

NGINX Modern Reference Architecture

(Scalability, Portability, Resiliency, Agility)

Shawn K.

What is “Modern Application”

- It MUST be
 - Microservices
 - Containerized
 - Cloud Native
- It CAN'T be
 - Monolith
 - Baremetal

What a Modern Application Architecture Provides

- **Scalability**

- Quickly and seamlessly scale up or down to accommodate spikes or reductions in demand, anywhere in the world

- **Portability**

- Runs on multi-clouds/on-prem, multi-devices

- **Resiliency**

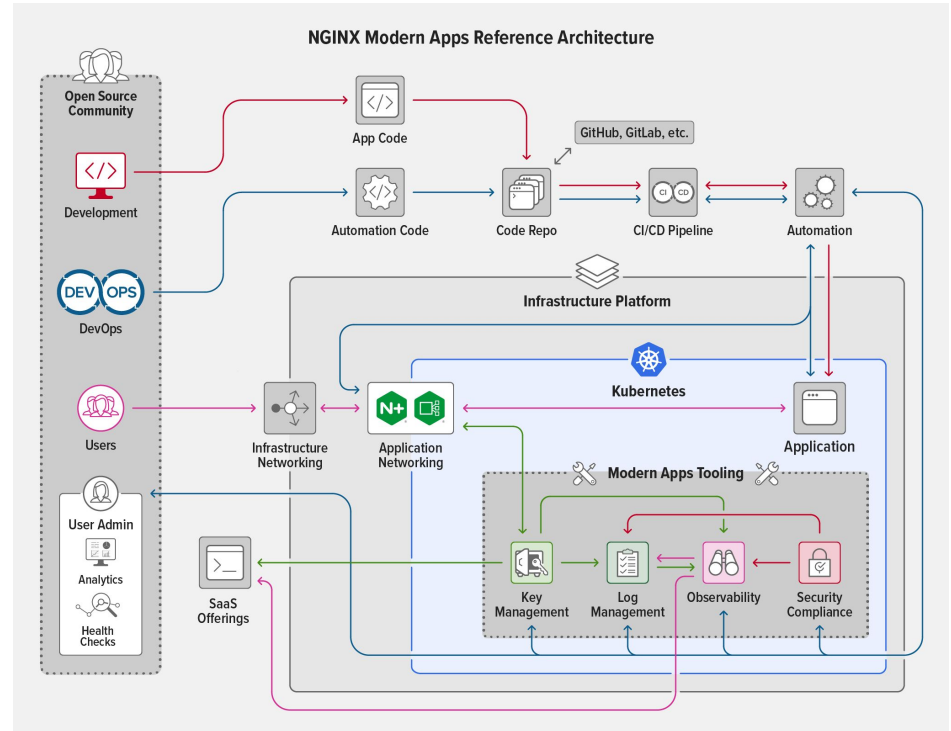
- Can failover to newly spun-up or virtual environments in different available regions, clouds, or data centers

- **Agility**

- Ability to update through automated CI/CD pipelines with higher code velocity and more frequent code pushes

What a Modern Application Architecture Provides

- **What are we trying to build**
 - Easy deployable K8s architecture
 - Easy button for KIC build & deploy
 - Stealable examples of how to do things
 - Modern app design principles
 - Pluggable deployment framework
- **What do have today**
 - [Open source](#)
 - Infrastructure as code w/ Pulumi
 - KIC image is built
 - K8s is deployed via AWS EKS
 - Log mgmt. Using Elastic tools
 - TLS enabled via Cert Manager
 - Demo app: Bank of Sirius (Google)



What Does Reference Architecture Do Today?

```
vpc - defines and installs the VPC and subnets to use with EKS
├─ eks - deploys EKS
│   └─ ecr - configures ECR for use in the cluster
│       └─ kic-image-build - builds KIC image for NGINX Plus
│           └─ kic-image-push - pushes KIC image built in previous step to ECR
│               └─ kic-helm-chart - deploys NGINX Ingress Controller to the EKS cluster
│                   └─ logstore - deploys a logstore (elasticsearch) to the EKS cluster
│                       └─ logagent - deploys a logging agent (filebeat) to the EKS cluster
│                           └─ certmgr - deploys the open source cert-manager.io helm chart to the EKS cluster
│                               └─ sirius - deploys a fork of Google's Bank of Anthos application to the EKS cluster
```

- **TODO**

- **Observability:** provided by Open Telemetry w/ Prometheus for metric storage & Grafana for visualization
- CD Examples
- Performance testing framework
- Admin cluster & app cluster segmentation

Getting Started w/ Pulumi for AWS

```
(venv) SEA-ML-00058228:kic-reference-architectures hankin$ ./bin/start.sh
Adding to [Users/hankin/pjt/github/shawnglx/kic-reference-architectures/bin/venv/bin] to PATH
Manage your Pulumi stacks by logging in.
Run 'pulumi login --help' for alternative login options.
Enter your access token from https://app.pulumi.com/account/tokens
or hit <ENTER> to log in using your browser
:
```

Welcome to Pulumi!

Pulumi helps you create, deploy, and manage infrastructure on any cloud using your favorite language. You can get started today with Pulumi at:

<https://www.pulumi.com/docs/get-started/>

Tip of the day: Resources you create with Pulumi are given unique names (a randomly generated suffix) by default. To learn more about auto-naming or customizing resource names see <https://www.pulumi.com/docs/intro/concepts/resources/#autonaming>.

Logged in to pulumi.com as shawnhankin (<https://app.pulumi.com/shawnhankin>)

NOTICE! This shell script will call the appropriate helper script depending on your answer to the next question.

This script currently supports standing up AWS, Linode, and Digital Ocean Kubernetes deployments, provided the correct credentials are supplied. It also supports the user of a kubeconfig file with a defined cluster name and context, which must be provided by the user.

Please read the documentation for more details.

Type a for AWS, d for Digital Ocean, k for kubeconfig, l for Linode? a

Calling AWS startup script

Enter the name of the Pulumi stack to use in all projects: mara-test

Submodule source found

Configuring all Pulumi projects to use the stack: mara-test

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Created stack 'mara-test'

Using AWS_PROFILE from environment:

Using AWS_DEFAULT_REGION from environment/config: us-east-2

Checking for required secrets

Create a password for the grafana admin user; this password will be used to access the Grafana dashboard

This should be an alphanumeric string without any shell special characters; it is presented in plain text

due to current limitations with Pulumi secrets. You will need this password to access the Grafana dashboard.

value:

error: configuration key 'aws:profile' not found for stack 'mara-test'

Validating AWS credentials

```
Version 1.10.2
Version and Account Information
Pulumi version is: v3.32.1
Pulumi user is: shawnhankin
Python version is: Python 3.9.13
Kubectl version information:
The connection to the server localhost:8080 was refused - did you specify the right host or port?
{
  "clientVersion": {
    "major": "1",
    "minor": "23",
    "gitVersion": "v1.23.6",
    "gitCommit": "ad338546d947756688a88a6822e9c11e7eac22",
    "gitTreeState": "clean",
    "buildDate": "2022-04-14T08:49:13Z",
    "goVersion": "go1.17.9",
    "compiler": "gc",
    "platform": "darwin/amd64"
  }
}
Python module information:
Package Version
-----
Arpeggio 1.10.2
attrs 21.4.0
awscli 1.22.101
botocore 1.24.46
certifi 2022.5.18.1
charset-normalizer 2.0.12
colorama 0.4.3
dill 0.3.5.1
distlib 0.3.5
docutils 0.15.2
fart 0.1.5
filelock 3.8.0
gitdb 4.0.9
gitPython 3.1.27
grpcio 1.43.0
idna 3.3
jmespath 1.0.0
kic-pulumi-utils 1.0.1.post1-git.852af9f6
linode-cli 5.17.2
litalc 1.4
nodeenv 1.6.0
packaging 21.3
parver 0.3.1
passlib 1.7.4
pip 22.2.2
pipenv 2022.8.24
platformdirs 3.20.1
protobuf 3.32.1
pulumi 3.32.1
pulumi-aws 5.4.0
pulumi-digitalocean 4.12.0
pulumi-docker 3.1.0
pulumi-eks 0.39.0
pulumi-kubernetes 3.19.1
pulumi-linode 3.7.1
pyasn1 0.4.8
pycryptodome 3.14.1
pyparsing 3.0.9
pyperclip 1.8.2
python-dateutil 2.8.2
PYAML 5.4.1
requests 2.27.1
rsa 4.7.2
s3transfer 0.5.2
semver 2.13.0
setuptools 62.3.2
setuptools-git-versioning 1.9.2
six 1.16.0
smp 5.0.0
terminaltables 3.1.10
toml 0.10.2
urllib3 1.26.9
virtualenv 20.16.3
virtualenv-clone 0.5.7
wheel 0.37.1
yamlreader 3.0.4
```

```
Python module information:
Package Version
-----
Arpeggio 1.10.2
attrs 21.4.0
awscli 1.22.101
botocore 1.24.46
certifi 2022.5.18.1
charset-normalizer 2.0.12
colorama 0.4.3
dill 0.3.5.1
distlib 0.3.5
docutils 0.15.2
fart 0.1.5
filelock 3.8.0
gitdb 4.0.9
gitPython 3.1.27
grpcio 1.43.0
idna 3.3
jmespath 1.0.0
kic-pulumi-utils 1.0.1.post1-git.852af9f6
linode-cli 5.17.2
litalc 1.4
nodeenv 1.6.0
packaging 21.3
parver 0.3.1
passlib 1.7.4
pip 22.2.2
pipenv 2022.8.24
platformdirs 3.20.1
protobuf 3.32.1
pulumi 3.32.1
pulumi-aws 5.4.0
pulumi-digitalocean 4.12.0
pulumi-docker 3.1.0
pulumi-eks 0.39.0
pulumi-kubernetes 3.19.1
pulumi-linode 3.7.1
pyasn1 0.4.8
pycryptodome 3.14.1
pyparsing 3.0.9
pyperclip 1.8.2
python-dateutil 2.8.2
PYAML 5.4.1
requests 2.27.1
rsa 4.7.2
s3transfer 0.5.2
semver 2.13.0
setuptools 62.3.2
setuptools-git-versioning 1.9.2
six 1.16.0
smp 5.0.0
terminaltables 3.1.10
toml 0.10.2
urllib3 1.26.9
virtualenv 20.16.3
virtualenv-clone 0.5.7
wheel 0.37.1
yamlreader 3.0.4
```

vpc - defines and installs the VPC and subnets to use with EKS

eks - deploys EKS

```
#####
#                                     #
#      A W S V P C                  #
#                                     #
#                                     #
#                                     #
#####
```

Previewing update (mara-test)

View Live: <https://app.pulumi.com/shawnhankim/aws-vpc/mara-test/previews/93c642a3-95d3-47ec-9154-c010b59a154c>

[resource plugin aws-5.4.0] installing

Downloading plugin: 0 B / 103.68 MiB [-----] 0.00%[resource plugin eks-0.39.0] installing

Downloading plugin: 679.83 KiB / 679.83 KiB [-----] 100.00% 0s

[resource plugin kubernetess-3.19.1] installing

[resource plugin digitalocean-4.12.0] installing

Downloading plugin: 0 B / 17.13 MiB [-----] 0.00%[resource plugin linode-3.7.1] installing

Downloading plugin: 1.12 MiB / 25.83 MiB [-----] 4.35% 00m30s[resource plugin docker-3.1.0] installing

Downloading plugin: 16.43 MiB / 16.43 MiB [-----] 100.00% 5s

Downloading plugin: 17.13 MiB / 17.13 MiB [-----] 100.00% 26s

Downloading plugin: 25.83 MiB / 25.83 MiB [-----] 100.00% 36s

Downloading plugin: 30.03 MiB / 30.03 MiB [-----] 100.00% 39s

Downloading plugin: 103.68 MiB / 103.68 MiB [-----] 100.00% 1m0s

Type	Name	Plan
pulumi:pulumi:Stack	aws-vpc-mara-test	create
aws:ec2:Vpc	eks-aws-vpc-mara-test	create
aws:ec2:InternetGateway	vpc-ig-aws-vpc-mara-test	create
aws:ec2:RouteTable	vpc-route-table-aws-vpc-mara-test	create
aws:ec2:Subnet	us-east-2a-k8s-public-aws-vpc-mara-test-0	create
aws:ec2:Subnet	us-east-2b-k8s-public-aws-vpc-mara-test-1	create
aws:ec2:Subnet	us-east-2c-k8s-private-aws-vpc-mara-test-0	create
aws:ec2:Subnet	us-east-2c-k8s-public-aws-vpc-mara-test-2	create
aws:ec2:Subnet	us-east-2b-k8s-private-aws-vpc-mara-test-1	create
aws:ec2:Subnet	us-east-2c-k8s-private-aws-vpc-mara-test-2	create
aws:ec2:SecurityGroup	eks-cluster-sg-aws-vpc-mara-test	create
aws:ec2:RouteTableAssociation	route-table-assoc-public-us-east-2b-1	create
aws:ec2:RouteTableAssociation	route-table-assoc-public-us-east-2a-0	create
aws:ec2:RouteTableAssociation	route-table-assoc-private-us-east-2a-aws-vpc-mara-test-0	create
aws:ec2:RouteTableAssociation	route-table-assoc-public-us-east-2c-2	create
aws:ec2:RouteTableAssociation	route-table-assoc-private-us-east-2b-aws-vpc-mara-test-1	create
aws:ec2:RouteTableAssociation	route-table-assoc-private-us-east-2c-aws-vpc-mara-test-2	create

Resources:

+ 17 to create

Updating (mara-test)

View Live: <https://app.pulumi.com/shawnhankim/aws-vpc/mara-test/updates/1>

Type	Name	Status
pulumi:pulumi:Stack	aws-vpc-mara-test	created
aws:ec2:Vpc	eks-aws-vpc-mara-test	created
aws:ec2:InternetGateway	vpc-ig-aws-vpc-mara-test	created
aws:ec2:Subnet	us-east-2a-k8s-public-aws-vpc-mara-test-0	created
aws:ec2:Subnet	us-east-2c-k8s-public-aws-vpc-mara-test-2	created
aws:ec2:Subnet	us-east-2b-k8s-public-aws-vpc-mara-test-1	created
aws:ec2:Subnet	us-east-2b-k8s-private-aws-vpc-mara-test-1	created
aws:ec2:Subnet	us-east-2a-k8s-private-aws-vpc-mara-test-0	created
aws:ec2:SecurityGroup	eks-cluster-sg-aws-vpc-mara-test	created
aws:ec2:Subnet	us-east-2c-k8s-private-aws-vpc-mara-test-2	created
aws:ec2:RouteTable	vpc-route-table-aws-vpc-mara-test	created
aws:ec2:RouteTableAssociation	route-table-assoc-private-us-east-2a-aws-vpc-mara-test-0	created
aws:ec2:RouteTableAssociation	route-table-assoc-private-us-east-2b-aws-vpc-mara-test-1	created
aws:ec2:RouteTableAssociation	route-table-assoc-private-us-east-2c-aws-vpc-mara-test-2	created
aws:ec2:RouteTableAssociation	route-table-assoc-public-us-east-2a-0	created
aws:ec2:RouteTableAssociation	route-table-assoc-public-us-east-2b-1	created
aws:ec2:RouteTableAssociation	route-table-assoc-public-us-east-2c-2	created

Outputs:

```
aws: [
  [0]: "us-east-2a"
  [1]: "us-east-2b"
  [2]: "us-east-2c"
]
vpc: {
  arn          : "arn:aws:ec2:us-east-2:64122230151:vpc/vpc-041a70230f358677f"
  assign_generated_ipv6_cidr_block : false
  cidr_block   : "10.100.0.0/16"
  default_network_acl_id : "acl-02a743d480b3ff4d2"
  default_route_table_id : "rtb-02b17ff0add9451f2"
  default_security_group_id : "sg-0958ad05644d79811"
  dhcp_options_id : "dopt-840002ed"
  enable_classiclink : false
  enable_classiclink_dns_support : false
  enable_dns_hostnames : true
  enable_dns_support : true
  id : "vpc-041a70230f358677f"
  instance_tenancy : "default"
  ipv6_network_length : 0
  main_route_table_id : "rtb-02b17ff0add9451f2"
  owner_id : "64122230151"
  tags : {
    Project : "aws-vpc"
    Stack : "mara-test"
    fs:blueops:owner: "H.Klm30RFS.com"
  }
  tags_all : {
    Project : "aws-vpc"
    Stack : "mara-test"
    fs:blueops:owner: "H.Klm30RFS.com"
  }
  urn : "urn:pulumi:mara-test::aws-vpc::aws:ec2:vpc::eks-aws-vpc-mara-test"
}
```

Resources:

+ 17 created

Duration: 29s

vpc - defines and installs the VPC and subnets to use with EKS

eks - deploys EKS

ecr - configures ECR for use in the cluster

AWS EKS

Previewing update (mara-test)

View Live: <https://app.pulumi.com/shawnhankin/aws-eks/mara-test/previews/0e2f15c4-45bb-4862-b7fd-08a4129a762>

Type	Name	Plan	Info
pulumi:pulumi:Stack	aws-eks-mara-test	create	2 warnings; 3 messages
aws:iam:Role	ec2-nodgroup-iam-role	create	
aws:iam:Role	eks-iam-role	create	
aws:iam:RolePolicyAttachment	eks-workernode-policy-attachment	create	
aws:iam:RolePolicyAttachment	ec2-container-ro-policy-attachment	create	
aws:iam:RolePolicyAttachment	eks-cni-policy-attachment	create	
aws:iam:RolePolicyAttachment	eks-cluster-policy-attachment	create	
aws:iam:RolePolicyAttachment	eks-service-policy-attachment	create	
aws:iam:InstanceProfile	node-group-profile-aws-eks-mara-test	create	
eks:index:Cluster	aws-eks-mara-test	create	
eks:index:ServiceRole	aws-eks-mara-test-instanceRole	create	
aws:iam:Role	aws-eks-mara-test-instanceRole-role	create	
aws:iam:RolePolicyAttachment	aws-eks-mara-test-instanceRole-3eb088f2	create	
aws:iam:RolePolicyAttachment	aws-eks-mara-test-instanceRole-03516f97	create	
aws:iam:RolePolicyAttachment	aws-eks-mara-test-instanceRole-elb295bd	create	
eks:index:RandomSuffix	aws-eks-mara-test-cfnStackName	create	
aws:ec2:SecurityGroup	aws-eks-mara-test-eksClusterSecurityGroup	create	
aws:ec2:SecurityGroupRule	aws-eks-mara-test-eksClusterInternetEgressRule	create	
aws:eks:Cluster	aws-eks-mara-test-eksCluster	create	
pulumi:providers:kubernetes	aws-eks-mara-test-eks-k8s	create	
eks:index:VpcCni	aws-eks-mara-test-vpc-cni	create	
aws:ec2:SecurityGroup	aws-eks-mara-test-nodeSecurityGroup	create	
aws:iam:InstanceProfile	aws-eks-mara-test-instanceProfile	create	
kubernetes:core/v1:ConfigMap	aws-eks-mara-test-nodeAccess	create	
aws:ec2:SecurityGroupRule	aws-eks-mara-test-eksExtApiServerClusterIngressRule	create	
aws:ec2:SecurityGroupRule	aws-eks-mara-test-eksNodeIngressRule	create	
aws:ec2:SecurityGroupRule	aws-eks-mara-test-eksClusterIngressRule	create	
aws:ec2:SecurityGroupRule	aws-eks-mara-test-eksNodeInternetEgressRule	create	
aws:ec2:SecurityGroupRule	aws-eks-mara-test-eksNodeClusterIngressRule	create	
aws:ec2:LaunchConfiguration	aws-eks-mara-test-nodeLaunchConfiguration	create	
aws:cloudFormation:Stack	aws-eks-mara-test-nodes	create	
pulumi:providers:kubernetes	aws-eks-mara-test-provider	create	

Diagnostics:

```
pulumi:pulumi:Stack (aws-eks-mara-test):
  vpc id: vpc-041a70230f358677f
  warning: aws:ec2:getSubnetIds:getSubnetIds verification warning: Deprecated Resource
  public subnets: ['subnet-059cb47a8858c7fc6', 'subnet-08fd5f6035468c09', 'subnet-0322839cabb62b9e']
  warning: aws:ec2:getSubnetIds:getSubnetIds verification warning: Deprecated Resource
  public subnets: ['subnet-0a633e4ab38385031', 'subnet-0bc572ce9741ecce7', 'subnet-025408ad9835964aa']
```

Updating (mara-test)

View Live: <https://app.pulumi.com/shawnhankin/aws-eks/mara-test/updates/1>

Type	Name	Status	Info
pulumi:pulumi:Stack	aws-eks-mara-test	created	2 warnings; 3 messages
aws:iam:Role	ec2-nodgroup-iam-role	created	
aws:iam:Role	eks-iam-role	created	
aws:iam:RolePolicyAttachment	eks-workernode-policy-attachment	created	
aws:iam:RolePolicyAttachment	eks-cni-policy-attachment	created	
aws:iam:RolePolicyAttachment	ec2-container-ro-policy-attachment	created	
aws:iam:InstanceProfile	node-group-profile-aws-eks-mara-test	created	
aws:iam:RolePolicyAttachment	eks-service-policy-attachment	created	
aws:iam:RolePolicyAttachment	eks-cluster-policy-attachment	created	
eks:index:Cluster	aws-eks-mara-test	created	
eks:index:ServiceRole	aws-eks-mara-test-instanceRole	created	
aws:iam:Role	aws-eks-mara-test-instanceRole-role	created	
aws:iam:RolePolicyAttachment	aws-eks-mara-test-instanceRole-3eb088f2	created	
aws:iam:RolePolicyAttachment	aws-eks-mara-test-instanceRole-elb295bd	created	
aws:iam:RolePolicyAttachment	aws-eks-mara-test-instanceRole-03516f97	created	
eks:index:RandomSuffix	aws-eks-mara-test-cfnStackName	created	
aws:ec2:SecurityGroup	aws-eks-mara-test-eksClusterSecurityGroup	created	
aws:iam:InstanceProfile	aws-eks-mara-test-instanceProfile	created	
aws:ec2:SecurityGroupRule	aws-eks-mara-test-eksClusterInternetEgressRule	created	
aws:eks:Cluster	aws-eks-mara-test-eksCluster	created	
aws:ec2:SecurityGroup	aws-eks-mara-test-nodeSecurityGroup	created	
eks:index:VpcCni	aws-eks-mara-test-vpc-cni	created	
pulumi:providers:kubernetes	aws-eks-mara-test-eks-k8s	created	
kubernetes:core/v1:ConfigMap	aws-eks-mara-test-nodeAccess	**failed**	1 error

Diagnostics:

```
kubernetes:core/v1:ConfigMap (aws-eks-mara-test-nodeAccess):
  error: failed to initialize discovery client: exec plugin: invalid apiVersion "client.authentication.k8s.io/v1alpha1"
```

pulumi:pulumi:Stack (aws-eks-mara-test):

```
vpc id: vpc-041a70230f358677f
warning: aws:ec2:getSubnetIds:getSubnetIds verification warning: Deprecated Resource
public subnets: ['subnet-059cb47a8858c7fc6', 'subnet-08fd5f6035468c09', 'subnet-0322839cabb62b9e']
warning: aws:ec2:getSubnetIds:getSubnetIds verification warning: Deprecated Resource
public subnets: ['subnet-0a633e4ab38385031', 'subnet-0bc572ce9741ecce7', 'subnet-025408ad9835964aa']
```

Resources:

+ 23 created

Duration: 10m27s

References

- Cloud Engineering Summit 2021: [Building a Modern App Reference Architecture for Kubernetes](#)
- [What is Infrastructure as Code? Introduction To Pulumi](#): Create an AWS S3 Website in under 5 min
- [MARA: Running on a Workstation Near You](#)

AWS AI Service

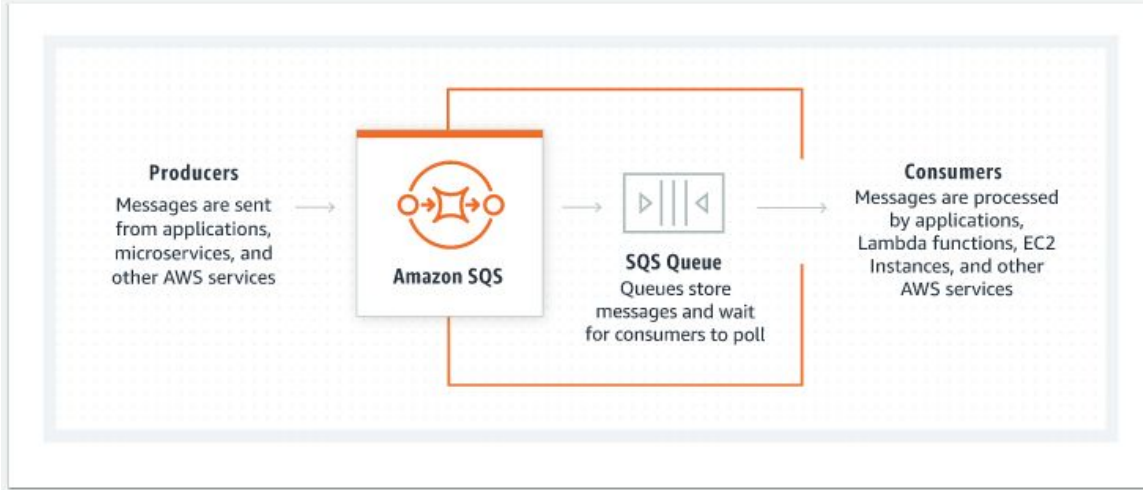
(Serverless Image Recognition System - Crawler)

Shawn K.

Amazon SQS: A message queuing service

- Amazon SQS provides queues for high-throughput, system-to-system messaging. You can use queues to decouple heavyweight processes and to buffer and batch work. Amazon SQS stores messages until microservices and serverless applications process them.

How it works



Amazon SQS: Benefits and Features

- **Highly scalable Standard and FIFO queues**
 - Queues scale elastically with your application. Nearly unlimited throughput and no limit to the number of messages per queue in Standard queues. First-In-First-Out delivery and exactly once processing in FIFO queues.
- **Durability and availability**
 - Your queues are distributed on multiple servers. Redundant infrastructure provides highly concurrent access to messages.
- **Security**
 - Protection in transit and at rest. Transmit sensitive data in encrypted queues. Send messages in a Virtual Private Cloud.
- **Batching**
 - Send, receive, or delete messages in batches of up to 10 messages or 256KB to save costs.

Amazon SQS: Use Cases



EMS

Petroleum retailers in Australia are improving the performance and safety of their service stations with an AWS IoT-enabled solution called Fuelsuite from EMS. Fuelsuite schedules messages to and from the edge devices by using Amazon SQS.

[Learn more](#) 



NASA

The NASA image & video library provides easy access to thousands of images, audio recordings and videos, documenting NASA's more than half a century of achievements in exploring the vast unknown. The architecture includes Amazon SQS to decouple incoming jobs from pipeline processes.

[Learn more](#) 