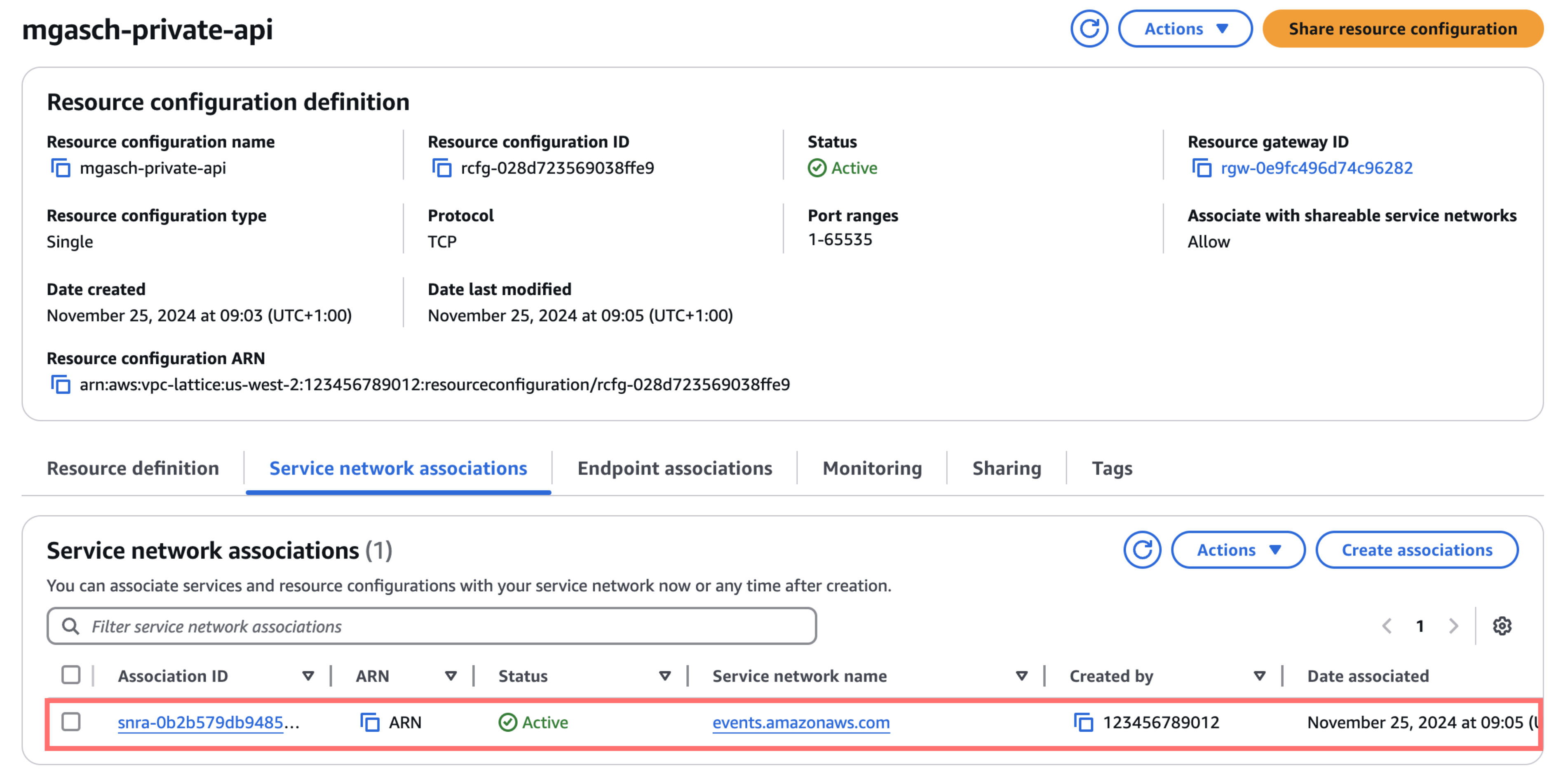
□ Principal ID	Principal type	Status
□ [redacted]	Account (External)	Associating

Security controls for providers

- Port ranges and association settings
- Fine-grained AWS RAM access controls
- End-to-end connectivity visibility

Security controls for providers

END-TO-END CONNECTIVITY VISIBILITY



mgasch-private-api

Resource configuration definition

Resource configuration name
mgasch-private-api

Resource configuration ID
rcfg-028d723569038ffe9

Status
✓ Active

Resource gateway ID
rgw-0e9fc496d74c96282

Resource configuration type
Single

Protocol
TCP

Port ranges
1-65535

Associate with shareable service networks
Allow

Date created
November 25, 2024 at 09:03 (UTC+1:00)

Date last modified
November 25, 2024 at 09:05 (UTC+1:00)

Resource configuration ARN
arn:aws:vpc-lattice:us-west-2:123456789012:resourceconfiguration/rcfg-028d723569038ffe9

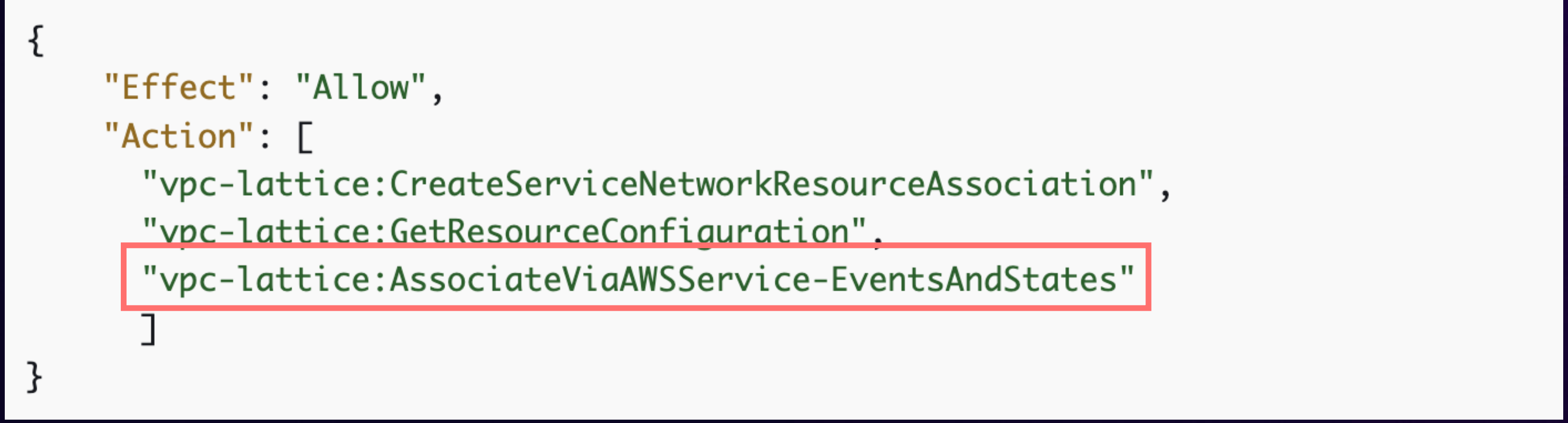
Service network associations (1)

You can associate services and resource configurations with your service network now or any time after creation.

□	Association ID	ARN	Status	Service network name	Created by	Date associated
□	snra-0b2b579db9485...	ARN	✓ Active	events.amazonaws.com	123456789012	November 25, 2024 at 09:05 (U

Security controls for providers

- Port ranges and association settings
- Fine-grained AWS RAM access controls
- End-to-end connectivity visibility
- Custom Resource Policies



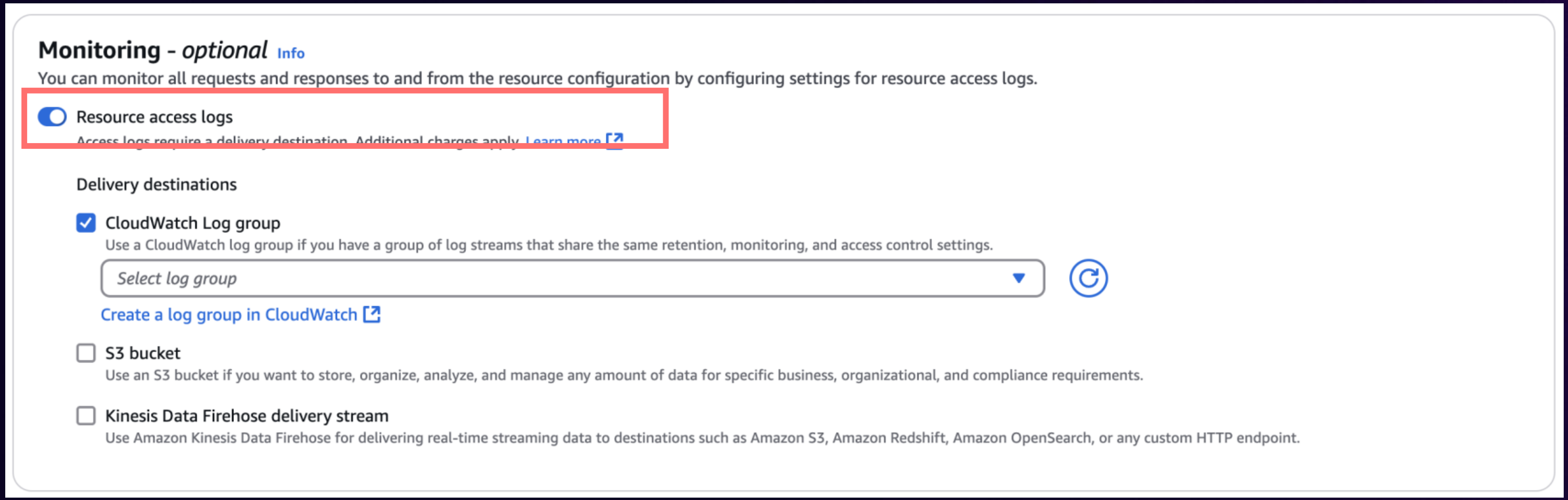
```
{
    "Effect": "Allow",
    "Action": [
      "vpc-lattice:CreateServiceNetworkResourceAssociation",
      "vpc-lattice:GetResourceConfiguration",
      "vpc-lattice:AssociateViaAWSService-EventsAndStates"
      ]
}
```

Security controls for providers

- Port ranges and association settings
- Fine-grained AWS RAM access controls
- End-to-end connectivity visibility
- Custom Resource Policies
- Access logs for Resource Configurations

Security controls for providers

ACCESS LOGS FOR RESOURCE CONFIGURATIONS



Monitoring - *optional* Info

You can monitor all requests and responses to and from the resource configuration by configuring settings for resource access logs.

● Resource access logs

Access logs require a delivery destination. Additional charges apply. Learn more

Delivery destinations

☑ CloudWatch Log group

Use a CloudWatch log group if you have a group of log streams that share the same retention, monitoring, and access control settings.

Select log group ▼

Create a log group in CloudWatch

□ S3 bucket

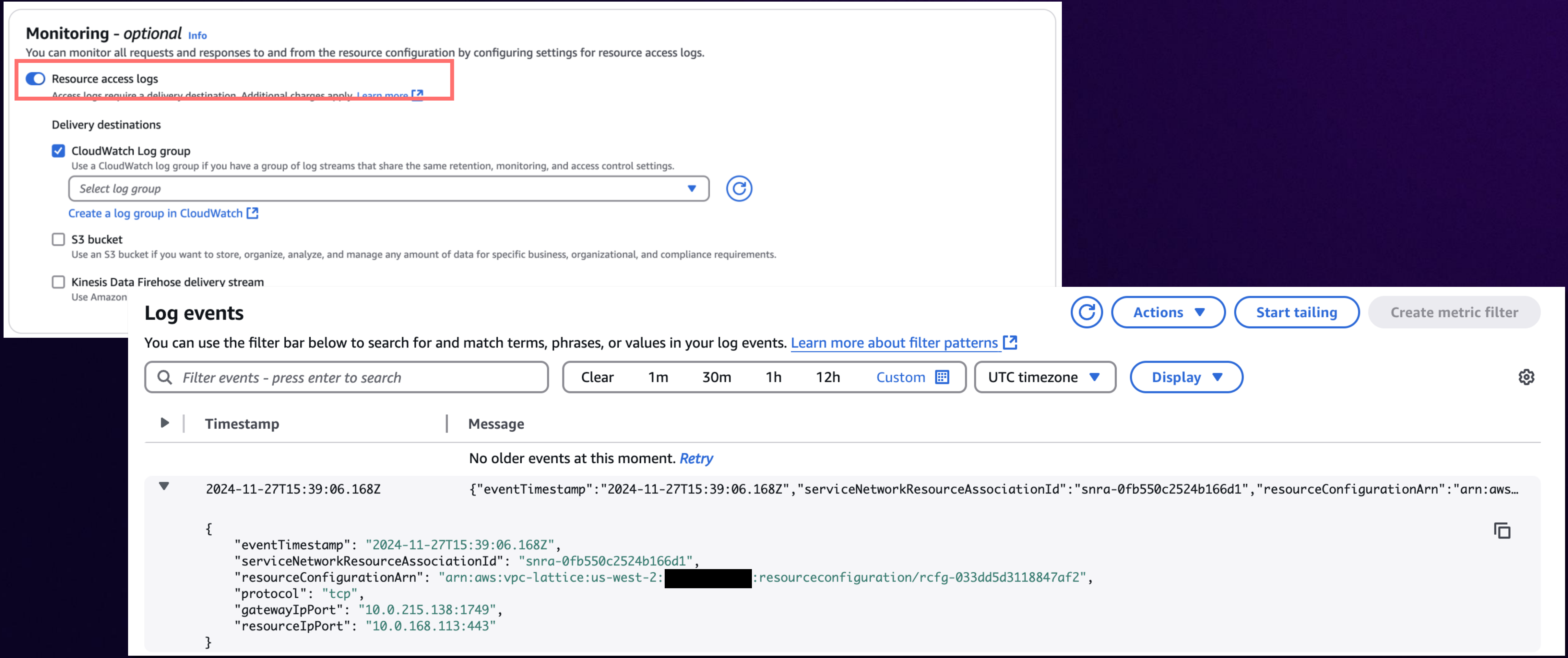
Use an S3 bucket if you want to store, organize, analyze, and manage any amount of data for specific business, organizational, and compliance requirements.

□ Kinesis Data Firehose delivery stream

Use Amazon Kinesis Data Firehose for delivering real-time streaming data to destinations such as Amazon S3, Amazon Redshift, Amazon OpenSearch, or any custom HTTP endpoint.

Security controls for providers

ACCESS LOGS FOR RESOURCE CONFIGURATIONS



Monitoring - *optional* Info

You can monitor all requests and responses to and from the resource configuration by configuring settings for resource access logs.

● Resource access logs

Access logs require a delivery destination. Additional charges apply. Learn more

Delivery destinations

☑ CloudWatch Log group

Use a CloudWatch log group if you have a group of log streams that share the same retention, monitoring, and access control settings.

Select log group ▼

Create a log group in CloudWatch

□ S3 bucket

Use an S3 bucket if you want to store, organize, analyze, and manage any amount of data for specific business, organizational, and compliance requirements.

□ Kinesis Data Firehose delivery stream

Use Amazon

Log events

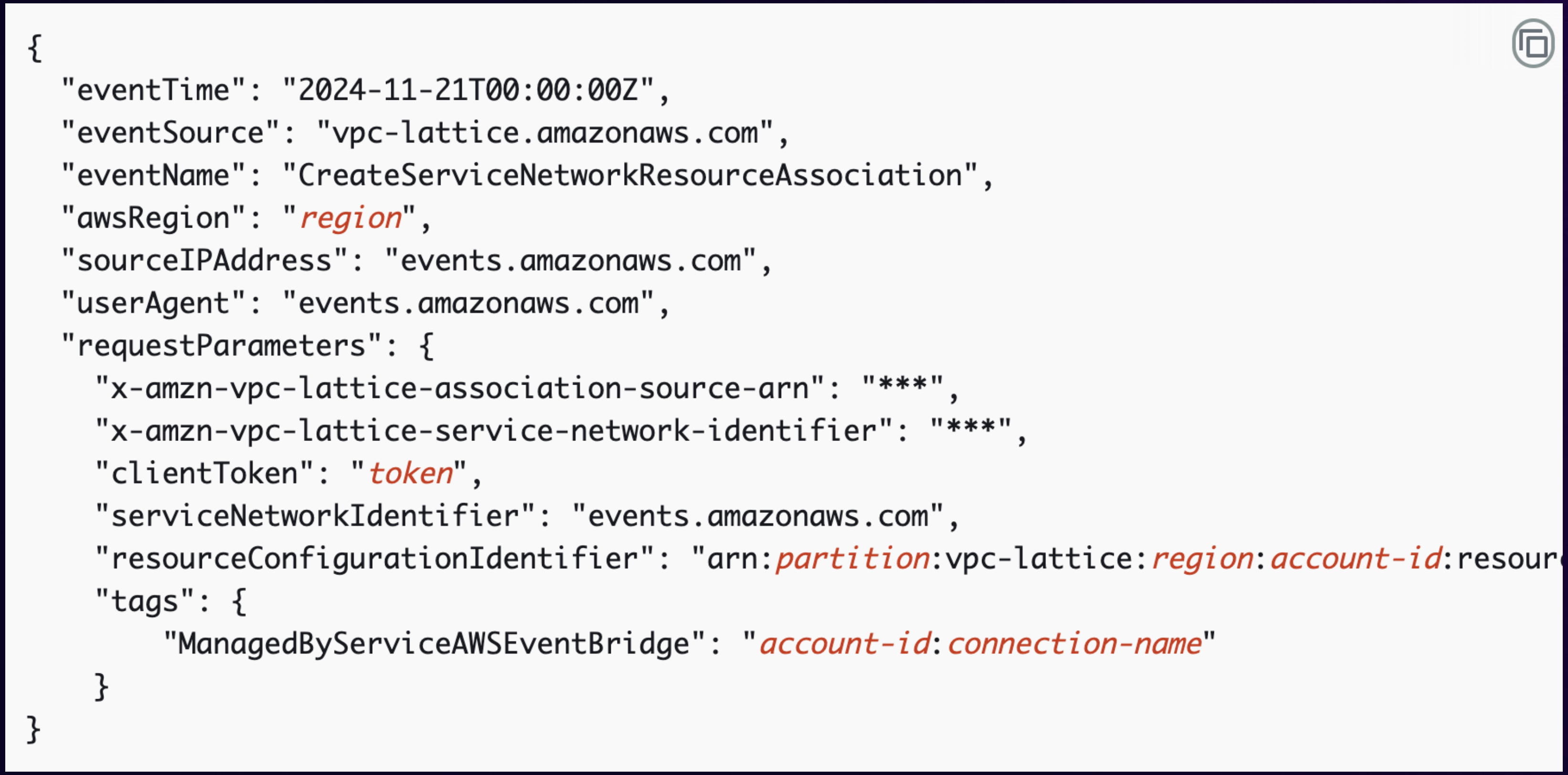
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

Timestamp	Message
	No older events at this moment. *Retry*
2024-11-27T15:39:06.168Z	{"eventTimestamp":"2024-11-27T15:39:06.168Z","serviceNetworkResourceAssociationId":"snra-0fb550c2524b166d1","resourceConfigurationArn":"arn:aws…

```
{
    "eventTimestamp": "2024-11-27T15:39:06.168Z",
    "serviceNetworkResourceAssociationId": "snra-0fb550c2524b166d1",
    "resourceConfigurationArn": "arn:aws:vpc-lattice:us-west-2:[redacted]:resourceconfiguration/rcfg-033dd5d3118847af2",
    "protocol": "tcp",
    "gatewayIpPort": "10.0.215.138:1749",
    "resourceIpPort": "10.0.168.113:443"
}
```

Security controls for providers

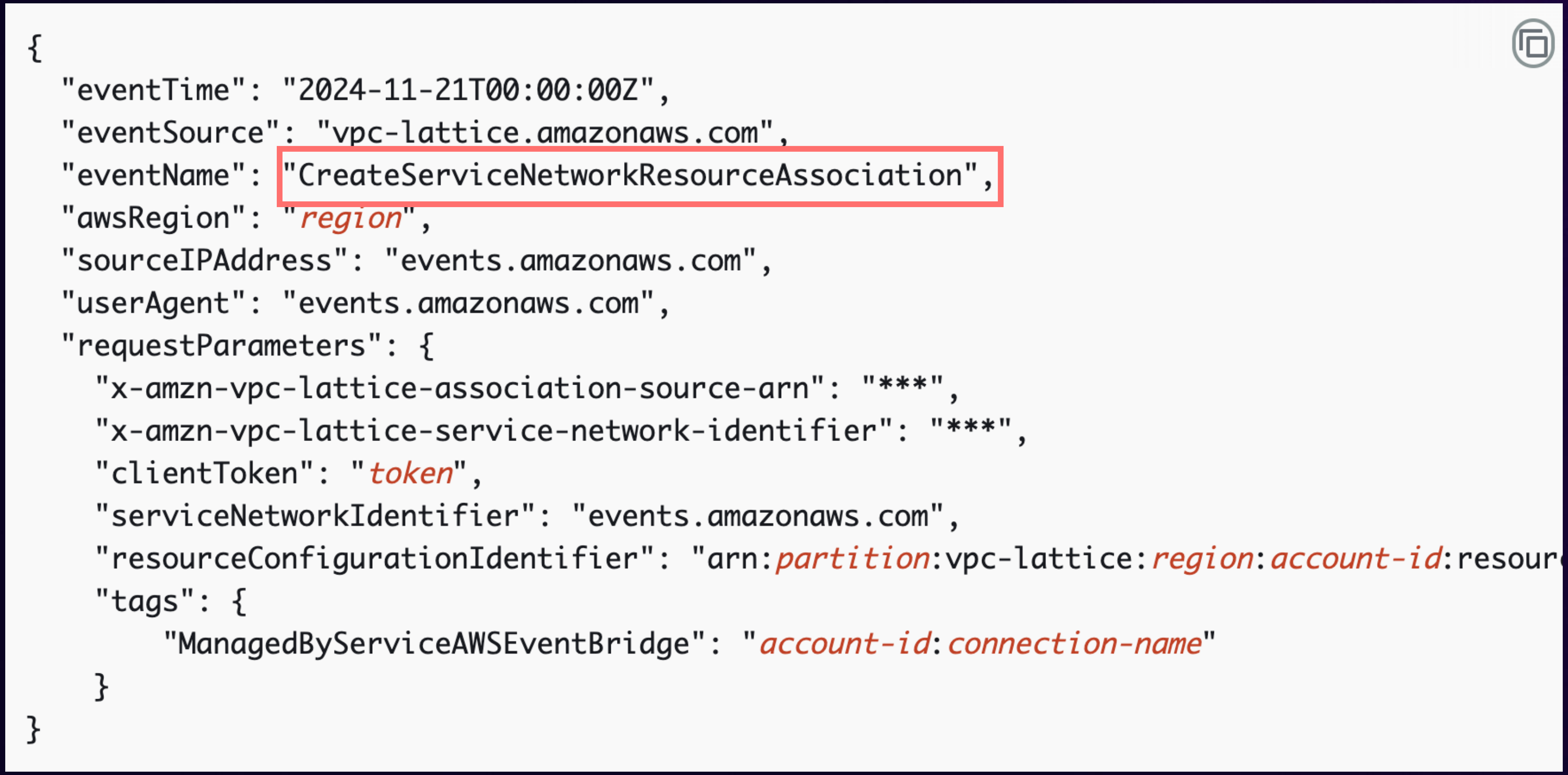
AWS CLOUDTRAIL LOGS



```
{
  "eventTime": "2024-11-21T00:00:00Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateServiceNetworkResourceAssociation",
  "awsRegion": "region",
  "sourceIPAddress": "events.amazonaws.com",
  "userAgent": "events.amazonaws.com",
  "requestParameters": {
    "x-amzn-vpc-lattice-association-source-arn": "***",
    "x-amzn-vpc-lattice-service-network-identifier": "***",
    "clientToken": "token",
    "serviceNetworkIdentifier": "events.amazonaws.com",
    "resourceConfigurationIdentifier": "arn:partition:vpc-lattice:region:account-id:resour
    "tags": {
        "ManagedByServiceAWSEventBridge": "account-id:connection-name"
    }
}
```

Security controls for providers

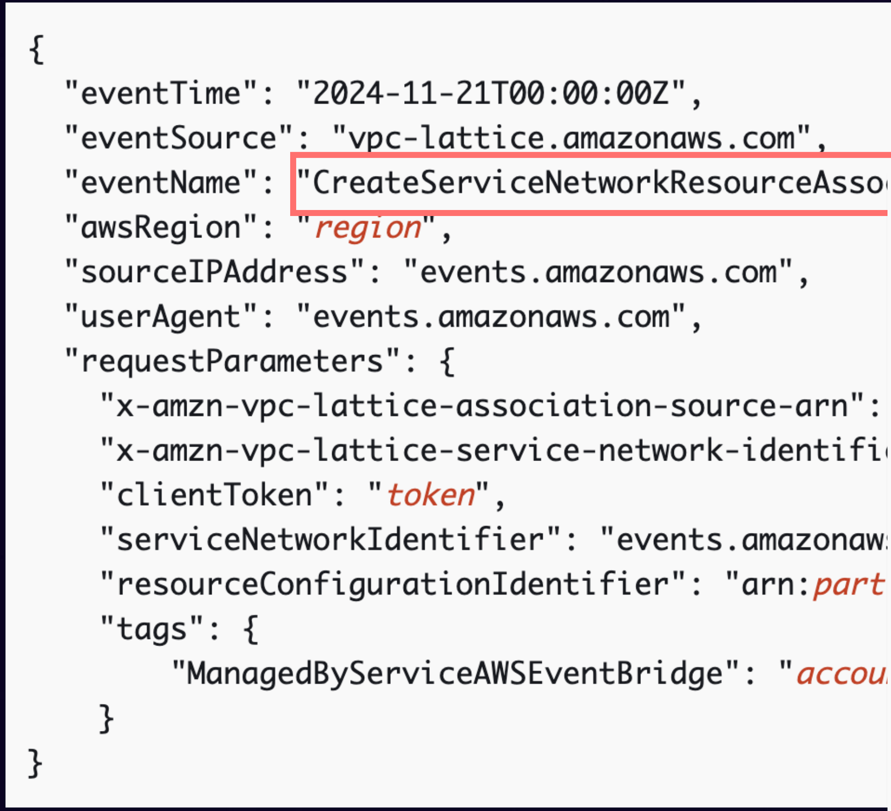
AWS CLOUDTRAIL LOGS



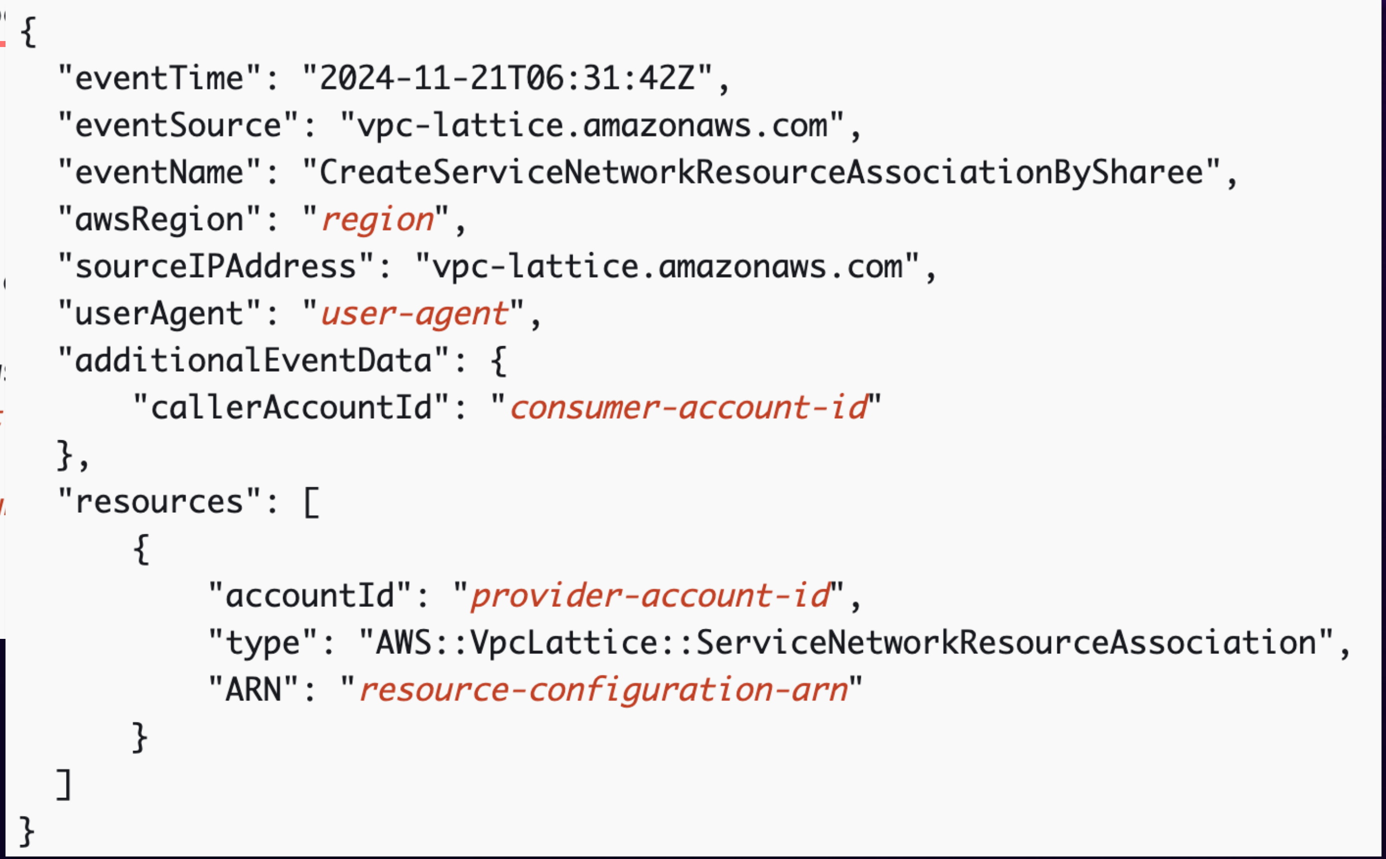
```
{
 "eventTime": "2024-11-21T00:00:00Z",
 "eventSource": "vpc-lattice.amazonaws.com",
 "eventName": "CreateServiceNetworkResourceAssociation",
 "awsRegion": "region",
 "sourceIPAddress": "events.amazonaws.com",
 "userAgent": "events.amazonaws.com",
 "requestParameters": {
  "x-amzn-vpc-lattice-association-source-arn": "***",
  "x-amzn-vpc-lattice-service-network-identifier": "***",
  "clientToken": "token",
  "serviceNetworkIdentifier": "events.amazonaws.com",
  "resourceConfigurationIdentifier": "arn:partition:vpc-lattice:region:account-id:resour
  "tags": {
    "ManagedByServiceAWSEventBridge": "account-id:connection-name"
  }
}
```

Security controls for providers

AWS CLOUDTRAIL LOGS



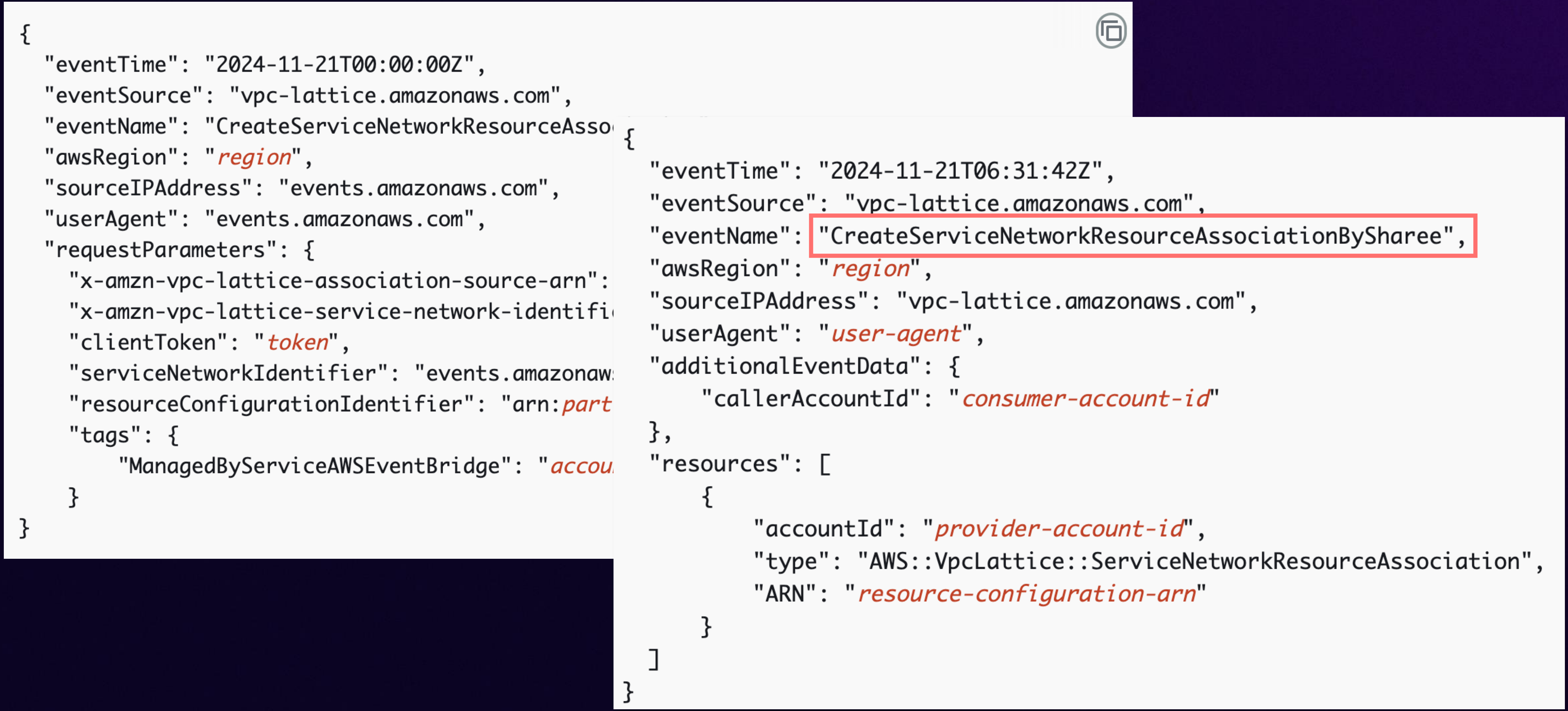
```
{
  "eventTime": "2024-11-21T00:00:00Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateServiceNetworkResourceAsso
  "awsRegion": "region",
  "sourceIPAddress": "events.amazonaws.com",
  "userAgent": "events.amazonaws.com",
  "requestParameters": {
    "x-amzn-vpc-lattice-association-source-arn":
    "x-amzn-vpc-lattice-service-network-identifi
    "clientToken": "token",
    "serviceNetworkIdentifier": "events.amazonaw
    "resourceConfigurationIdentifier": "arn:part
    "tags": {
        "ManagedByServiceAWSEventBridge": "accou
    }
}
```



```
{
  "eventTime": "2024-11-21T06:31:42Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateServiceNetworkResourceAssociationBySharee",
  "awsRegion": "region",
  "sourceIPAddress": "vpc-lattice.amazonaws.com",
  "userAgent": "user-agent",
  "additionalEventData": {
      "callerAccountId": "consumer-account-id"
  },
  "resources": [
      {
          "accountId": "provider-account-id",
          "type": "AWS::VpcLattice::ServiceNetworkResourceAssociation",
          "ARN": "resource-configuration-arn"
      }
  ]
}
```

Security controls for providers

AWS CLOUDTRAIL LOGS



```
{
  "eventTime": "2024-11-21T00:00:00Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateServiceNetworkResourceAsso
  "awsRegion": "region",
  "sourceIPAddress": "events.amazonaws.com",
  "userAgent": "events.amazonaws.com",
  "requestParameters": {
    "x-amzn-vpc-lattice-association-source-arn":
    "x-amzn-vpc-lattice-service-network-identifi
    "clientToken": "token",
    "serviceNetworkIdentifier": "events.amazonaw
    "resourceConfigurationIdentifier": "arn:part
    "tags": {
        "ManagedByServiceAWSEventBridge": "accou
    }
}
```

```
{
  "eventTime": "2024-11-21T06:31:42Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateServiceNetworkResourceAssociationBySharee",
  "awsRegion": "region",
  "sourceIPAddress": "vpc-lattice.amazonaws.com",
  "userAgent": "user-agent",
  "additionalEventData": {
      "callerAccountId": "consumer-account-id"
  },
  "resources": [
      {
          "accountId": "provider-account-id",
          "type": "AWS::VpcLattice::ServiceNetworkResourceAssociation",
          "ARN": "resource-configuration-arn"
      }
  ]
}
```

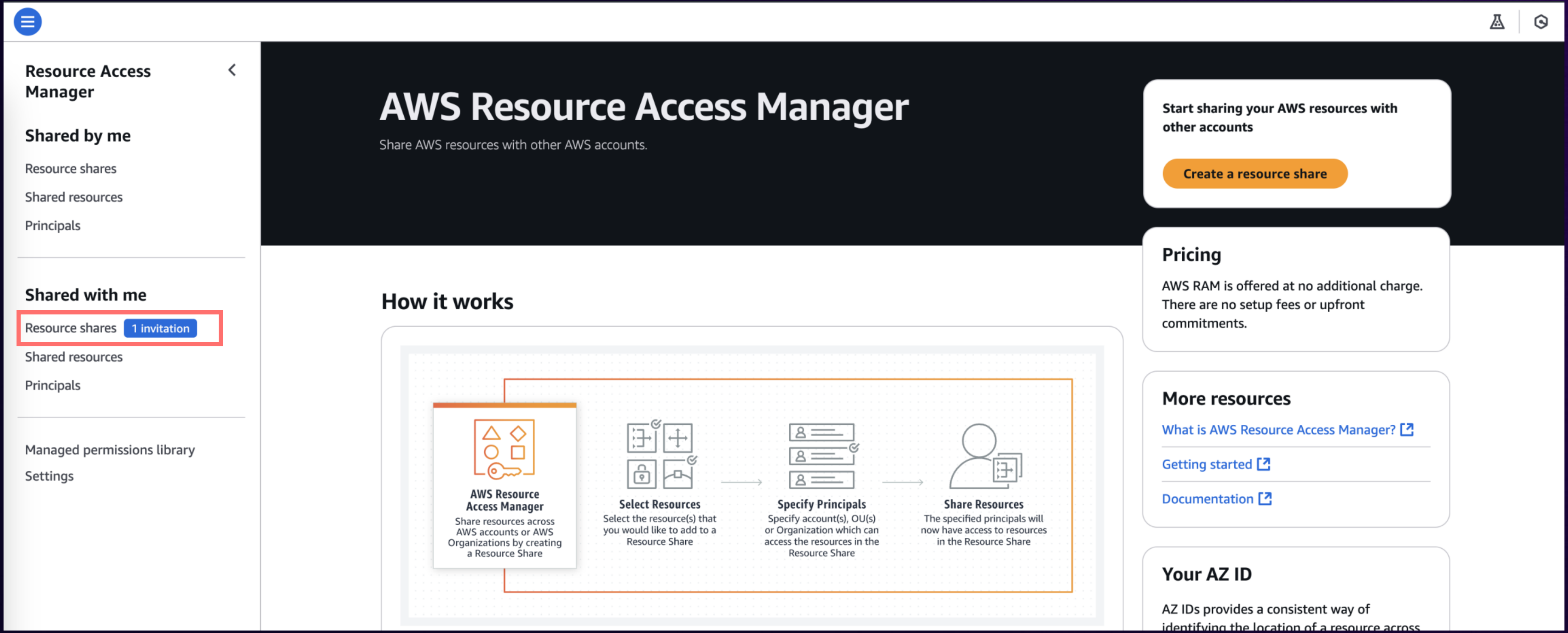
Security Controls for Consumers

Security controls for consumers

- Explicit acceptance of resource shares
  - Unless AWS Organizations are used

Security controls for consumers

EXPLICIT ACCEPTANCE OF RESOURCE SHARES



Resource Access Manager

Shared by me

- Resource shares
- Shared resources
- Principals

Shared with me

- Resource shares 1 invitation
- Shared resources
- Principals

Managed permissions library

Settings

AWS Resource Access Manager

Share AWS resources with other AWS accounts.

How it works

AWS Resource Access Manager
Share resources across AWS accounts or AWS Organizations by creating a Resource Share

Select Resources
Select the resource(s) that you would like to add to a Resource Share

Specify Principals
Specify account(s), OU(s) or Organization which can access the resources in the Resource Share

Share Resources
The specified principals will now have access to resources in the Resource Share

Start sharing your AWS resources with other accounts

Create a resource share

Pricing

AWS RAM is offered at no additional charge. There are no setup fees or upfront commitments.

More resources

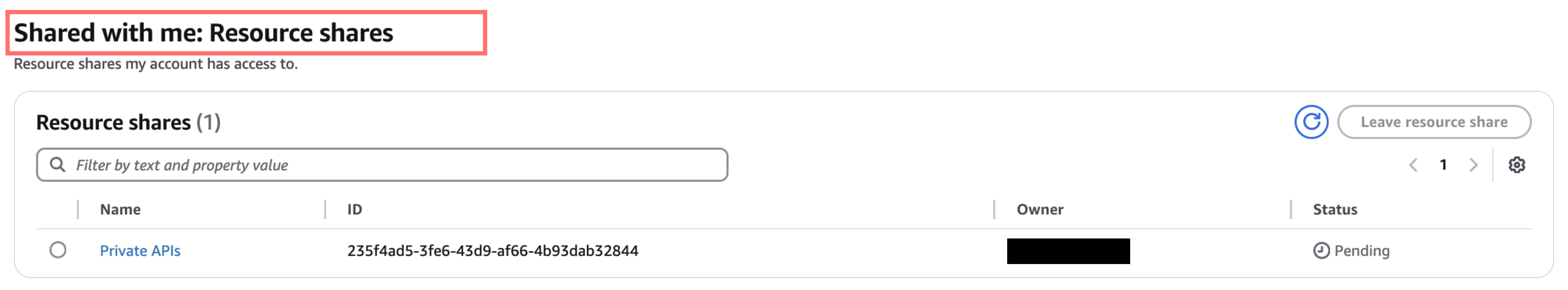
- What is AWS Resource Access Manager?
- Getting started
- Documentation

Your AZ ID

AZ IDs provides a consistent way of identifying the location of a resource across

Security controls for consumers

EXPLICIT ACCEPTANCE OF RESOURCE SHARES



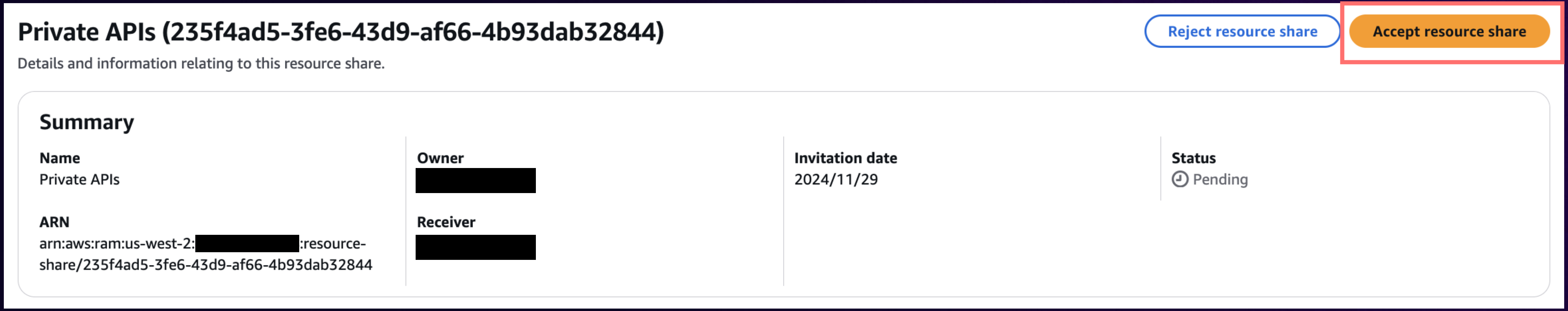
Shared with me: Resource shares

Resource shares my account has access to.

	Name	ID	Owner	Status
○	Private APIs	235f4ad5-3fe6-43d9-af66-4b93dab32844	[redacted]	Pending

Security controls for consumers

EXPLICIT ACCEPTANCE OF RESOURCE SHARES



Private APIs (235f4ad5-3fe6-43d9-af66-4b93dab32844)

Details and information relating to this resource share.

Summary

Name
Private APIs

ARN
arn:aws:ram:us-west-2:[redacted]:resource-share/235f4ad5-3fe6-43d9-af66-4b93dab32844

Owner
[redacted]

Receiver
[redacted]

Invitation date
2024/11/29

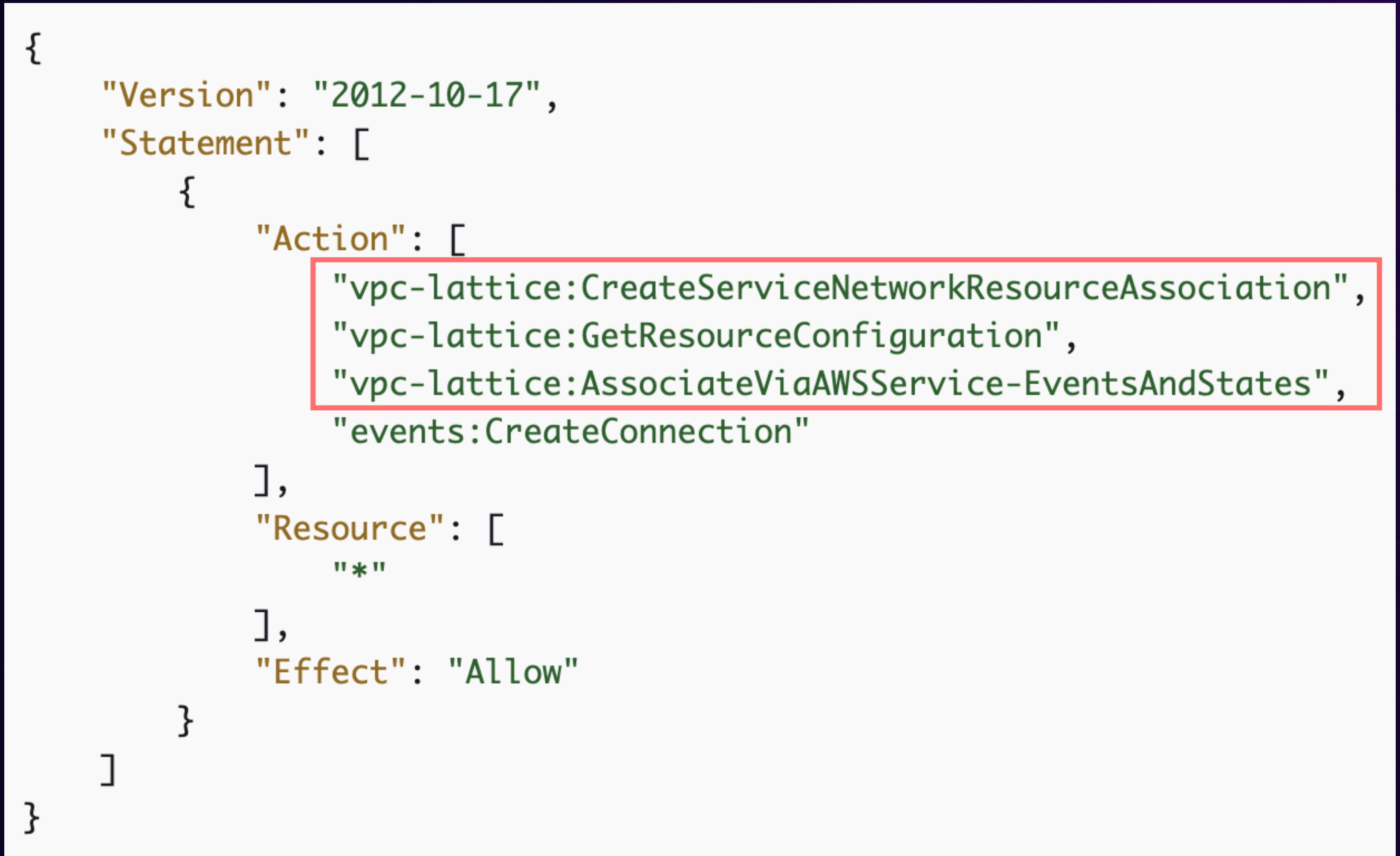
Status
Pending

Security controls for consumers

- Explicit acceptance of resource shares
  - Unless AWS Organizations are used
- EventBridge permissions for private connectivity
  - API destinations (unchanged)
  - Additional permissions for private connections

Security controls for consumers

EVENTBRIDGE PERMISSIONS FOR PRIVATE CONNECTIVITY



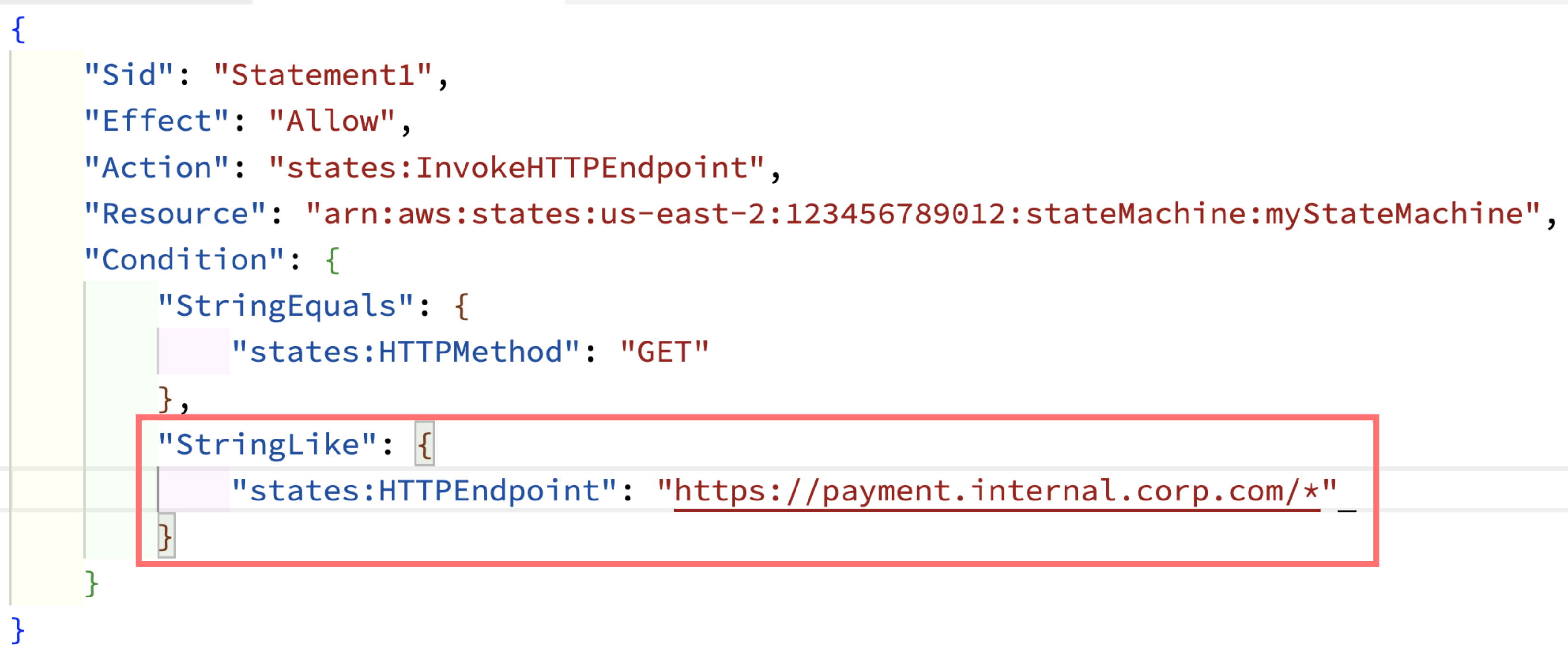
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "vpc-lattice:CreateServiceNetworkResourceAssociation",
                "vpc-lattice:GetResourceConfiguration",
                "vpc-lattice:AssociateViaAWSService-EventsAndStates",
                "events:CreateConnection"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Security controls for consumers

- Explicit acceptance of resource shares
  - Unless AWS Organizations are used
- EventBridge permissions for private connectivity
  - API destinations (unchanged)
  - Additional permissions for private connections
- Step Functions permissions for private connectivity
  - RetrieveConnectionCredentials (unchanged)
  - Secrets Manager Get/Describe (unchanged)
  - Flexible Conditions on API Endpoints (unchanged)

Security controls for consumers

STEP FUNCTIONS PERMISSIONS FOR PRIVATE CONNECTIVITY



```
{
    "Sid": "Statement1",
    "Effect": "Allow",
    "Action": "states:InvokeHTTPEndpoint",
    "Resource": "arn:aws:states:us-east-2:123456789012:stateMachine:myStateMachine",
    "Condition": {
        "StringEquals": {
            "states:HTTPMethod": "GET"
        },
        "StringLike": {
            "states:HTTPEndpoint": "https://payment.internal.corp.com/*"
        }
    }
}
```

Reliable integration

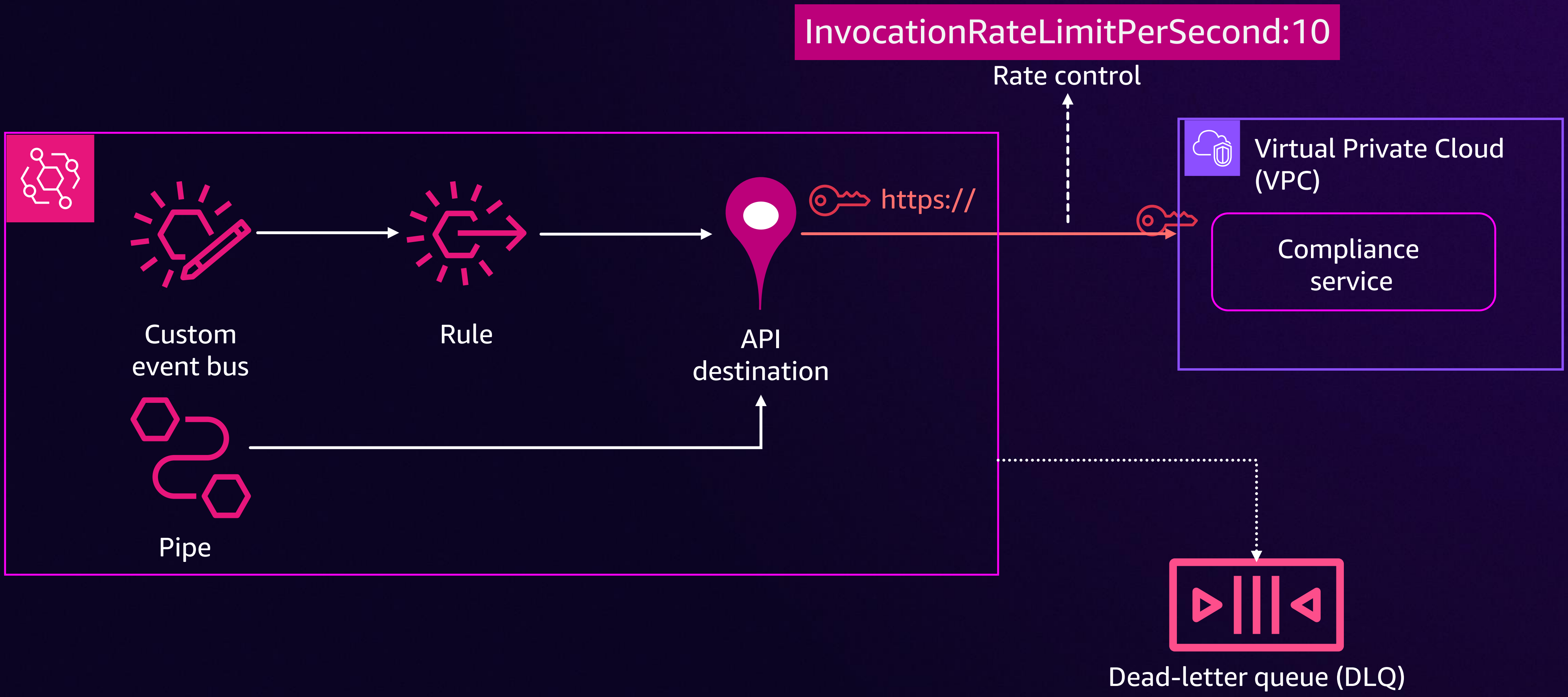
Private APIs integration tenets

Simple developer experience

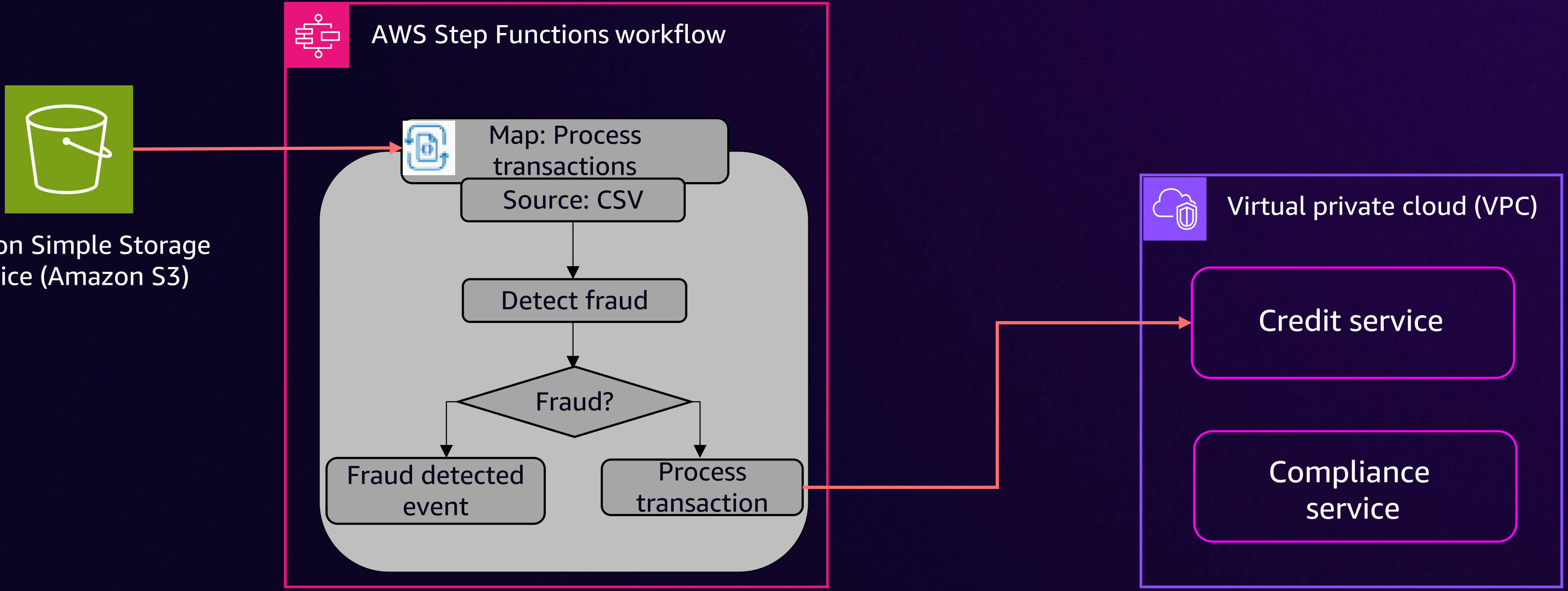
Secure by design

Reliable integration

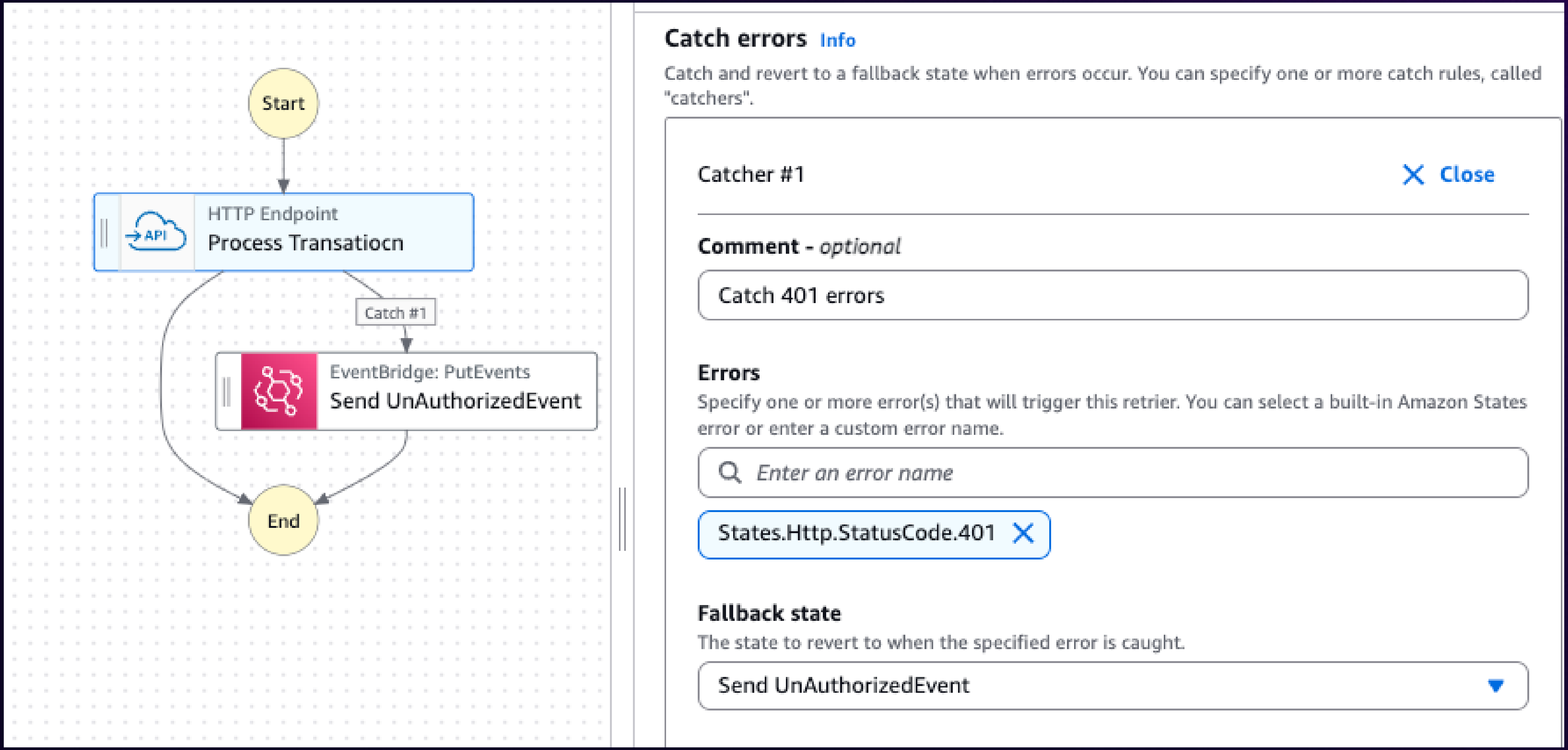
Rate limit and error handling



Resiliency with Step Functions


AWS Step Functions workflow
Map: Process transactions
Source: CSV
Detect fraud
Fraud?
Fraud detected event
Process transaction
Amazon Simple Storage Service (Amazon S3)
Virtual private cloud (VPC)
Credit service
Compliance service

Resiliency with Step Functions - Catch errors



Catch errors Info

Catch and revert to a fallback state when errors occur. You can specify one or more catch rules, called "catchers".

Catcher #1 ✕ Close

Comment - *optional*

Catch 401 errors

Errors

Specify one or more error(s) that will trigger this retrier. You can select a built-in Amazon States error or enter a custom error name.

Enter an error name

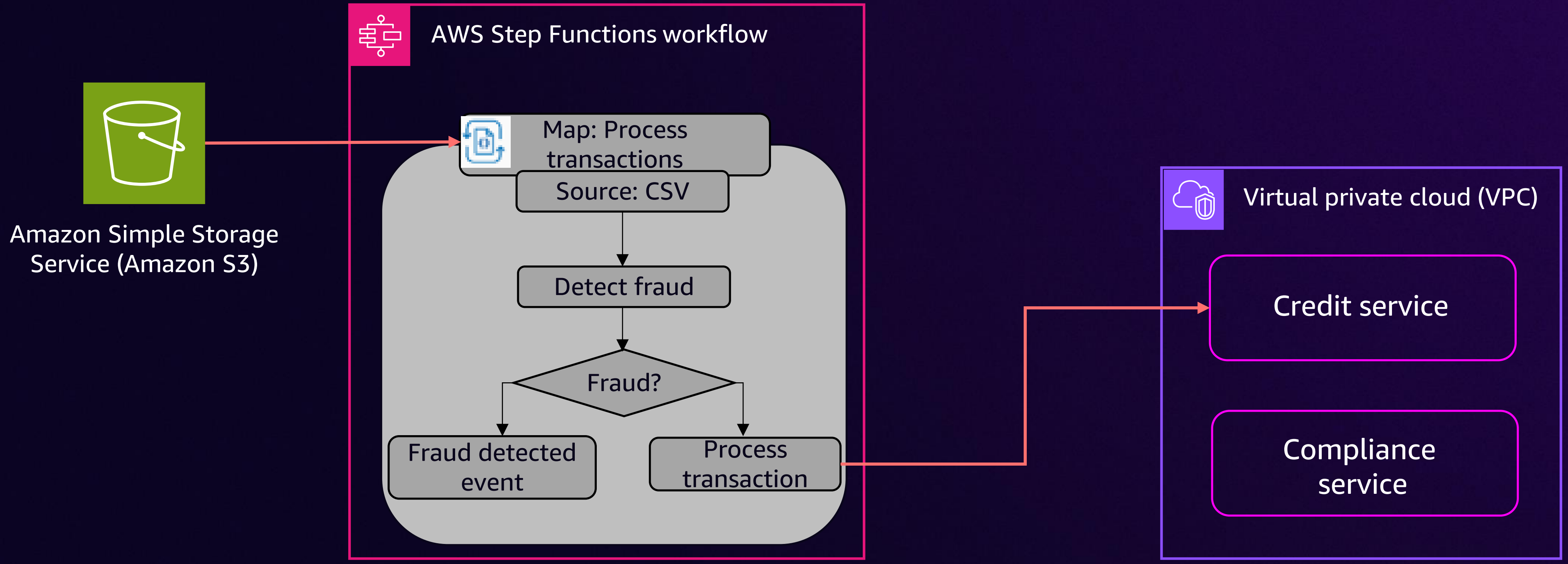
States.Http.StatusCode.401 ✕

Fallback state

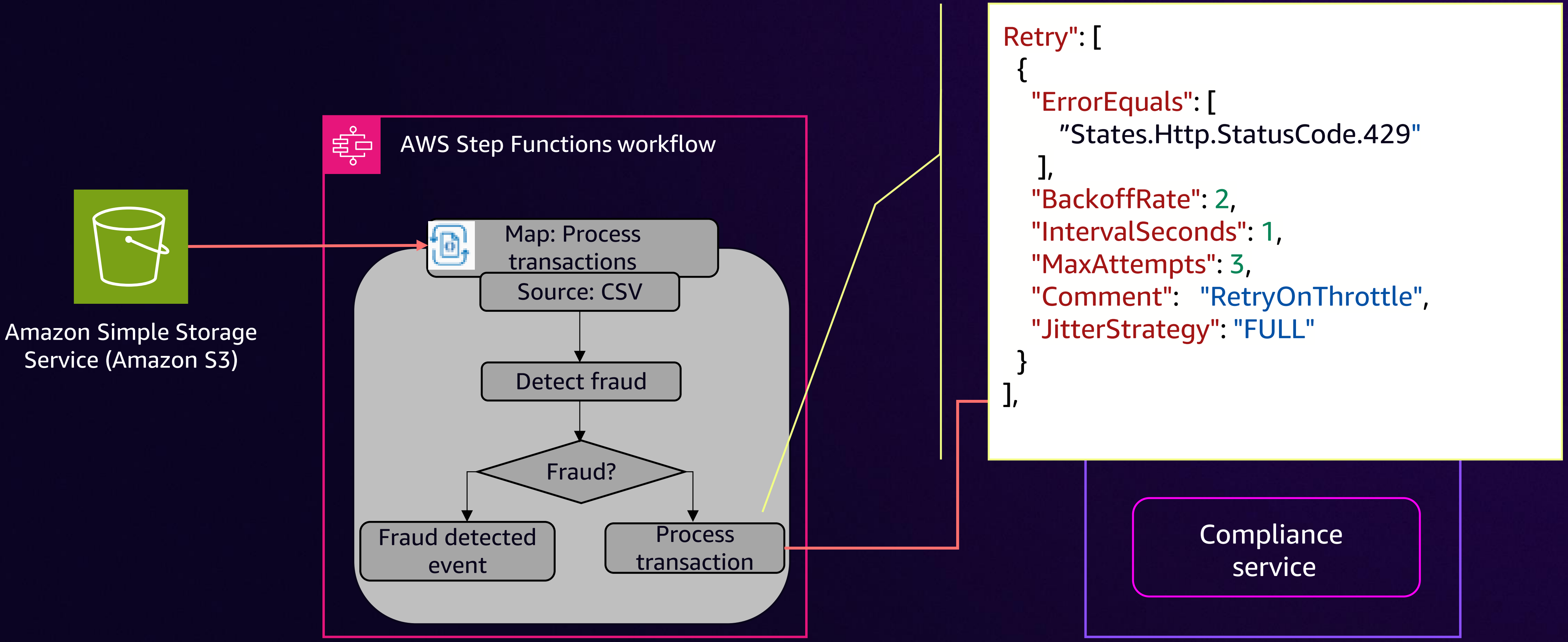
The state to revert to when the specified error is caught.

Send UnAuthorizedEvent ▼

Resiliency with Step Functions - Retries


Amazon Simple Storage Service (Amazon S3)
AWS Step Functions workflow
Map: Process transactions
Source: CSV
Detect fraud
Fraud?
Fraud detected event
Process transaction
Virtual private cloud (VPC)
Credit service
Compliance service

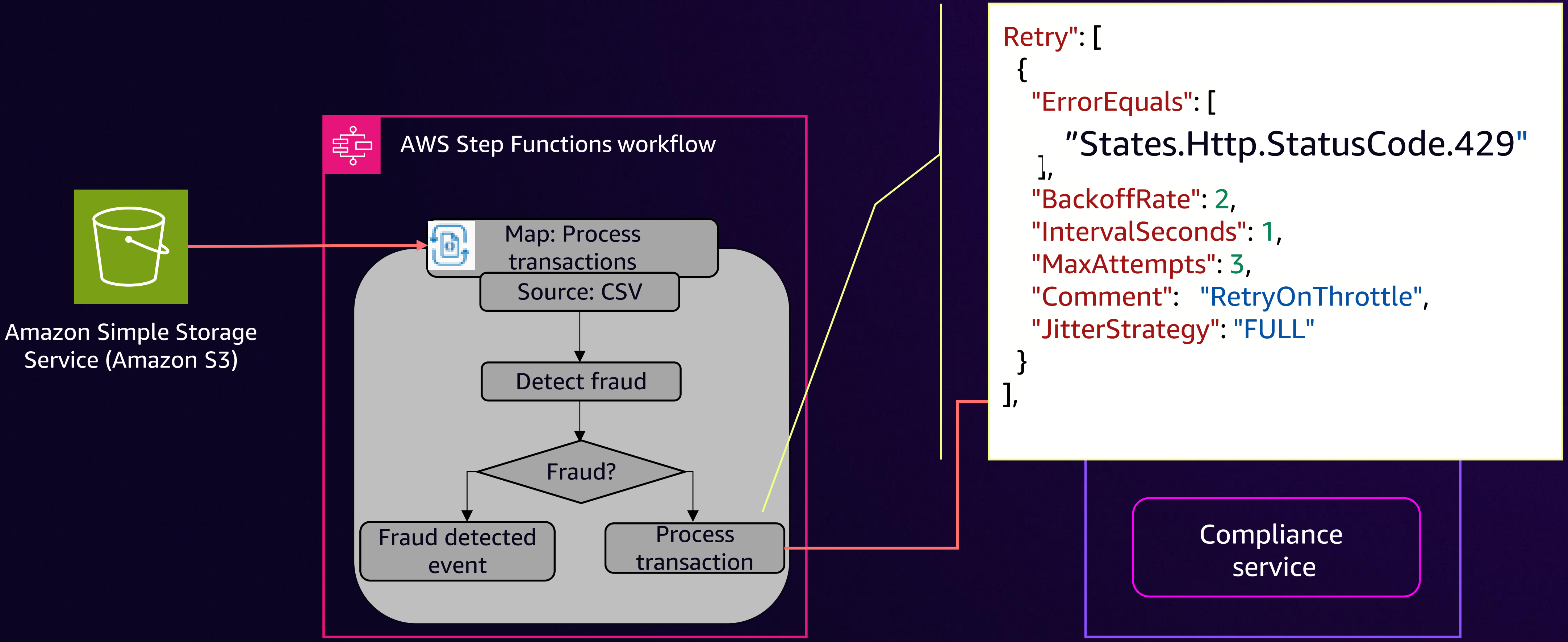
Resiliency with Step Functions - Retries



Amazon Simple Storage Service (Amazon S3)
AWS Step Functions workflow
Map: Process transactions
Source: CSV
Detect fraud
Fraud?
Fraud detected event
Process transaction
Compliance service

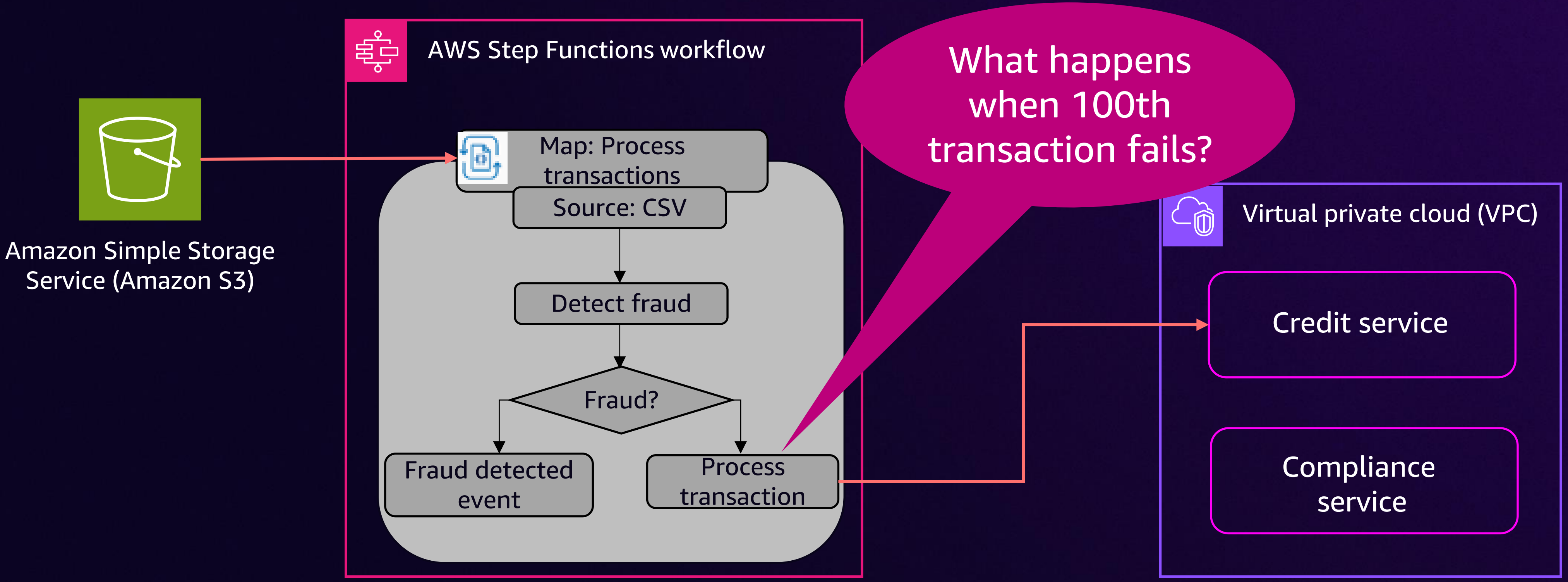
```
Retry": [
 {
  "ErrorEquals": [
     ”States.Http.StatusCode.429"
   ],
  "BackoffRate": 2,
  "IntervalSeconds": 1,
  "MaxAttempts": 3,
  "Comment":   "RetryOnThrottle",
  "JitterStrategy": "FULL"
 }
],
```

Resiliency with Step Functions - Retries


AWS Step Functions workflow
Amazon Simple Storage Service (Amazon S3)
Map: Process transactions
Source: CSV
Detect fraud
Fraud?
Fraud detected event
Process transaction
Compliance service

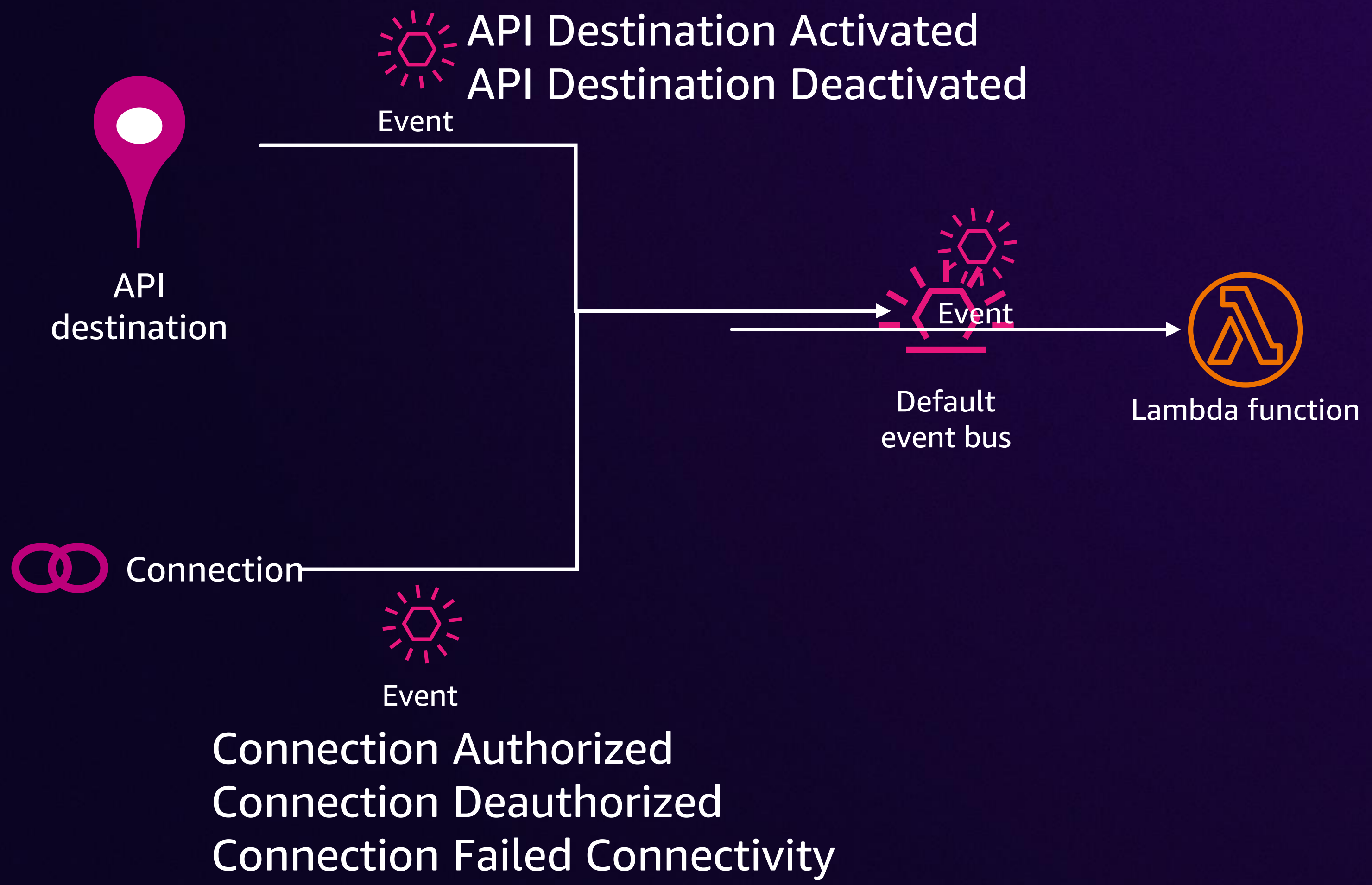
```
Retry": [
 {
  "ErrorEquals": [
     "States.Http.StatusCode.429"
   ],
  "BackoffRate": 2,
  "IntervalSeconds": 1,
  "MaxAttempts": 3,
  "Comment":  "RetryOnThrottle",
  "JitterStrategy": "FULL"
 }
],
```

Resiliency with Step Functions - Redrive


Amazon Simple Storage Service (Amazon S3)
AWS Step Functions workflow
Map: Process transactions
Source: CSV
Detect fraud
Fraud?
Fraud detected event
Process transaction
Virtual private cloud (VPC)
Credit service
Compliance service

What happens when 100th transaction fails?

Automation with service events

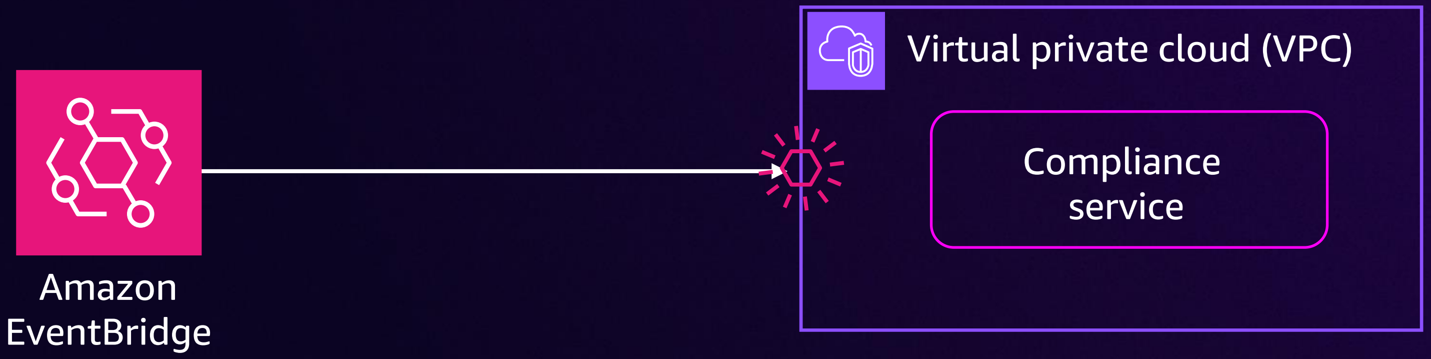


API Destination Activated
API Destination Deactivated

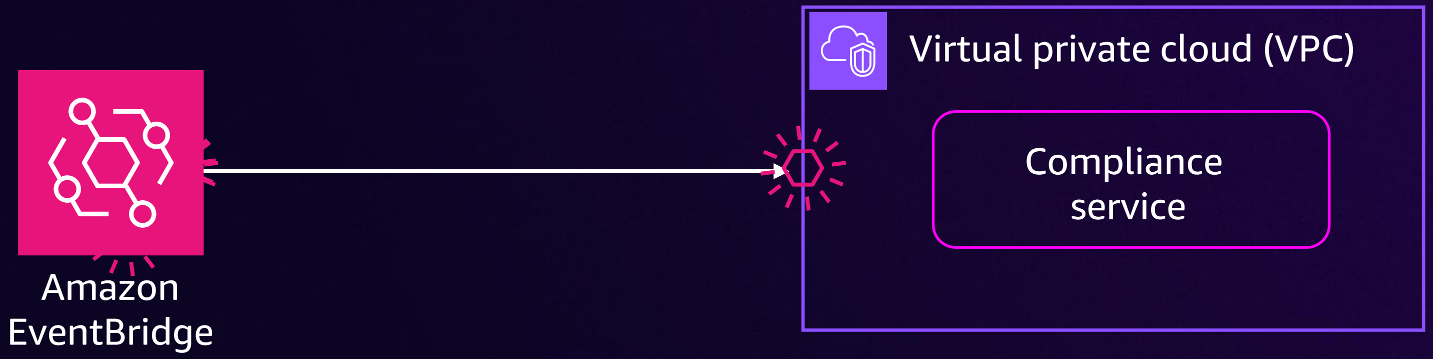
Connection Authorized
Connection Deauthorized
Connection Failed Connectivity

Best practices and considerations

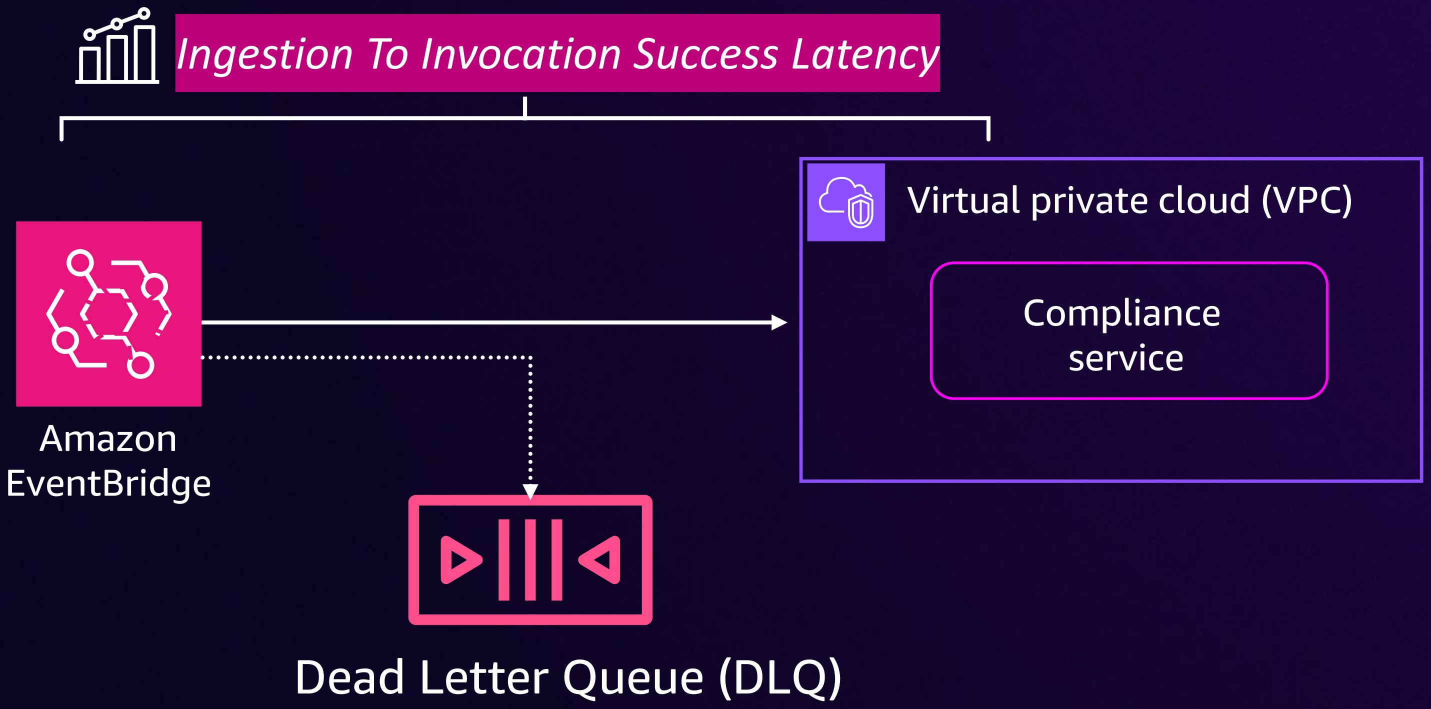
Rate control and DLQ



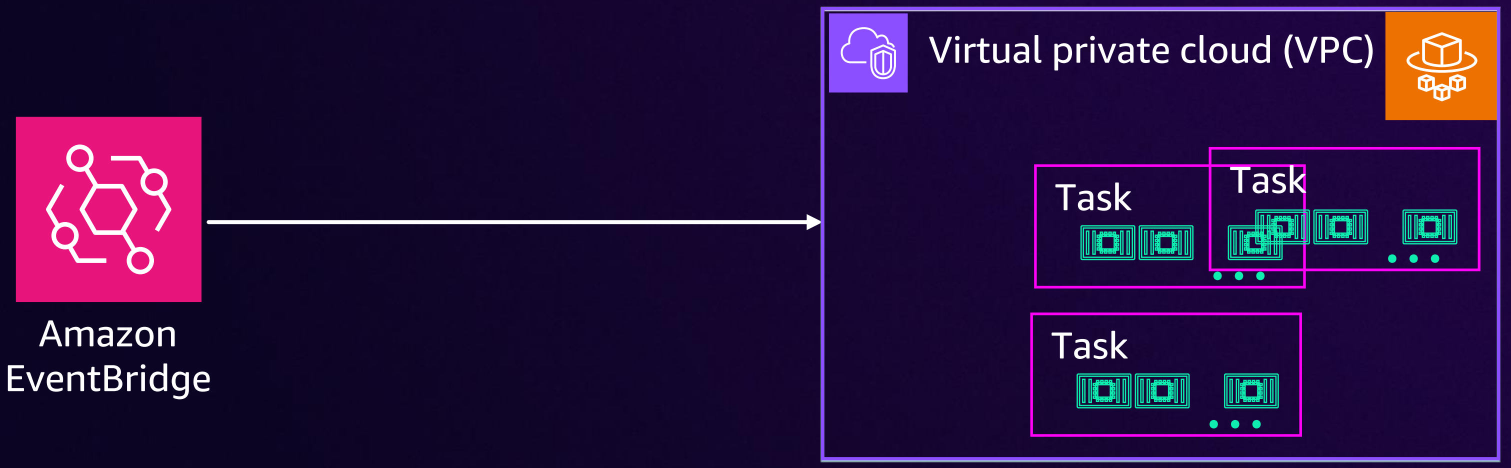
Rate control and DLQ



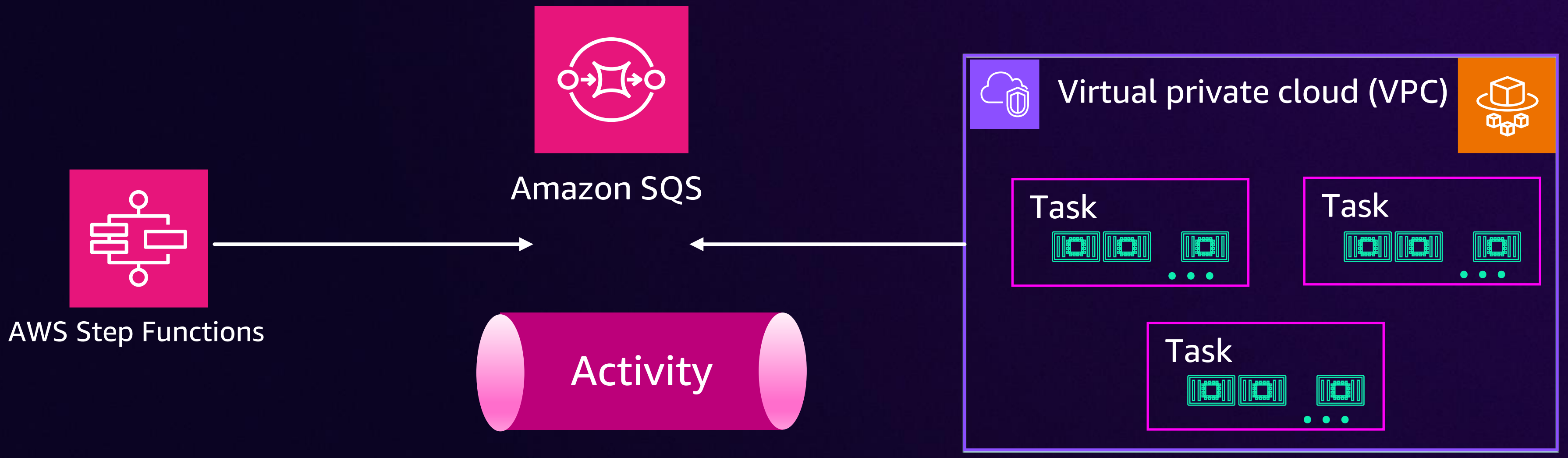
Rate control and DLQ


Ingestion To Invocation Success Latency
Virtual private cloud (VPC)
Compliance service
Amazon EventBridge
Dead Letter Queue (DLQ)

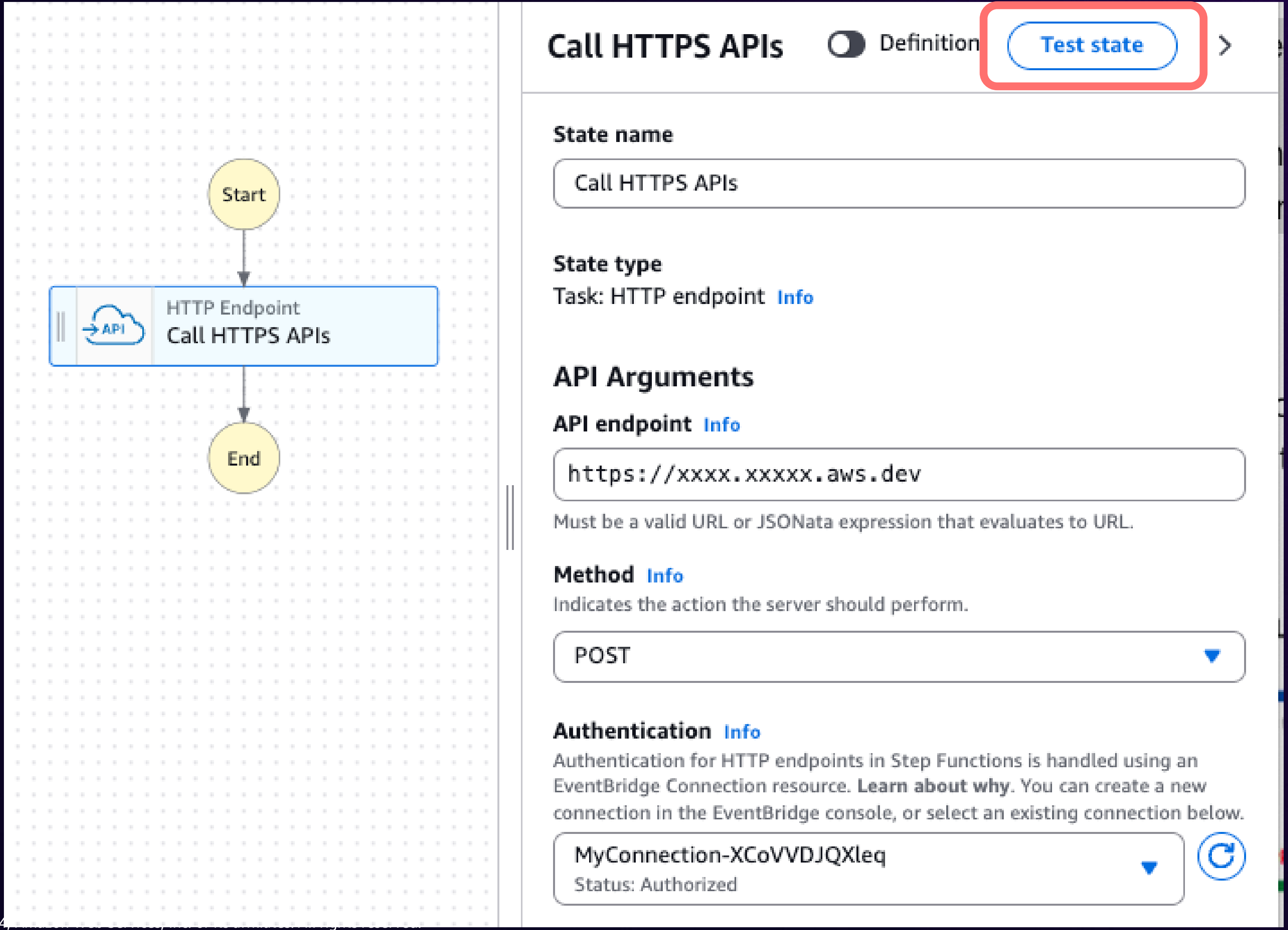
Scale consumers to meet the demand



Scaling containers to meet the demand



Use Test state to test API connections



Call HTTPS APIs

State name

Call HTTPS APIs

State type

Task: HTTP endpoint

API Arguments

API endpoint

```
https://xxxx.xxxxx.aws.dev
```

Must be a valid URL or JSONata expression that evaluates to URL.

Method

Indicates the action the server should perform.

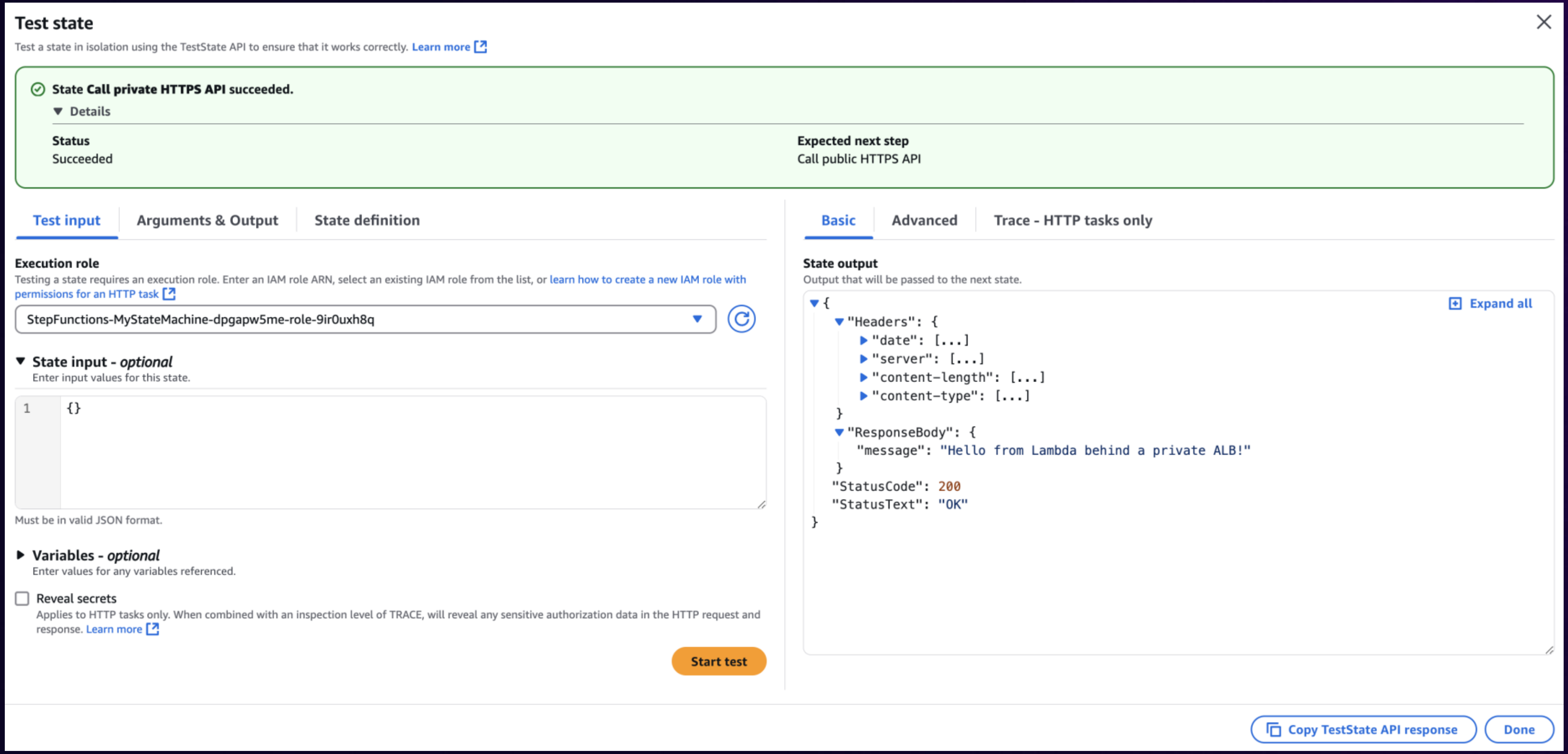
POST

Authentication

Authentication for HTTP endpoints in Step Functions is handled using an EventBridge Connection resource. **Learn about why**. You can create a new connection in the EventBridge console, or select an existing connection below.

MyConnection-XCoVVDJQXleq
Status: Authorized

Use Test state to test API connections



Test state

Test a state in isolation using the TestState API to ensure that it works correctly. Learn more

State **Call private HTTPS API** succeeded.

▼ Details

Status
Succeeded

Expected next step
Call public HTTPS API

Execution role

Testing a state requires an execution role. Enter an IAM role ARN, select an existing IAM role from the list, or learn how to create a new IAM role with permissions for an HTTP task

StepFunctions-MyStateMachine-dpgapw5me-role-9ir0uxh8q

▼ State input - *optional*
Enter input values for this state.

```
{}
```

Must be in valid JSON format.

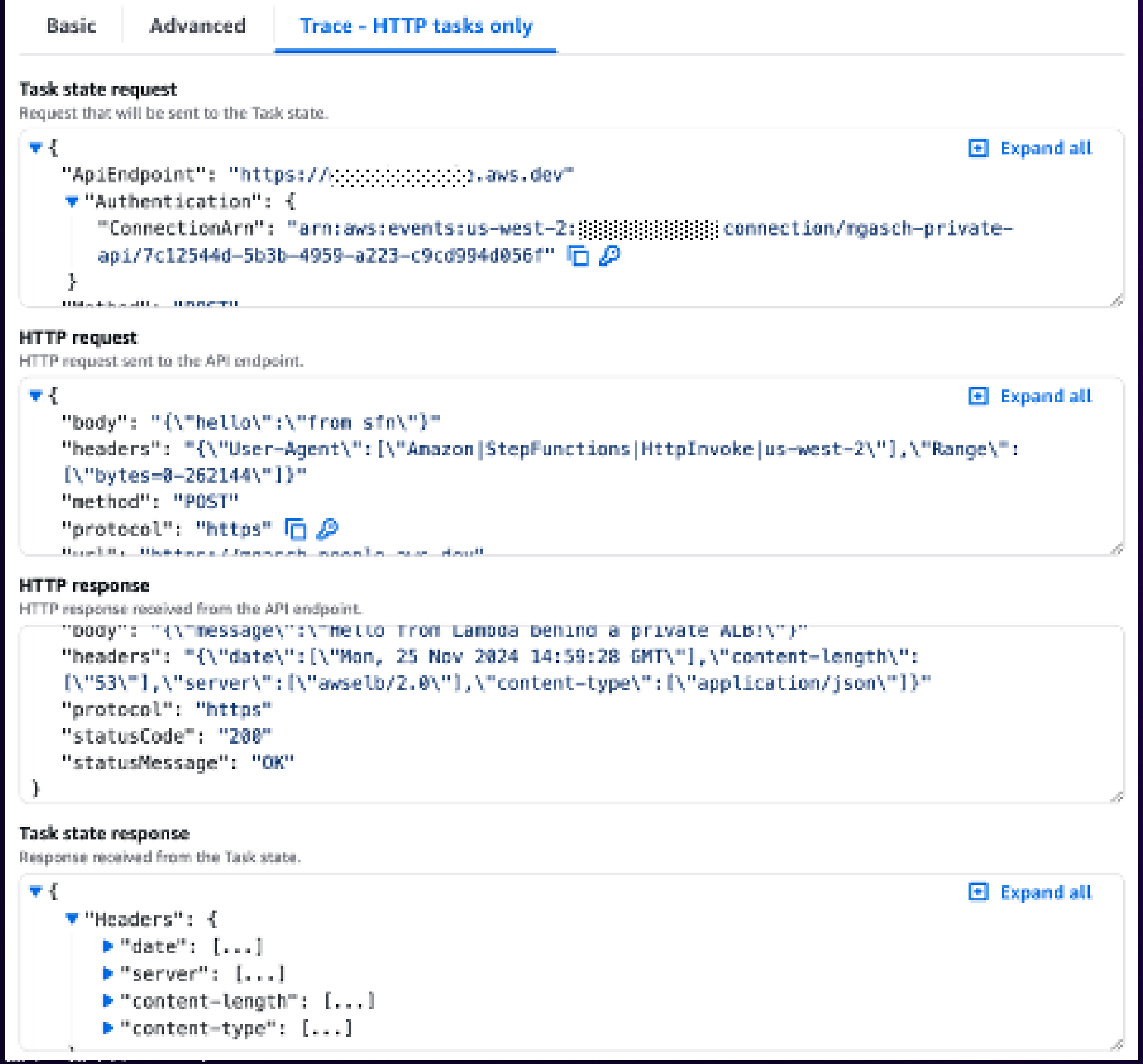
▶ Variables - *optional*
Enter values for any variables referenced.

□ Reveal secrets
Applies to HTTP tasks only. When combined with an inspection level of TRACE, will reveal any sensitive authorization data in the HTTP request and response. Learn more

State output
Output that will be passed to the next state.

```
▼{
  ▼"Headers": {
    ▶"date": [...]
    ▶"server": [...]
    ▶"content-length": [...]
    ▶"content-type": [...]
  }
  ▼"ResponseBody": {
    "message": "Hello from Lambda behind a private ALB!"
  }
  "StatusCode": 200
  "StatusText": "OK"
}
```

Use Test state to test API connections



Task state request

Request that will be sent to the Task state.

```
{
  "ApiEndpoint": "https://[redacted].aws.dev"
  "Authentication": {
    "ConnectionArn": "arn:aws:events:us-west-2:[redacted]connection/mgasch-private-
    api/7c12544d-5b3b-4959-a223-c9cd994d056f"
  }
```

HTTP request

HTTP request sent to the API endpoint.

```
{
  "body": "{\"hello\":\"from sfn\"}"
  "headers": "{\"User-Agent\":[\"Amazon|StepFunctions|HttpInvoke|us-west-2\"],\"Range\":
  [\"bytes=0-262144\"]}"
  "method": "POST"
  "protocol": "https"
```

HTTP response

HTTP response received from the API endpoint.

```
  "body": "{\"message\":\"Hello from Lambda behind a private ALB!\"}"
  "headers": "{\"date\":[\"Mon, 25 Nov 2024 14:59:28 GMT\"],\"content-length\":
  [\"53\"],\"server\":[\"awselb/2.0\"],\"content-type\":[\"application/json\"]}"
  "protocol": "https"
  "statusCode": "200"
  "statusMessage": "OK"
}
```

Task state response

Response received from the Task state.

```
{
  "Headers": {
    "date": [...]
    "server": [...]
    "content-length": [...]
    "content-type": [...]
```

Things to know

- Understand the quotas
- Can’t share amazon/amazonaws.com addresses
- Private DNS is not currently supported
- Image, audio and video content are not supported with Step Functions

Pricing

Pricing at a glance

EventBridge API destinations

Public and **private** APIs: $0.20/M invocations

No charges for authorization credentials in AWS Secrets Manager

Billed in 64 KB chunks

Step Functions HTTP tasks

No change in pricing for Step Functions

All prices for us-east-1. AWS data transfer charges, AWS PrivateLink and VPC Lattice data processing charges apply.

Wrap-up

Additional resources

https://s12d.com/api313

Thank you!

Please complete the session survey in the mobile app