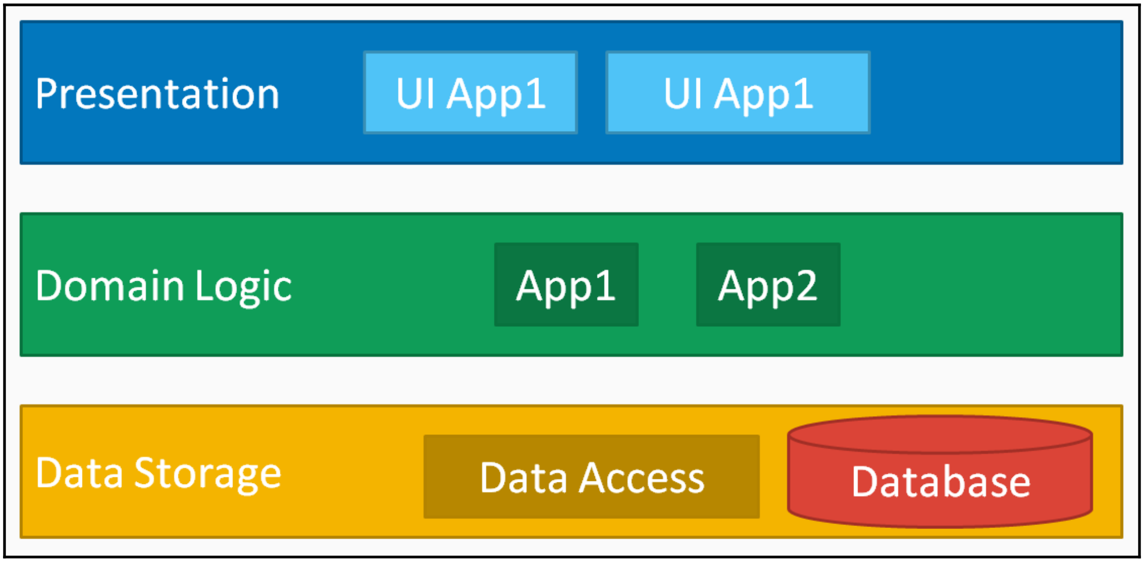
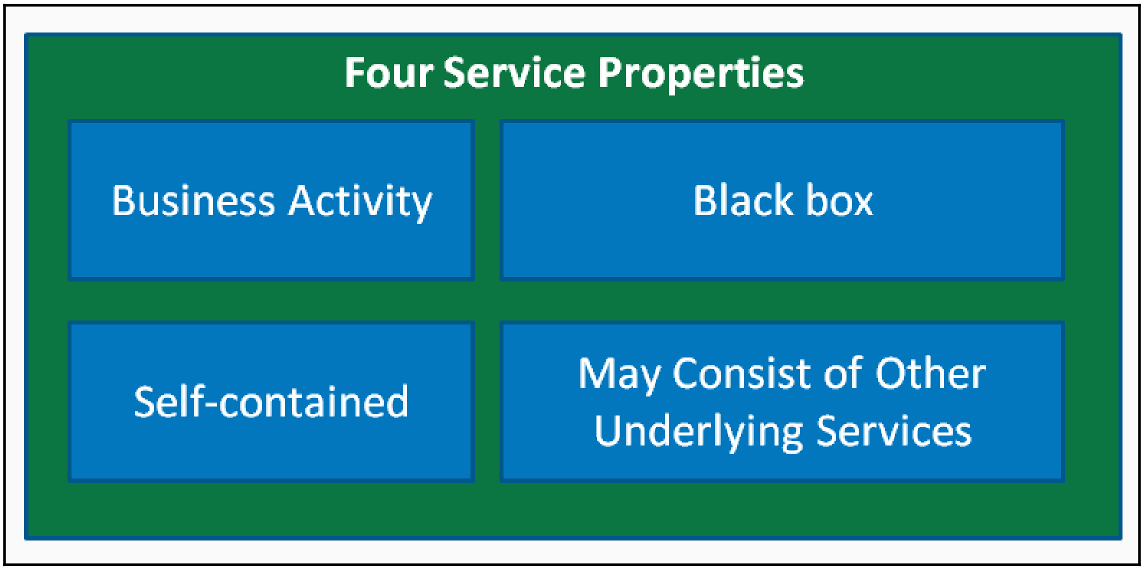
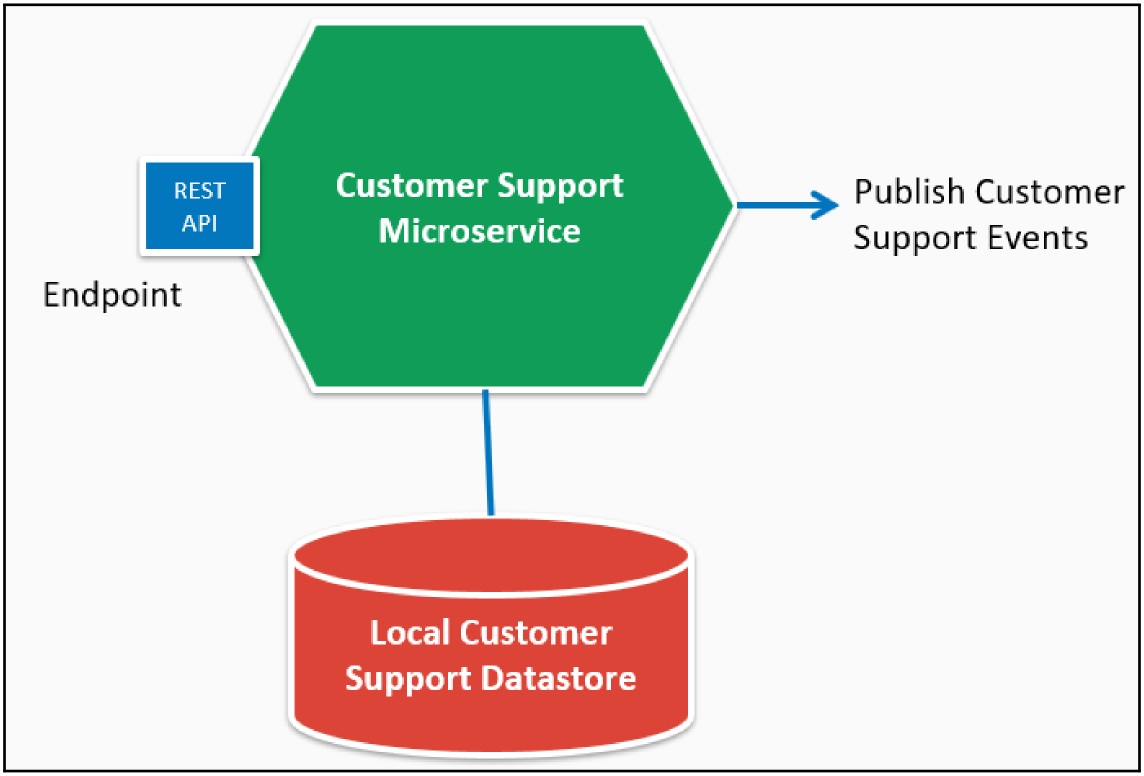
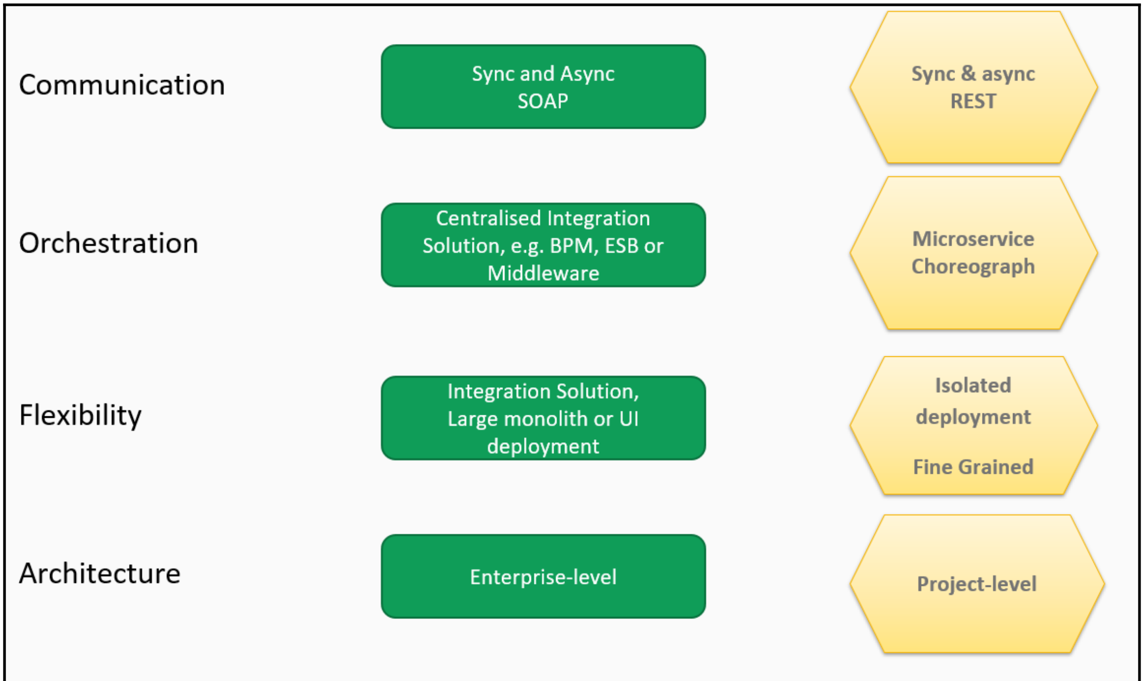
Chapter 1: Serverless Microservices Architectures and Patterns






REST API
Endpoint
Customer Support Microservice
Publish Customer Support Events
Local Customer Support Datastore



Communication

Sync and Async SOAP

Sync & async REST

Orchestration

Centralised Integration Solution, e.g. BPM, ESB or Middleware

Microservice Choreograph

Flexibility

Integration Solution, Large monolith or UI deployment

Isolated deployment

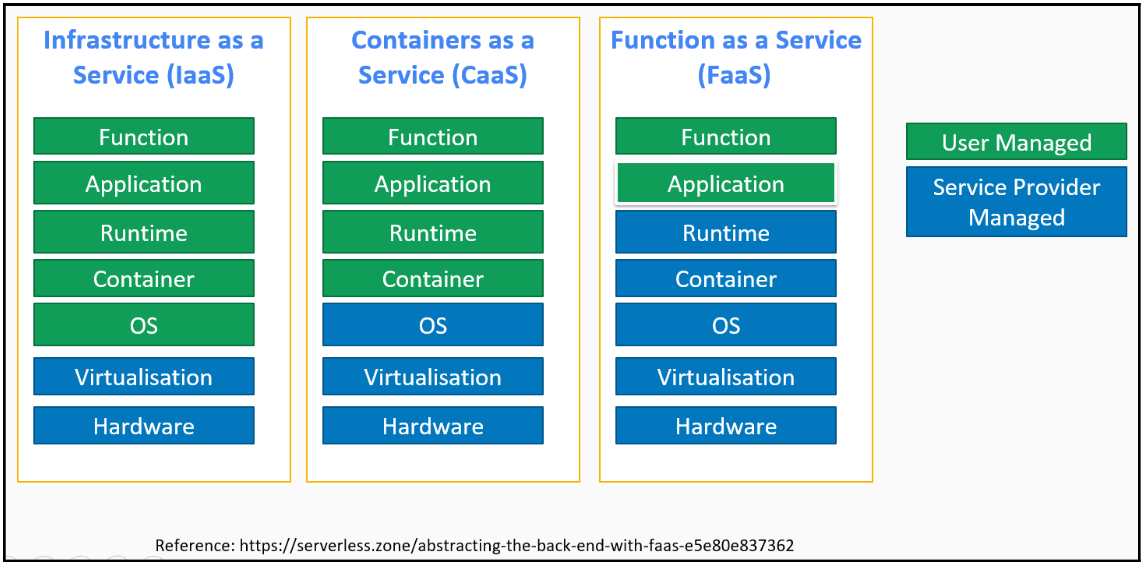
Fine Grained

Architecture

Enterprise-level

Project-level

Reference: Microservices Flexible Software Architecture by Eberhard Wolff

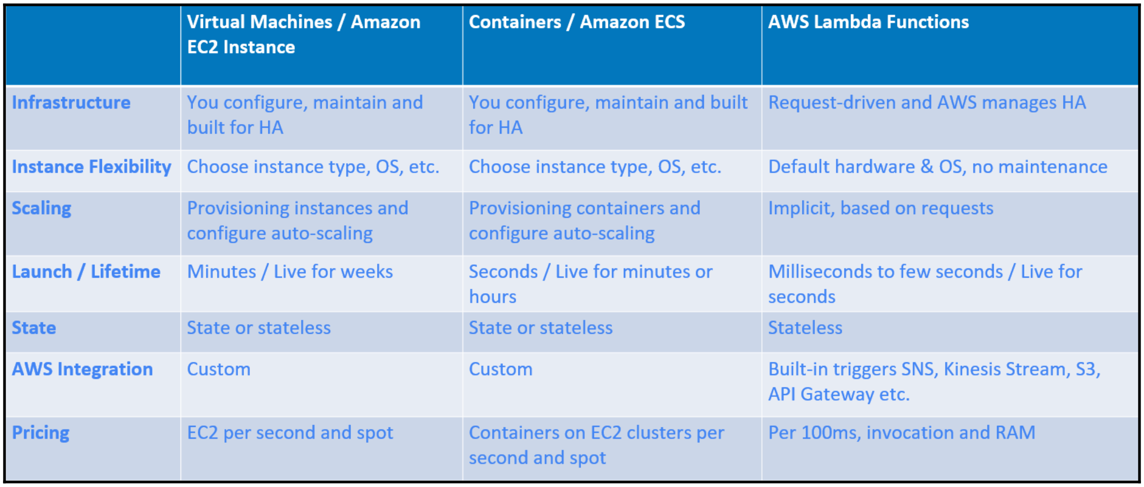


	Infrastructure as a Service (IaaS)	Containers as a Service (CaaS)	Function as a Service (FaaS)
Function	🟩	🟩	🟩
Application	🟩	🟩	🟩
Runtime	🟩	🟩	🟦
Container	🟩	🟩	🟦
OS	🟩	🟦	🟦
Virtualisation	🟦	🟦	🟦
Hardware	🟦	🟦	🟦

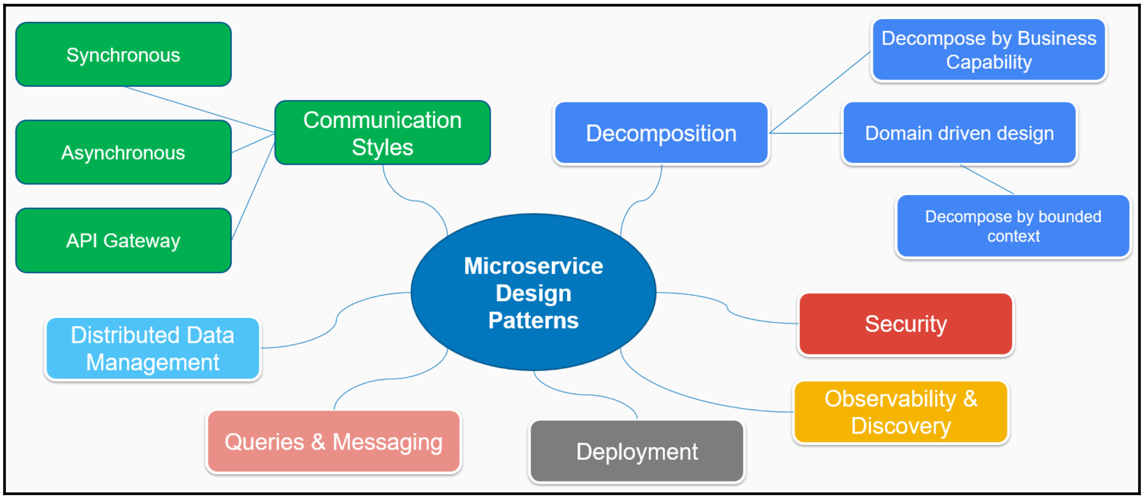
🟩 User Managed

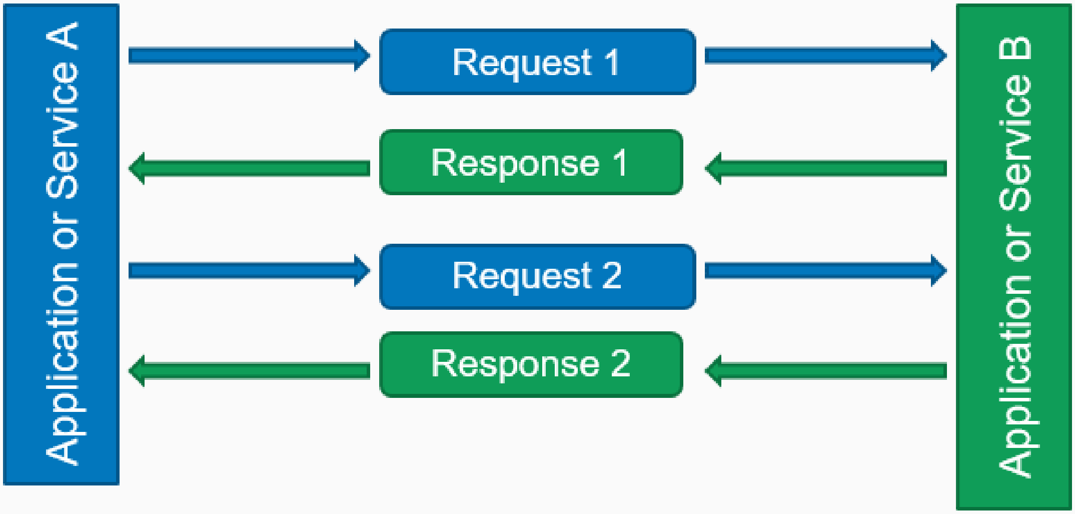
🟦 Service Provider Managed

Reference: https://serverless.zone/abstracting-the-back-end-with-faas-e5e80e837362

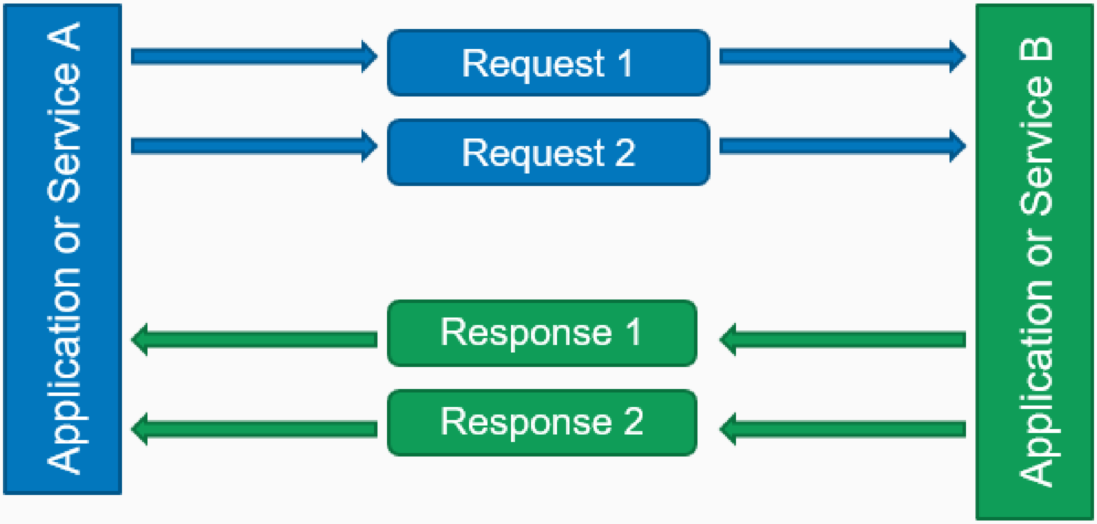


	Virtual Machines / Amazon EC2 Instance	Containers / Amazon ECS	AWS Lambda Functions
Infrastructure	You configure, maintain and built for HA	You configure, maintain and built for HA	Request-driven and AWS manages HA
Instance Flexibility	Choose instance type, OS, etc.	Choose instance type, OS, etc.	Default hardware & OS, no maintenance
Scaling	Provisioning instances and configure auto-scaling	Provisioning containers and configure auto-scaling	Implicit, based on requests
Launch / Lifetime	Minutes / Live for weeks	Seconds / Live for minutes or hours	Milliseconds to few seconds / Live for seconds
State	State or stateless	State or stateless	Stateless
AWS Integration	Custom	Custom	Built-in triggers SNS, Kinesis Stream, S3, API Gateway etc.
Pricing	EC2 per second and spot	Containers on EC2 clusters per second and spot	Per 100ms, invocation and RAM

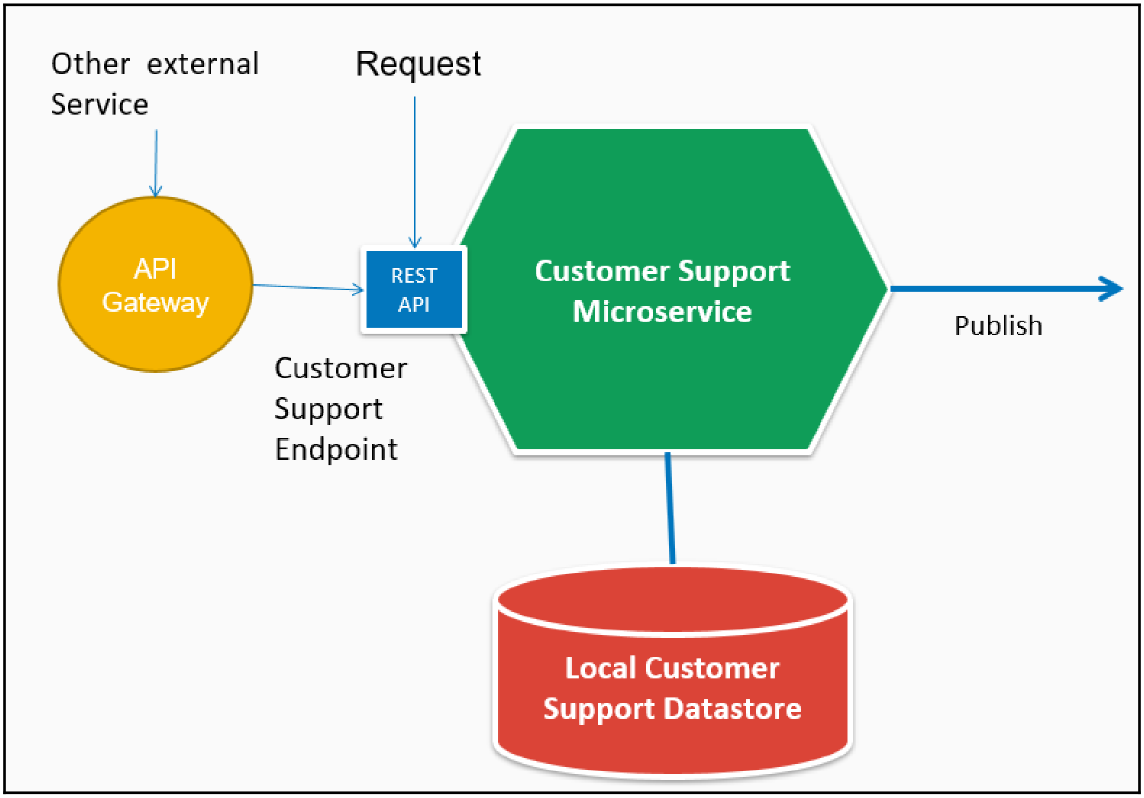

Synchronous
Asynchronous
API Gateway
Communication Styles
Decomposition
Decompose by Business Capability
Domain driven design
Decompose by bounded context
Microservice Design Patterns
Distributed Data Management
Security
Queries & Messaging
Deployment
Observability & Discovery

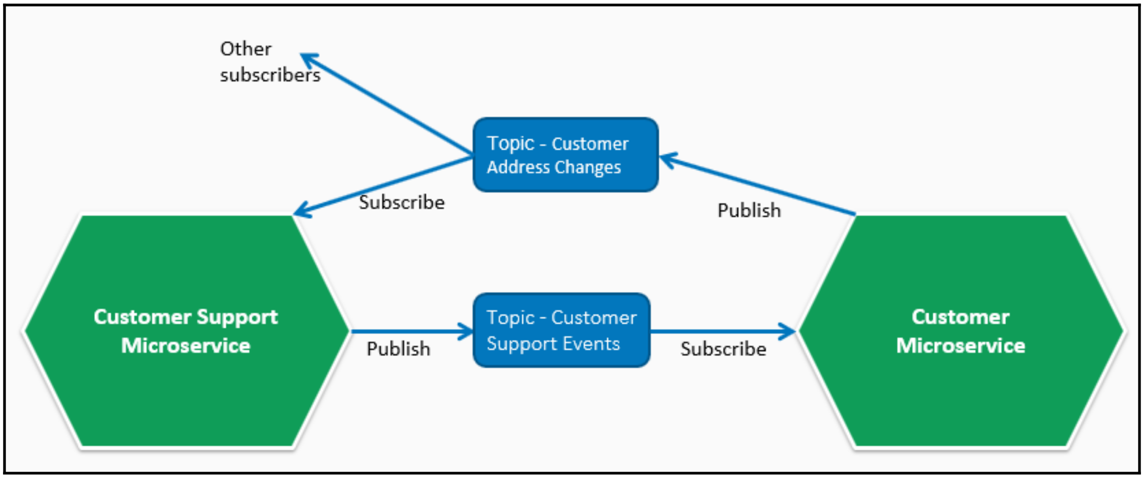


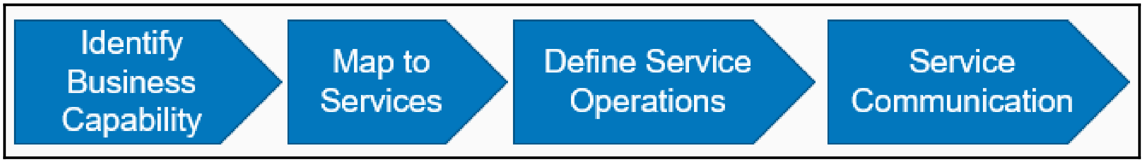
Synchronous Calls



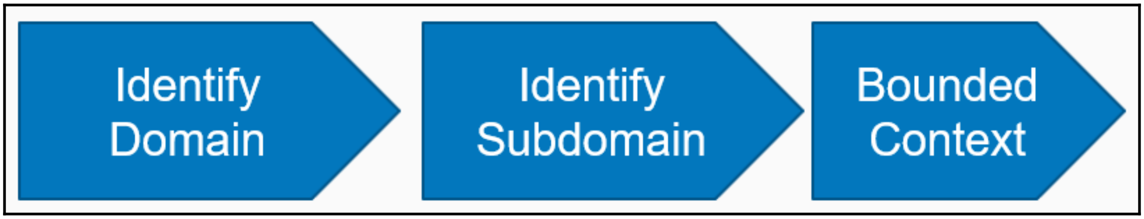
Asynchronous Calls


Other external Service
Request
API Gateway
REST API
Customer Support Microservice
Publish
Customer Support Endpoint
Local Customer Support Datastore

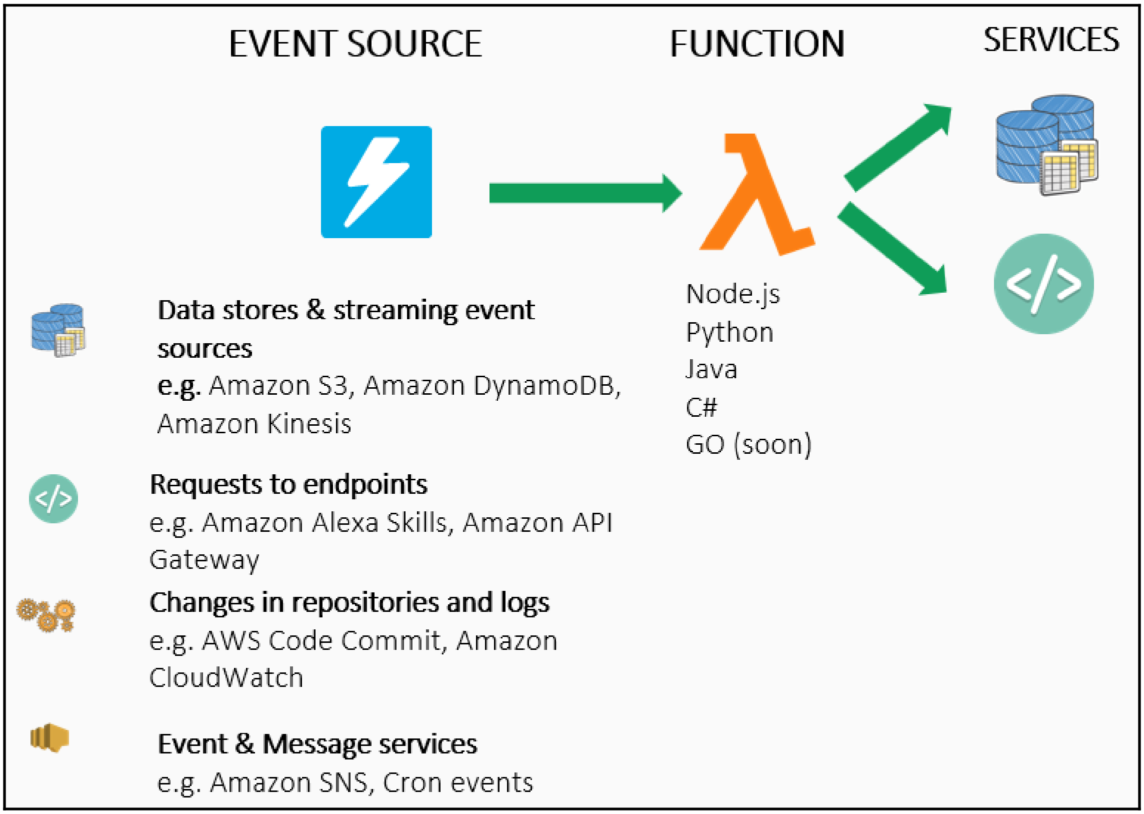

Other subscribers
Topic - Customer Address Changes
Subscribe
Publish
Customer Support Microservice
Publish
Topic - Customer Support Events
Subscribe
Customer Microservice



Identify Business Capability → Map to Services → Define Service Operations → Service Communication



Identify Domain → Identify Subdomain → Bounded Context



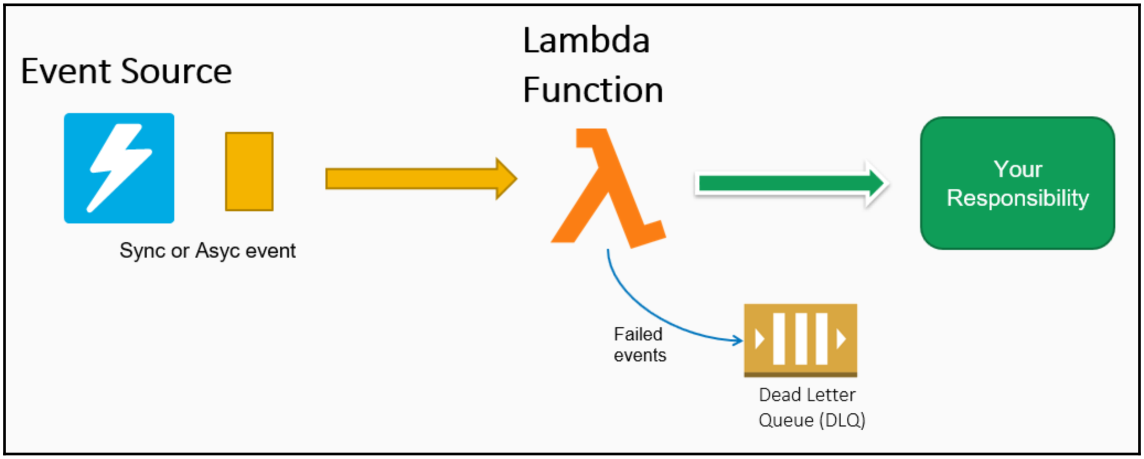
Node.js
Python
Java
C#
GO (soon)

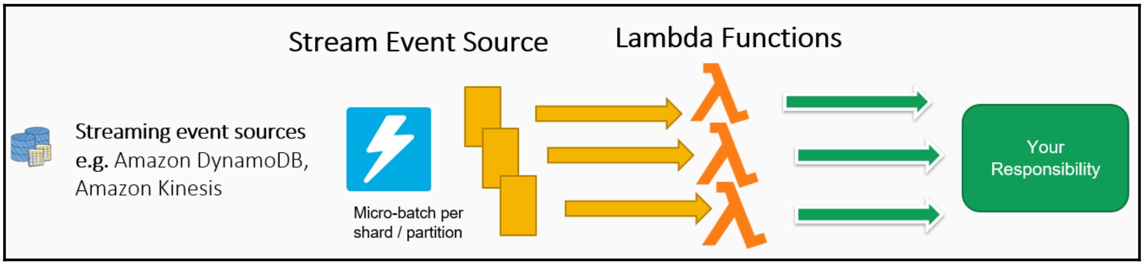
Data stores & streaming event sources
e.g. Amazon S3, Amazon DynamoDB, Amazon Kinesis

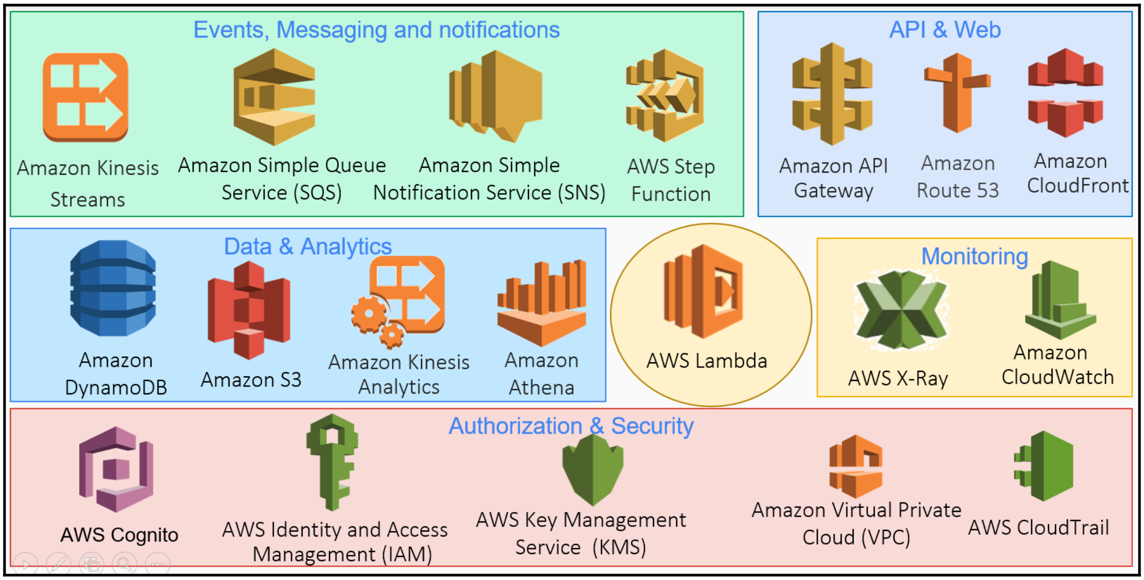
Requests to endpoints
e.g. Amazon Alexa Skills, Amazon API Gateway

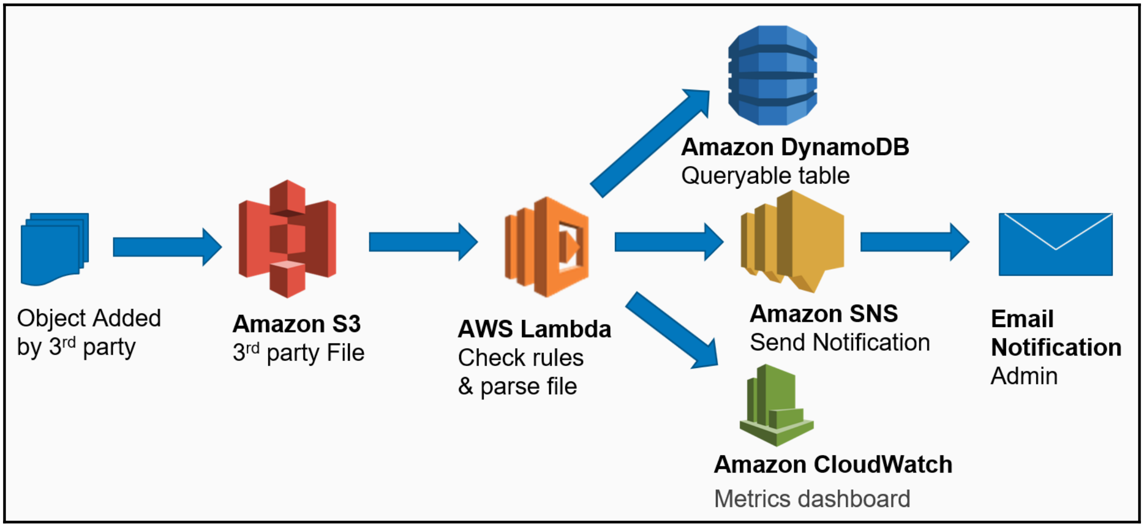
Changes in repositories and logs
e.g. AWS Code Commit, Amazon CloudWatch

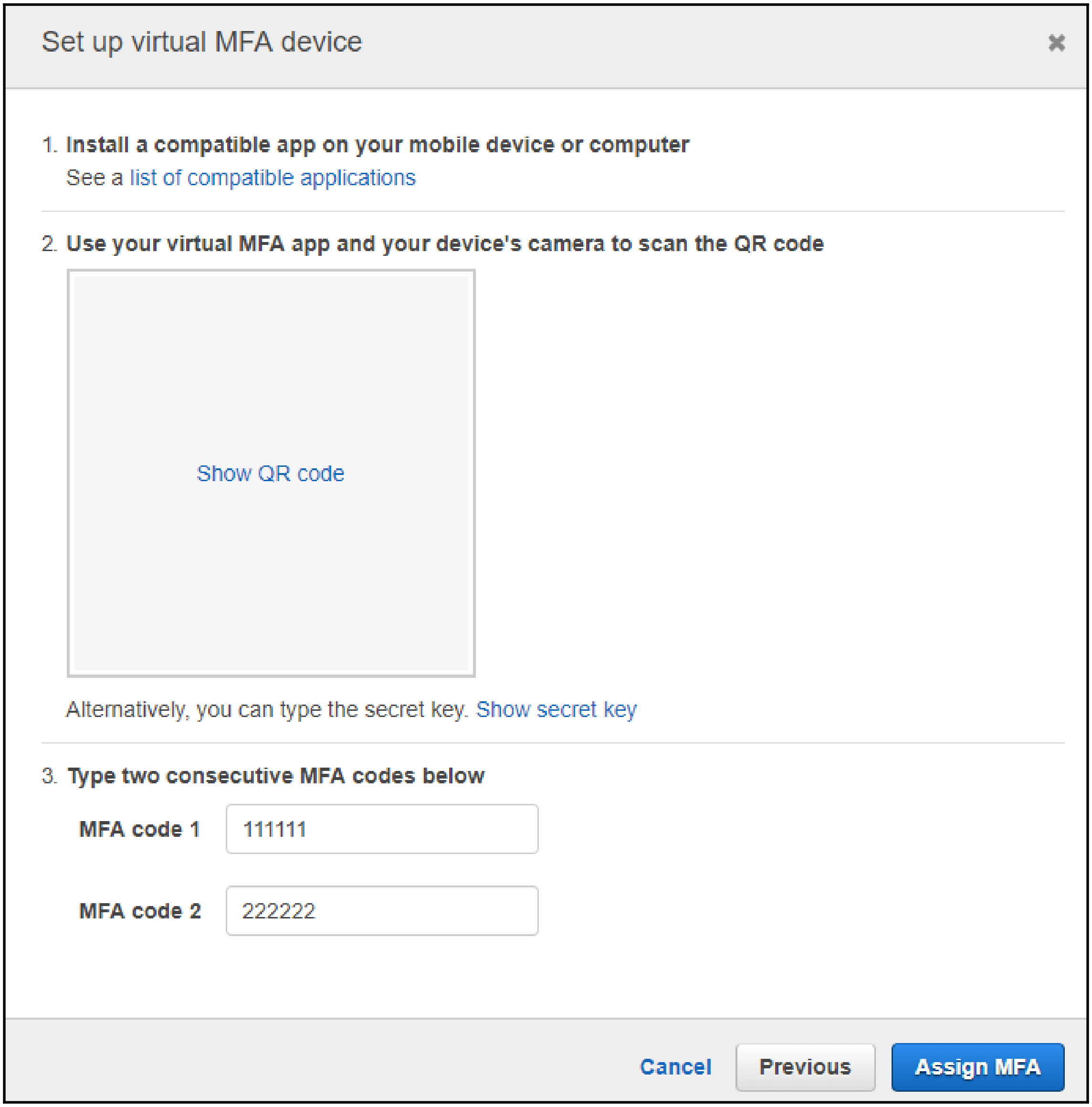
Event & Message services
e.g. Amazon SNS, Cron events


Event Source
Lambda Function
Sync or Asyc event
Your Responsibility
Failed events
Dead Letter Queue (DLQ)


Stream Event Source
Lambda Functions
Streaming event sources e.g. Amazon DynamoDB, Amazon Kinesis
Micro-batch per shard / partition
Your Responsibility


Events, Messaging and notifications
Amazon Kinesis Streams
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
AWS Step Function
API & Web
Amazon API Gateway
Amazon Route 53
Amazon CloudFront
Data & Analytics
Amazon DynamoDB
Amazon S3
Amazon Kinesis Analytics
Amazon Athena
AWS Lambda
Monitoring
AWS X-Ray
Amazon CloudWatch
Authorization & Security
AWS Cognito
AWS Identity and Access Management (IAM)
AWS Key Management Service (KMS)
Amazon Virtual Private Cloud (VPC)
AWS CloudTrail


Amazon DynamoDB
Queryable table
Object Added
by 3rd party
Amazon S3
3rd party File
AWS Lambda
Check rules
& parse file
Amazon SNS
Send Notification
Email
Notification
Admin
Amazon CloudWatch
Metrics dashboard



Set up virtual MFA device

1. **Install a compatible app on your mobile device or computer**
   See a list of compatible applications

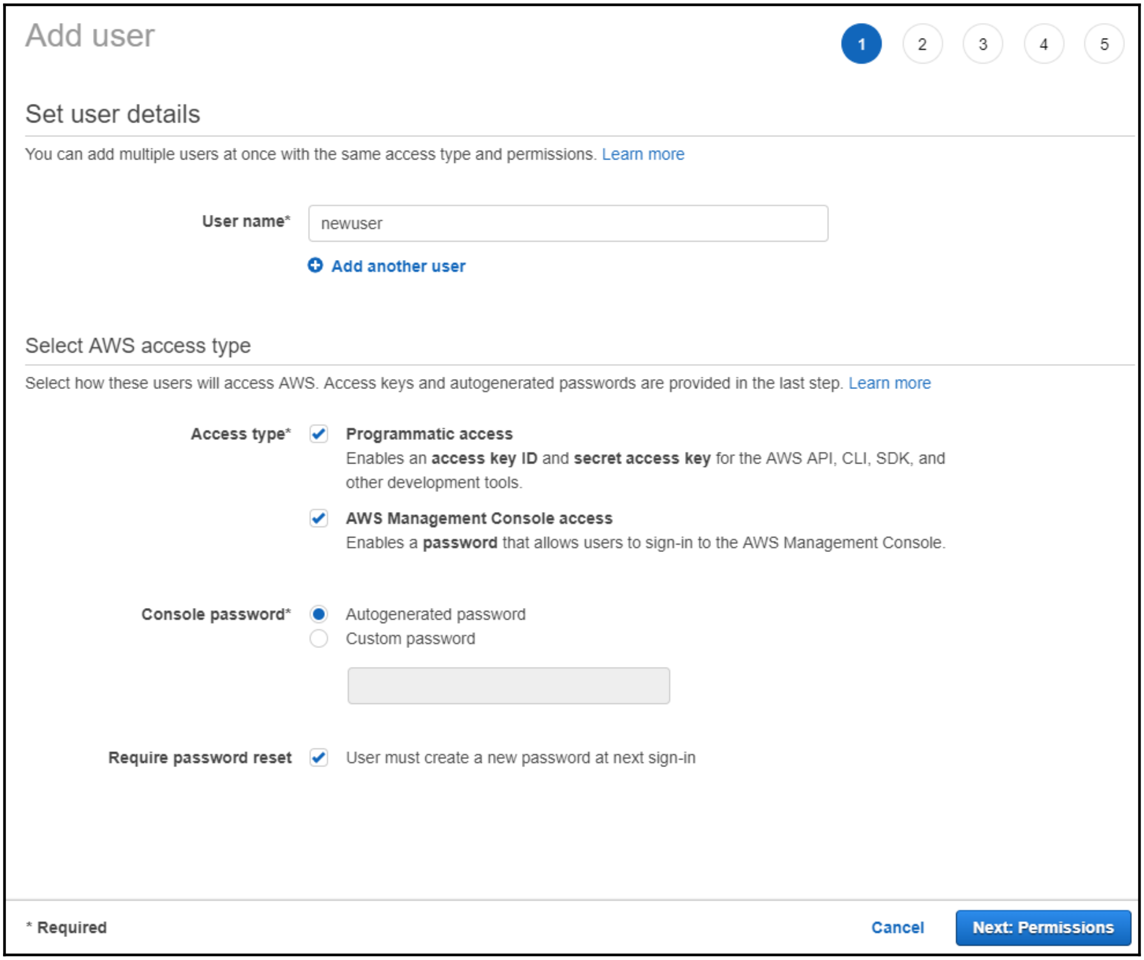
2. **Use your virtual MFA app and your device's camera to scan the QR code**

Alternatively, you can type the secret key. Show secret key

3. **Type two consecutive MFA codes below**

MFA code 1 111111

MFA code 2 222222



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* newuser

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

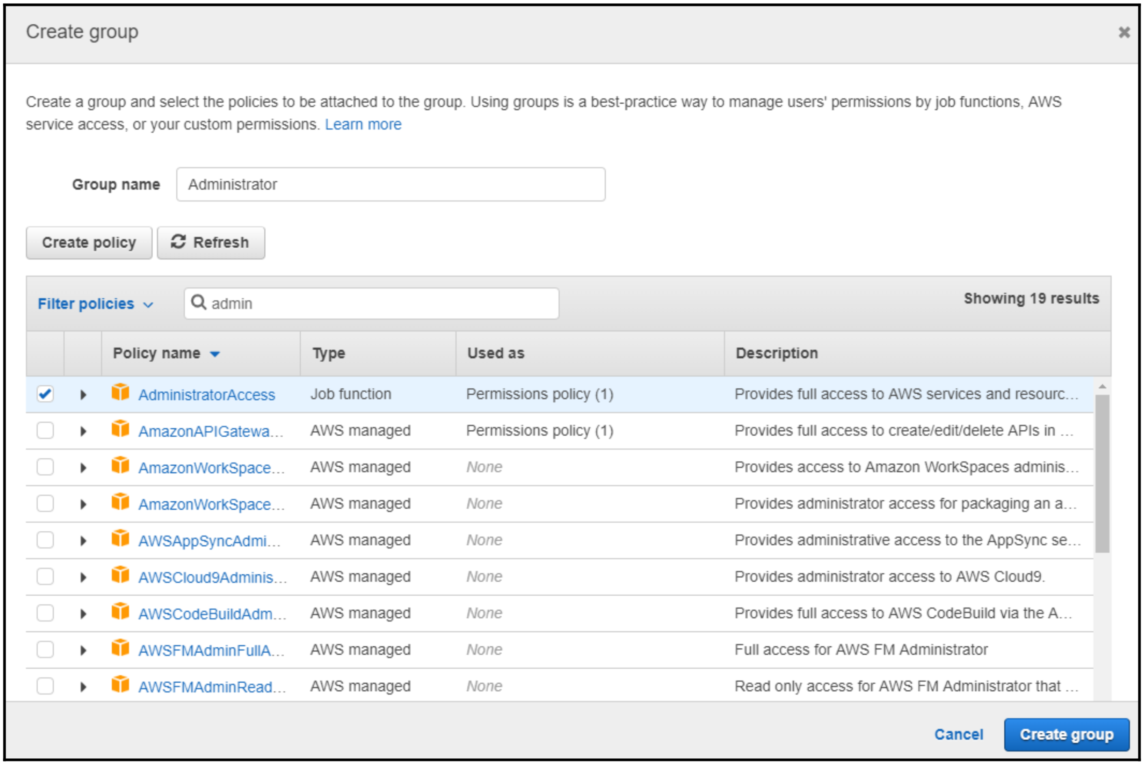
Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ● Autogenerated password
○ Custom password

Require password reset ☑ User must create a new password at next sign-in

* Required



Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

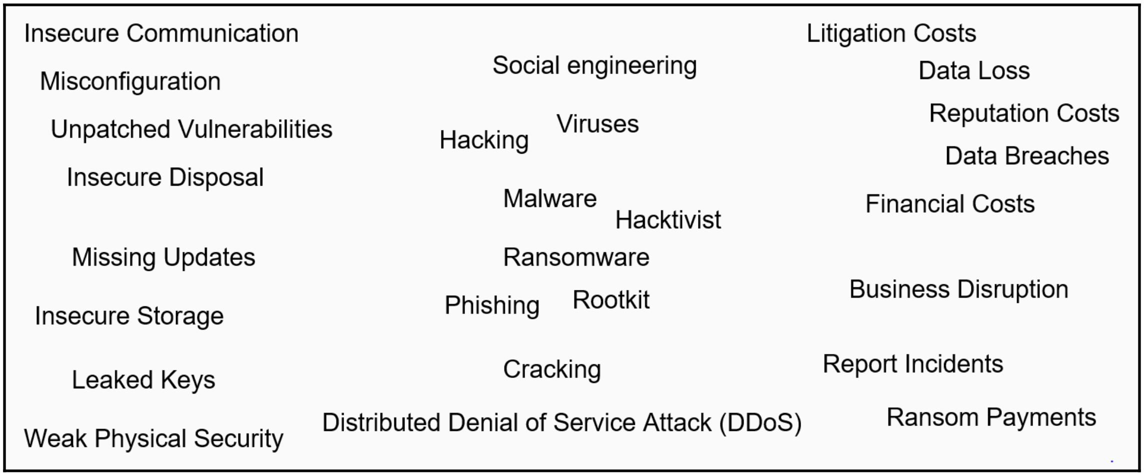
Group name: Administrator

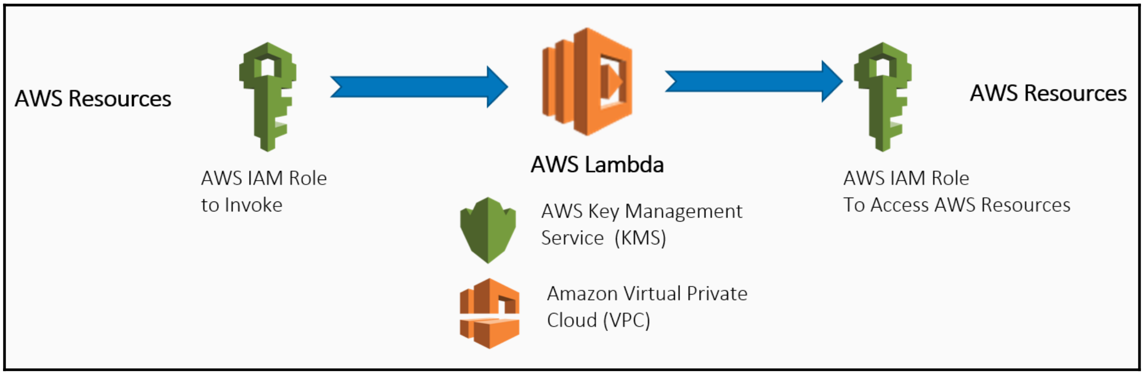
admin

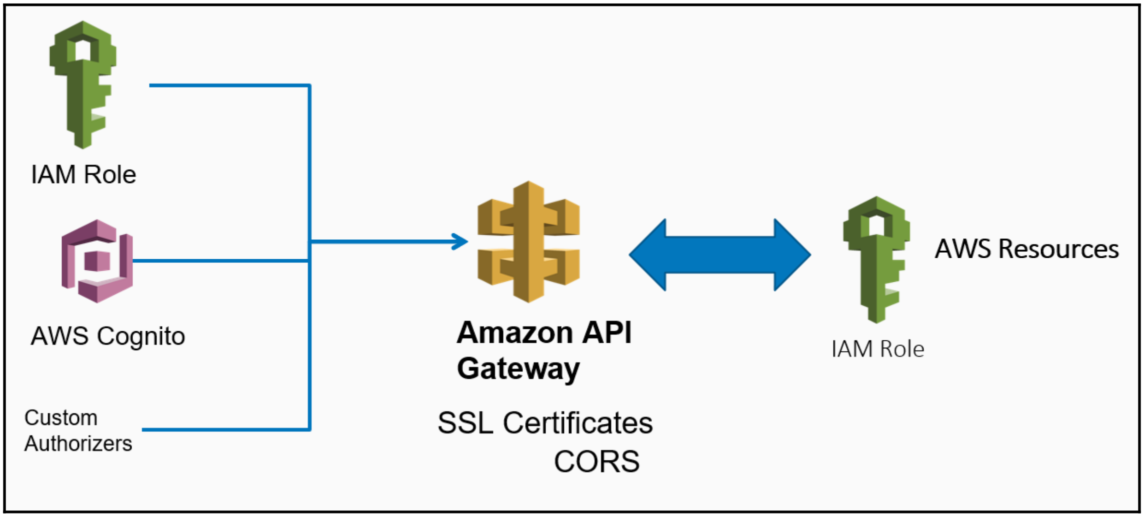
Showing 19 results

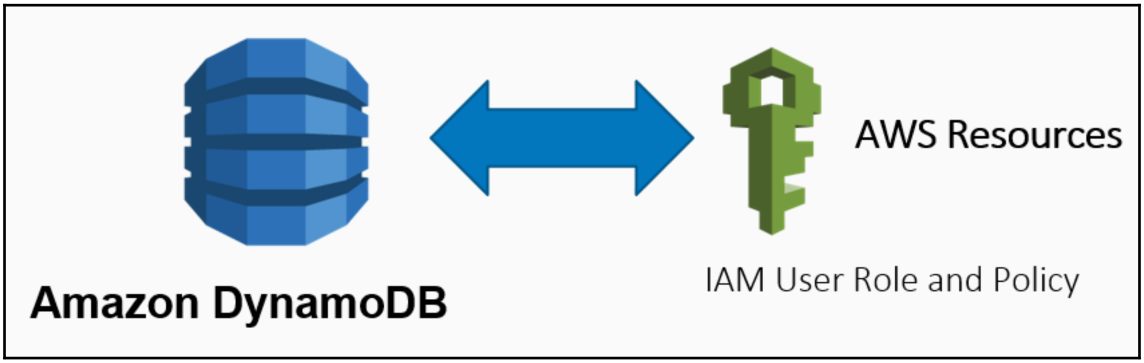
		Policy name	Type	Used as	Description
☑	▸	AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and resourc…
□	▸	AmazonAPIGatewa…	AWS managed	Permissions policy (1)	Provides full access to create/edit/delete APIs in …
□	▸	AmazonWorkSpace…	AWS managed	*None*	Provides access to Amazon WorkSpaces adminis…
□	▸	AmazonWorkSpace…	AWS managed	*None*	Provides administrator access for packaging an a…
□	▸	AWSAppSyncAdmi…	AWS managed	*None*	Provides administrative access to the AppSync se…
□	▸	AWSCloud9Adminis…	AWS managed	*None*	Provides administrator access to AWS Cloud9.
□	▸	AWSCodeBuildAdm…	AWS managed	*None*	Provides full access to AWS CodeBuild via the A…
□	▸	AWSFMAdminFullA…	AWS managed	*None*	Full access for AWS FM Administrator
□	▸	AWSFMAdminRead…	AWS managed	*None*	Read only access for AWS FM Administrator that …

Chapter 2: Creating Your First Serverless Data API





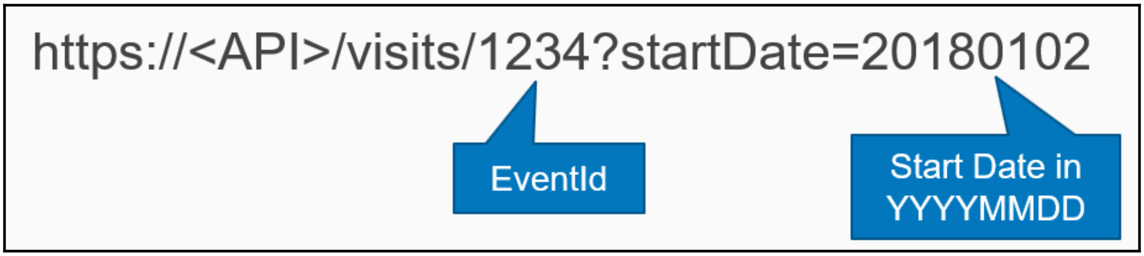

IAM Role
AWS Cognito
Custom
Authorizers
Amazon API
Gateway
SSL Certificates
CORS
IAM Role
AWS Resources


Amazon DynamoDB
AWS Resources
IAM User Role and Policy

AWS CloudTrail

Amazon CloudWatch

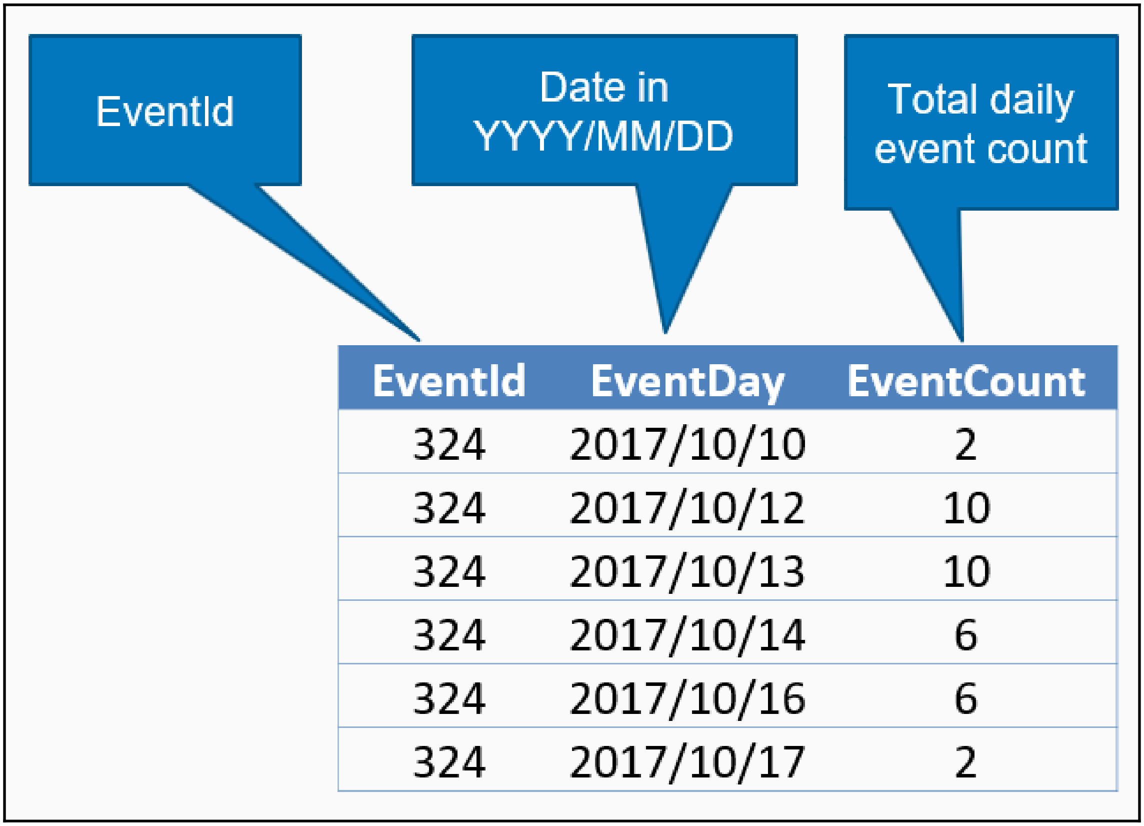
AWS X-ray



https://<API>/visits/1234?startDate=20180102

EventId

Start Date in YYYYMMDD

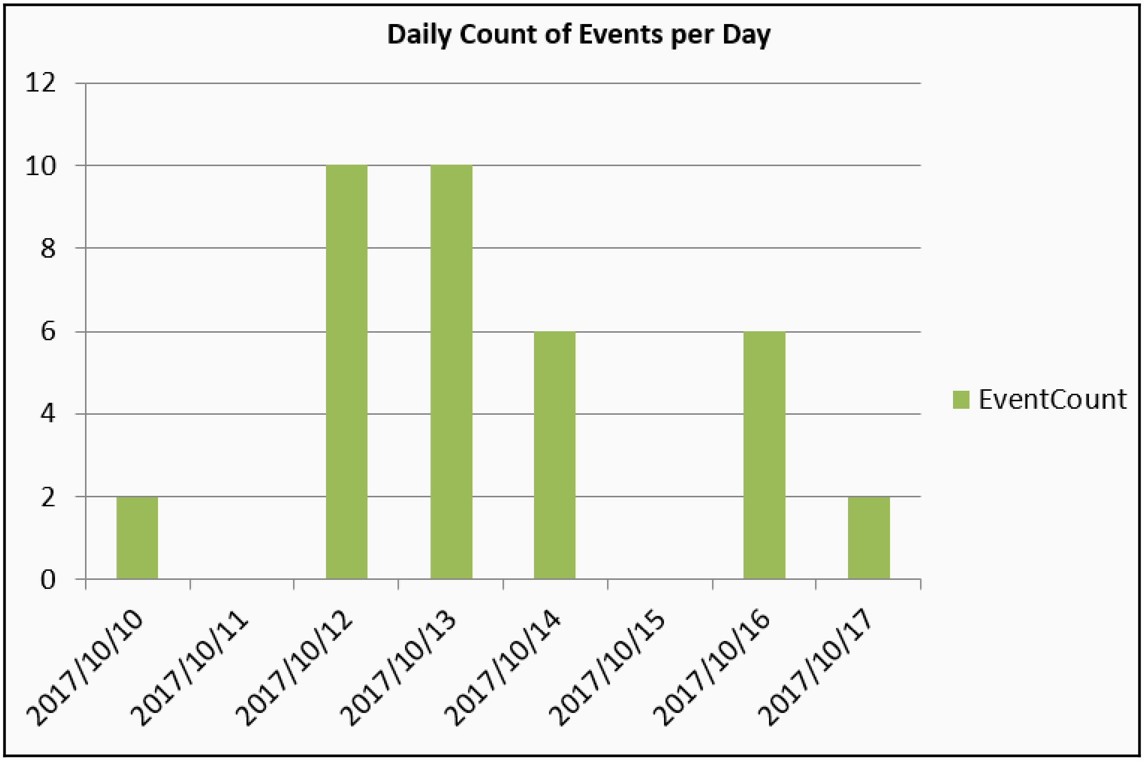


EventId

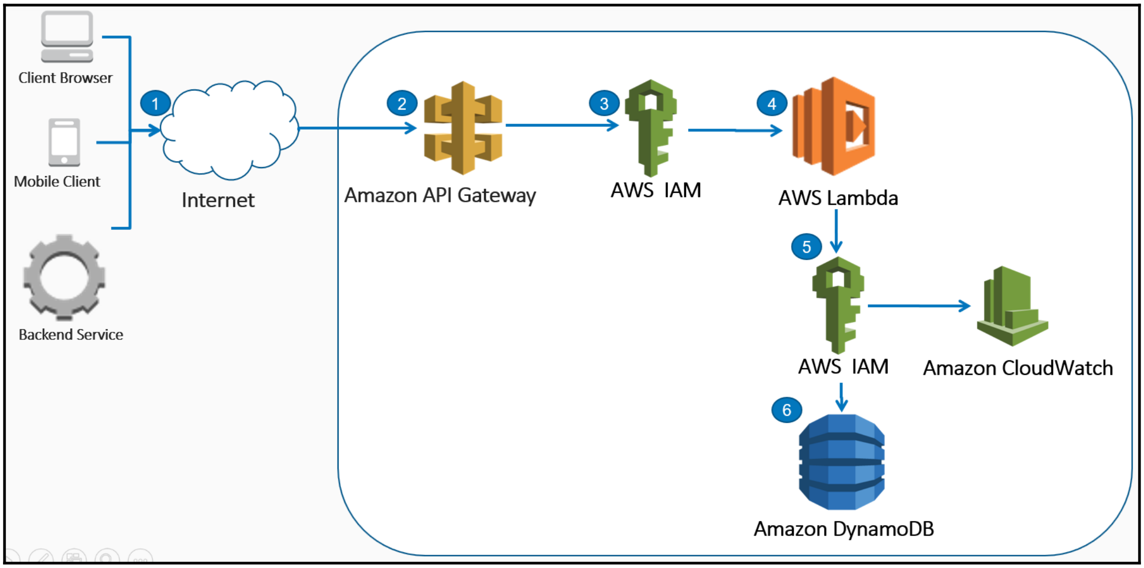
Date in YYYY/MM/DD

Total daily event count

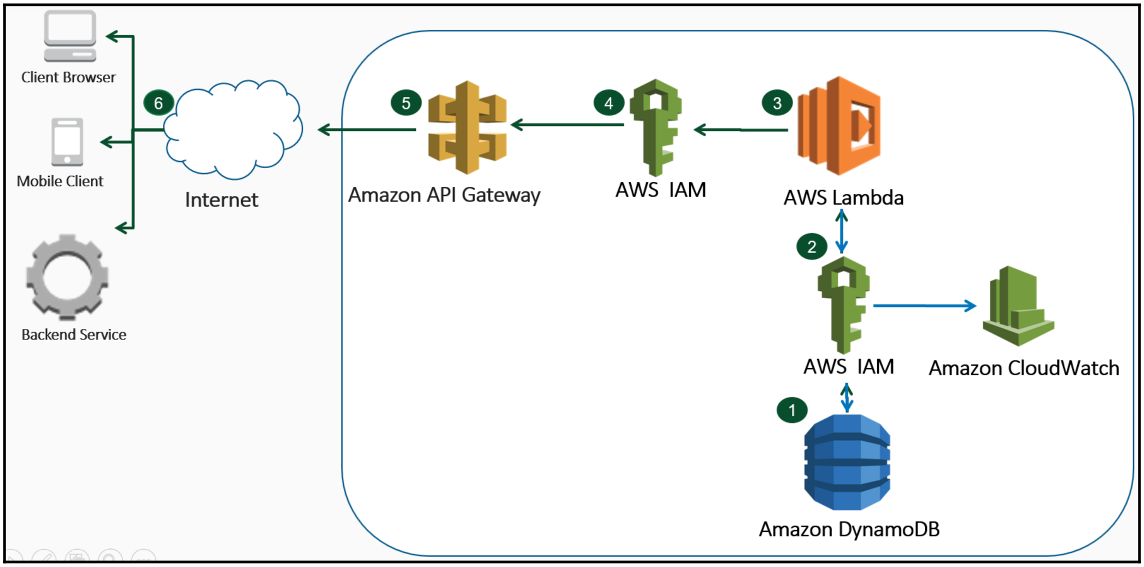
EventId	EventDay	EventCount
324	2017/10/10	2
324	2017/10/12	10
324	2017/10/13	10
324	2017/10/14	6
324	2017/10/16	6
324	2017/10/17	2

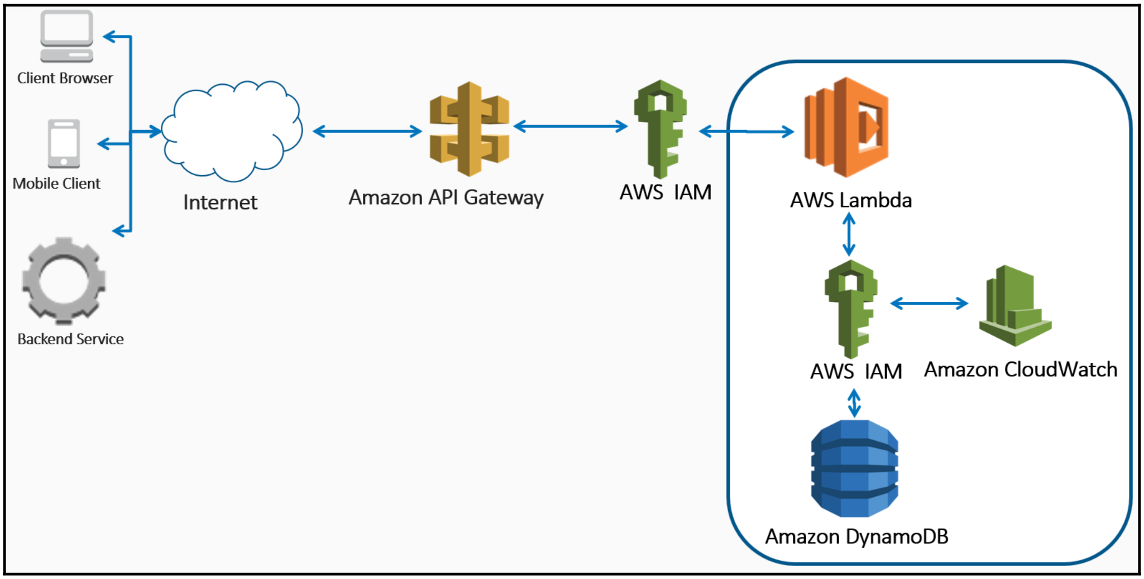


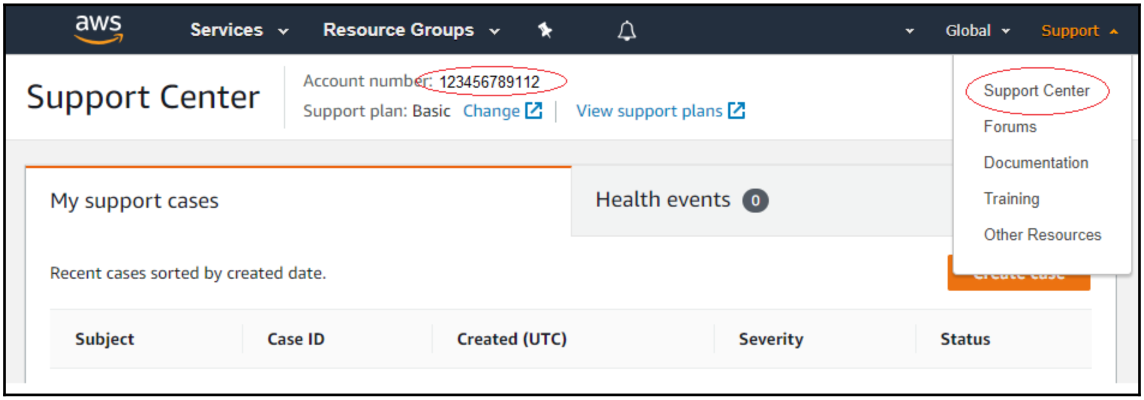
Daily Count of Events per Day
12
10
8
6
4
2
0
2017/10/10
2017/10/11
2017/10/12
2017/10/13
2017/10/14
2017/10/15
2017/10/16
2017/10/17
🟩 EventCount



Client Browser
Mobile Client
Backend Service
1
Internet
2
Amazon API Gateway
3
AWS IAM
4
AWS Lambda
5
AWS IAM
Amazon CloudWatch
6
Amazon DynamoDB


Client Browser
Mobile Client
Backend Service
6
Internet
5
Amazon API Gateway
4
AWS IAM
3
AWS Lambda
2
AWS IAM
Amazon CloudWatch
1
Amazon DynamoDB


Client Browser
Mobile Client
Backend Service
Internet
Amazon API Gateway
AWS IAM
AWS Lambda
AWS IAM
Amazon CloudWatch
Amazon DynamoDB



Support Center

Account number: 123456789112

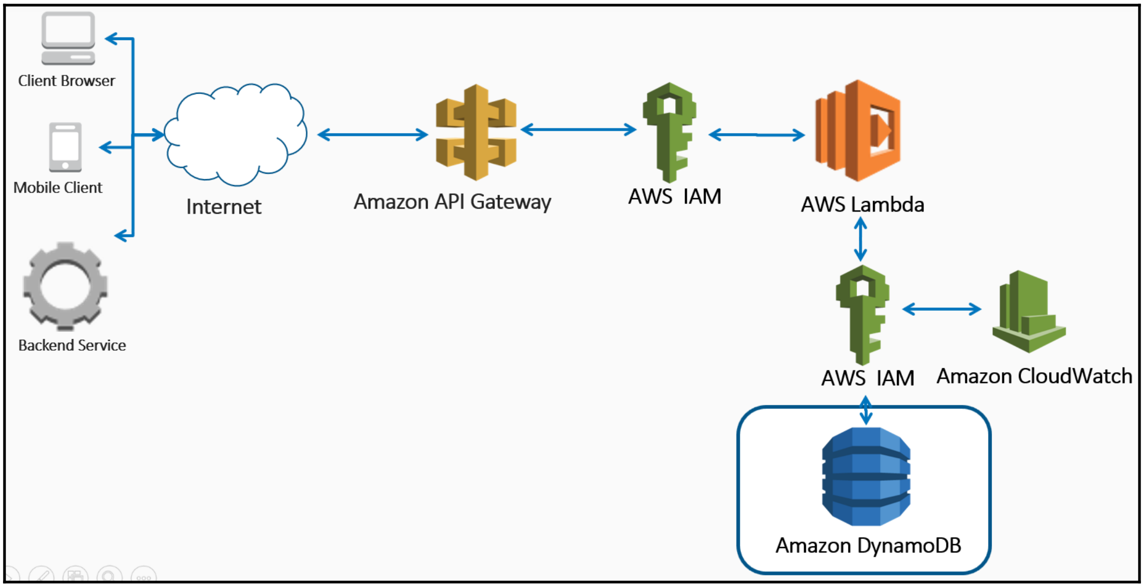
Support plan: Basic Change | View support plans

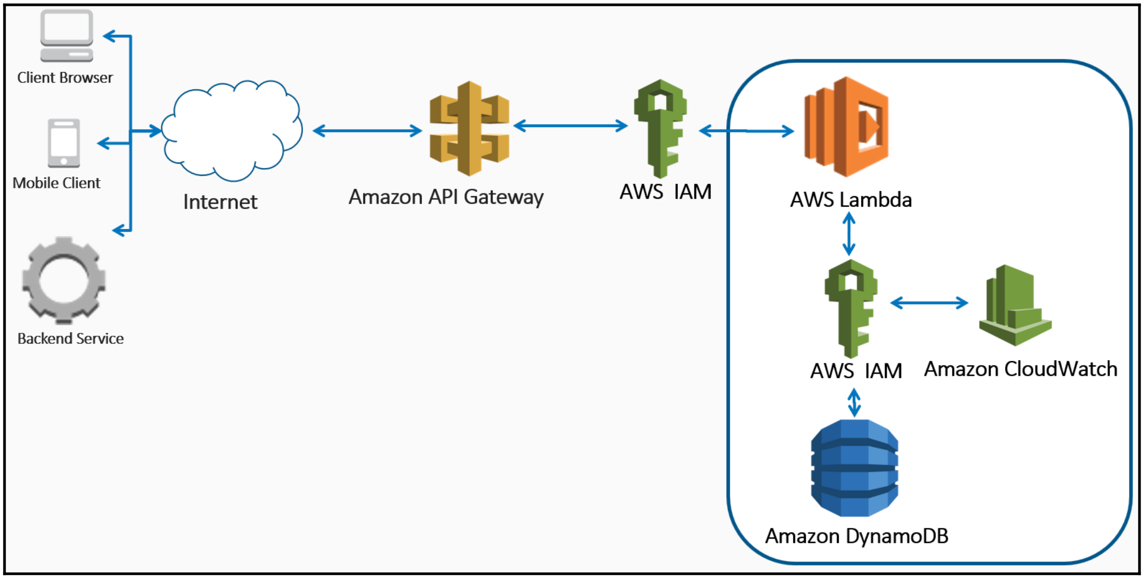
My support cases

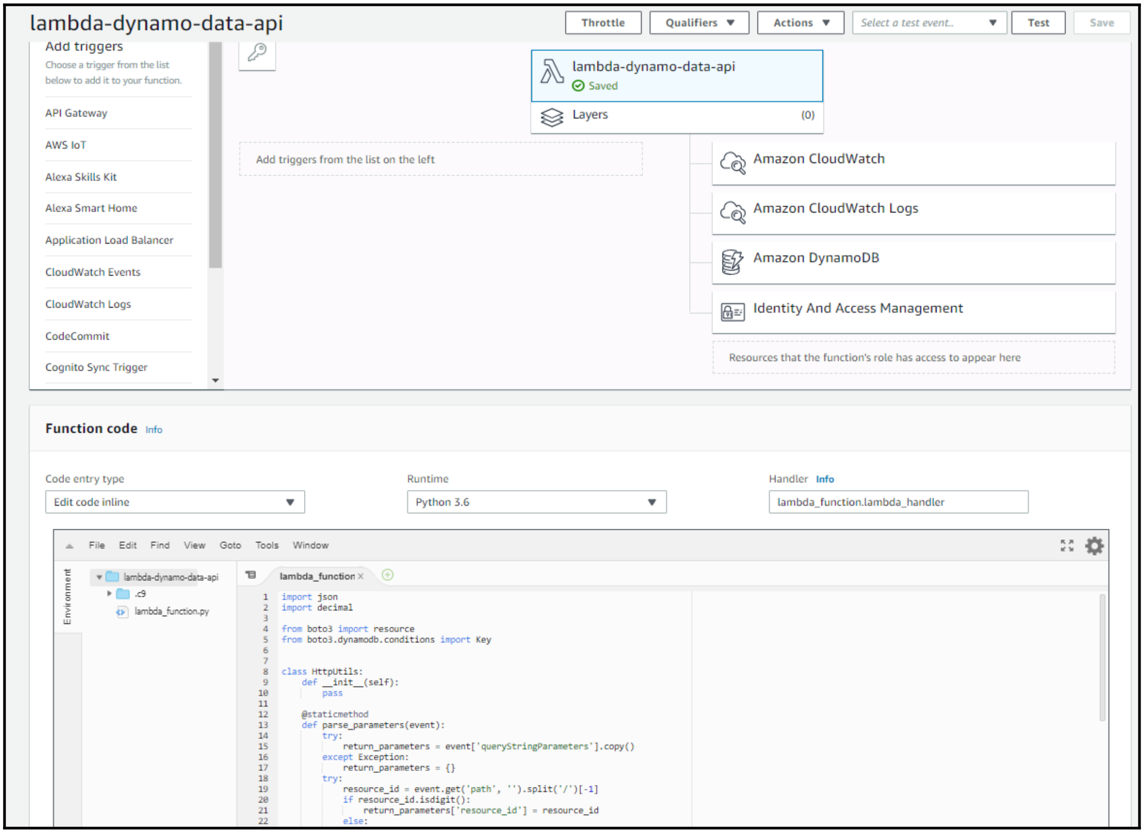
Health events 0

Recent cases sorted by created date.

Subject	Case ID	Created (UTC)	Severity	Status




Client Browser
Mobile Client
Backend Service
Internet
Amazon API Gateway
AWS IAM
AWS Lambda
AWS IAM
Amazon CloudWatch
Amazon DynamoDB



Code entry type: Edit code inline

Runtime: Python 3.6

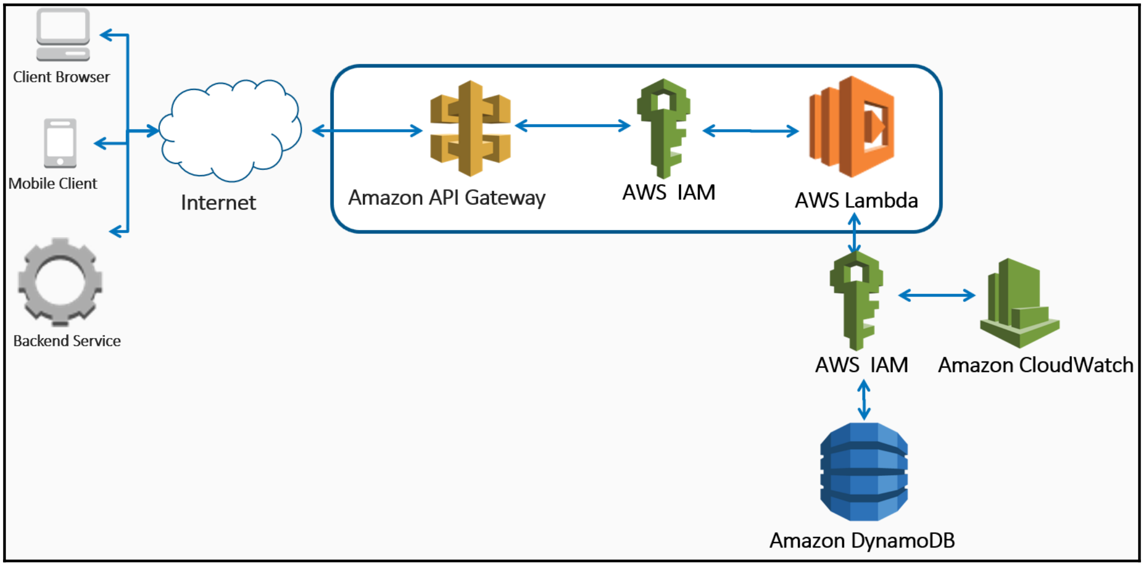
Handler: lambda_function.lambda_handler

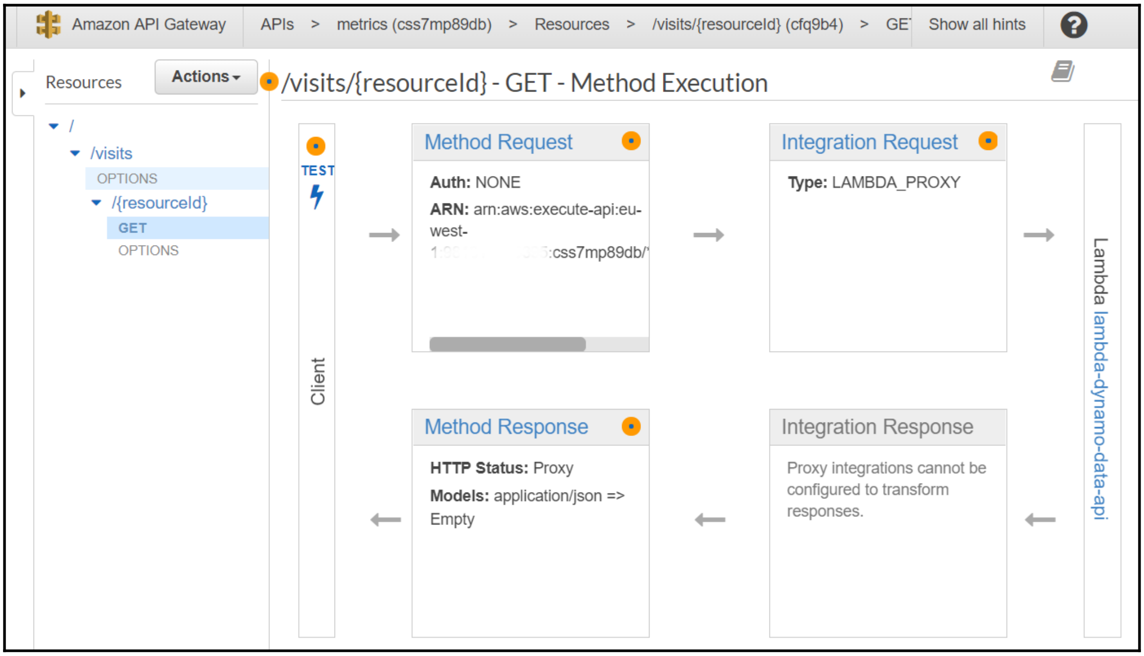
```python
import json
import decimal

from boto3 import resource
from boto3.dynamodb.conditions import Key


class HttpUtils:
    def __init__(self):
        pass

    @staticmethod
    def parse_parameters(event):
        try:
            return_parameters = event['queryStringParameters'].copy()
        except Exception:
            return_parameters = {}
        try:
            resource_id = event.get('path', '').split('/')[-1]
            if resource_id.isdigit():
                return_parameters['resource_id'] = resource_id
            else:
```




Amazon API Gateway
APIs > metrics (css7mp89db) > Resources > /visits/{resourceId} (cfq9b4) > GE
Show all hints
Resources
Actions
/
/visits
OPTIONS
/{resourceId}
GET
OPTIONS
TEST
Client
Lambda lambda-dynamo-data-api

/visits/{resourceId} - GET - Method Execution

Method Request

Auth: NONE

ARN: arn:aws:execute-api:eu-west-1[redacted]:css7mp89db/'

Integration Request

Type: LAMBDA_PROXY

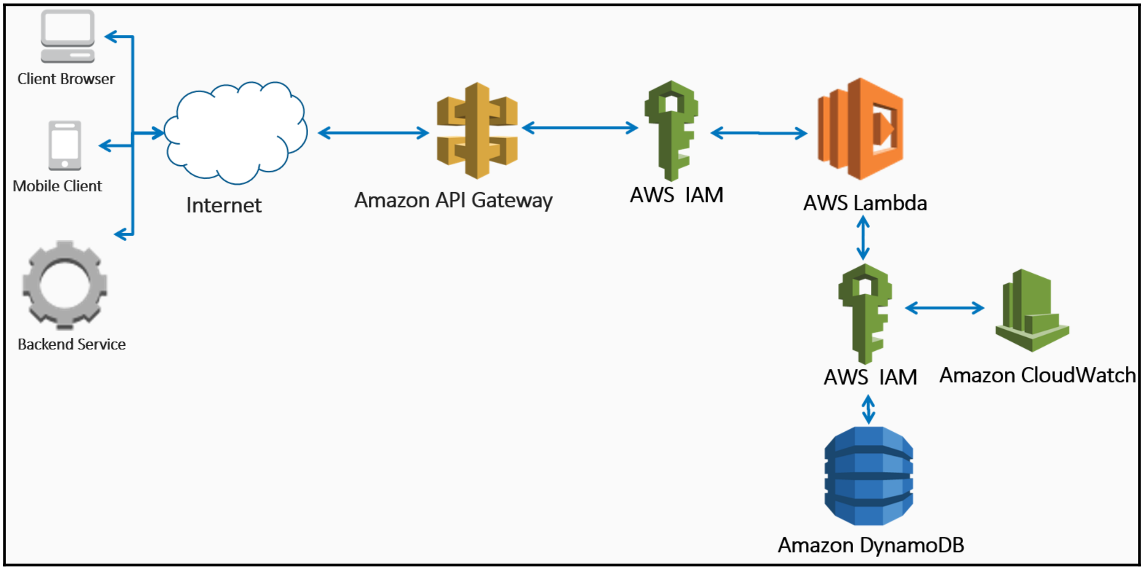
Method Response

HTTP Status: Proxy

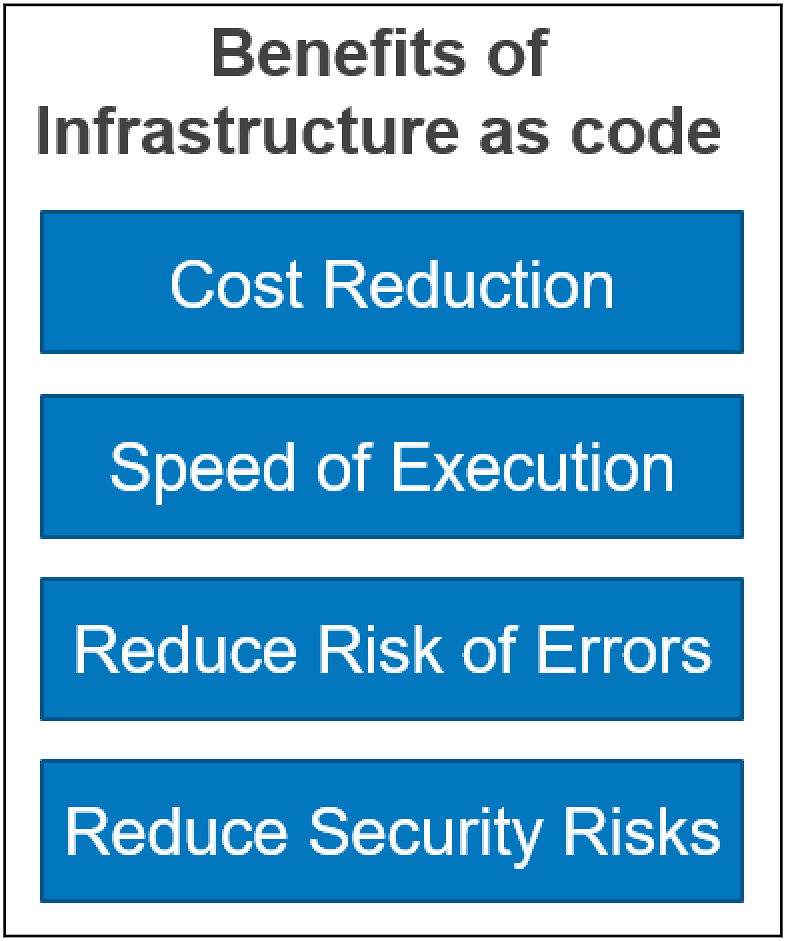
Models: application/json => Empty

Integration Response

Proxy integrations cannot be configured to transform responses.


Client Browser
Mobile Client
Backend Service
Internet
Amazon API Gateway
AWS IAM
AWS Lambda
AWS IAM
Amazon CloudWatch
Amazon DynamoDB

Chapter 3: Deploying Your Serverless Stack



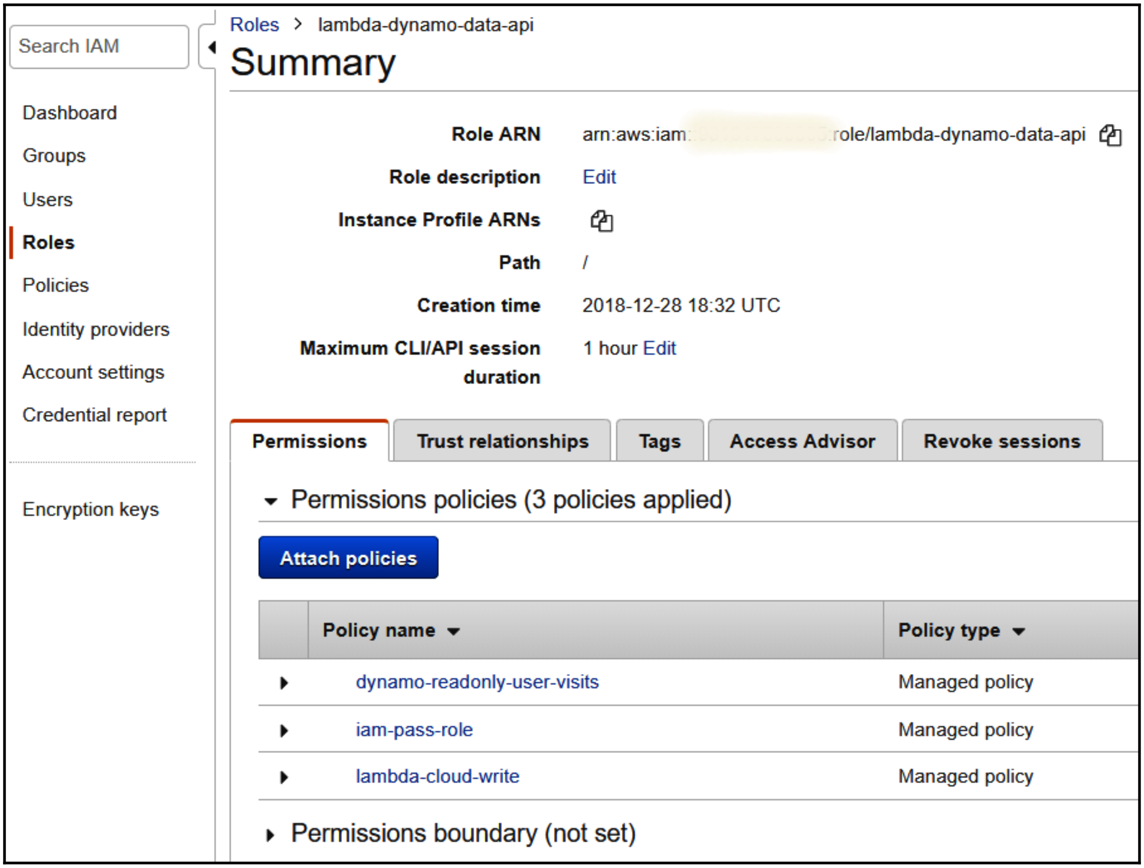
Benefits of Infrastructure as code

Cost Reduction

Speed of Execution

Reduce Risk of Errors

Reduce Security Risks



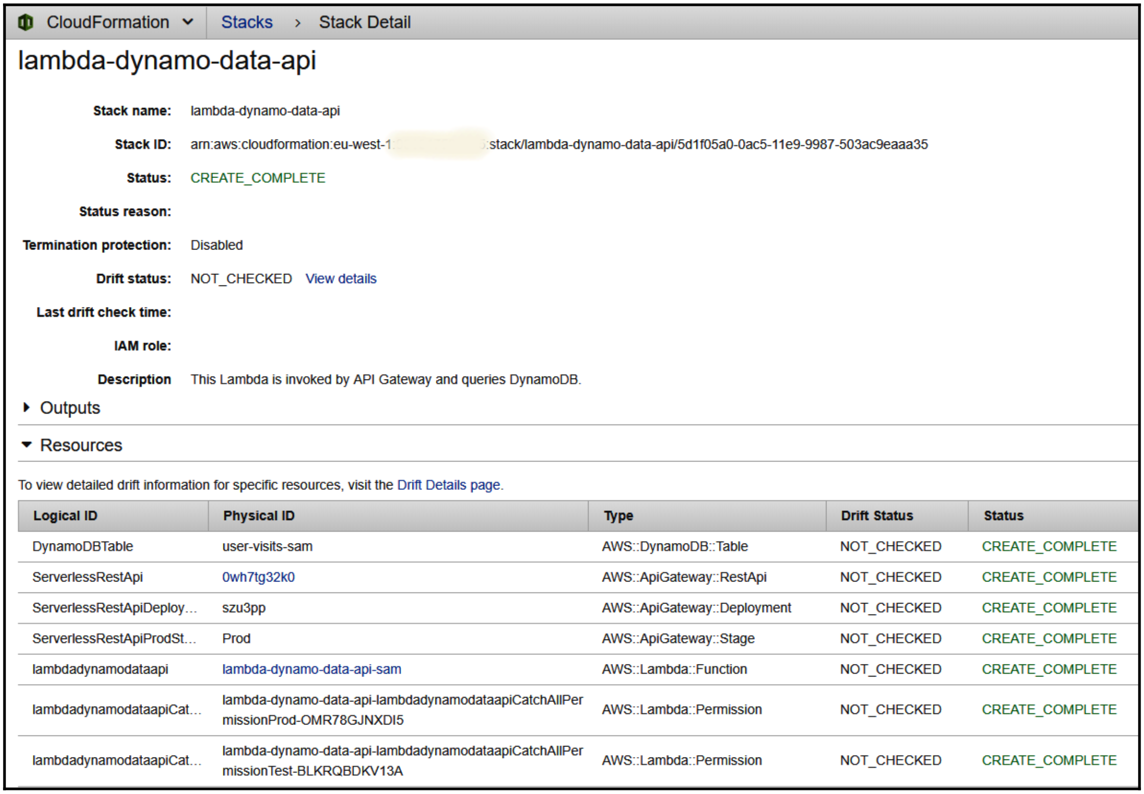
Summary

Role ARN	arn:aws:iam:[redacted]:role/lambda-dynamo-data-api
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2018-12-28 18:32 UTC
Maximum CLI/API session duration	1 hour Edit

▾ Permissions policies (3 policies applied)

Policy name ▾	Policy type ▾
▸ dynamo-readonly-user-visits	Managed policy
▸ iam-pass-role	Managed policy
▸ lambda-cloud-write	Managed policy

▸ Permissions boundary (not set)



lambda-dynamo-data-api

Stack name: lambda-dynamo-data-api

Stack ID: arn:aws:cloudformation:eu-west-1[redacted]:stack/lambda-dynamo-data-api/5d1f05a0-0ac5-11e9-9987-503ac9eaaa35

Status: CREATE_COMPLETE

Status reason:

Termination protection: Disabled

Drift status: NOT_CHECKED View details

Last drift check time:

IAM role:

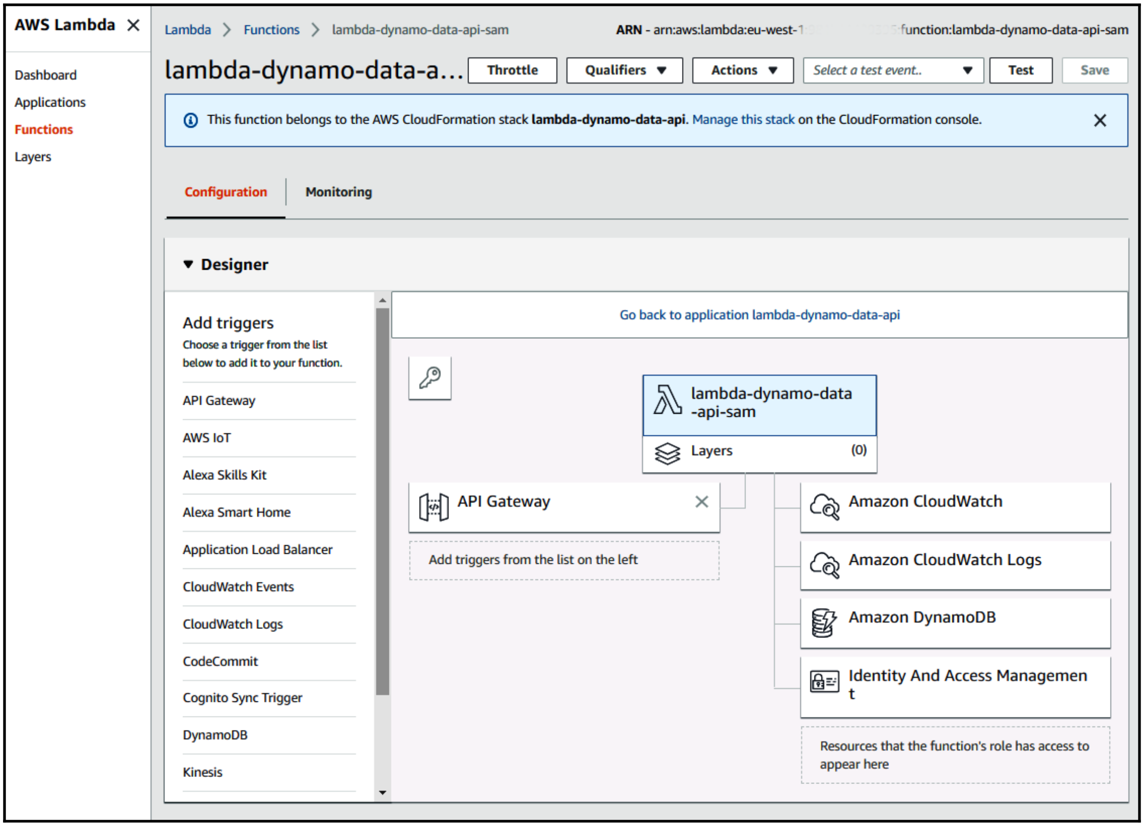
Description This Lambda is invoked by API Gateway and queries DynamoDB.

▸ Outputs

▾ Resources

To view detailed drift information for specific resources, visit the Drift Details page.

Logical ID	Physical ID	Type	Drift Status	Status
DynamoDBTable	user-visits-sam	AWS::DynamoDB::Table	NOT_CHECKED	CREATE_COMPLETE
ServerlessRestApi	0wh7tg32k0	AWS::ApiGateway::RestApi	NOT_CHECKED	CREATE_COMPLETE
ServerlessRestApiDeploy...	szu3pp	AWS::ApiGateway::Deployment	NOT_CHECKED	CREATE_COMPLETE
ServerlessRestApiProdSt...	Prod	AWS::ApiGateway::Stage	NOT_CHECKED	CREATE_COMPLETE
lambdadynamodataapi	lambda-dynamo-data-api-sam	AWS::Lambda::Function	NOT_CHECKED	CREATE_COMPLETE
lambdadynamodataapiCat...	lambda-dynamo-data-api-lambdadynamodataapiCatchAllPermissionProd-OMR78GJNXDI5	AWS::Lambda::Permission	NOT_CHECKED	CREATE_COMPLETE
lambdadynamodataapiCat...	lambda-dynamo-data-api-lambdadynamodataapiCatchAllPermissionTest-BLKRQBDKV13A	AWS::Lambda::Permission	NOT_CHECKED	CREATE_COMPLETE



ARN - arn:aws:lambda:eu-west-1[redacted]function:lambda-dynamo-data-api-sam

lambda-dynamo-data-a...

ⓘ This function belongs to the AWS CloudFormation stack **lambda-dynamo-data-api**. Manage this stack on the CloudFormation console. ✕

Add triggers

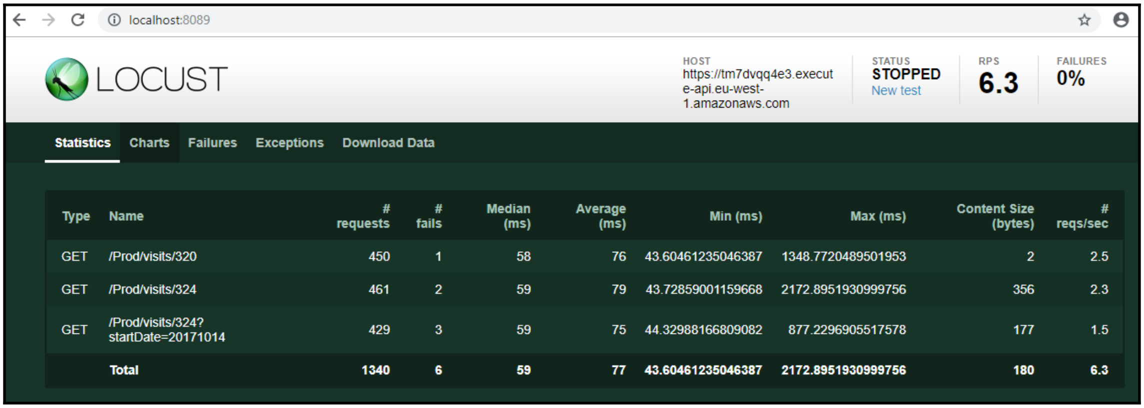
Choose a trigger from the list below to add it to your function.

Go back to application lambda-dynamo-data-api

Add triggers from the list on the left

Resources that the function's role has access to appear here

Chapter 4: Testing Your Serverless Microservice



HOST https://tm7dvqq4e3.execute-api.eu-west-1.amazonaws.com

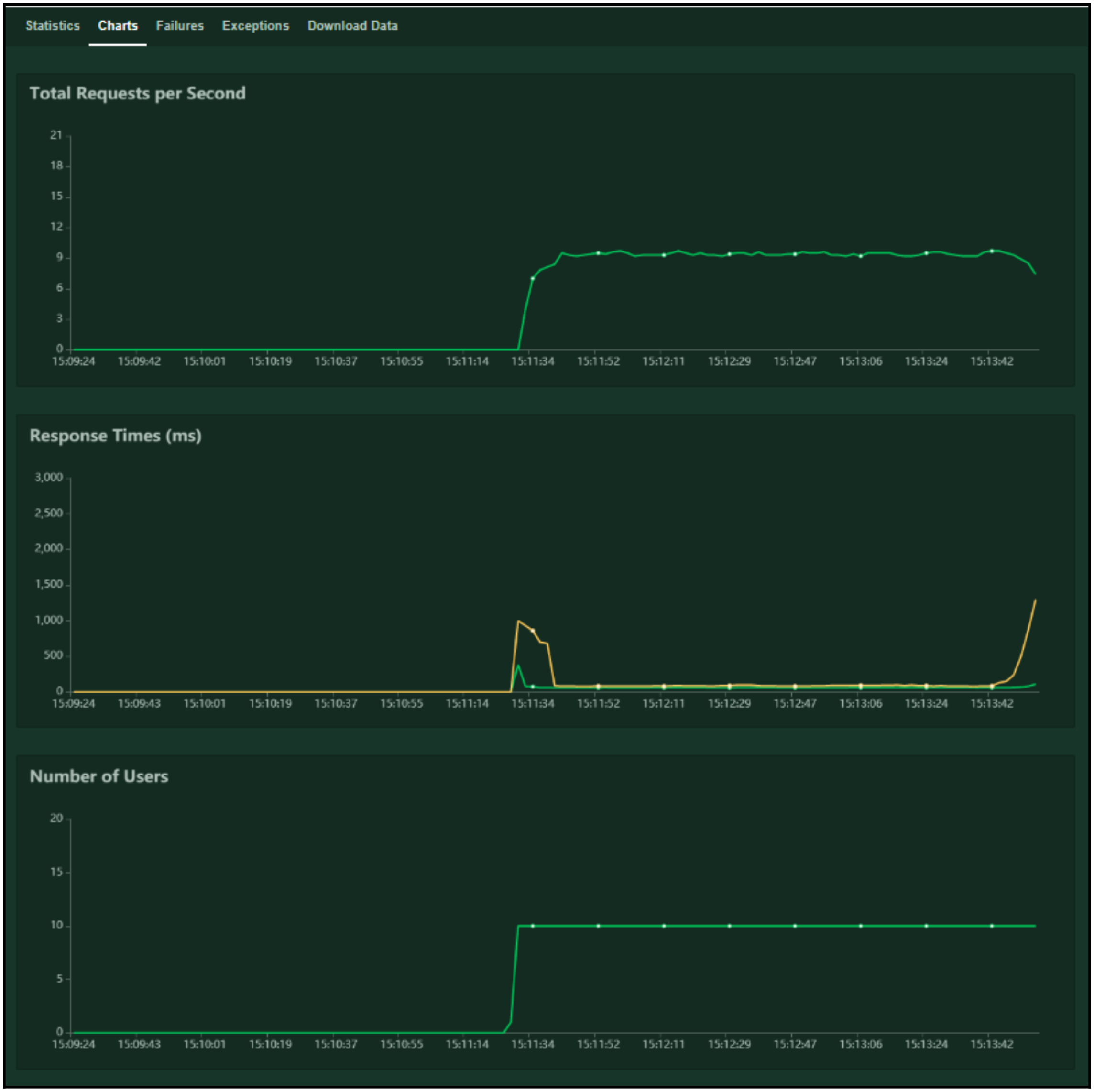
STATUS STOPPED

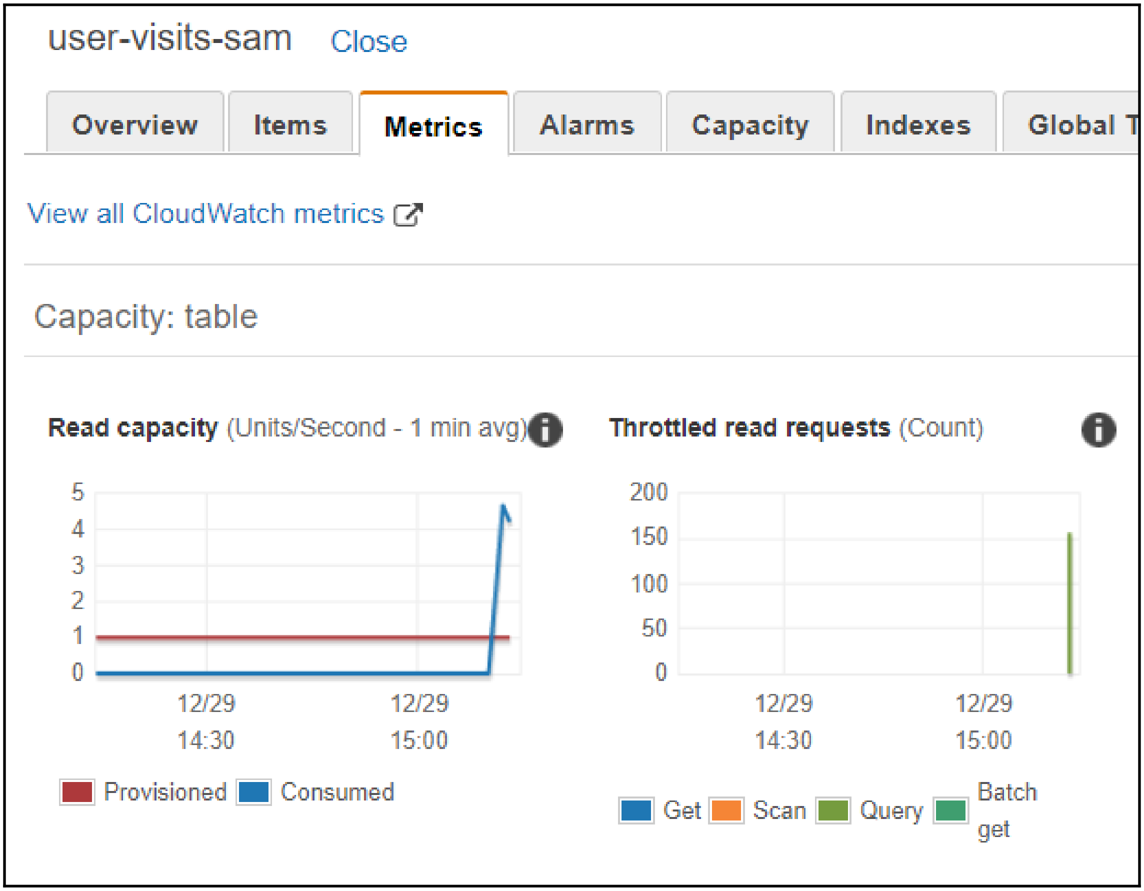
New test

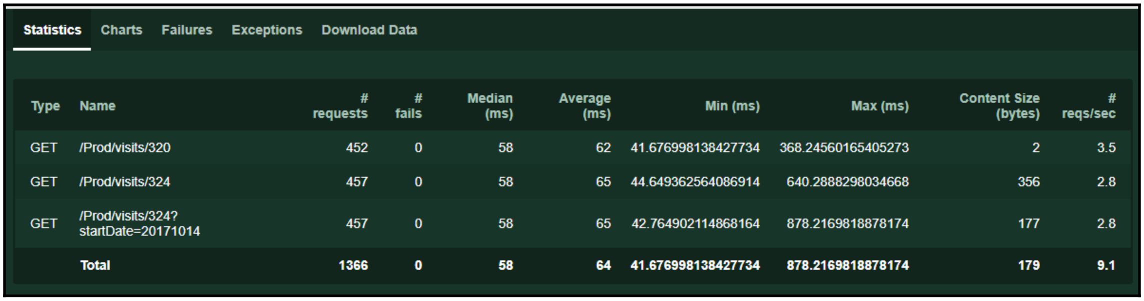
RPS 6.3

FAILURES 0%

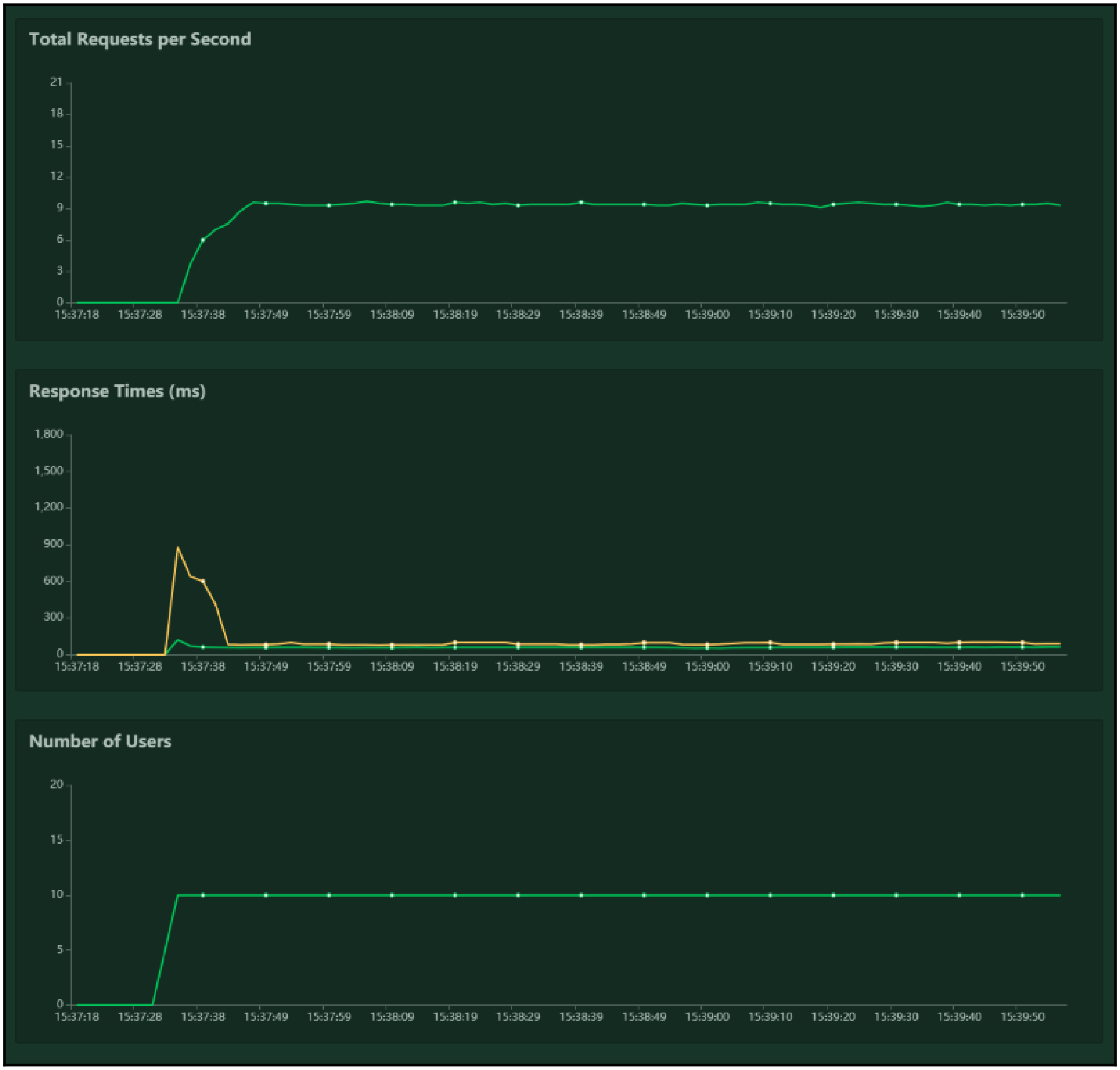
Type	Name	# requests	# fails	Median (ms)	Average (ms)	Min (ms)	Max (ms)	Content Size (bytes)	# reqs/sec
GET	/Prod/visits/320	450	1	58	76	43.60461235046387	1348.7720489501953	2	2.5
GET	/Prod/visits/324	461	2	59	79	43.72859001159668	2172.8951930999756	356	2.3
GET	/Prod/visits/324?startDate=20171014	429	3	59	75	44.32988166809082	877.2296905517578	177	1.5
	Total	**1340**	**6**	**59**	**77**	**43.60461235046387**	**2172.8951930999756**	**180**	**6.3**


Statistics
Charts
Failures
Exceptions
Download Data
Total Requests per Second
21
18
15
12
9
6
3
0
15:09:24
15:09:42
15:10:01
15:10:19
15:10:37
15:10:55
15:11:14
15:11:34
15:11:52
15:12:11
15:12:29
15:12:47
15:13:06
15:13:24
15:13:42
Response Times (ms)
3,000
2,500
2,000
1,500
1,000
500
0
15:09:24
15:09:43
15:10:01
15:10:19
15:10:37
15:10:55
15:11:14
15:11:34
15:11:52
15:12:11
15:12:29
15:12:47
15:13:06
15:13:24
15:13:42
Number of Users
20
15
10
5
0
15:09:24
15:09:43
15:10:01
15:10:19
15:10:37
15:10:55
15:11:14
15:11:34
15:11:52
15:12:11
15:12:29
15:12:47
15:13:06
15:13:24
15:13:42

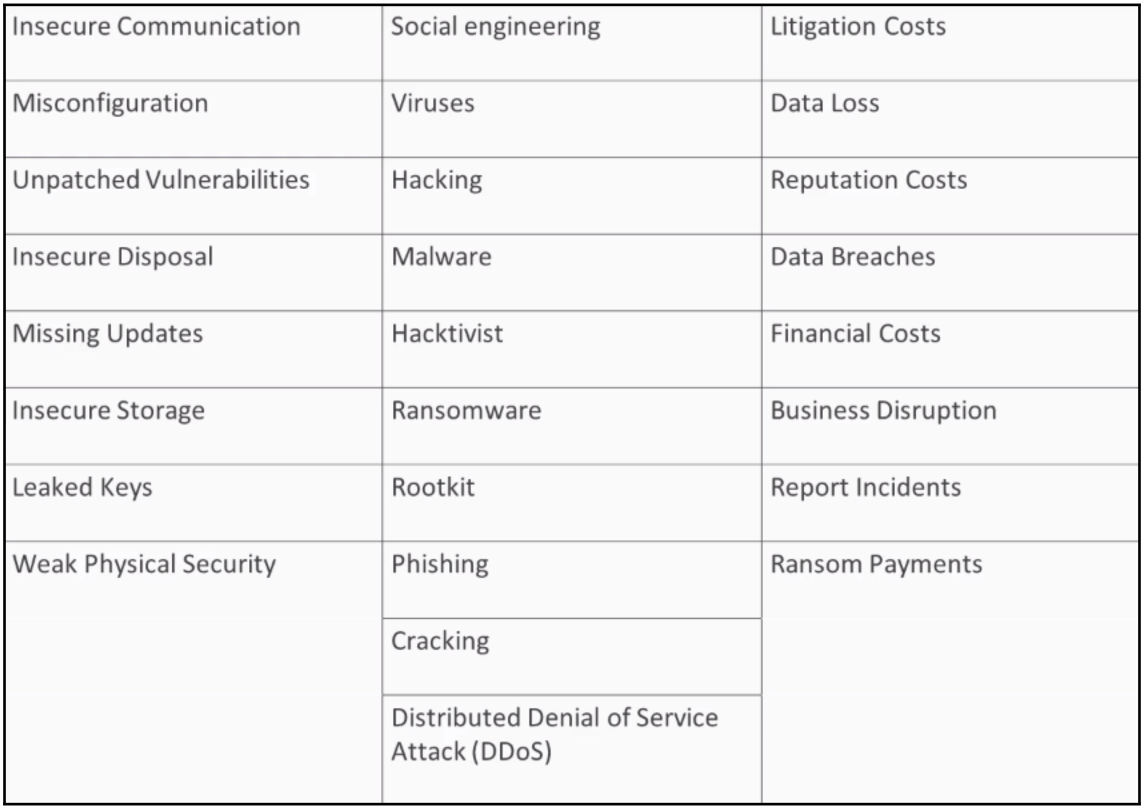




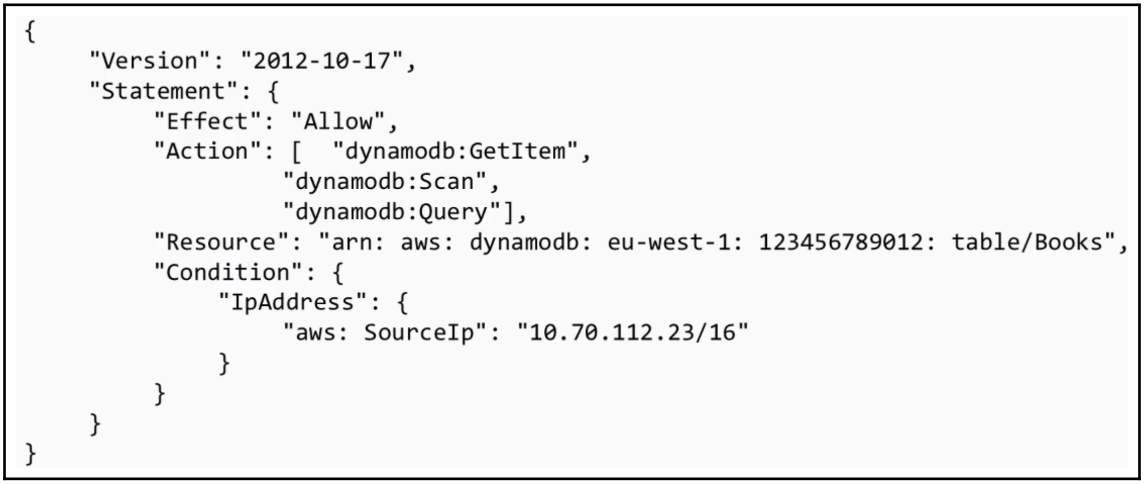
Type	Name	# requests	# fails	Median (ms)	Average (ms)	Min (ms)	Max (ms)	Content Size (bytes)	# reqs/sec
GET	/Prod/visits/320	452	0	58	62	41.676998138427734	368.24560165405273	2	3.5
GET	/Prod/visits/324	457	0	58	65	44.649362564086914	640.2888298034668	356	2.8
GET	/Prod/visits/324? startDate=20171014	457	0	58	65	42.764902114868164	878.2169818878174	177	2.8
	Total	**1366**	**0**	**58**	**64**	**41.676998138427734**	**878.2169818878174**	**179**	**9.1**


Total Requests per Second
21
18
15
12
9
6
3
0
15:37:18
15:37:28
15:37:38
15:37:49
15:37:59
15:38:09
15:38:19
15:38:29
15:38:39
15:38:49
15:39:00
15:39:10
15:39:20
15:39:30
15:39:40
15:39:50
Response Times (ms)
1,800
1,500
1,200
900
600
300
0
15:37:18
15:37:28
15:37:38
15:37:49
15:37:59
15:38:09
15:38:19
15:38:29
15:38:39
15:38:49
15:39:00
15:39:10
15:39:20
15:39:30
15:39:40
15:39:50
Number of Users
20
15
10
5
0
15:37:18
15:37:28
15:37:38
15:37:49
15:37:59
15:38:09
15:38:19
15:38:29
15:38:39
15:38:49
15:39:00
15:39:10
15:39:20
15:39:30
15:39:40
15:39:50

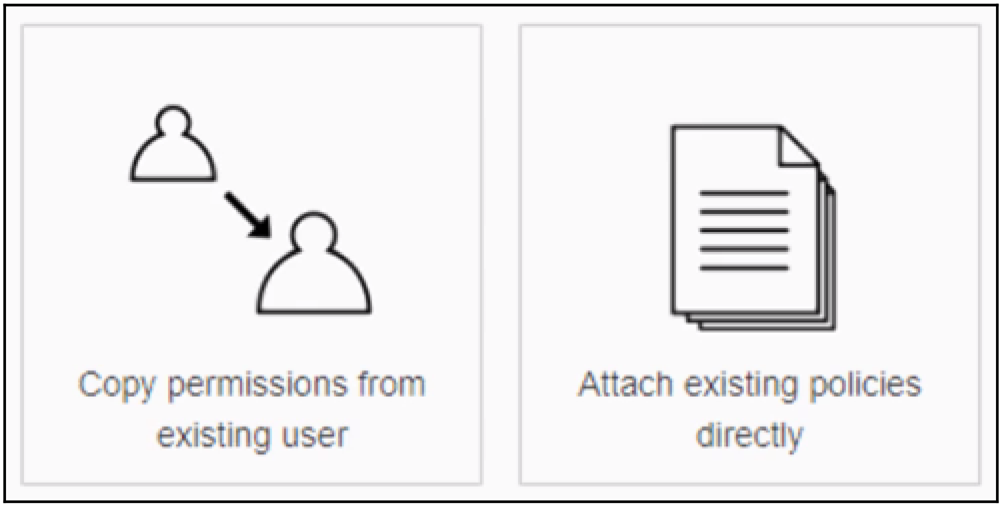
Chapter 5: Securing Your Microservice

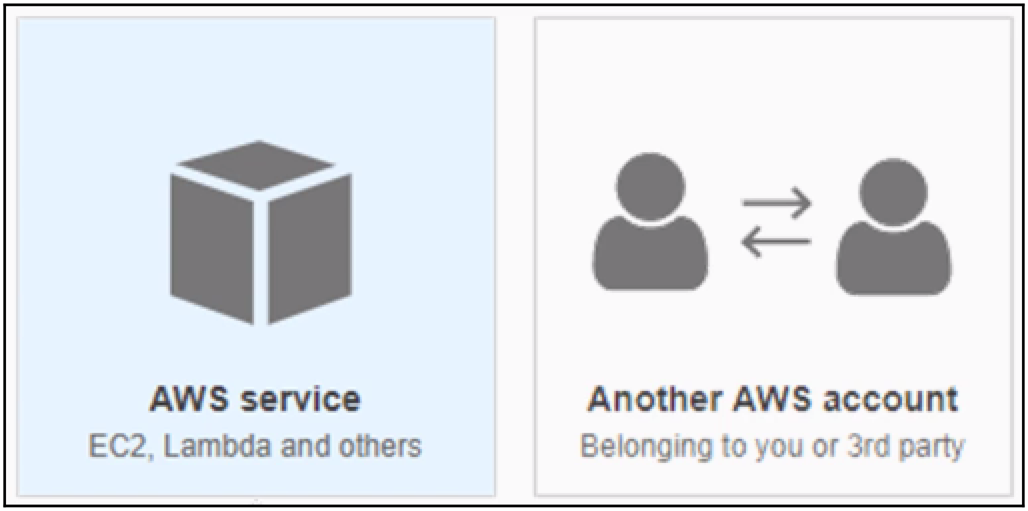


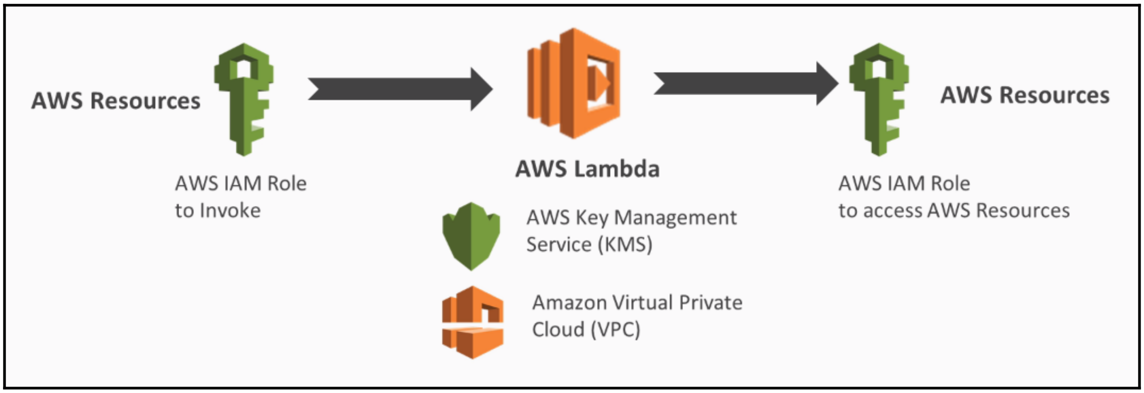
Insecure Communication	Social engineering	Litigation Costs
Misconfiguration	Viruses	Data Loss
Unpatched Vulnerabilities	Hacking	Reputation Costs
Insecure Disposal	Malware	Data Breaches
Missing Updates	Hacktivist	Financial Costs
Insecure Storage	Ransomware	Business Disruption
Leaked Keys	Rootkit	Report Incidents
Weak Physical Security	Phishing	Ransom Payments
	Cracking	
	Distributed Denial of Service Attack (DDoS)	

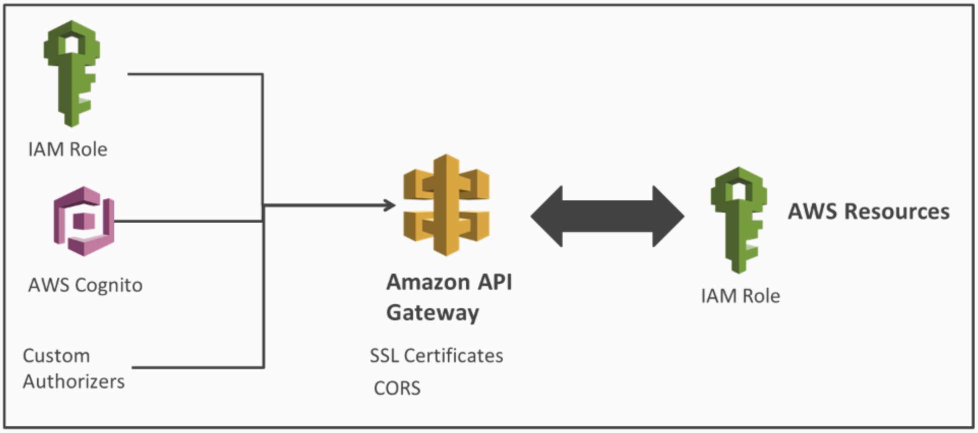


```
{
     "Version": "2012-10-17",
     "Statement": {
          "Effect": "Allow",
          "Action": [   "dynamodb:GetItem",
                    "dynamodb:Scan",
                    "dynamodb:Query"],
          "Resource": "arn: aws: dynamodb: eu-west-1: 123456789012: table/Books",
          "Condition": {
               "IpAddress": {
                    "aws: SourceIp": "10.70.112.23/16"
               }
          }
     }
}
```


Copy permissions from existing user
Attach existing policies directly


AWS service
EC2, Lambda and others
Another AWS account
Belonging to you or 3rd party


AWS Resources
AWS IAM Role
to Invoke
AWS Lambda
AWS Key Management
Service (KMS)
Amazon Virtual Private
Cloud (VPC)
AWS Resources
AWS IAM Role
to access AWS Resources



https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-to-api.html