# Introduction to Security and Architecture on AWS

AWS ARCHITECTURE CORE CONCEPTS

# Security and Architecture Overview

# Overview

Reviewing core concepts around security and architecture

Exploring the AWS Shared Responsibility Model

Introducing the AWS Well Architected Framework

Examining fault tolerance and high availability on AWS

Understanding provided tools for compliance

# Acceptable Use Policy

AWS's policy for acceptable and unacceptable uses of their cloud platform.  All users must agree with this policy to have an account on the platform.

# Acceptable Use Policy

**Sending unsolicited mass emails is prohibited**

**Hosting or distributing harmful content is prohibited**

**Penetration tests are allowed for a list of specific services**

# Least Privilege Access

When granting permission for a user to access AWS resources, you should grant them the minimum permissions needed to complete their tasks and no more.

# Shared Responsibility Model

“Security and Compliance is a shared responsibility between AWS and the customer.”

**Amazon Web Services, Shared Responsibility Model**

# Shared Responsibility Summary

## AWS Responsibility

AWS is responsible for the security of the cloud

## Customer Responsibility

Customer is responsible for security in the cloud

# Shared Responsibility Model

## AWS Responsibility

**Access & Training for Amazon Employees**

**Global Data Centers & Underlying Network**

**Hardware for Global Infrastructure**

**Configuration Management for Infrastructure**

**Patching Cloud Infrastructure & Services**

## Customer Responsibility

**Individual Access to Cloud Resources & Training**

**Data Security & Encryption** (both in transit and at rest)

**Operating System, Network, and Firewall Configuration**

**All Code Deployed onto Cloud Infrastructure**

**Patching guest OS and custom applications**

# AWS Well-architected Framework

# AWS Well-architected Framework

The Well-architected Framework is a collection of best practices across five key pillars for how to best create systems that create business value on AWS.

# Pillars of the Well-architected Framework

**Operational Excellence**

Running and monitoring systems for business value

**Security**

Protecting information and business assets

**Reliability**

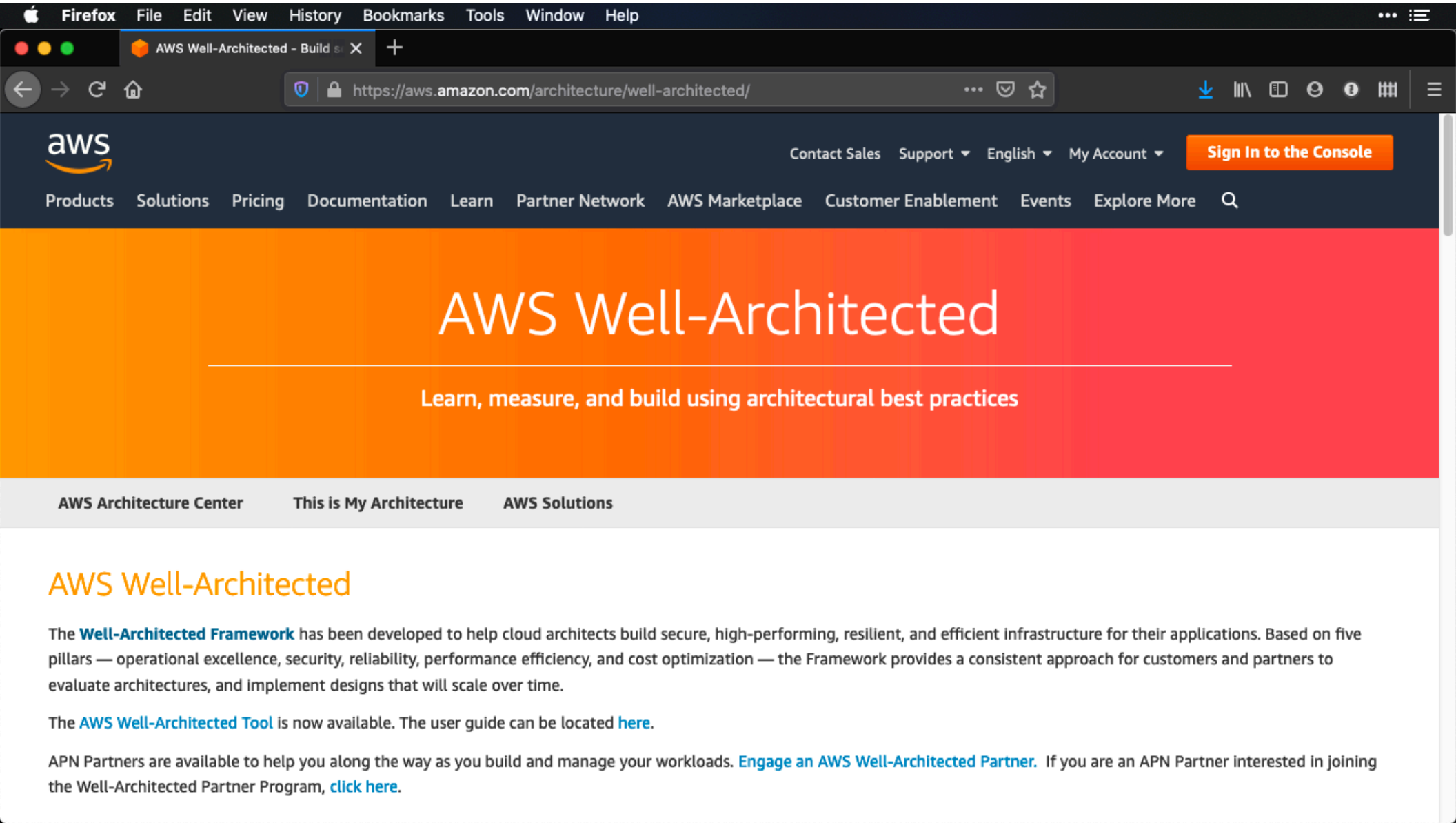
Enabling infrastructure to recover from disruptions

**Performance Efficiency**

Using resources efficiently to achieve business value

**Cost Optimization**

Achieving minimal costs for the desired value


Firefox File Edit View History Bookmarks Tools Window Help
AWS Well-Architected - Build
https://aws.amazon.com/architecture/well-architected/
aws
Contact Sales
Support
English
My Account
Sign In to the Console
Products
Solutions
Pricing
Documentation
Learn
Partner Network
AWS Marketplace
Customer Enablement
Events
Explore More
AWS Well-Architected
Learn, measure, and build using architectural best practices
AWS Architecture Center
This is My Architecture
AWS Solutions
AWS Well-Architected
The Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars — operational excellence, security, reliability, performance efficiency, and cost optimization — the Framework provides a consistent approach for customers and partners to evaluate architectures, and implement designs that will scale over time.
The AWS Well-Architected Tool is now available. The user guide can be located here.
APN Partners are available to help you along the way as you build and manage your workloads. Engage an AWS Well-Architected Partner. If you are an APN Partner interested in joining the Well-Architected Partner Program, click here.

# High-availability and Fault Tolerance

“Everything fails all the time.”

**Werner Vogels - CTO, Amazon**

# Reliability on AWS

## Fault Tolerance

Being able to support the failure of components within your architecture

## High Availability

Keeping your entire solution running in the expected manner despite issues that may occur

# Building Solutions on AWS

**Most managed AWS services provide high-availability out of the box**

**When building solutions directly on EC2 fault tolerance must be architected**

**Multiple availability zones should be leveraged**

**Some services can enable fault tolerance in your custom applications**

- Simple Queue Service (SQS)
- Route 53

# Compliance

# Common Compliance Standards

**PCI-DSS**

Compliance standard for processing credit cards

**HIPAA**

Compliance standard for healthcare data

**SOC 1, SOC 2, SOC 3**

Third-party reviews of operational processes

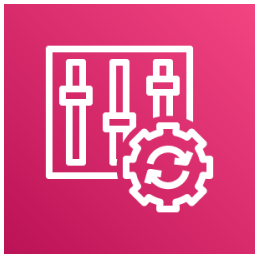
**FedRAMP**

Standards for US government data handling

**ISO 27018**

Standard for handling Personally Identifiable Info

# Compliance Services



**AWS Config**

Provides conformance packs for standards

**AWS Artifact**

Provides self-service access to reports

**Amazon GuardDuty**

Provides intelligent threat detection

# Summary

- Reviewed core concepts around security and architecture
- Explored the AWS Shared Responsibility Model
- Introduced the AWS Well-architected Framework
- Examined fault tolerance and high availability on AWS
- Understood provided tools for compliance

# AWS Identities and User Management

# Least Privilege Access

When granting permission for a user to access AWS resources, you should grant them the minimum permissions needed to complete their tasks and no more.

# Overview

Introducing AWS Identity and Access Management (IAM)

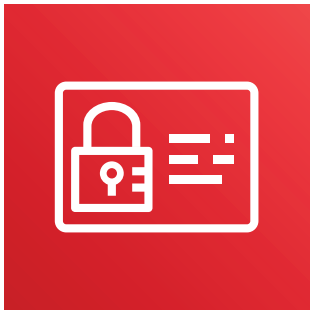
Reviewing the IAM identity types

Enabling Multi-factor Authentication (MFA)

Introducing Amazon Cognito

# Introduction to AWS IAM

# AWS Identity & Access Management (IAM)



**Service that controls access to AWS resources**

**Using the service is free**

**Manages both authentication and authorization**

**Supports identity federation through SAML providers including Active Directory**

# AWS IAM Identities

**Users**

Account for a single individual to access AWS resources

**Groups**

Allows you to manage permissions for a group of IAM users

**Roles**

Enables a user or AWS service to assume permissions for a task

# Policies in AWS IAM


A JSON document that defines permissions for an AWS IAM identity (principal)

Defines both the AWS services that the identity can access and what actions can be taken on that service

Can be either customer managed or managed by AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        },
        {
            "Effect": "Deny",
            "NotAction": "s3:*",
            "NotResource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

- Statement is allowing an action
- Enables all actions on S3
- This is enables for this one bucket and its contents

- Next is a Deny statement
- It denies all S3 actions for any bucket that is not the one listed here

# AWS IAM Best Practices

## Multi-Factor Authentication

Provides additional security with either a physical or virtual device that generates a token for login

## Least Privilege Access

Users should only be granted access to AWS resources that are required for their current tasks

# Creating and Managing IAM Users

# Demo

Creating an IAM user

Configuring permissions for IAM users

Creating an IAM group

Attaching permissions to an IAM group

# Enabling Multi-factor Authentication

# Demo

**Enabling MFA for the root user**

**Enabling MFA for an IAM user**

# Amazon Cognito

# Amazon Cognito

A managed service that enables you to handle authentication and aspects of authorization for your custom web and mobile applications through AWS.

# Amazon Cognito

- User directory service for custom applications
- Provides UI components for many platforms
- Provides security capabilities to control account access
- Enables controlled access to AWS resources
- Can work with social and enterprise identity providers

# Amazon Cognito Identity Providers

# Summary

Introduced AWS Identity and Access Management (IAM)

Reviewed the IAM identity types

Enabled Multi-factor Authentication (MFA)

Introduced Amazon Cognito

# Disaster Recovery on AWS

"**Disaster recovery** (DR) is about preparing for and recovering from a disaster. Any event that has a negative impact on a company's business continuity or finances could be termed a disaster. This includes hardware or software failure, a network outage, a power outage, physical damage to a building like fire or flooding, human error, or some other significant event. "

**Amazon Web Services**

# Needs for Disaster Recovery

**Data Center**

**Cloud Deployment**

# Overview

Understanding the need for a disaster recovery strategy

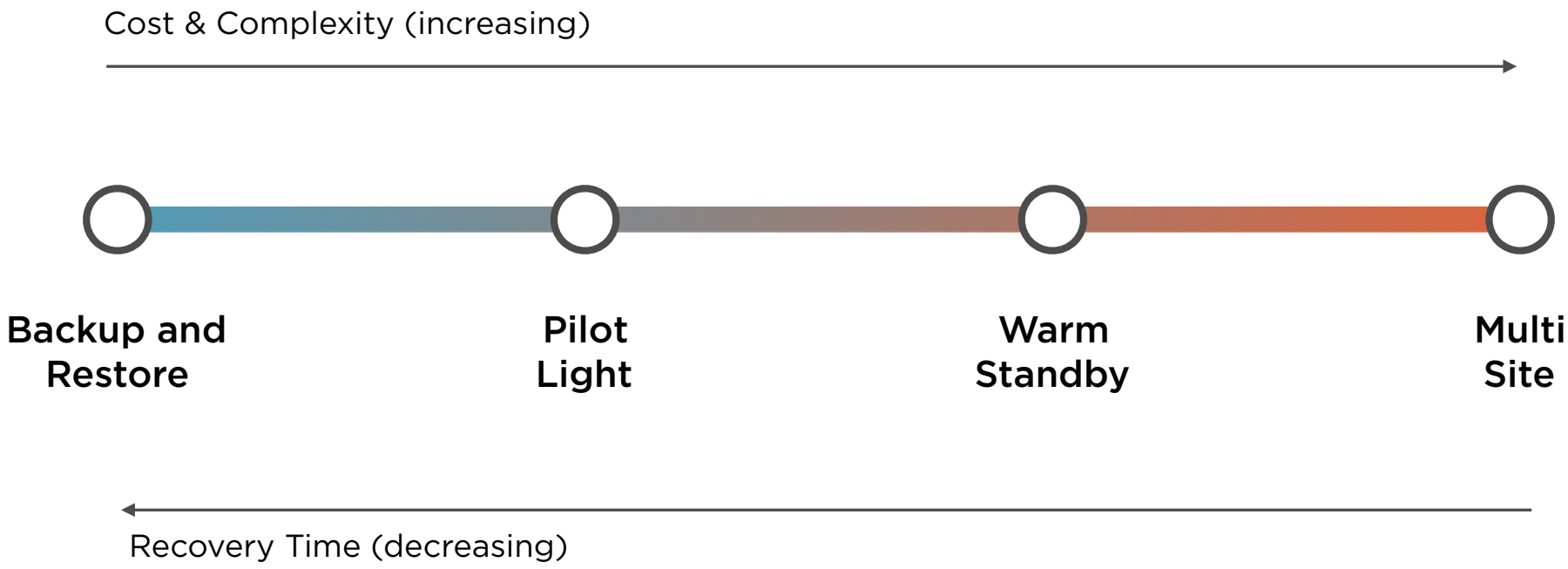
Reviewing the four different disaster recovery approaches on AWS

Exploring the factors to know when selecting an approach

Examining specific scenarios and disaster recovery needs

# Disaster Recovery Architectures

# Disaster Recovery Scenarios



# Backup and Restore

Production data is backed up into Amazon S3

Data can be stored in either standard or archival storage classes

EBS data can be stored as snapshots in Amazon S3 also

In a Disaster Recovery event, a process is started to launch new environment

This approach has the longest recovery time

# Pilot Light

**Key infrastructure components are kept running in the cloud**

**Designed to reduce recovery time over the Backup and Restore approach**

**Does incur cost of this infrastructure continually running in the cloud**

**AMI's are prepared for additional systems and can be launched quickly**

“The **pilot light** method gives you a quicker recovery time than the backup-and-restore method because the core pieces of the system are already running and are continually kept up to date.”

**Amazon Web Services**

# Warm Standby

A scaled-down version of the full environment is running in the cloud

Critical systems can be running on less capable instance types

Instance types and other systems can be ramped up for disaster recovery event

Does incur cost of this infrastructure continually running in the cloud

# Multi Site

**Full environment is running in the cloud at all times**

**Utilizes instance types needed for production not just recovery**

**Provides a near seamless recovery process**

**Incurs the most cost over the other approaches**

# Selecting a Disaster Recovery Architecture

# Disaster Recovery Approach Considerations

**Recovery Time Objective**
**(RTO)**

**Recovery Point Objective**
**(RPO)**

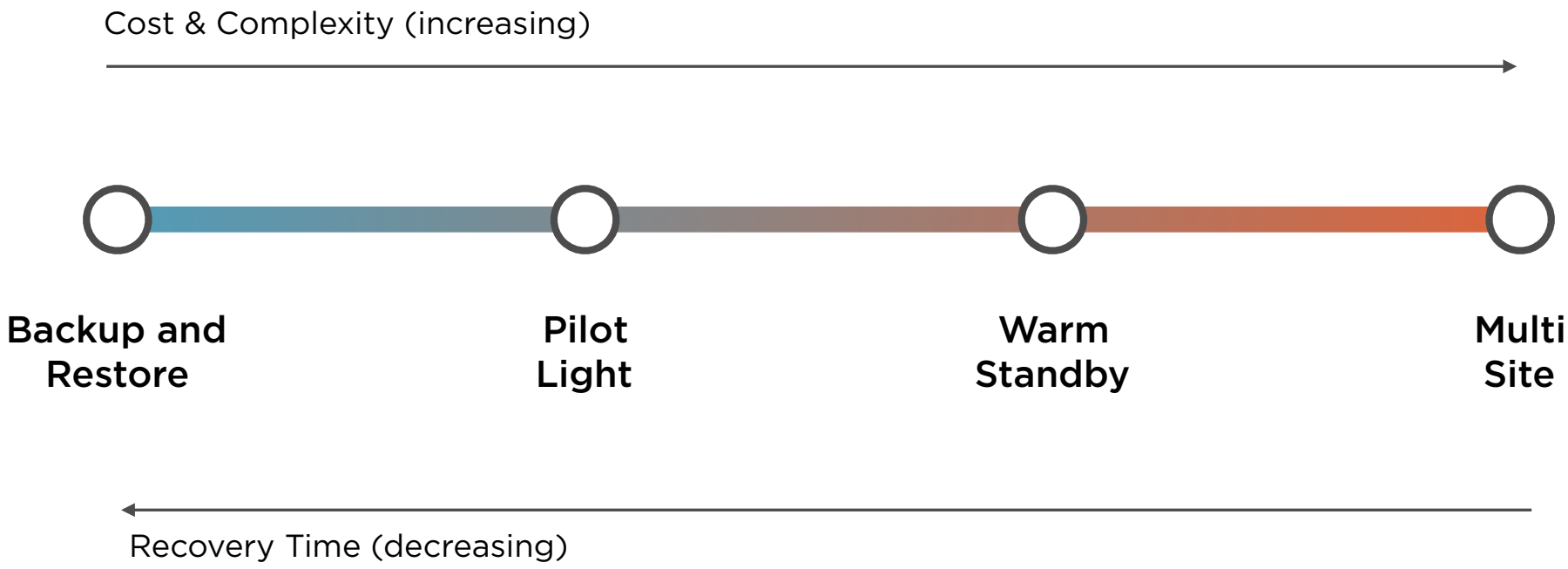
# Recovery Time Objective (RTO)

The time it takes to get your systems back up and running to the ideal business state after a disaster recovery event.

# Recovery Point Objective (RPO)

The amount of data loss (in terms of time) for a production system during a disaster recovery event.

# Disaster Recovery Scenarios



# Summary

Understood the need for a disaster recovery strategy

Reviewed the four different disaster recovery approaches on AWS

Explored the factors to know when selecting an approach

Examined specific scenarios and disaster recovery needs

# Architecting Applications on Amazon EC2

# Overview

Reviewing scaling approaches and services for Amazon EC2

Examining approaches for controlling access to Amazon EC2 instances

Exploring services to protect infrastructure from hacking and attacks

Introducing developer tools on AWS

Reviewing approaches for launching pre-defined solutions on Amazon EC2

# Scaling EC2 Infrastructure

# Scaling on Amazon EC2

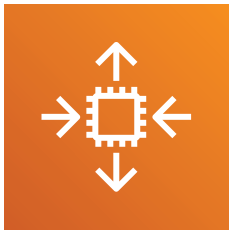
## Vertical Scaling

You “scale up” your instance type to a larger instance type with additional resources

## Horizontal Scaling

You “scale out” and add additional instances to handle the demand of your application

# Amazon EC2 Horizontal Scaling Services



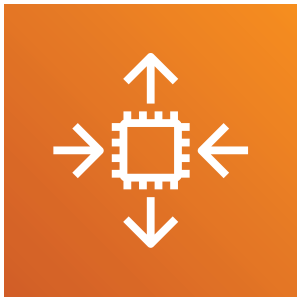
**Auto-scaling Group**

Set of EC2 instances with rules for scaling & management

**Elastic Load Balancer**

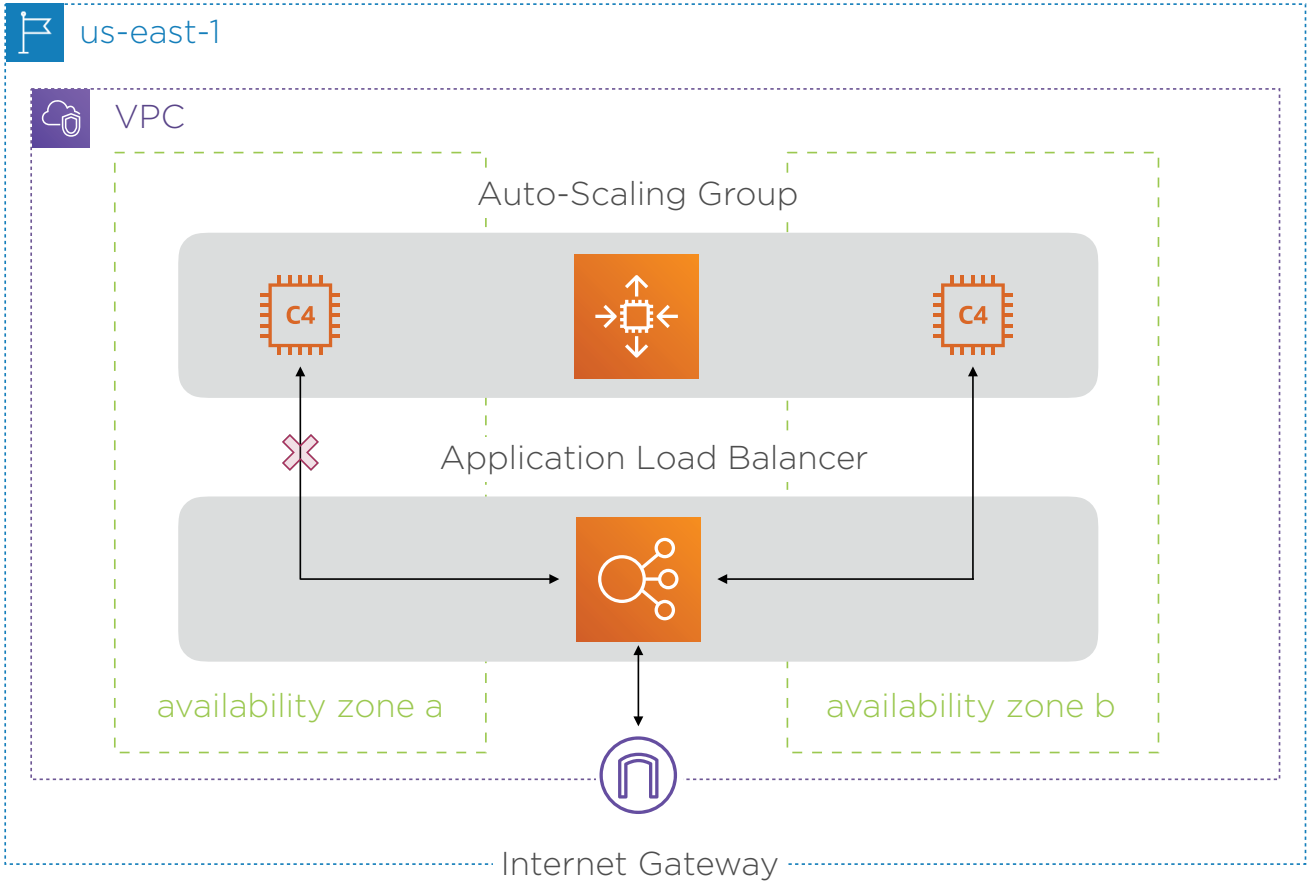
Distributes traffic across multiple targets

# Amazon EC2 Auto-Scaling Group



- **Launch template defines the instance configuration for the group**
- **Defines the minimum, maximum, and desired number of instances**
- **Performs health checks on each instance**
- **Exists within 1 or more availability zones in a single region**
- **Works with on-demand and spot instances**

# Amazon EC2 Horizontal Scaling Example



# AWS Secrets Manager

- Secure way to integrate credentials, API keys, tokens, and other secret content
- Integrates natively with RDS, DocumentDB, and Redshift
- Can auto-rotate credentials with integrated services
- Enables fine-grained access control to secrets

# Controlling Access to EC2 Instances

# Security in Amazon VPC

## Security groups

Enables firewall-like controls for resources within the VPC

## Network ACL's

Controls inbound and outbound traffic for subnets within the VPC

## AWS VPN

Secure access to an entire VPC using an encrypted tunnel

# Security Groups

- Serve as a firewall for your EC2 instances
- Control inbound and outbound traffic
- Works at the instance level
- EC2 instances can belong to multiple security groups
- VPC's have default security groups
- Must be explicitly associated with an EC2 instance
- By default all outbound traffic is allowed

# Network ACL

**Works at the subnet level with an VPC**

**Enables you to allow and deny traffic**

**Each VPC has a default ACL that allows all inbound and outbound traffic**

**Custom ACL's deny all traffic until rules are added**

# AWS VPN

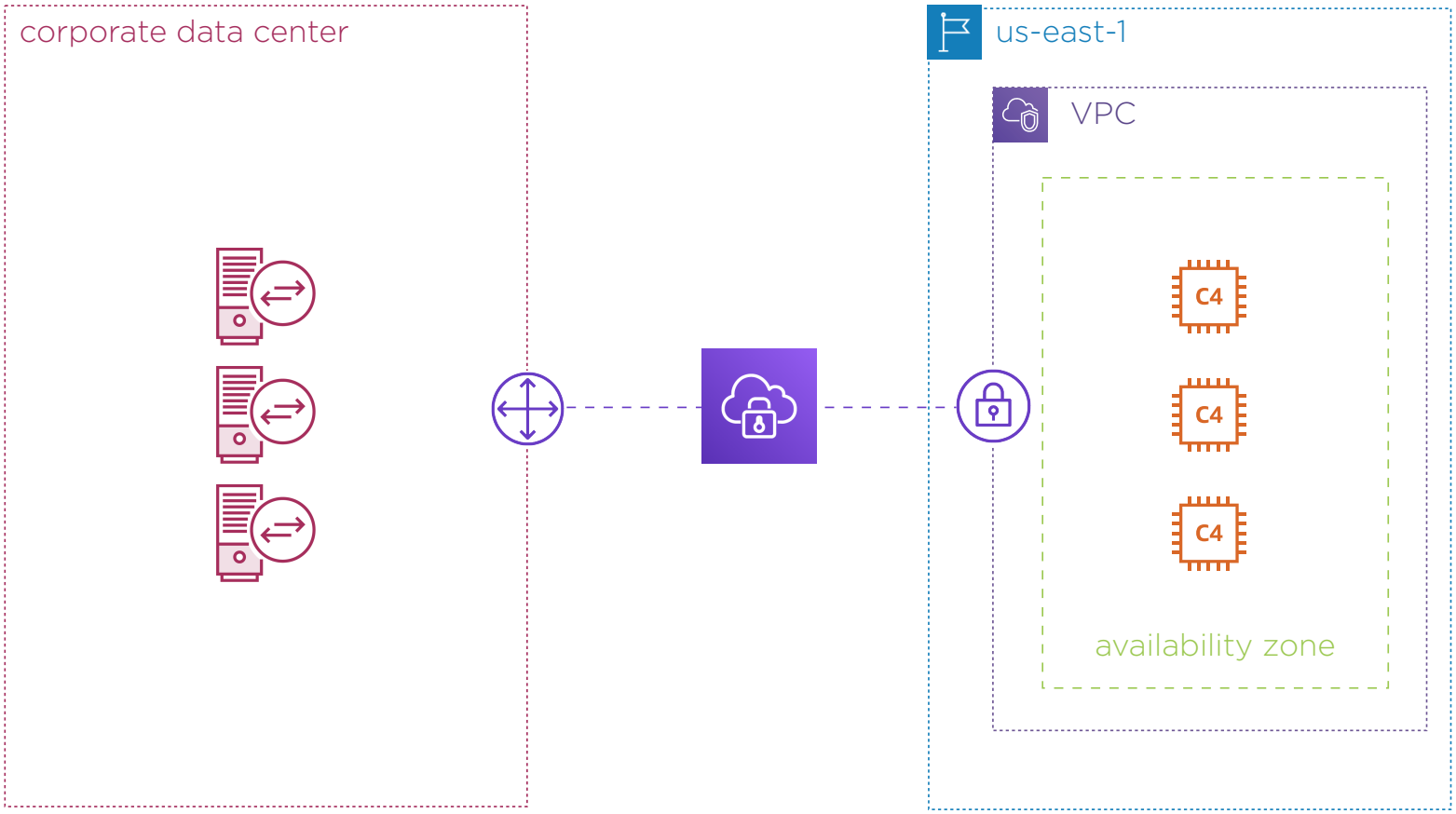
**Creates an encrypted tunnel into your VPC**

**Can be used to connect your data center or even individual client machines**

**Supported in two services:**

- Site-to-site VPN
- Client VPN

# AWS Site-to-site VPN Example



# Protecting Infrastructure from Attacks

# Security Services

**AWS Shield**

Managed DDoS protection service for apps on AWS

**Amazon Macie**

Data protection service powered by machine learning

**Amazon Inspector**

Automated security assessment service for EC2 instances

# Distributed Denial of Service (DDoS)

A type of attack where a server or group of servers are flooded with more traffic than they can handle in a coordinated effort to bring the system down.

# AWS Shield

**Provides protection against DDoS attacks for apps running on AWS**

**Enables on-going threat detection and mitigation**

**Has two different service levels:**

- Standard
- Advanced

# Amazon Macie

Utilizes machine learning to analyze data stored in Amazon S3

It can detect personal information and intellectual property in S3

Provides dashboards that show how the data is being stored and accessed

Enables alerts if it detects anything unusual about data access

# Amazon Inspector

**Enables scanning of Amazon EC2 instances for security vulnerabilities**

**Charged by instance per assessment run**

**Two types of rules packages:**

- Network reachability assessment
- Host assessment

# Deploying Pre-defined Solutions

# Deploying Pre-defined Solutions on AWS

**AWS Service Catalog**

Managed catalog of IT services on AWS for an organization

**AWS Marketplace**

Catalog of software to run on AWS from third-party providers

# AWS Service Catalog

- Targeted to serve as an organizational service catalog for the cloud
- Can include single server image to multi-tier custom applications
- Enables organizations to leverage services that meet compliance
- Supports a lifecycle for services released in the catalog

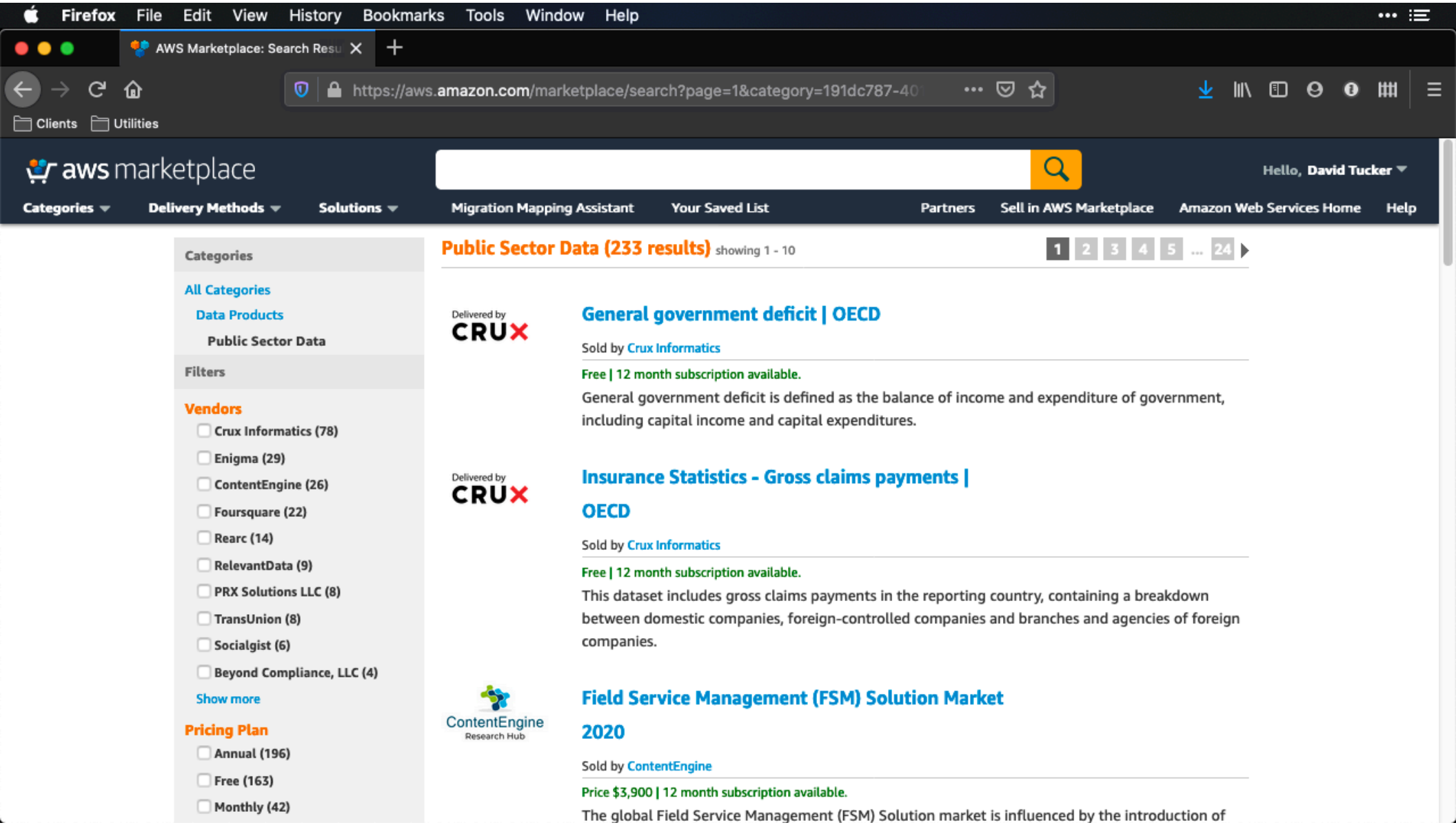
# AWS Marketplace

**Curated catalog of third-party solutions for customers to run on AWS**

**Provides AMI's, CloudFormation stacks, and SaaS based solutions**

**Enables different pricing options to overcome licensing in the cloud**

**Charges appear on your AWS bill**


Firefox File Edit View History Bookmarks Tools Window Help
AWS Marketplace: Search Resu
https://aws.amazon.com/marketplace/search?page=1&category=191dc787-40
Clients Utilities
aws marketplace
Hello, David Tucker
Categories Delivery Methods Solutions Migration Mapping Assistant Your Saved List Partners Sell in AWS Marketplace Amazon Web Services Home Help
Categories
All Categories
Data Products
Public Sector Data
Filters
Vendors
Crux Informatics (78)
Enigma (29)
ContentEngine (26)
Foursquare (22)
Rearc (14)
RelevantData (9)
PRX Solutions LLC (8)
TransUnion (8)
Socialgist (6)
Beyond Compliance, LLC (4)
Show more
Pricing Plan
Annual (196)
Free (163)
Monthly (42)
Public Sector Data (233 results) showing 1 - 10
1 2 3 4 5 ... 24
Delivered by CRUX
General government deficit | OECD
Sold by Crux Informatics
Free | 12 month subscription available.
General government deficit is defined as the balance of income and expenditure of government, including capital income and capital expenditures.
Delivered by CRUX
Insurance Statistics - Gross claims payments | OECD
Sold by Crux Informatics
Free | 12 month subscription available.
This dataset includes gross claims payments in the reporting country, containing a breakdown between domestic companies, foreign-controlled companies and branches and agencies of foreign companies.
ContentEngine Research Hub
Field Service Management (FSM) Solution Market 2020
Sold by ContentEngine
Price $3,900 | 12 month subscription available.
The global Field Service Management (FSM) Solution market is influenced by the introduction of

# Developer Tools

# AWS Developer Services

AWS
CodeCommit

AWS
CodeBuild

AWS
CodeDeploy

AWS
CodePipeline

AWS
CodeStar

# AWS CodeCommit

- Managed source control service
- Utilizes Git for repositories
- Control access with IAM policies
- Serves as an alternative to Github and Bitbucket

# AWS CodeBuild

**Fully managed build and continuous integration service on AWS**

**Don’t have to worry about maintaining infrastructure**

**Charged per minute for compute resources you utilize**

# AWS CodeDeploy

**Managed deployment service for deploying your custom applications**

**Deploys to Amazon EC2, AWS Fargate, AWS Lambda, and on-premise servers**

**Provides dashboard for deployments in the AWS Console**

# AWS CodePipeline

**Fully-managed continuous delivery service on AWS**

**Provides the capabilities to automate building, testing, and deploying**

**Integrates with other developer tools as well as Github**

# AWS CodeStar

Workflow tool that automates the use of the other developer services

Creates a complete continuous delivery toolchain for a custom application

Provides custom dashboards and configurations in the AWS Console

You only are charged for the other services you leverage

# Summary

# Summary

Reviewed scaling approaches and services for Amazon EC2

Examined approaches for controlling access to Amazon EC2 instances

Explored services to protect infrastructure from hacking and attacks

Introduced developer tools on AWS

Reviewed approaches for launching pre-defined solutions on Amazon EC2