
aws
INNOVATE
MODERN APPLICATIONS EDITION
27&28 October 2021

Implementing GraphQL API security best practices with AWS AppSync

Derek Bingham

Senior Developer Advocate
Amazon Web Services

@deekob

Production-ready GraphQL requirements

- Protect access
  - Only authorized access
  - Support multiple access patterns
- Protect availability
  - Maintain service uptime
  - Limit availability to trusted sources
  - Block bad actors
- Protect performance
  - Monitor constantly
  - Analyze in real time
  - Improve over time
- Deploy reliably
  - Infrastructure as code
  - Repeatable

AWS AppSync

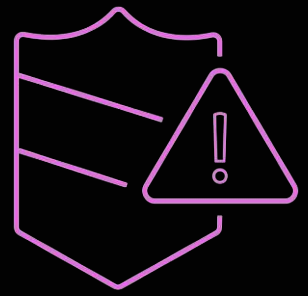
Managed serverless GraphQL service

Connect to data sources in your account

Add data sync, real-time, and offline capabilities for any data source or API

GraphQL facade for any AWS service

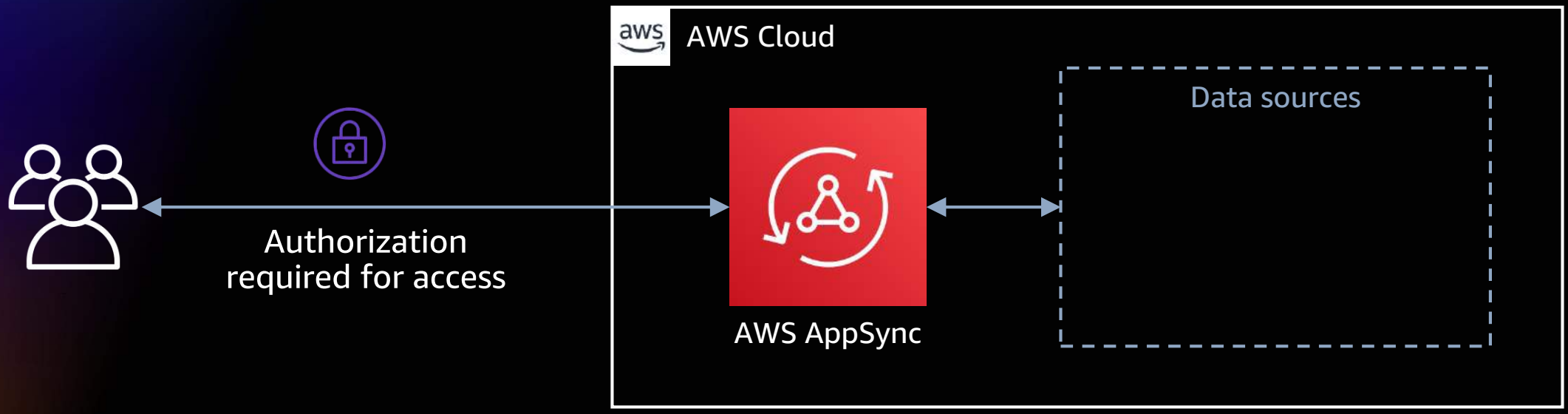
Conflict detection and resolution in the cloud



Enterprise security features: AWS WAF(Web Application Firewall) , AuthZ modes, access controls, monitoring

Protecting access to your API

AWS AppSync: Secure and protected endpoints



All requests must be authorized (no anonymous public access)

AWS AppSync: Authorization modes

API key

OpenID Connect

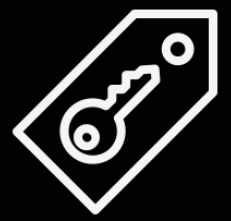
Amazon Cognito
User Pools

IAM

Choose the right AuthZ mode to fit the access use case

AWS AppSync: Authorization modes

API key



- Use HTTP header `x-api-key`
- Hardcoded in application

When to use

- Getting started
- With public APIs
- No specific AuthZ requirements
- B2B, machine to machine

AWS AppSync: Authorization modes

Amazon Cognito user pools

- Granular access control with AWS AppSync directives

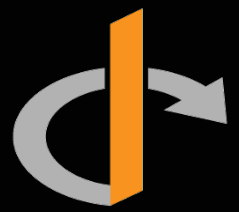
```
type Query {
  posts:[Post!]!
    @aws_auth(cognito_groups:
      ["Bloggers", "Readers"])
}
```

- Sign in with Amazon Cognito User Pools
- Use JSON web tokens (JWTs)

- **When to use**
- Authenticating users in app
- Connecting social identities
- Interacting with other AWS services

AWS AppSync: Authorization modes

Openid connect



- Granular access control based on claims

```
#set( $userGroups =
  ctx.identity.claims.get("oidc:groups”))
#set( $allowedGroups = ["Bloggers", "Readers"] )
#foreach( $userGroup in $userGroups )
  #if( $allowedGroups.contains($userGroup) )
    #set( $isStaticGroupAuthorized = true )
    #break
  #end
#end
#if( !($isStaticGroupAuthorized == true ) )
  $util.unauthorized()
#end
```

- Sign in with OIDC idP
- Use JWTs

- **When to use**
- Existing user directory
- Authenticating users in app
- Not interacting with other AWS services

aws

AWS AppSync: Authorization modes

AWS Identity and access management (IAM)

Granular access control with AWS IAM policy

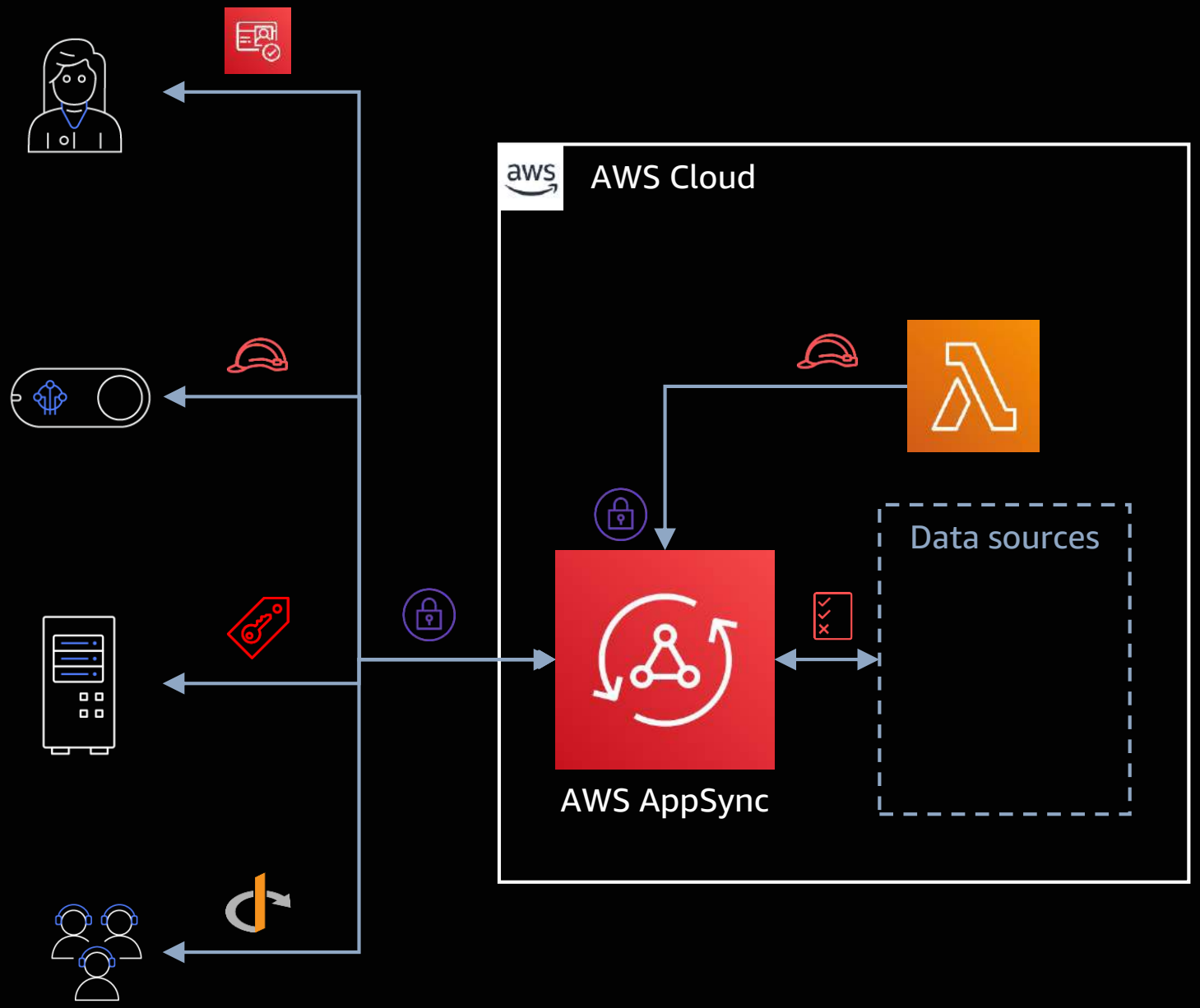
```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["appsync:GraphQL"],
    "Resource": [
      "arn:*:apis/GraphQLApiId/types/Query/fields/<field>",
      "arn:*:apis/GraphQLApiId/types/Mutation/fields/<field>",
      "arn:*:apis/GraphQLApiId/types/Post/fields/<field>"
    ]
  }]
}
```

- Backend systems
- AWS credentials
- IoT systems

- **When to use**
- Amazon Elastic Container Service (Amazon ECS) instances
- AWS Lambda functions

Multi-auth

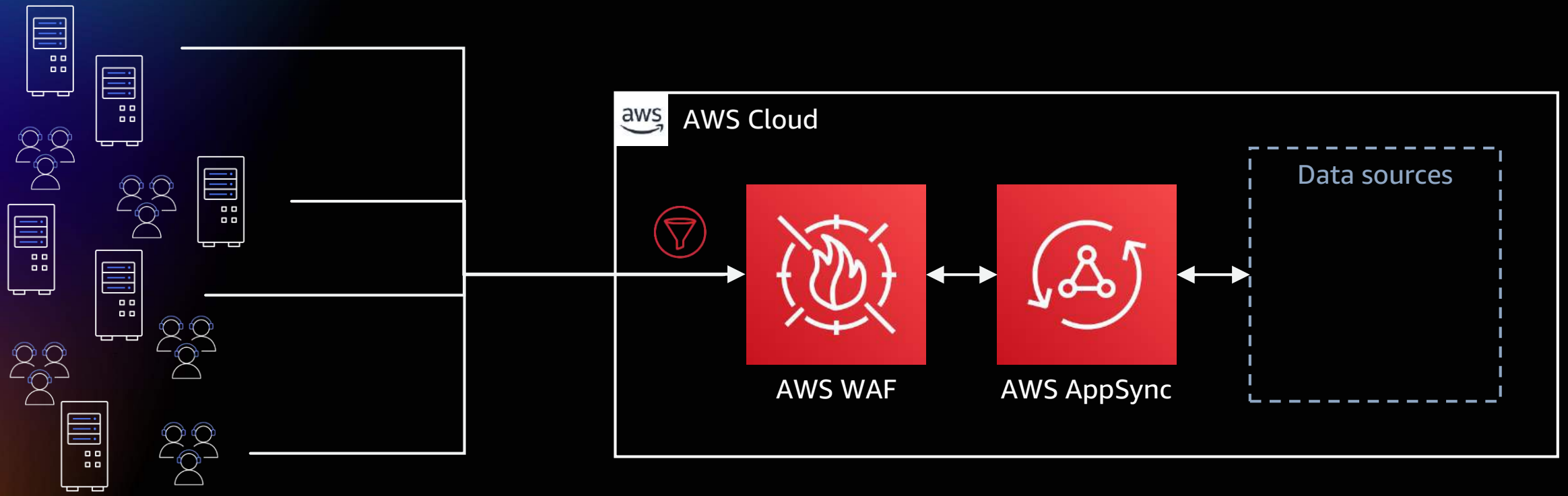
- Do authorization on
  - Type
  - Operation
  - Field
- Select default auth mode
- Specify additional providers



Demo – Implementing AuthZ

Protecting availability of your API

AWS AppSync: Secure and protected endpoints



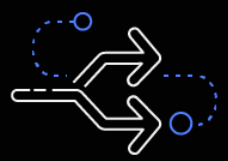
AWS WAF – protects against exploits that impact security, availability

AWS WAF: Web Application Firewall

Frictionless setup – deploy without changing your existing architecture, and no need to configure TLS / SSL or DNS

Low operation overhead – managed rules from AWS and AWS Marketplace, ready to use AWS CloudFormation templates, and built-in SQLi / XSS detection

Customizable security – highly flexible rule engine that can inspect any part of incoming request under single-millisecond latency

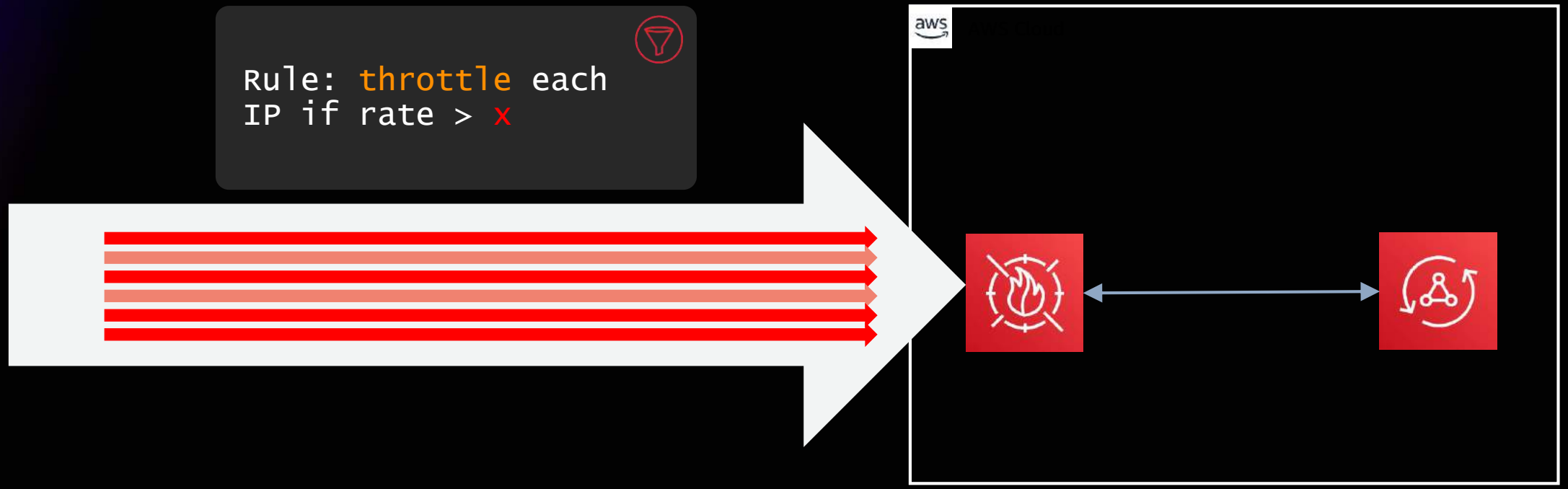


Simply pull in third-party rules – within the WAF console, you can pivot to AWS Marketplace to select industry-leading security vendor rules to pull into AWS WAF

AWS WAF: Use cases with AWS AppSync

- Protect against flooding
- Turn off introspection
- Support B2B APIs using API key
- Limit access to Amazon VPC resources only

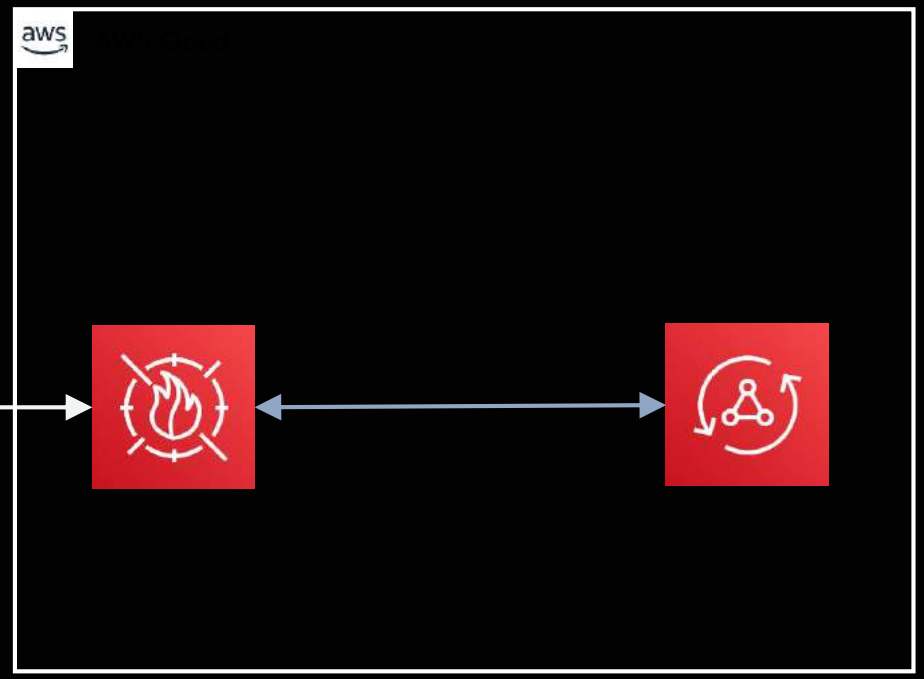
Protect against flooding



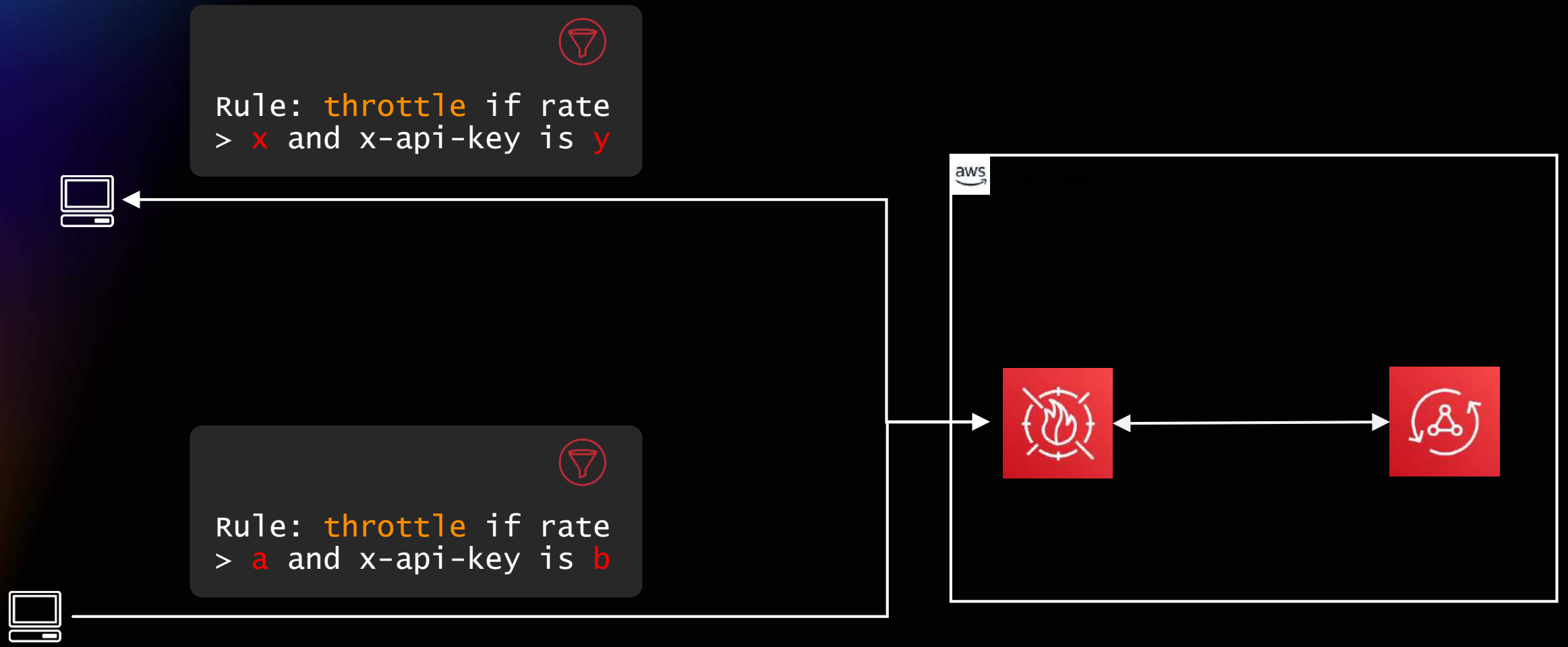
Turn off introspection: Schema not discoverable

```
{
  __schema {
    types {
      name
    }
  }
}
```

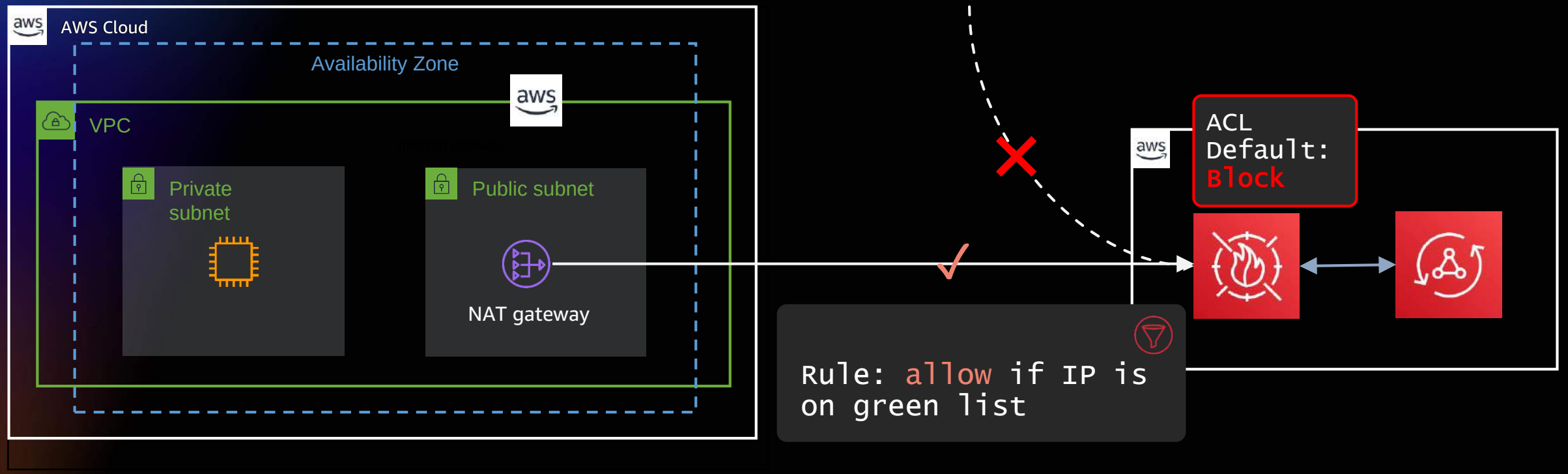
```
Rule: block if body
contains "__schema"
```



Support B2B APIs using API key



VPC-only access: Greenlist NAT gateway IP

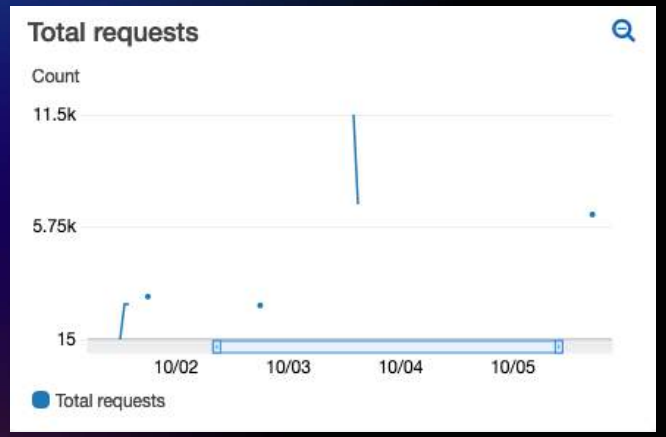


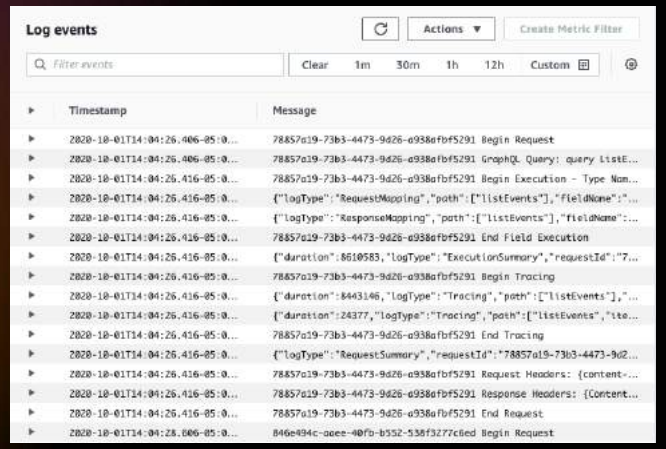
Demo – Implementing Protection

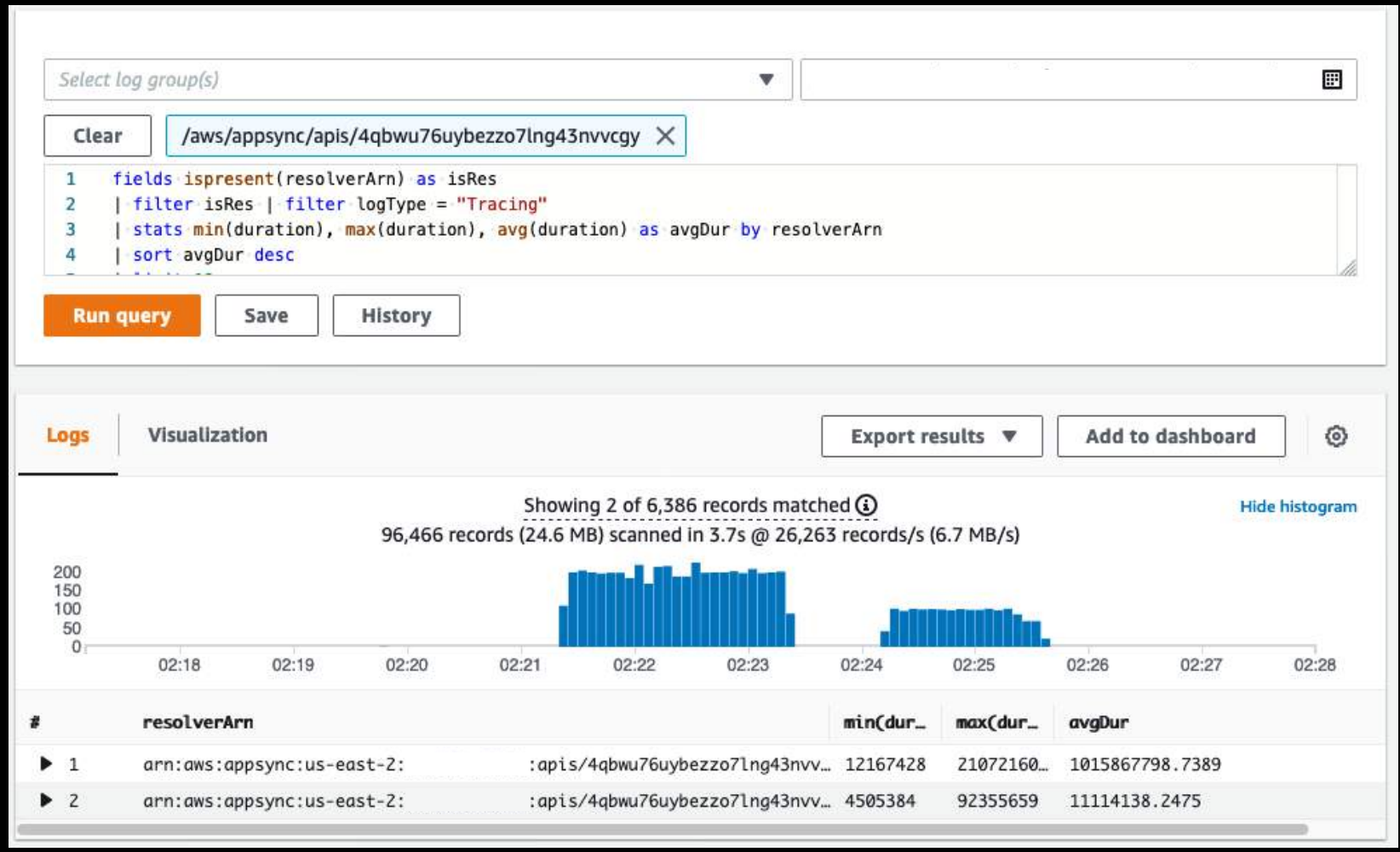
Observing your API

Monitor

Amazon CloudWatch metrics, logs, and log insights

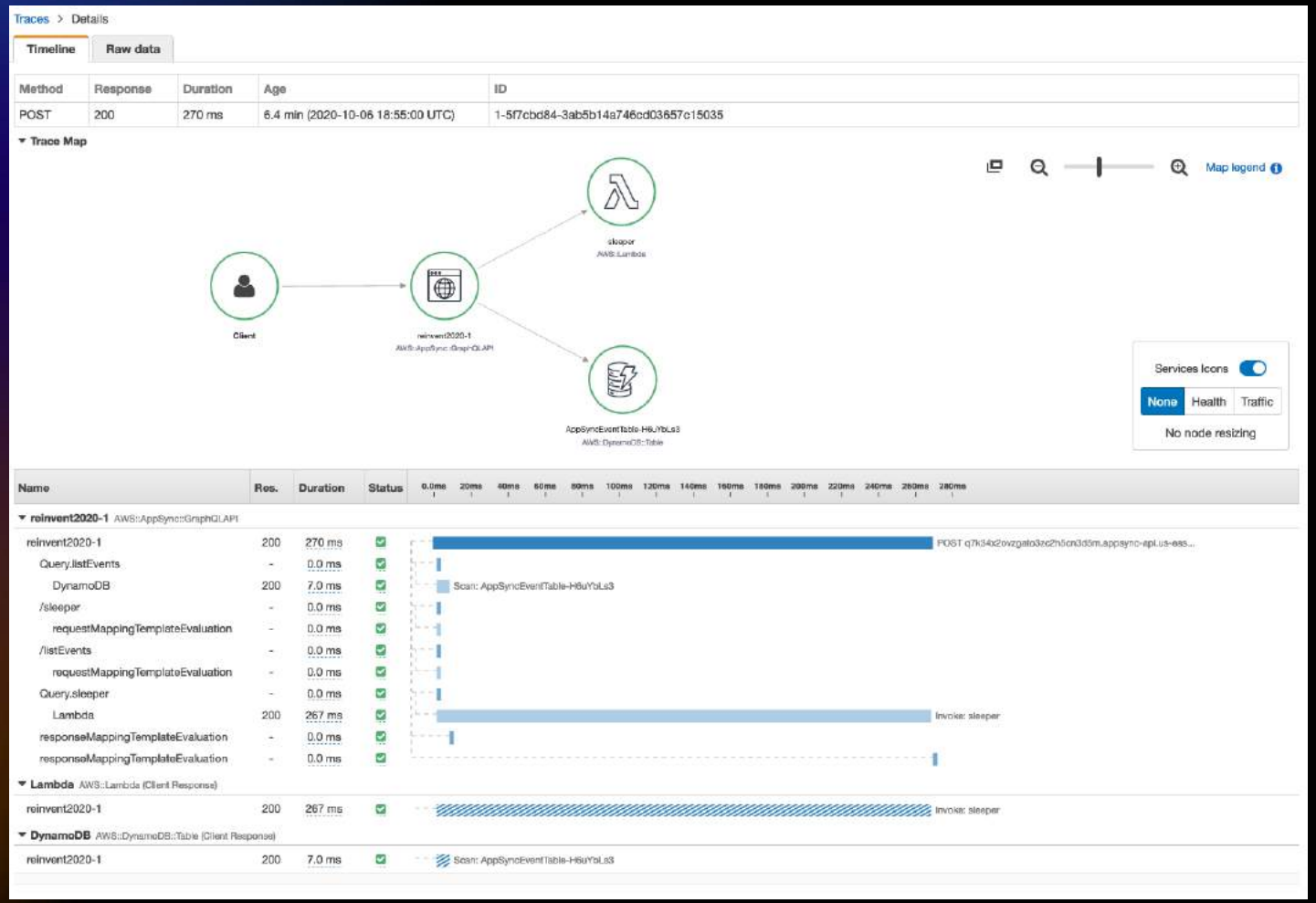






Trace

AWS X-Ray

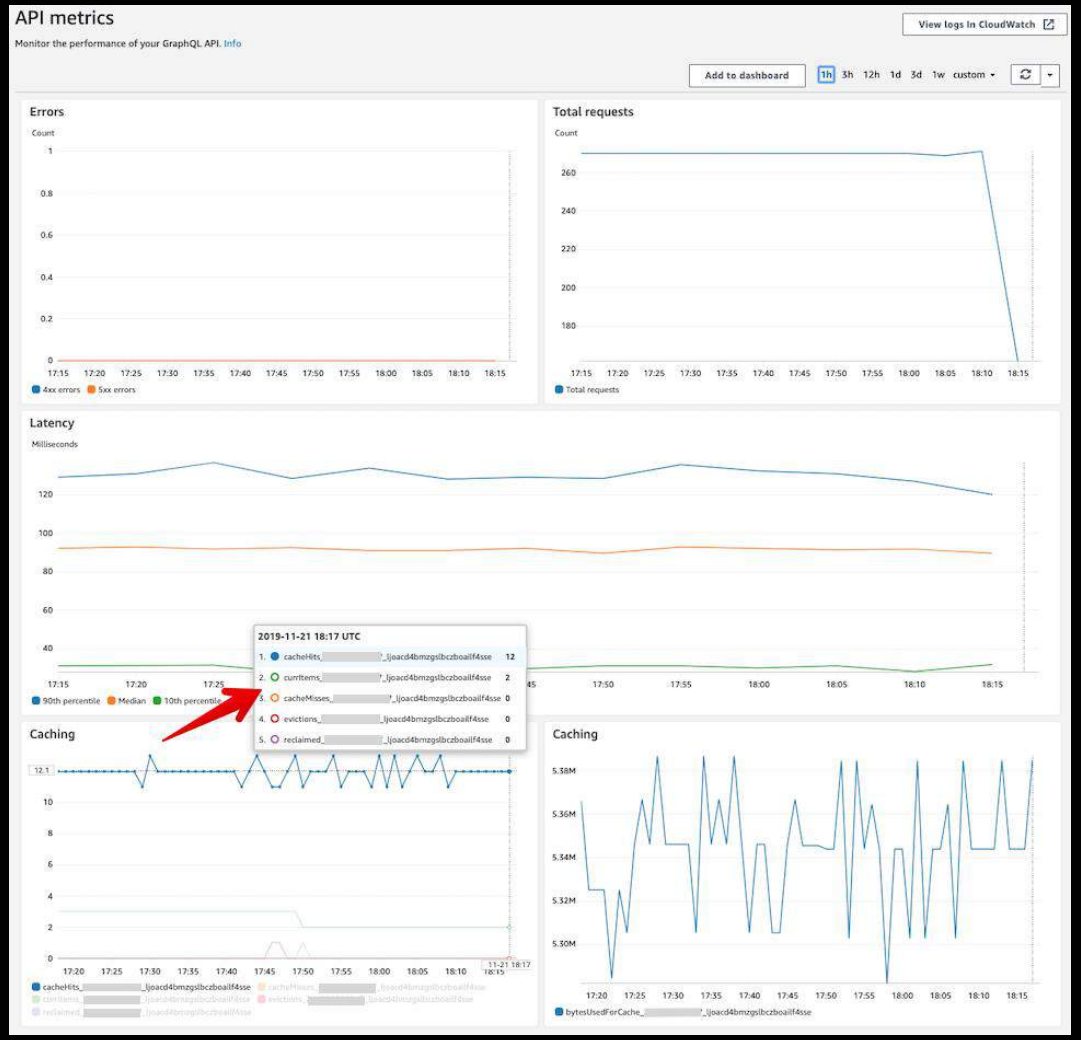


- E2E tracing
- Near real time
- Request visibility
- Identify performance bottlenecks

Optimize

AWS AppSync cache

- Managed server-side caching
- Full API caching
- Per resolver caching
- Encryption

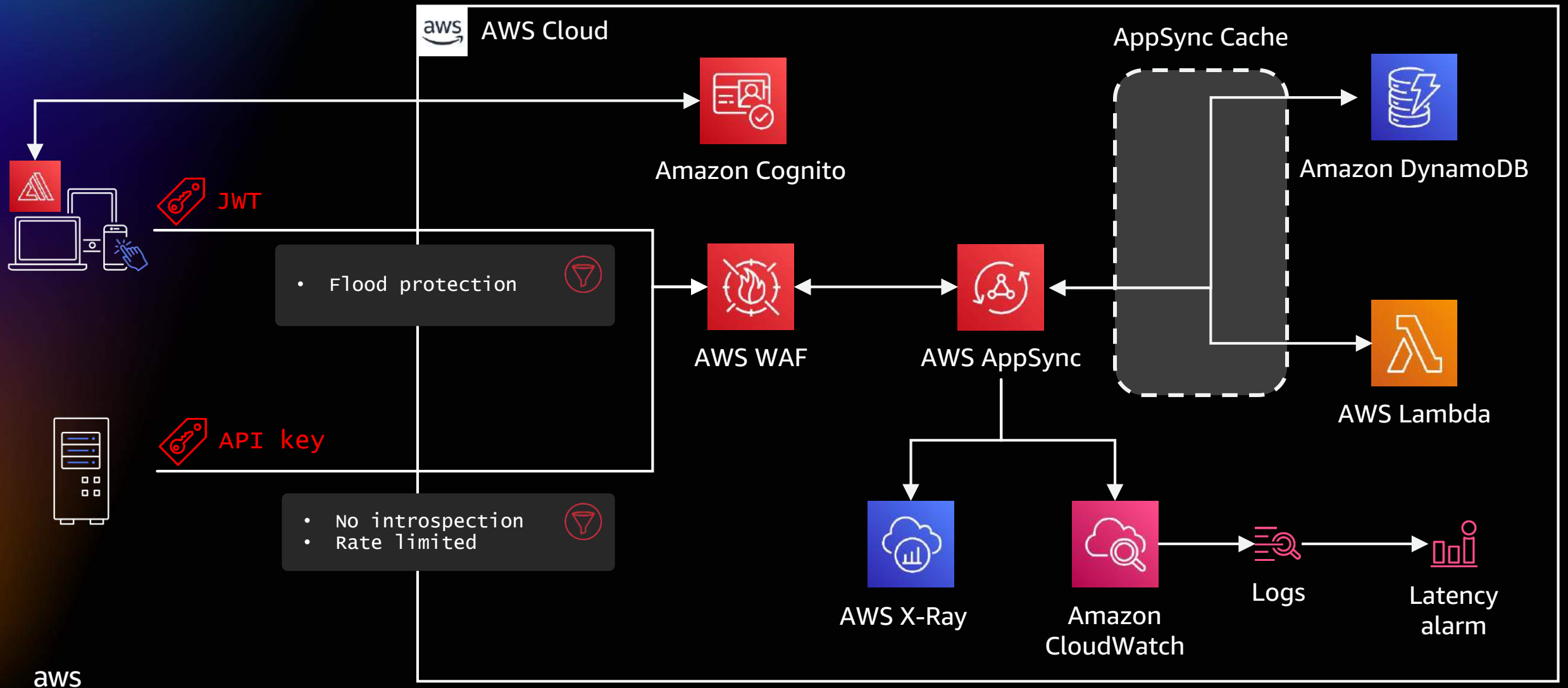


Demo – Implementing Observability

Production looks like…

Production-ready GraphQL with AWS AppSync

Deployed with AWS CDK



Go build!

https://github.com/deekob/appsync_reference

AWS AppSync resources

Website
https://aws.amazon.com/appsync/

Docs
https://docs.aws.amazon.com/appsync/

Github
https://github.com/aws/aws-appsync-community

Blog
https://aws.amazon.com/appsync/blog/

More resources
https://aws.amazon.com/appsync/resources/

Visit the Modern Applications Resource Hub for more resources

Dive deeper with these resources to help you develop an effective plan for your modernization journey.

- Build modern applications on AWS e-book
- Build mobile and web apps faster e-book
- Modernize today with containers on AWS e-book
- Adopting a modern Dev+Ops model e-book
- Modern apps need modern ops e-book
- Determining the total cost of ownership: Comparing Serverless and Server-based technologies paper
- Continuous learning, continuous modernization e-book
- … and more!

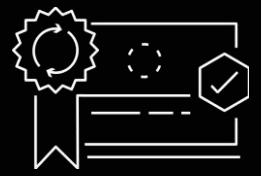
https://bit.ly/3yfOvbK

Visit resource hub »

AWS Training and Certification

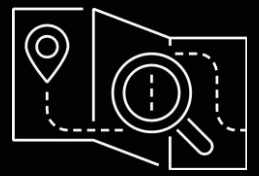
Accelerate modernization with continuous learning

Free digital courses, including:
Architecting serverless solutions
Getting started with DevOps on AWS



Earn an industry-recognized credential:
AWS Certified Developer – Associate
AWS Certified DevOps – Professional

Hands-on classroom training (available virtually) including:
Running containers on Amazon Elastic Kubernetes Service (Amazon EKS)
Advanced developing on AWS



Create a self-paced learning roadmap
AWS ramp-up guide - Developer
AWS ramp-up guide - DevOps

Take Developer and DevOps training today

Learn more about Modernization training for you and your team

Thank you for attending AWS Innovate Modern Applications Edition

We hope you found it interesting! A kind reminder to **complete the survey.**
Let us know what you thought of today's event and how we can improve the event experience for you in the future.


aws-apj-marketing@amazon.com


twitter.com/AWSCloud


facebook.com/AmazonWebServices


youtube.com/user/AmazonWebServices


slideshare.net/AmazonWebServices


twitch.tv/aws

Thank you!

Derek Bingham

Senior Developer Advocate

Amazon Web Services

 **@deekob**