

A large, light gray circular icon containing a white right-pointing triangle, resembling a play button or a video thumbnail.

AWS Cloud Practitioner Course

Michael J.
Shannon

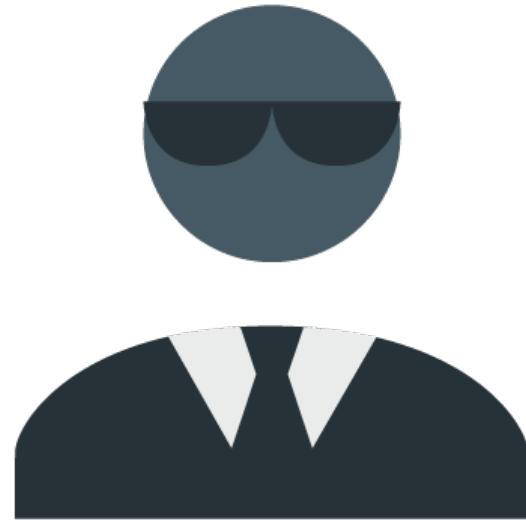
IT/Security Consultant,
Instructor, and
Author



Welcome to AWS Cloud Practitioner Course

DAY ONE

- Segment 1: Cloud Concepts
- Segment 2: Networking Technologies
- Segment 3: AWS Account Basics
- Segment 4: Compute Technologies



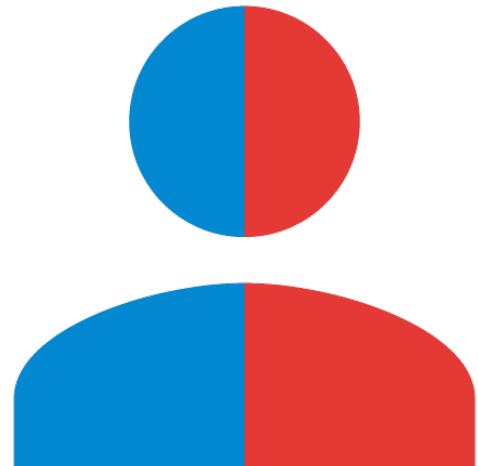
@iconshock.com



Segment 1: Cloud Concepts

AWS Cloud Practitioner Exam

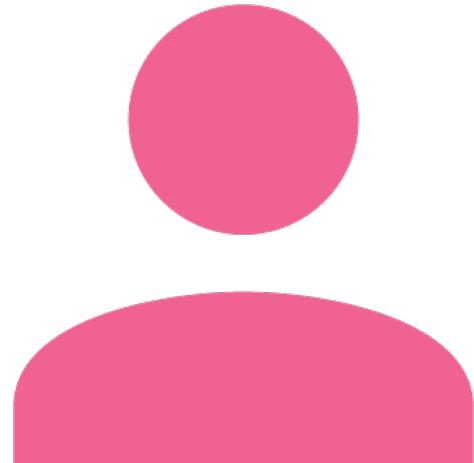
- AWS Certified Cloud Practitioner (CLF-C01)
- For candidates who have the skills and knowledge required to successfully validate a general understanding of the AWS Cloud
- There are two types of questions:
 - Multiple-choice: Has one correct response and three incorrect responses (distractors)
 - Multiple-response: Has two correct responses out of five options



@iconshock.com

AWS Cloud Practitioner Exam

- Uses a scaled score from 100 through 1000, with a minimum passing score of 700
- The examination uses a compensatory scoring model, which means that you do not need to “pass” the individual sections, only the overall examination
- The exam is \$100 USD and candidates have 90 minutes to complete the exam



@iconshock.com

Exam Domains and Weightings

Domain	% of Exam
Domain 1: Cloud Concepts	28%
Domain 2: Security	24%
Domain 3: Technology	36%
Domain 4: Billing and Pricing	12%
Total	100%

Supporting Documentation

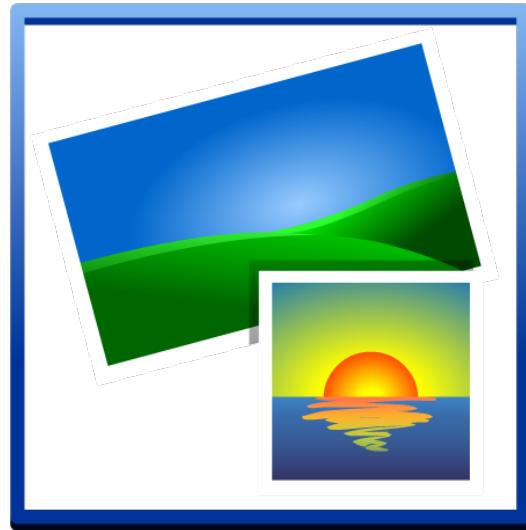
- AWS Whitepapers (Kindle and .PDF)
 - Overview of Amazon Web Services whitepaper, April 2017
 - Architecting for the Cloud: AWS Best Practices whitepaper, Feb 2016
 - How AWS Pricing Works whitepaper, March 2016
 - The Total Cost of (Non) Ownership of Web Applications in the Cloud whitepaper, Aug 2012
 - Compare AWS Support Plans webpage



@iconshock.com

Additional Study Materials

- Getting Started with AWS (Kindle Edition) – free at Amazon
- AWS Certified Cloud Practitioner Complete Video Course by Richard A. Jones
- AWS Cloud Security Complete Video Course by Michael J. Shannon



@iconshock.com

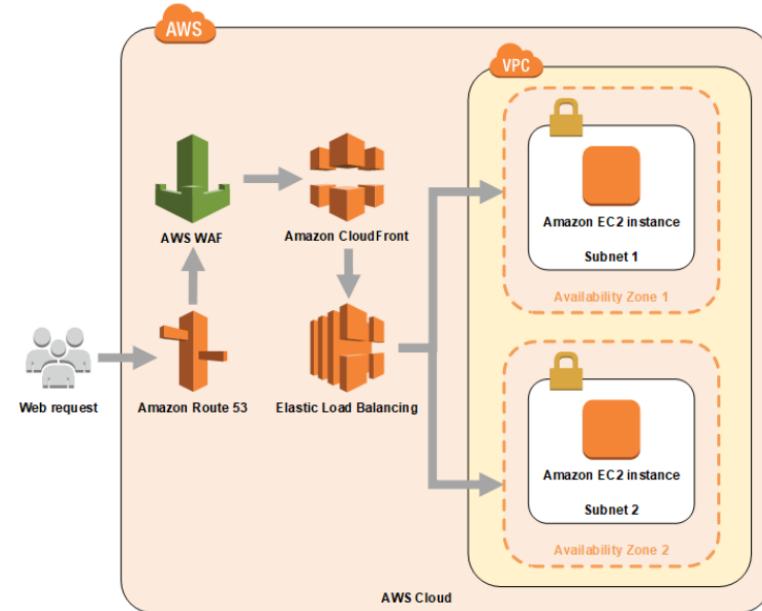
Cloud Computing Defined

- Cloud computing is a model that allows for expedient, on-demand networked access to a shared pool of configurable computing resources
- Resources include networks, servers, databases, object storage, applications, and various services that can be rapidly provisioned and released with minimal management work or service provider collaboration



5 Characteristics of Cloud Services

- The traditional cloud model promotes availability and is composed of five essential characteristics:
 - On-demand self-service**
 - Broad network access**
 - Resource pooling**
 - Rapid elasticity**
 - Measured Service**



Key Enabling Technologies

1. Fast and highly available wide-area networks
2. Powerful, inexpensive server computers
3. Advanced automation and orchestration tools
4. High-performance virtualization for commodity hardware



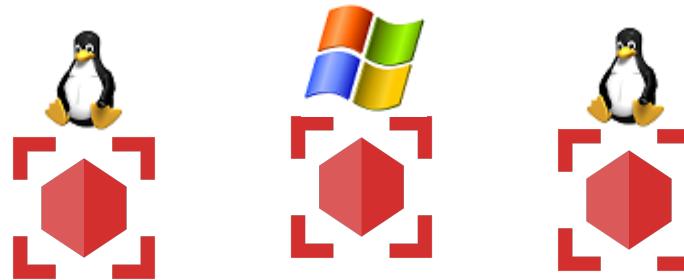
@iconshock.com

Virtualization Components

- A hypervisor is the software that generates and controls a virtual infrastructure allowing multiple OSs to run on a single physical machine
- The system running the hypervisor is called the “host”
- The virtual machines running on the host are “guests”
- Proprietary hypervisors: Hyper-V, vSphere/ESXi, OVM, and FusionSphere
- Open source hypervisors: KVM, OpenVZ, Red Hat, Xen

Type 1 Hypervisor

Virtual Machines



**Paravirtualization
Drivers and Tools**



Hypervisor



Physical Host

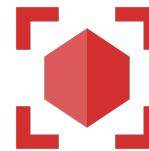
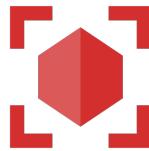
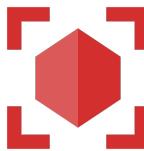


Hardware-Assisted Virtualization

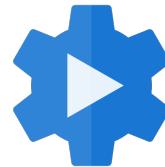
- With hardware-assisted virtualization the operating system has direct access to resources without any emulation or OS modification
- Intel (Intel VT) and AMD(AMD-V) have supporting virtualization technologies providing a set of new instructions and – crucially - a new privilege level
- The hypervisor can now run at Ring -1 so the guest operating systems can run in Ring 0
- There's no need for paravirtualization, the VMM does less work, and the performance hit is reduced

Type 2 Hypervisor

Virtual Machines



Drivers and Tools



Hypervisor



Operating System

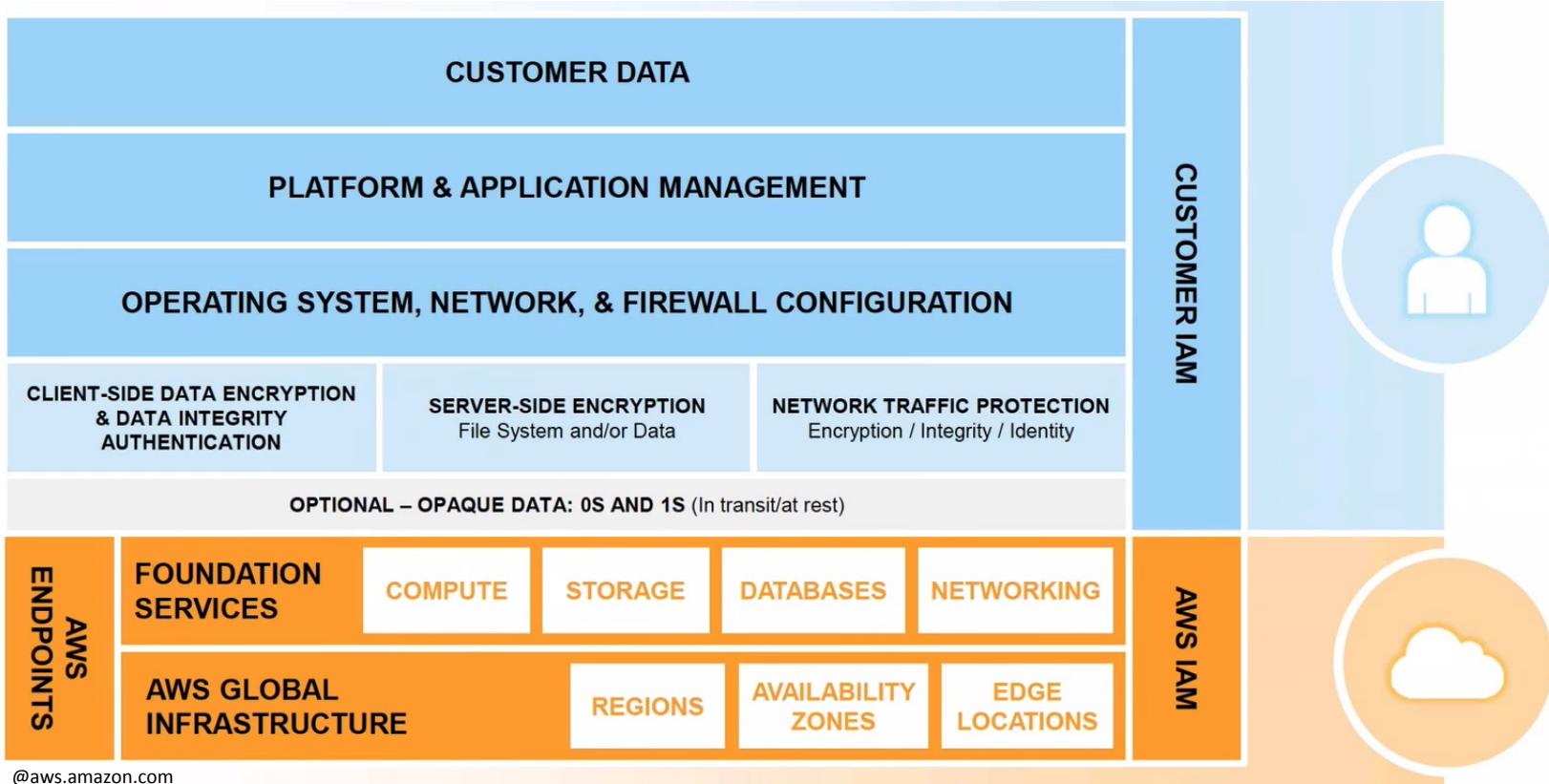


Physical Host



Pearson

Infrastructure as a Service at AWS



@aws.amazon.com

Platform-as-a-Service (PaaS)

- Offers capability to deploy consumer-created or acquired applications onto the cloud infrastructure
- Created using programming languages, libraries, services, and tools supported by the cloud provider
- The customer doesn't manage or control the underlying cloud infrastructure
- The customer **will** control the deployed applications and often configuration settings for the application-hosting environment

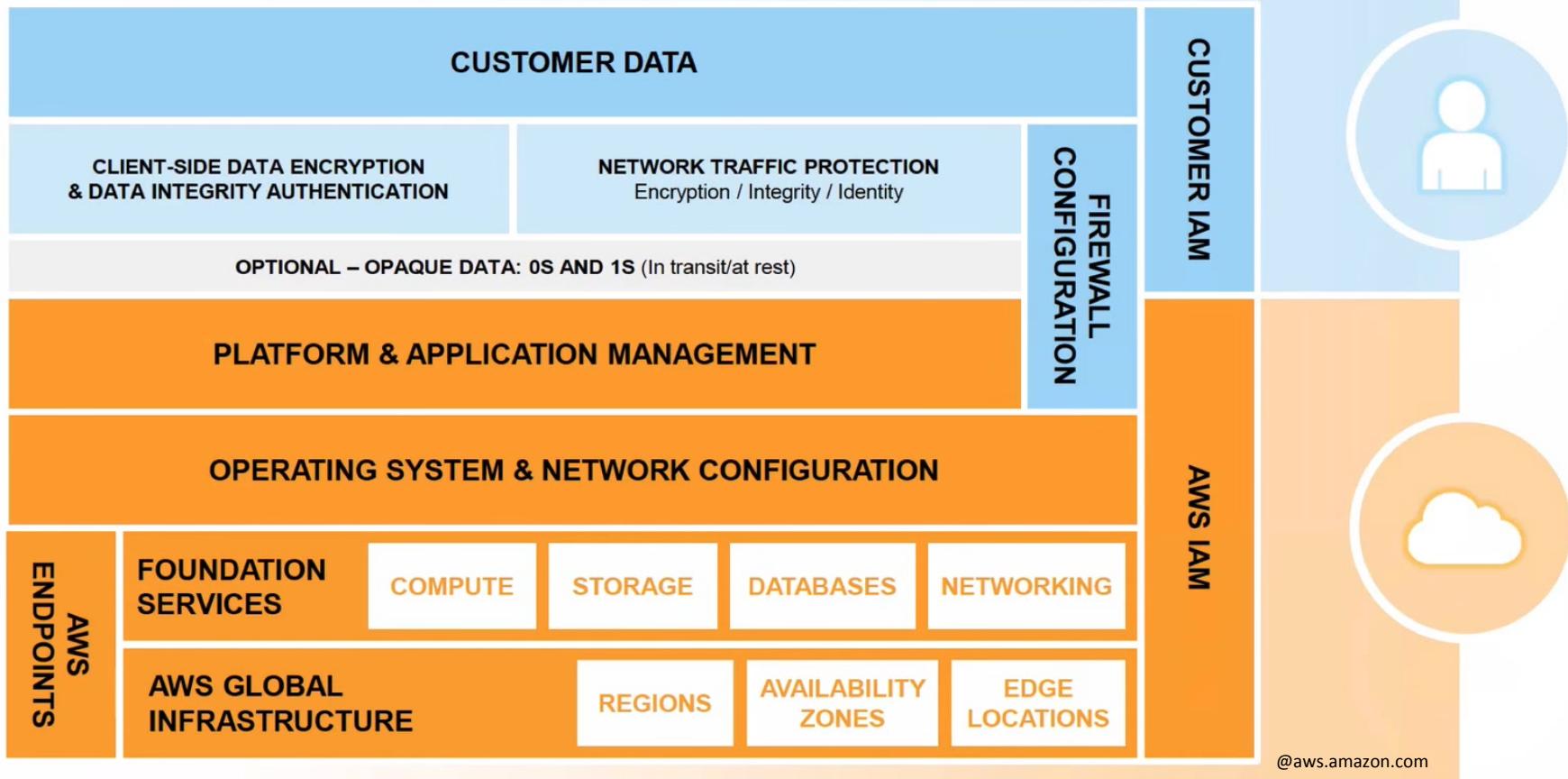
Platform-as-a-Service (PaaS)

- .NET, Java, Ruby, Python, Go, JSON, YAML, etc.
- Amazon Web Services examples
 - Lightsail
 - Amazon Aurora DB
 - Lambda
 - Elastic Beanstalk
 - CloudFront



@iconshock.com

Platform-as-a-Service

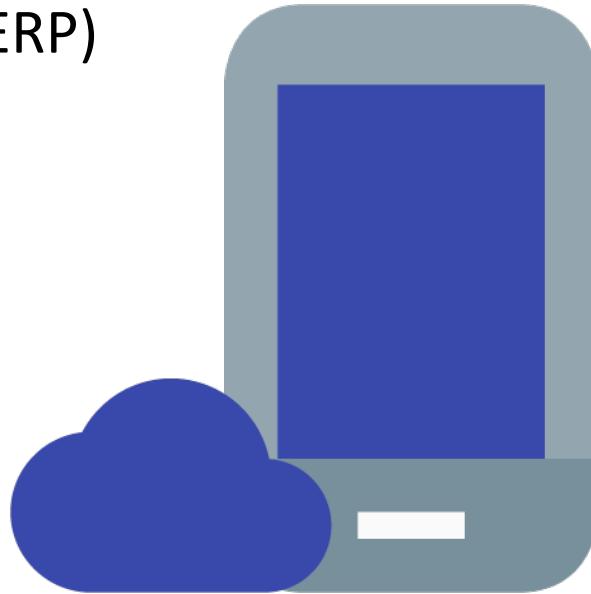


Software-as-a-Service (SaaS)

- Customer uses the service provider's applications running on a cloud infrastructure
- The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface
- The consumer doesn't manage or control the underlying infrastructure or even individual application capabilities
- There are possible exceptions of limited user-specific application configuration settings

Software-as-a-Service (SaaS)

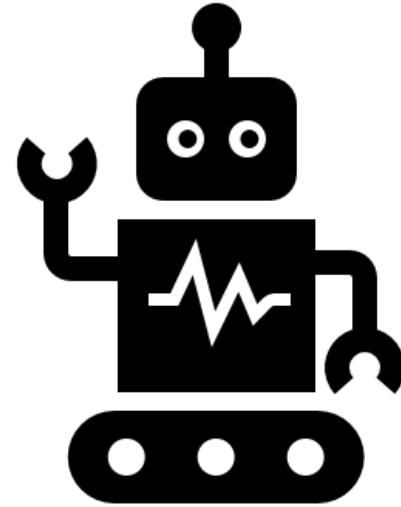
- Customer Relationship Management (CRM)
- Enterprise Resource Planning (ERP)
- Community services
- Billing services
- Analytics services
- Personal storage services
- Security services



@iconshock.com

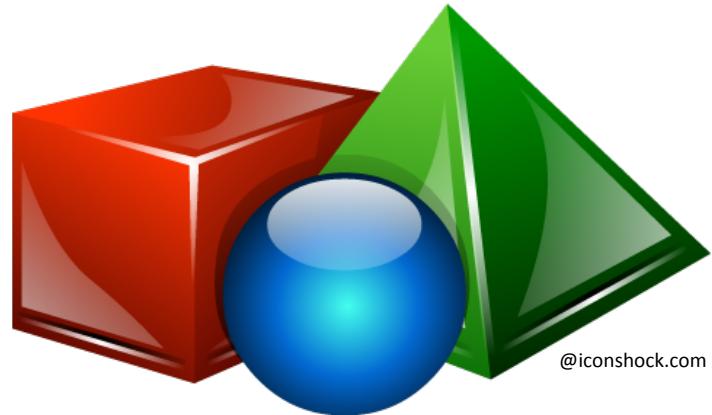
*-as-a-Service

- Database as a Service (DBaaS)
- Communications as a Service (CaaS)
- Business Process as a Service (BPaaS)
- Security as a Service (MSSPs)
- Malware as a Service (MaaS)
- Anything as a Service (XaaS)



Cloud Deployment Models

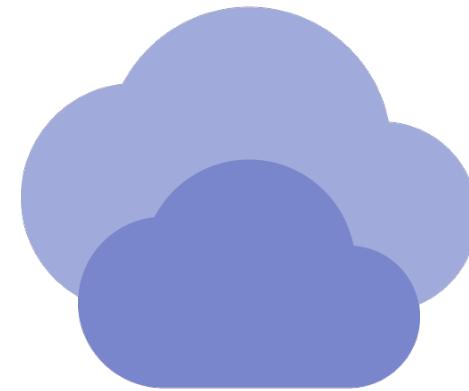
- This decision will have a significant impact on the organization regarding:
 - Costs and budgets
 - Risk treatment and handling
 - Resource allocation
 - Business strategy and objectives
 - Governance and regulations



@iconshock.com

Public Cloud Deployment

- Public cloud is provisioned for open use by the general public
- It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them yet exists on the premises of the cloud provider
- AWS fully deploys the cloud and all applications run in their cloud
- They are either created there or migrated from an existing infrastructure



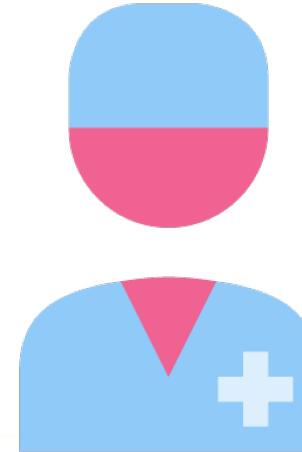
@iconshock.com

On-Premise Cloud Deployment

- The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units or organizational units)
- It may be owned, managed, and operated by the organization, a third-party, or some combination of them
- Offers the same benefits of a public cloud without giving up control, privacy, and security
- May be necessary due to regulations (HIPAA)
- **Private cloud may exist on or off premises**

Community Cloud Deployment

- Provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns
- It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them
- Common examples are healthcare and finance communities
- AWS has substantial compliance and governance service offerings

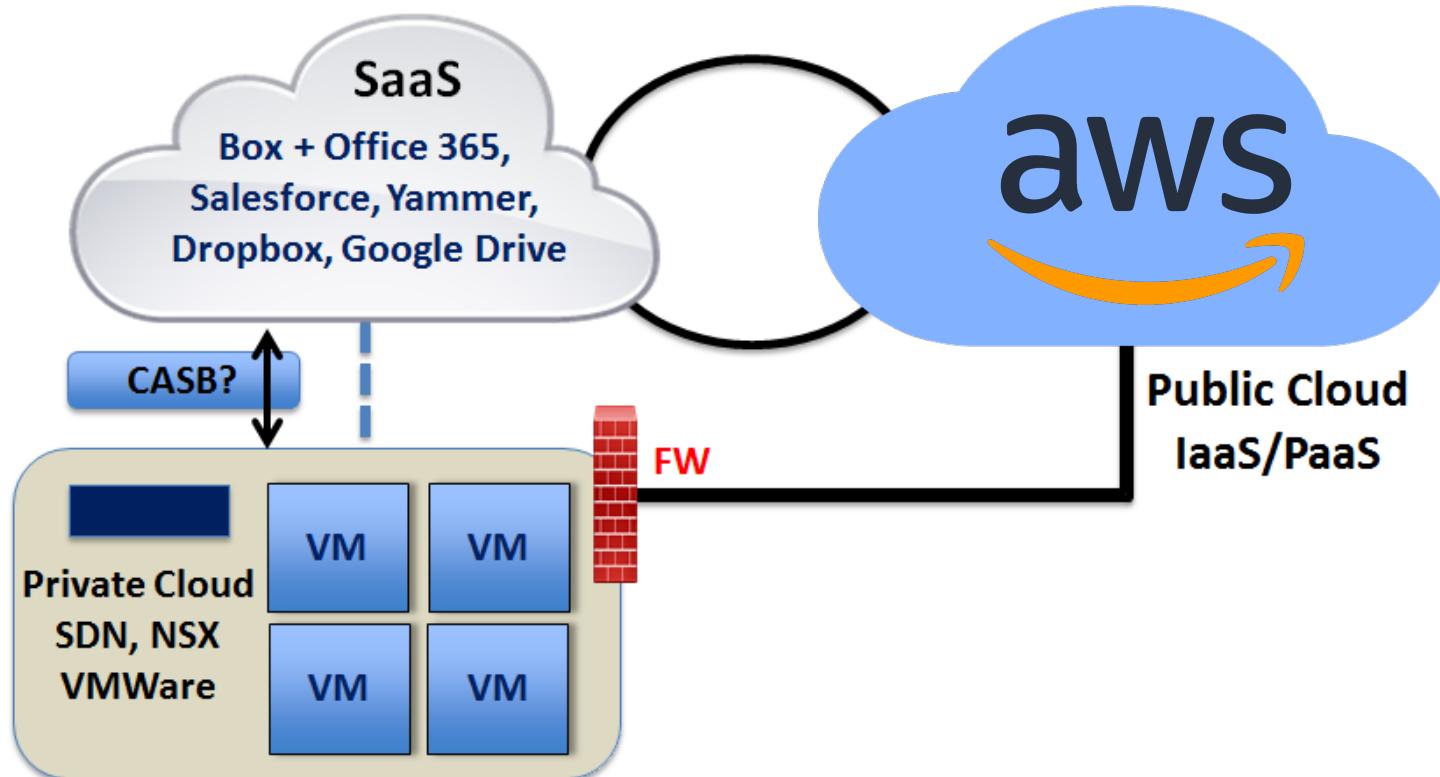


@iconshock.com

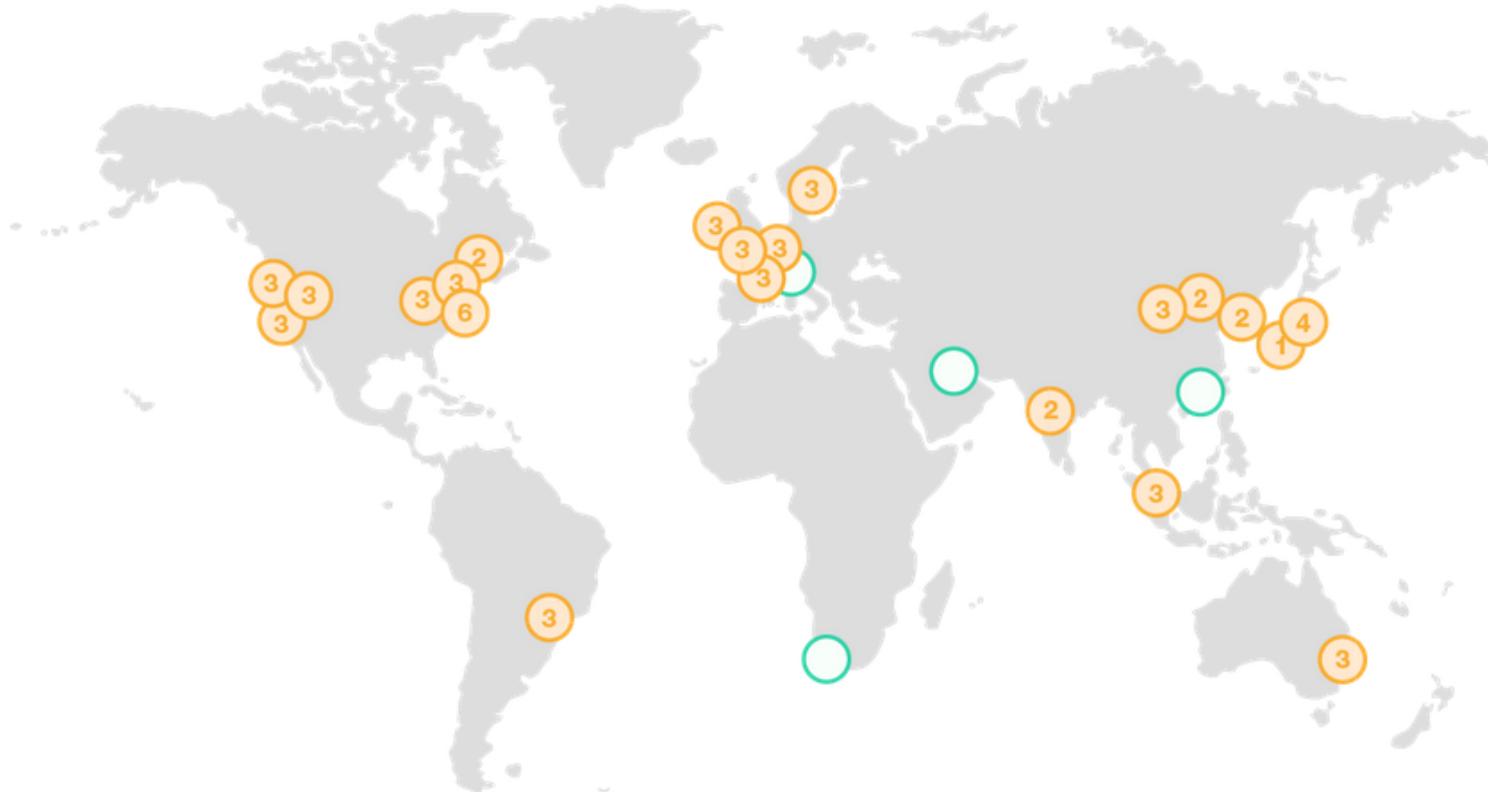
Hybrid Cloud Deployment

- A combination of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities
- They are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)
- Organizations may need to keep certain resources internal and private for mission-criticality or regulatory reasons
- Often involves “Bursting Up” to the cloud as needed
- **Simply using SaaS solutions does not make it a hybrid**

Hybrid Cloud Deployment

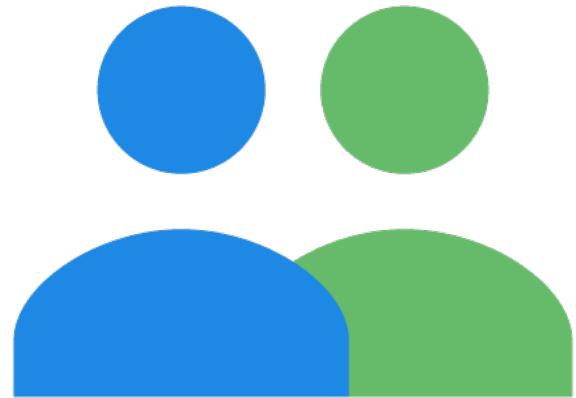


AWS Global Infrastructure



AWS Shared Responsibility Model

- Customers have complete control over their content and are responsible for managing critical content security:
 - Content stored on AWS
 - AWS services used with the content
 - The country where content is stored
 - The format and structure
 - Access to that content



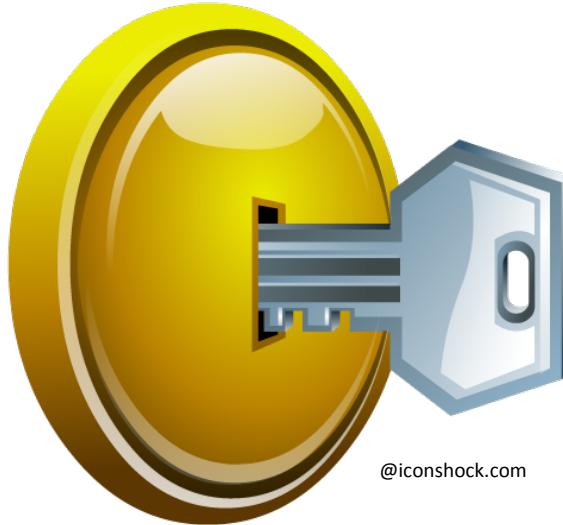
@iconshock.com

AWS Responsibilities

- AWS operates and manages the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.
- The AWS global infrastructure is designed to security best practices and security compliance standards on top of some of the most secure computing infrastructure in the world.
- AWS provides tools and information to assist customers in their efforts to account for and validate that controls are operating effectively in their extended IT environment.

AWS Responsibilities

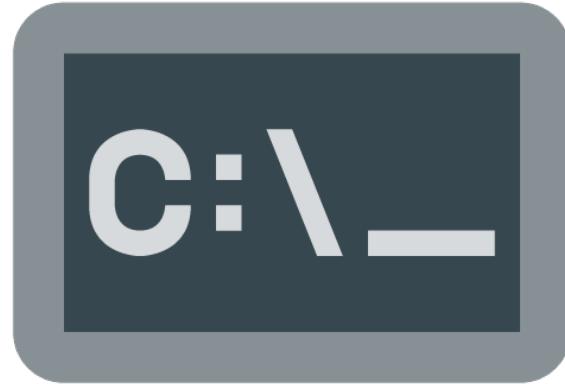
- Nondescript, undisclosed locations
- 24/7 security staffing
- MFA for facility entry
- Continuous monitoring, logging, and auditing



@iconshock.com

AWS Responsibilities

- Automated change control process
- Physical access requires authorization with frequent refreshing
- Bastion servers act as gateways for privileged access
- Network boundary devices monitor and audit access
- Intrusion detection and analysis

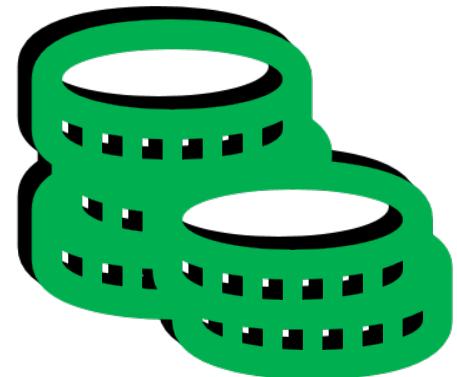


@iconshock.com

AWS Cloud and its Value Proposition

- **Cost**

- Some customers experience 50% or more cost reduction from their previous private cloud or traditional hosted data center
- Eliminates large upfront investments for: cabling, cooling, power, networks, racks, servers, storage, certifications, and labor
- Cost reduction due to economy of scale
- Pay-as-you-go and pay-as-you-use



The AWS Value Proposition

- **Agility**
 - Companies can leverage the infrastructure for speed, experimentation and innovation
 - Rapidly respond to markets trends and new potential
 - AWS provides many tools for cost-effective experimentation and DIY projects
- **Universal (Ubiquitous) Access**
 - Represents anywhere, anytime access to resources



@iconshock.com

The AWS Value Proposition

- **Elasticity**
 - Unlimited scalability and dynamic provisioning & deprovisioning of processing, storage, database, and memory
 - Allows organizations to shift and pool resources over different infrastructures to avoid overprovisioning and cost overruns
 - Scalability is different than elasticity as it increases (only) workloads over existing hardware resources only
- **Demand-driven service**
 - An online portal that allows consumers the ability to provision cloud resources as needed automatically and rapidly without human interaction in most scenarios

Other Cloud Characteristics

- **Auto-Scaling**
 - Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost
 - CSPs allow for easy setup of application scaling for multiple resources across multiple services in minutes
 - Service offer simple, powerful user interfaces that let you build scaling plans for instances, fleets, tasks, database tables, indexes, and replicas

Key Aspects of AWS Cloud Economics

- **Pay-as-you-go (and grow)**
 - Charging model that allows you to pay based on compute and storage resources used or by the second/minute/hour
 - Most providers offer calculators and consultancy



@aws.amazon.com

Key Aspects of AWS Cloud Economics

- **Metering**
 - The ability of provider to automate the tracking of all resources to support the measured usage service
 - Facilitates the pay-as-you-go and demand-driven features of CSPs for billing, monitoring, and reporting
- **Cloud Bursting**
 - The process of running applications on internal resources or a private cloud then “bursting up” to a public/hybrid cloud solution
 - Typically recommended for non-critical, high performance applications hosting non-sensitive data

Key Aspects of AWS Cloud Economics

- **Chargeback**
 - Accounting approach that decentralizes the cost of IT services and applies them to the budgets of the teams or business units
 - Eliminates the need to consolidate all service costs under one bill
 - Many private clouds and internal IT departments will use the term “showback” instead



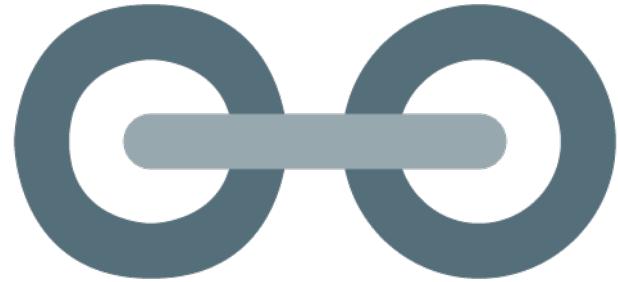
@iconshock.com



Segment 2: Networking Technology

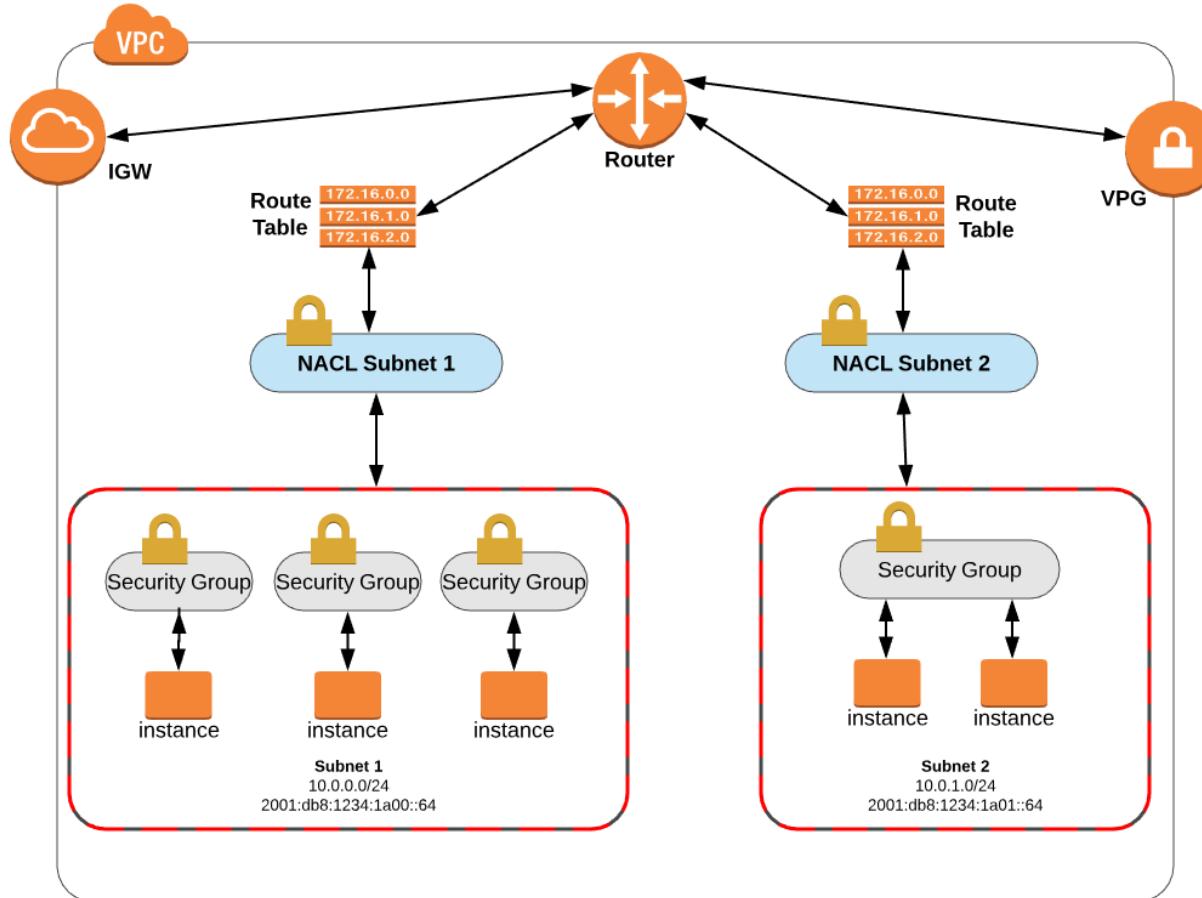
Core Networking Services

- AWS Core networking services are combined with Content Delivery
- The **Virtual Private Cloud (VPC)** is one of the primary and initial core AWS services
- VPC allows you to set up a logically isolated segment of the AWS Cloud where you can define and launch AWS resources in a virtual network

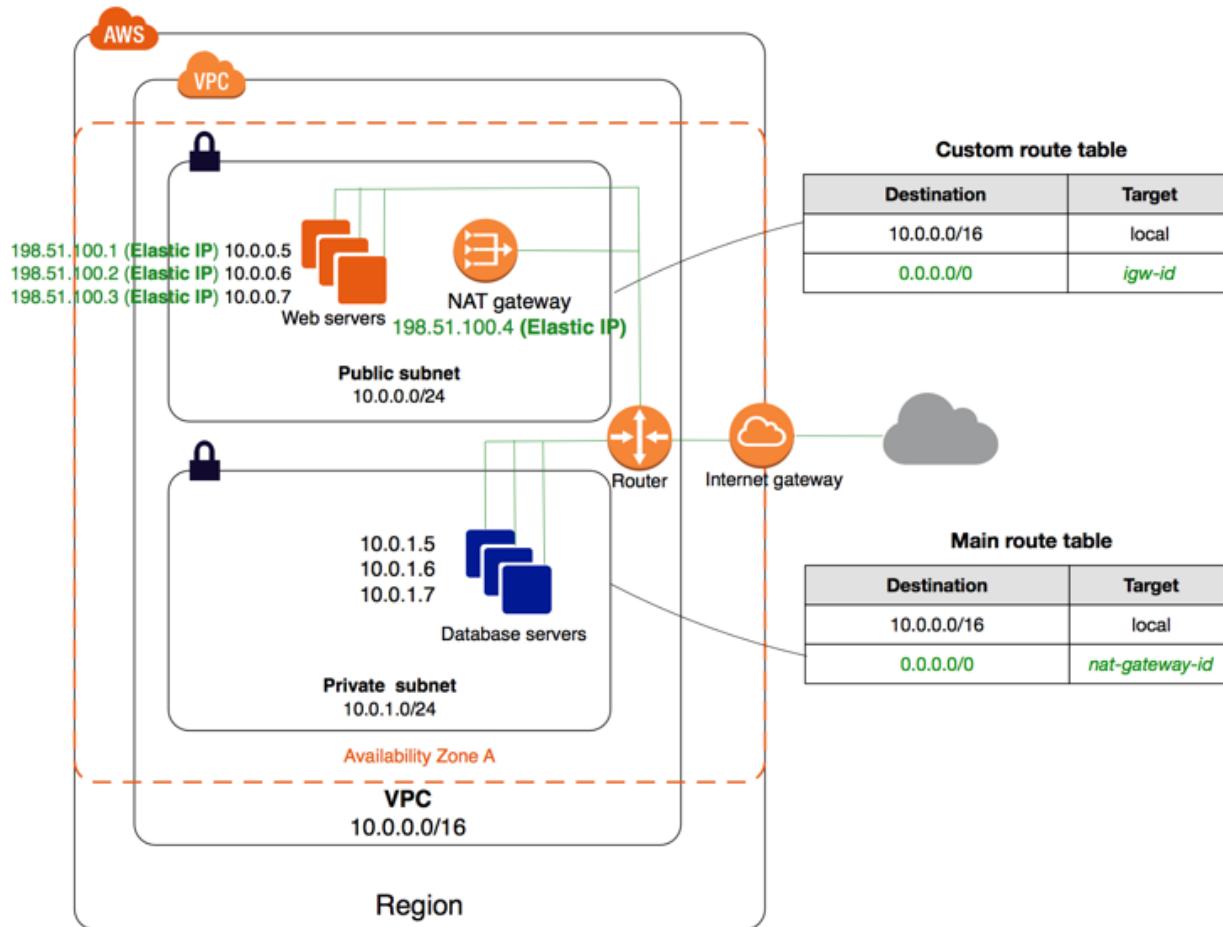


@iconshock.com

Network Design



Evaluating Networking Requirements



VPC with Public & Private Subnets

VPC Management Console +

https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#wizardSelector: ... ★ Search

Most Visited

aws Services Resource Groups * shankhantoo

Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

VPC with Public and Private Subnets Selected

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

Creates:

A /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via Network Address Translation (NAT). (Hourly charges for NAT devices apply.)

Select

```
graph TD; Internet["Internet, S3, DynamoDB, SNS, SQS, etc."] --- VPC[Amazon Virtual Private Cloud]; VPC --- PublicSubnet[Public Subnet]; VPC --- PrivateSubnet[Private Subnet]; PublicSubnet --- NAT[NAT]; PrivateSubnet --- NAT
```

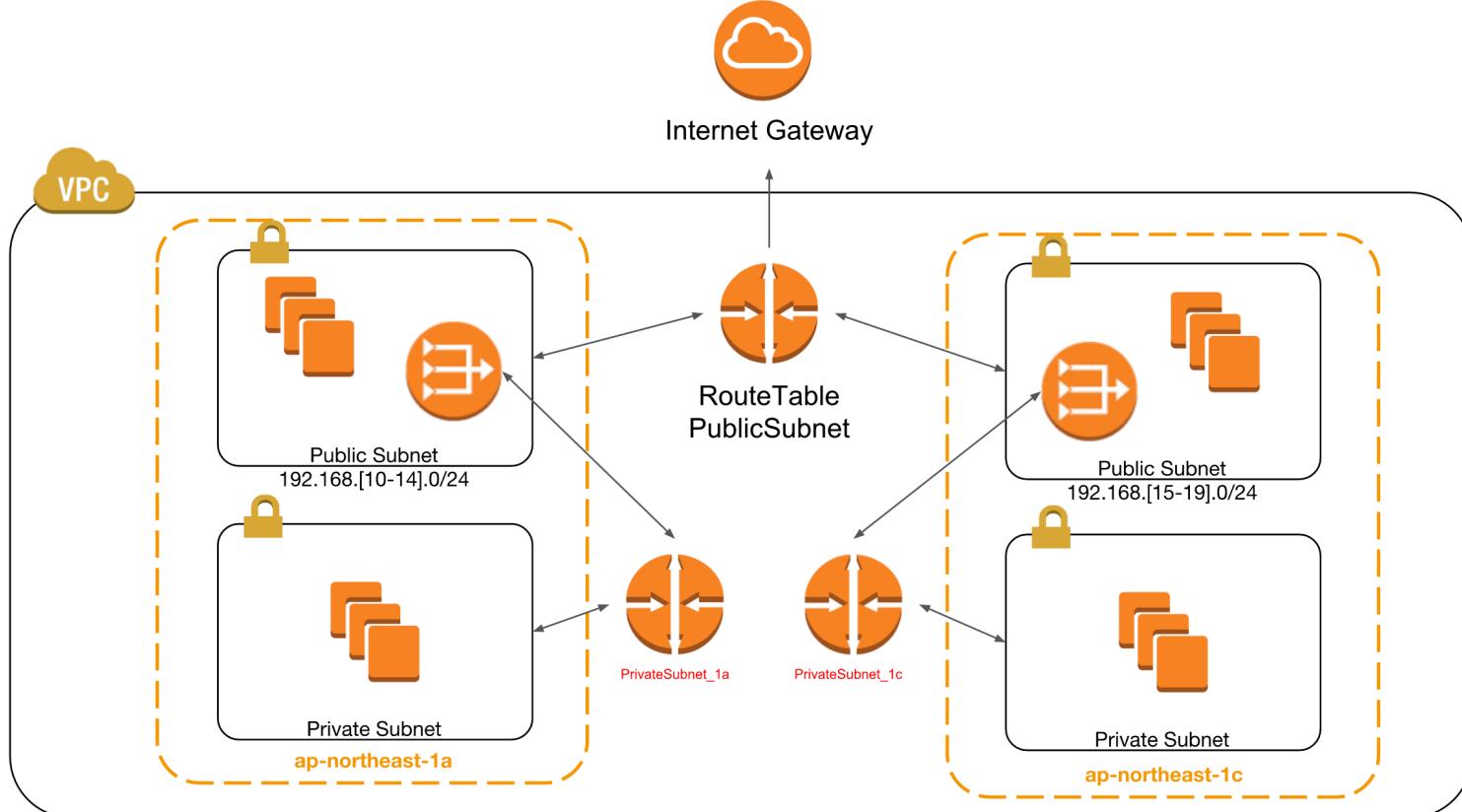
Options for Accessing the VPC

- **Internet-only**
 - Carefully plan routing and server placement in public and private subnets
 - Encrypt application and administrative traffic using SSL/TLS, or build custom user VPN solutions
 - Use security groups and NACLs
- **IPSec over the Internet**
 - Establish a private IPSec connection using IKEv1 and IPSec using standard AWS VPN facilities
 - Or establish customer- specific VPN software infrastructure in the cloud, and on-premises

Options for Protecting VPC

- **AWS Direct Connect without IPSec**
 - Depending on your data protection requirements, you might not need additional protection over private peering.
- **AWS Direct Connect with IPSec**
 - Establish a private IPSec connection using IKEv1 and IPSec using standard AWS VPN facilities
 - Or establish customer- specific VPN software infrastructure in the cloud, and on-premises
- **Hybrid**
 - Using a combination of these approaches with adequate protection mechanisms for each connectivity approach

NAT Gateways

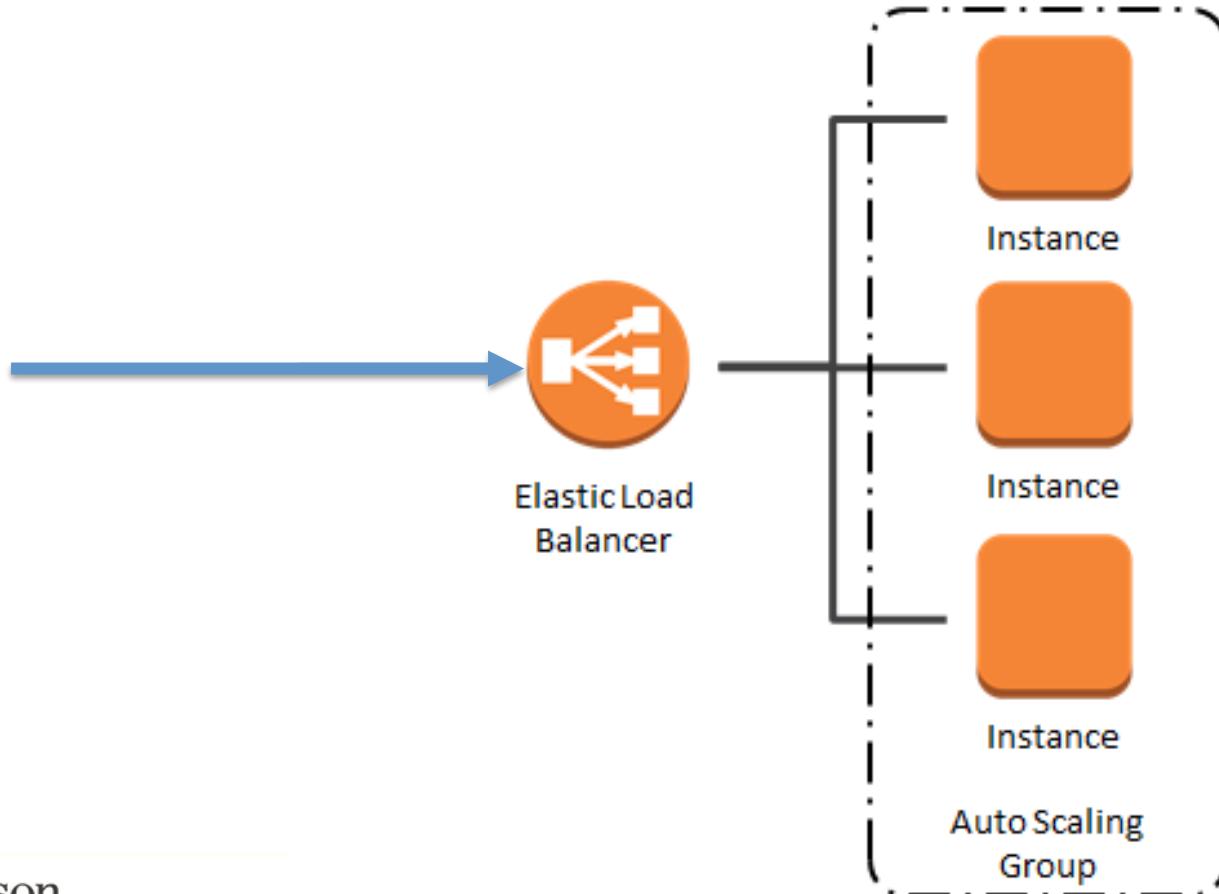


Core Networking Services

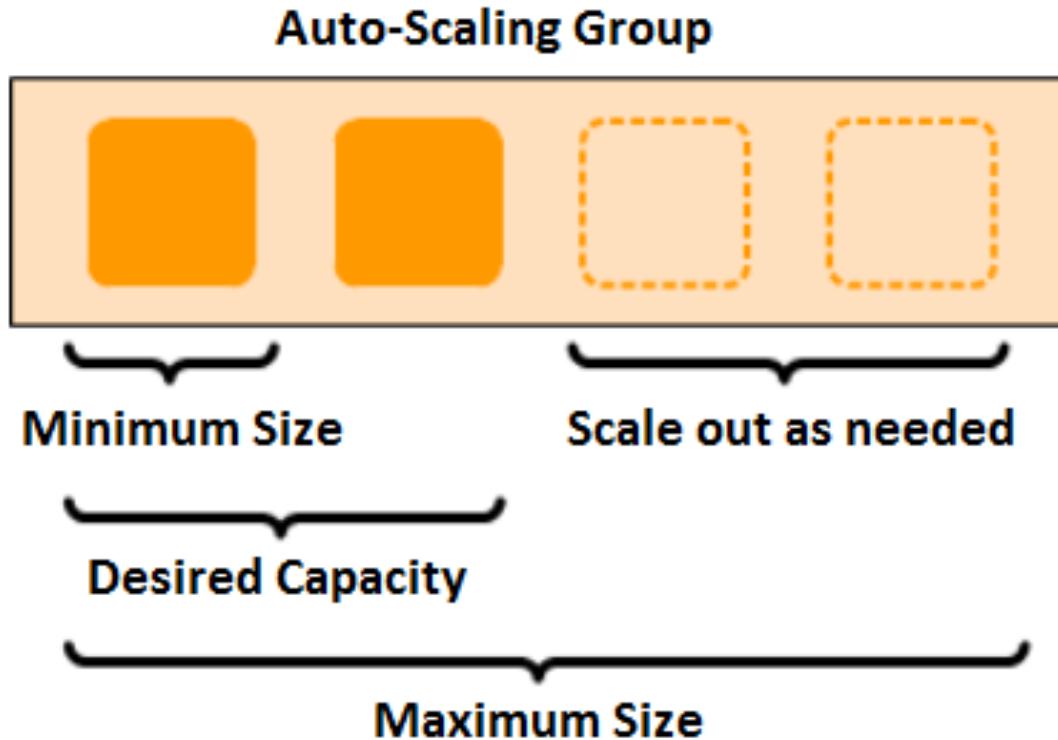
- **Elastic Load Balancing (ELB)** automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses
- It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones
- Elastic Load Balancing offers three types of load balancers:
 - Application Load Balancer
 - Network Load Balancer
 - Classic Load Balancer



Elastic Load Balancing



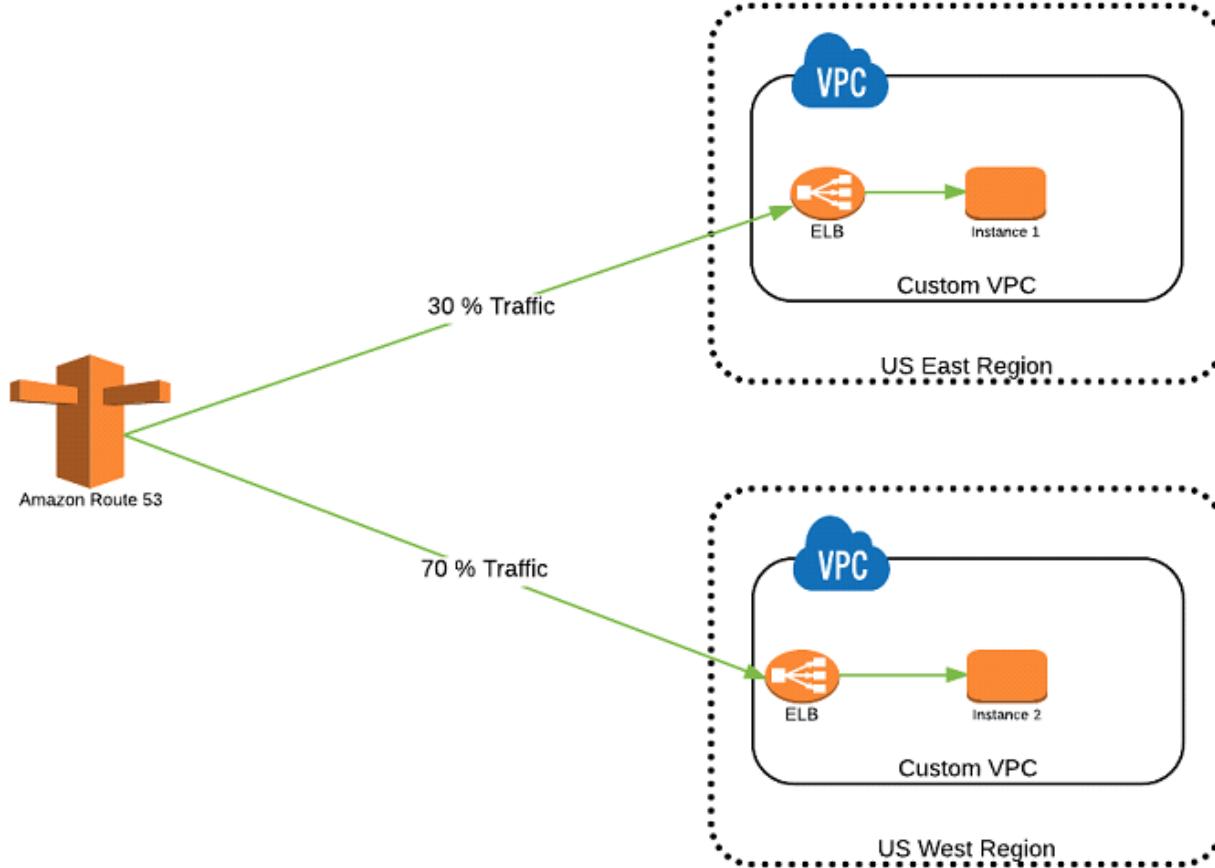
Auto-Scaling Groups



Core Networking Services

- **Amazon Route 53** is a highly available and scalable cloud Domain Name System (DNS) web service
- It is designed to provide an extremely reliable and cost-effective way to route end users to Internet applications by translating human readable names to IPv4 and IPv6 addresses
- Route 53 effectively connects user requests to infrastructure running in AWS (e.g. EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets) and can also be used to route users to infrastructure outside of AWS

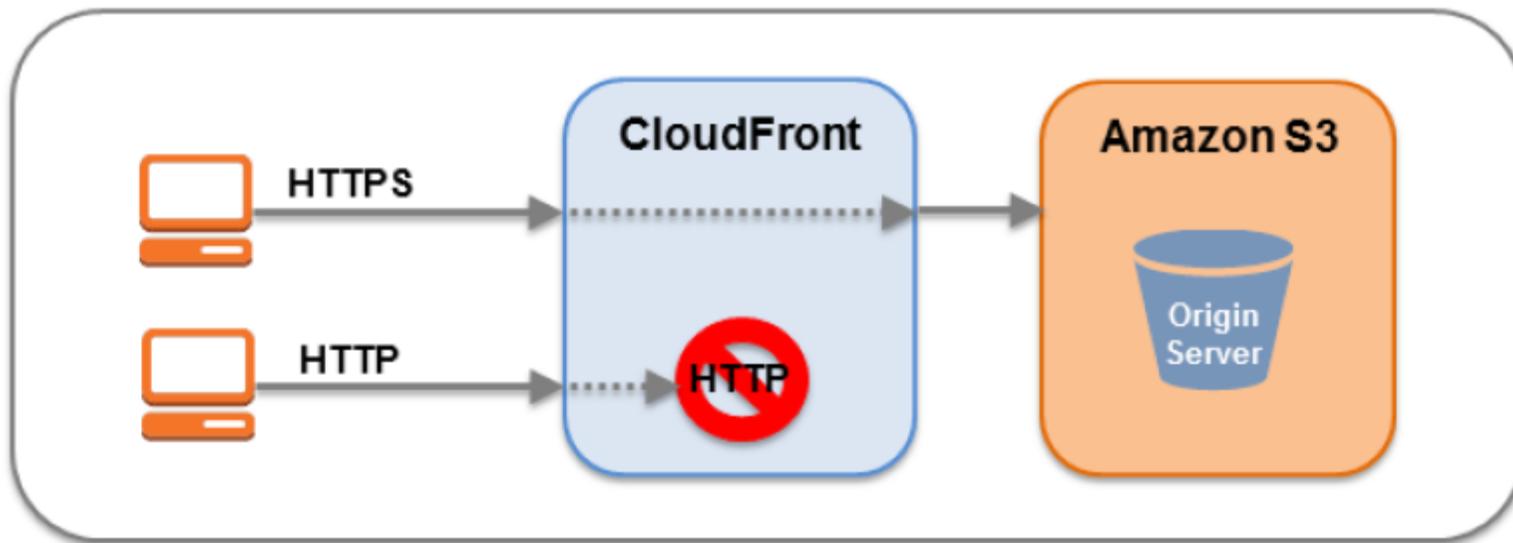
AWS Route 53



Core Networking Services

- **Amazon CloudFront** is a fast CDN service
- It securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds within a developer-friendly environment
- CloudFront is integrated with AWS – both physical locations that are directly connected to the AWS global edge locations and various service endpoints
- Functions seamlessly with Route 53, S3 storage, Elastic Load Balancing, EC2, and AWS Shield

Amazon CloudFront



Amazon CloudFront

AWS Services Resource Groups ▾

mjshannawstest Global Support ▾

Step 1: Select delivery method

Step 2: Create distribution

Select a delivery method for your content.

?

Web

Create a web distribution if you want to:

- Speed up distribution of static and dynamic content, for example, .html, .css, .php, and graphics files.
- Distribute media files using HTTP or HTTPS.
- Add, update, or delete objects, and submit data from web forms.
- Use live streaming to stream an event in real time.

You store your files in an origin - either an Amazon S3 bucket or a web server. After you create the distribution, you can add more origins to the distribution.

Get Started

RTMP

Create an RTMP distribution to speed up distribution of your streaming media files using Adobe Flash Media Server's RTMP protocol. An RTMP distribution allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location. Note the following:

- To create an RTMP distribution, you must store the media files in an Amazon S3 bucket.
- To use CloudFront live streaming, create a web distribution.

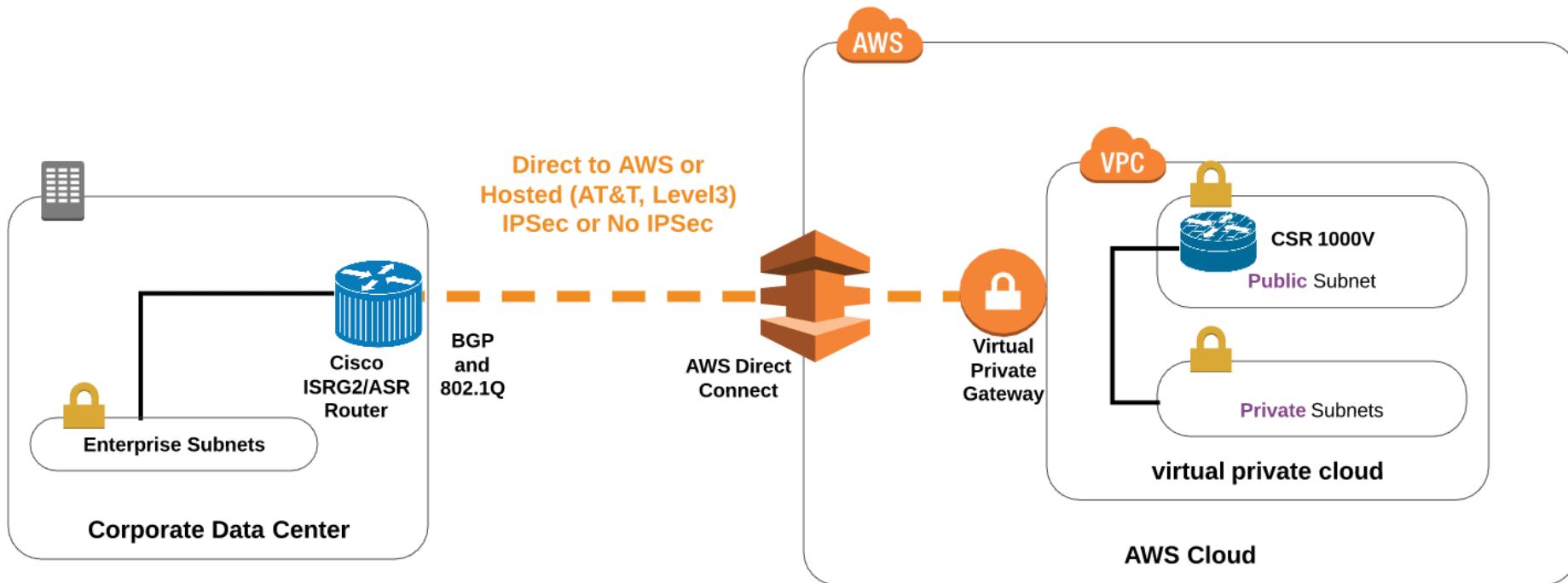
Get Started

Cancel

Core Networking Services

- **AWS Direct Connect** makes it easy to establish a dedicated network connection from your premises to AWS
- Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or co-location environment
- In many cases Direct Connect can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections

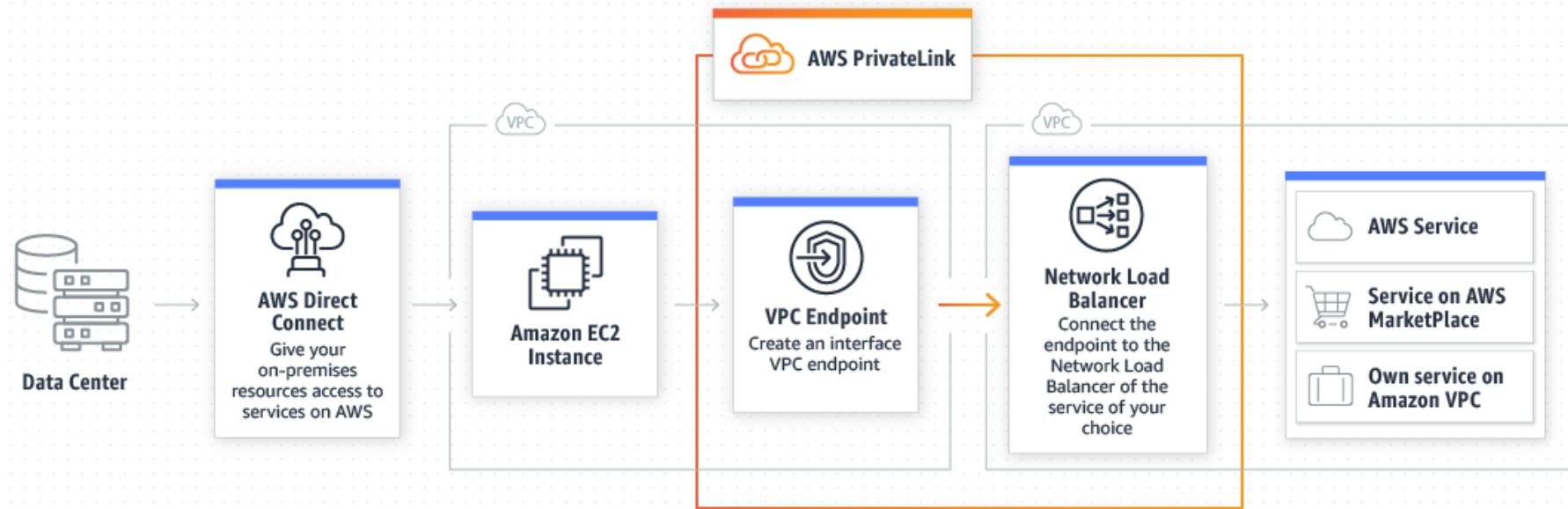
Using a Direct Connect Solution



Core Networking Services

- **AWS PrivateLink** simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet
- The service provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network
- PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture.

AWS PrivateLink



Core Networking Services

- **Amazon API Gateway** is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale
- Using the AWS Management Console, you can create an API to access data, business logic, or functionality from your back-end services
- API Gateway handles all the tasks involved in receiving and processing hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management

Core Networking Services

- **AWS Transit Gateway** is a service that allows customers to connect their VPCs and their on-premises networks to a single gateway
- As you grow the number of workloads running on AWS, you need to be able to scale your networks across multiple accounts and Amazon VPCs to keep up with the growth
- For on-premises connectivity, you need to attach your AWS VPN to each individual Amazon VPC
- This solution can be time consuming to build and hard to manage when the number of VPCs grows into the hundreds

VPN Connections

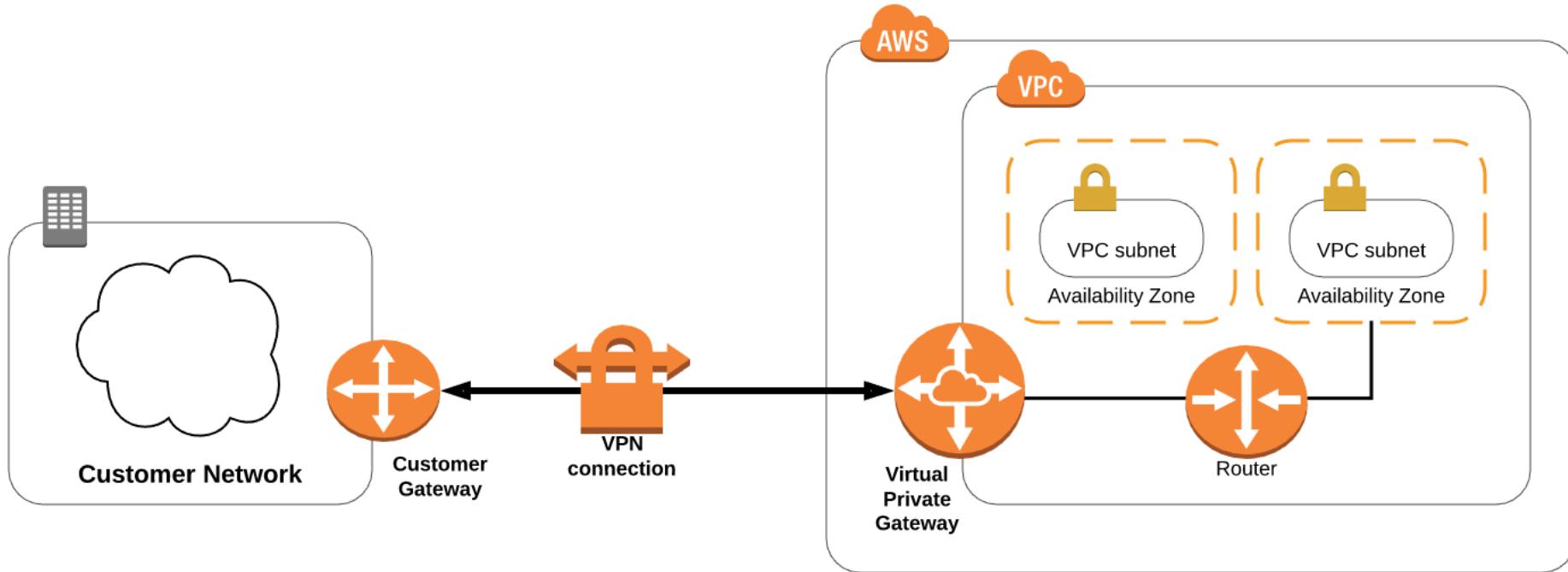
VPN Connectivity Option	Description
AWS Site-to-Site VPN	Create a managed IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a virtual private gateway provides two VPN endpoints (tunnels) for automatic failover. You configure your customer gateway on the remote side of the VPN connection.
AWS VPN CloudHub	If you have multiple branch offices, you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks.
Third party software VPN Appliance	Use an EC2 instance from the marketplace such as Cisco, Palo Alto Networks, Fortinet, and others



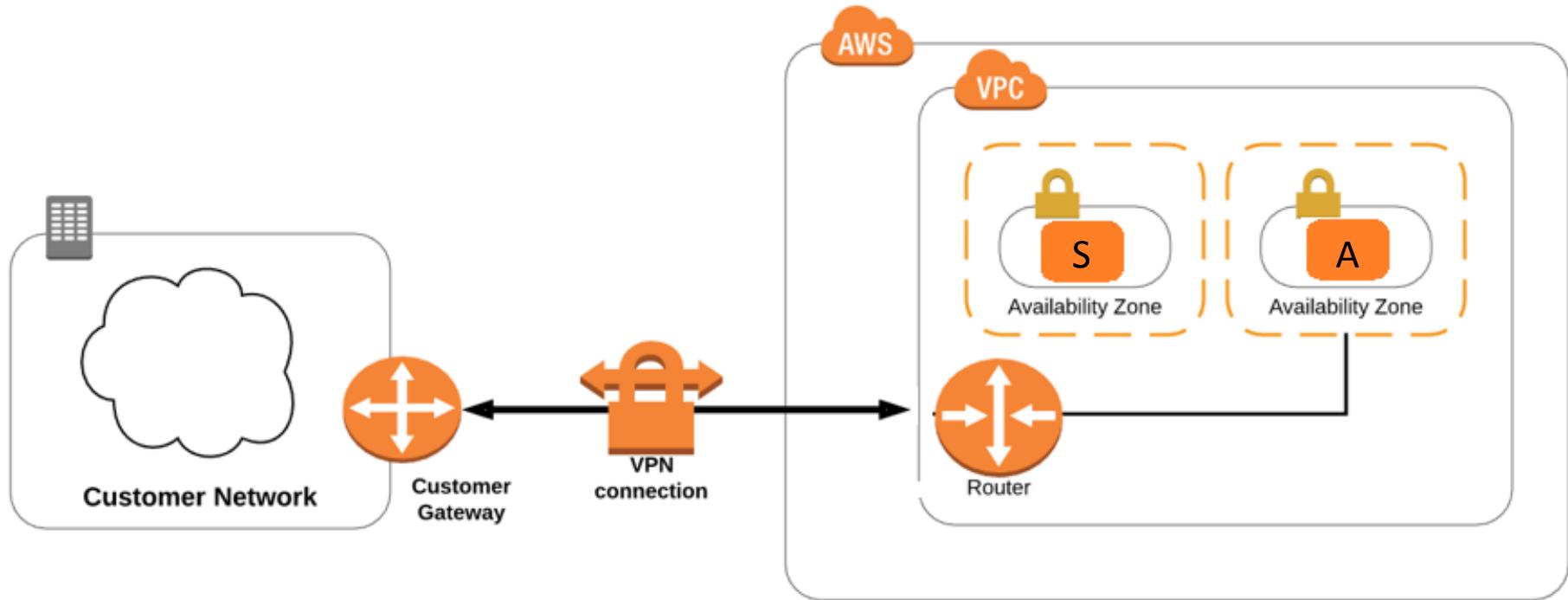
AWS Site-to-Site (Managed) VPN

- Instances that you launch into a VPC can't communicate with your own (remote) network by default.
- In a VPC, a VPN connection refers to the connection between your VPC and your own network.
 1. Attach a virtual private gateway to the VPC
 2. Create a custom route table
 3. Update the security group rules
 4. Create an AWS managed VPN connection

Single Managed VPN Connection



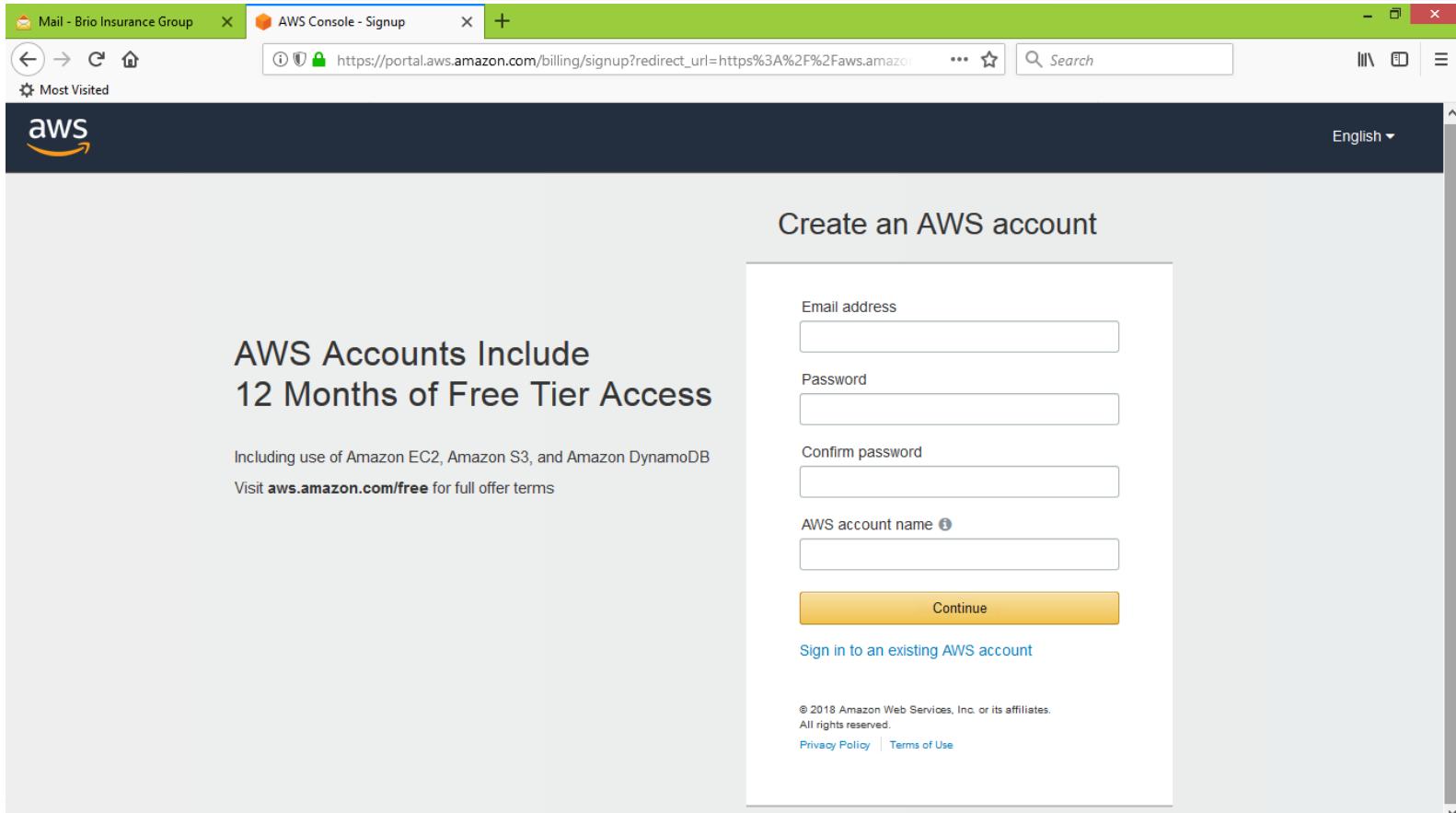
Using an Instance to Terminate VPN





Segment 3: AWS Account Basics

Credentials: AWS Root Account



The screenshot shows a web browser window with two tabs: "Mail - Brio Insurance Group" and "AWS Console - Signup". The "AWS Console - Signup" tab is active, displaying the "Create an AWS account" form. The form includes fields for Email address, Password, Confirm password, and AWS account name, each with a corresponding input box. A large yellow "Continue" button is positioned below the password fields. Below the form, there is a link to "Sign in to an existing AWS account". At the bottom of the page, there is a copyright notice for Amazon Web Services and links to "Privacy Policy" and "Terms of Use".

Mail - Brio Insurance Group X AWS Console - Signup +

https://portal.aws.amazon.com/billing/signup?redirect_url=https%3A%2F%2Faws.amazon.com%2Fsignups%2Froot%2Fcreate%2F

Search

Most Visited

aws English ▾

Create an AWS account

AWS Accounts Include
12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB
Visit aws.amazon.com/free for full offer terms

Email address

Password

Confirm password

AWS account name ⓘ

Continue

Sign in to an existing AWS account

© 2018 Amazon Web Services, Inc. or its affiliates.
All rights reserved.

[Privacy Policy](#) | [Terms of Use](#)

Credentials: AWS Root Account



Root user sign in i

Email: @.net

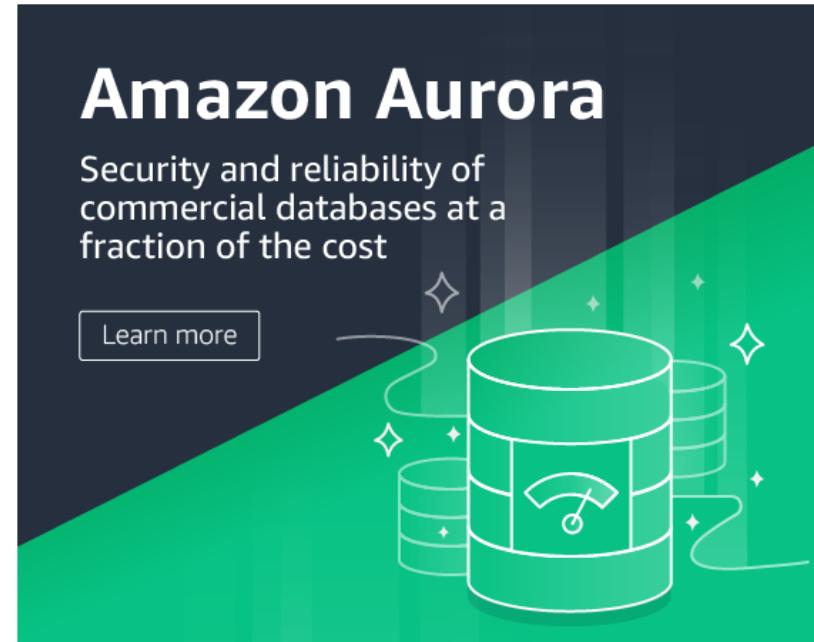
Password

[Forgot password?](#)

[Sign in](#)

[Sign in to a different account](#)

[Create a new AWS account](#)



The image is an advertisement for Amazon Aurora. It features a dark blue header with the text "Amazon Aurora" in large white letters. Below the header, a green diagonal band contains the text "Security and reliability of commercial databases at a fraction of the cost". A "Learn more" button is located in the lower-left area of the dark section. The right side of the ad is a green background with white line-art illustrations of three cylindrical database storage units. One unit has a Wi-Fi signal icon on it. Small white stars and sparkles are scattered around the cylinders.

Passwords

- AWS Account
 - Individual IAM user accounts
 - AWS Discussion Forums
 - AWS Support Center
-
- AWS passwords can be up to 128 characters long and contain special characters
 - You are encouraged to create long and strong passwords that cannot be easily guessed



Signing In to Your Accounts

Your sign-in page URL has the following format, by default.

```
https://Your_AWS_Account_ID.signin.aws.amazon.com/console/
```

If you create an AWS account alias for your AWS account ID, your sign-in page URL will look like the following example.

```
https://Your_Alias.signin.aws.amazon.com/console/
```

Creating an Alias

IAM Management Console Customize Copy Link

https://219258942154.signin.aws.amazon.com/console

Welcome to Identity and Access Management

IAM users sign-in link:

IAM Resources

Users: 0	Roles: 0
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

Security Status: 1 out of 5 complete.

- Delete your root access keys
- ⚠ Activate MFA on your root account
- ⚠ Create individual IAM users
- ⚠ Use groups to assign permissions
- ⚠ Apply an IAM password policy

Feature Spotlight: Introduction to AWS IAM

Additional Information

- IAM best practices
- IAM documentation
- Web Identity Federation Playground
- Policy Simulator
- Videos, IAM release history and additional resources



Feedback

English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Credential Usage Options

Credential Type	Use	Description
Passwords	AWS root account or IAM user account login to the AWS Management Console	A string of characters used to log into your AWS account or IAM account. AWS passwords must be a minimum of 6 characters and may be up to 128 characters.
Multi-Factor Authentication (MFA)	AWS root account or IAM user account login to the AWS Management Console	A six-digit single-use code that is required in addition to your password to log in to your AWS Account or IAM user account.
Access Keys	Digitally signed requests to AWS APIs (using the AWSSDK, CLI, or REST/Query APIs)	Includes an access key ID and a secret access key. You use access keys to digitally sign programmatic requests that you make to AWS.

Credential Usage Options

Credential Type	Use	Description
Key Pairs	<ul style="list-style-type: none">· SSH login to EC2 instances· CloudFront signed URLs· Windows instances	To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. Linux instances have no password, and you use a key pair to log in using SSH. With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP.
X.509 Certificates	<ul style="list-style-type: none">· Digitally signed SOAP requests to AWS APIs· SSL server certificates for HTTPS	X.509 certificates are only used to sign SOAP-based requests (currently used only with Amazon S3). You can have AWS create an X.509 certificate and private key that you can download, or you can upload your own certificate by using the Credential Report .

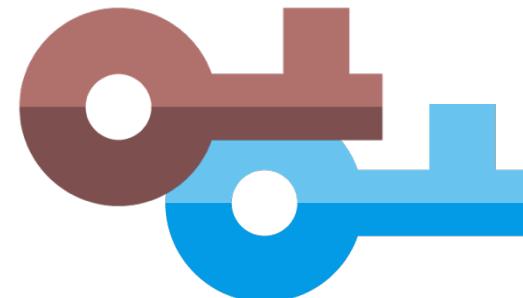
AWS Multi-Factor Authentication

- Provide a six-digit single-use code in addition to your standard credentials before given access to the AWS Account settings or AWS services and resources
- AWS MFA supports the use of both hardware tokens and virtual MFA devices



Key Pairs

- Amazon EC2 uses public–key cryptography to encrypt and decrypt login information
- Public–key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data
- The public and private keys are known as a key pair



EC2 Instance Key Pairs

Select an existing key pair or create a new key pair X

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

No key pairs found

⚠ No key pairs found

You don't have any key pairs. Please create a new key pair by selecting the **Create a new key pair** option above to continue.

[Cancel](#) Launch Instances

Creating Key Pairs

The screenshot shows the AWS EC2 Management Console interface. The top navigation bar includes tabs for 'Amazon EC2 Key Pairs - Amazon' and 'EC2 Management Console'. The main content area has a title 'Create Key Pair' and a search bar. A message states 'You do not have any Key Pairs in this region.' Below it, a call-to-action button says 'Click the "Create Key Pair" button to create your first Key Pair.' A large blue 'Create Key Pair' button is prominently displayed. On the left, a sidebar lists various AWS services under categories like NETWORK & SECURITY, LOAD BALANCING, AUTO SCALING, and SYSTEMS MANAGER SERVICES. The 'Key Pairs' option is selected and highlighted with an orange border. At the bottom right of the main content area, there are three small square icons.

Creating Key Pairs

The screenshot shows the AWS EC2 Management Console interface. On the left, a sidebar lists various AWS services: Snapshots, NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs), LOAD BALANCING (Load Balancers, Target Groups), AUTO SCALING (Launch Configurations, Auto Scaling Groups), and SYSTEMS MANAGER SERVICES (Run Command, State Manager, Configuration Compliance, Automations). The 'Key Pairs' option is selected. In the main content area, there are three buttons: 'Create Key Pair' (highlighted in blue), 'Import Key Pair', and 'Delete'. Below these buttons is a search bar with the placeholder 'Filter by attributes or search by keyword'. A table lists existing key pairs, with 'AWS-Crash-Keys' selected. The table columns are 'Key pair name' and 'Fingerprint'. The 'Fingerprint' column for 'AWS-Crash-Keys' displays the value: 07:1d:df:f0:c4:2f:99:0e:30:78:ed:c8:8d:eb:54:01:c8:3d:2c:cb. A modal dialog box titled 'Opening AWS-Crash-Keys.pem' is overlaid on the page. It contains the message: 'You have chosen to open: AWS-Crash-Keys.pem which is: Text Document from: https://us-east-2.console.aws.amazon.com'. It asks, 'What should Firefox do with this file?'. There are two radio button options: 'Open with Notepad (default)' and 'Save File' (which is selected). A checkbox at the bottom says 'Do this automatically for files like this from now on.' At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

AWS Command Line Interface

The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home#/users\\$new?step=final&accessKey&login](https://console.aws.amazon.com/iam/home#/users$new?step=final&accessKey&login). The page is titled "Add user" and displays a four-step process: 1. Details (grey), 2. Permissions (grey), 3. Review (grey), and 4. Complete (blue). A "Success" message box is open, stating: "You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time." It includes a link to sign-in: "Users with AWS Management Console access can sign-in at: <https://4.signin.aws.amazon.com/console>". Below this, a table lists a single user: "Administrator". The table columns are "User", "Access key ID", "Secret access key", and "Email login instructions". The "Access key ID" is AKIAIIBX4IGZMHPPV4XA, and the "Secret access key" is masked as ***** Show. A "Send email" button is next to the "Email login instructions" column. At the bottom right of the table is a "Close" button.

User	Access key ID	Secret access key	Email login instructions
Administrator	AKIAIIBX4IGZMHPPV4XA	***** Show	Send email

AWS Command Line Interface

AWS Command Line Interface

<https://aws.amazon.com/cli/>

The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

The AWS CLI introduces a new set of simple [file commands](#) for efficient file transfers to and from Amazon S3.



[Getting Started »](#)



[CLI Reference »](#)



[GitHub Project »](#)



[Community Forum »](#)

Windows

Download and run the [64-bit](#) or [32-bit](#) Windows installer.

Mac and Linux

Requires [Python 2.6.5](#) or higher.
Install using [pip](#).

```
pip install awscli
```

Amazon Linux

The AWS CLI comes pre-installed on [Amazon Linux AMI](#).

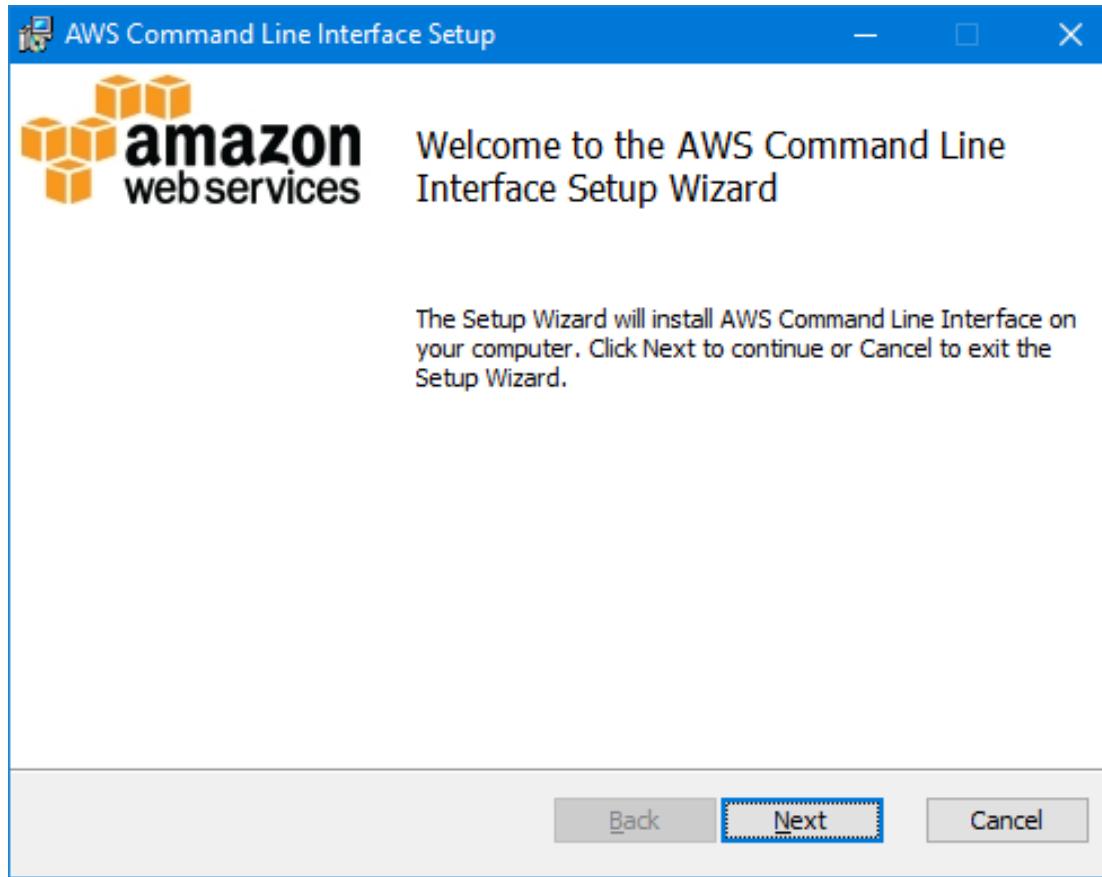
Release Notes

Check out the [Release Notes](#) for more information on the latest version.

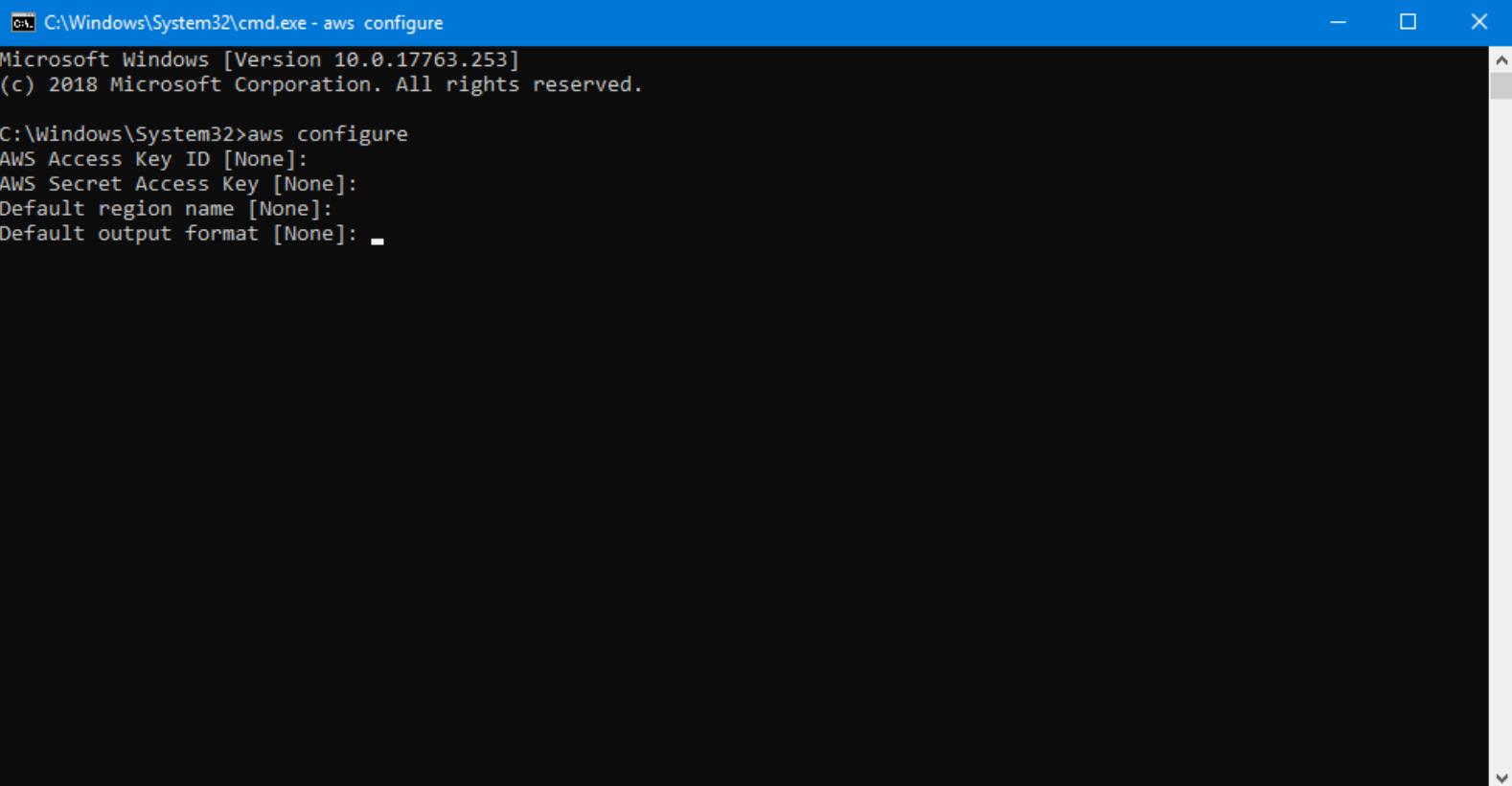


Pearson

AWS Command Line Interface



AWS Command Line Interface



C:\Windows\System32\cmd.exe - aws configure

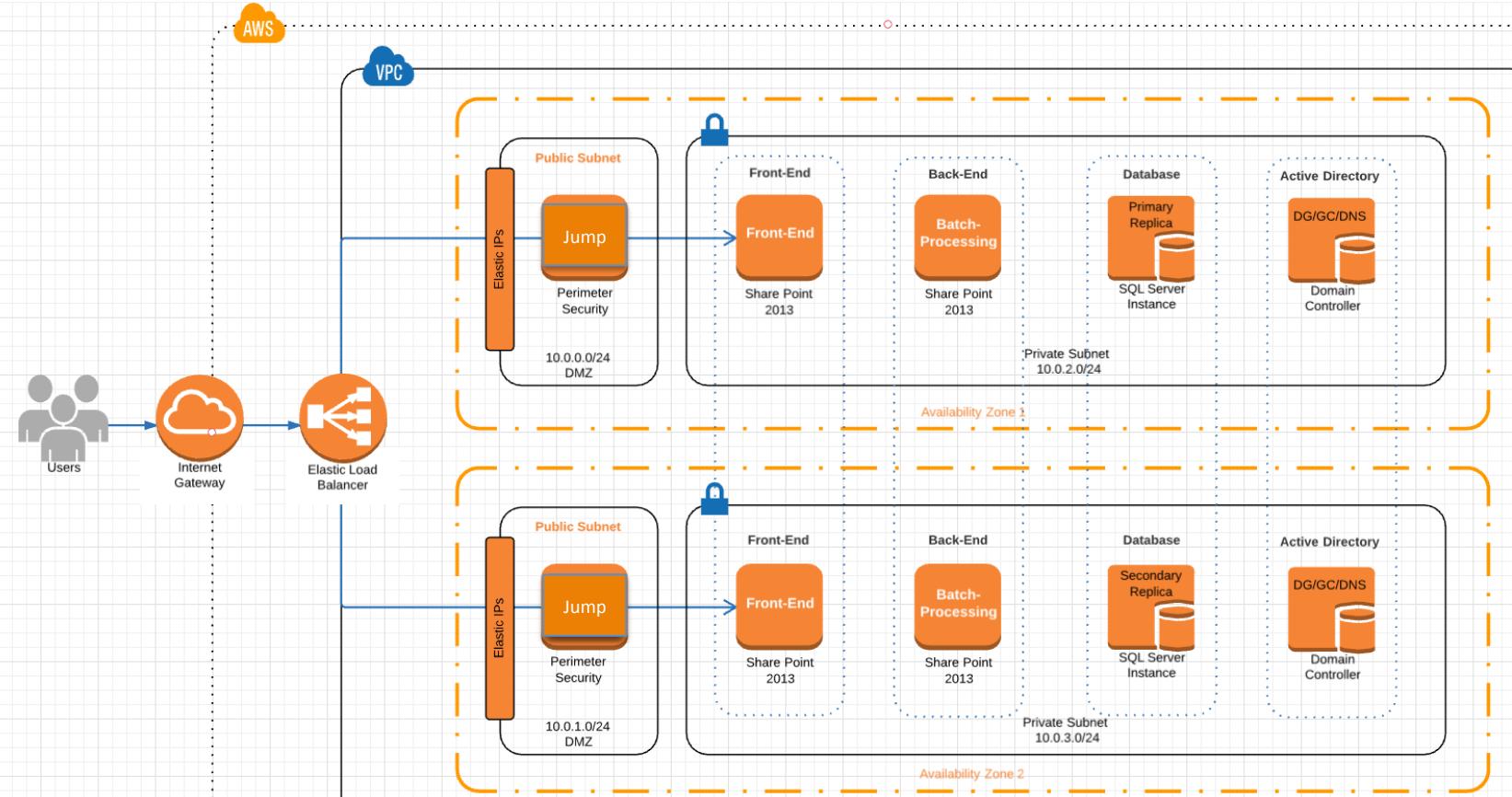
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

```
C:\Windows\System32>aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]: -
```

Access Keys

- AWS requires that all API requests must include a digital signature that is used to verify the requestor identity
- Digital signature is calculated using a cryptographic hash (HMAC-SHA256) where the input to the function in this case includes the text of your request and your secret access key
- Offers message integrity and anti-replay protection
- Required to sign message using a key derived from your secret access key instead of using the secret access key itself

Using a Bastion Host (Jump)





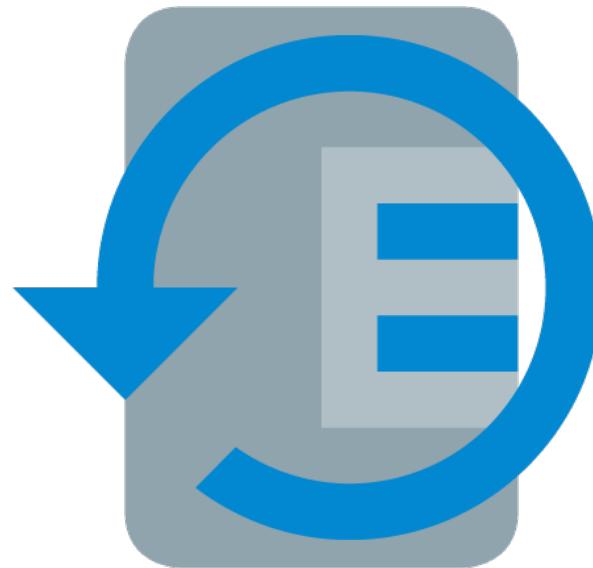
Segment 4: Compute Technologies

Core Compute Services

- **Amazon Elastic Compute Cloud (Amazon EC2)** is a web service that provides secure, resizable compute capacity in the cloud
- The Amazon EC2 simple web service interface gives you complete control of your computing resources and lets you run on Amazon's proven computing environment
- EC2 reduces the time required to obtain and boot new server instances (Amazon EC2 instances) to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change

AWS EC2 Instance Types

- **On-Demand** Instances – you pay for compute capacity by the hour with no long-term commitments
- **Reserved** Instances –offer you a significant discount (up to 75%) compared to On-Demand instance pricing
- **Spot** Instances - allow you to bid on spare Amazon EC2 computing capacity.

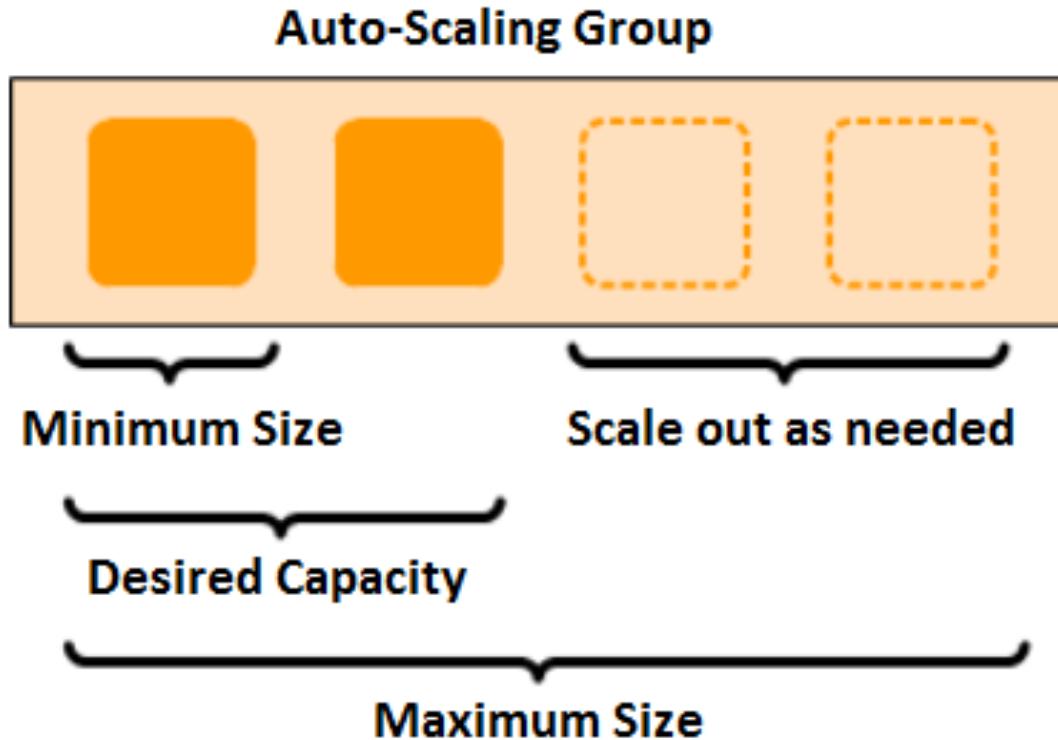


@iconshock.com

Core Compute Services

- **Amazon EC2 Auto Scaling** helps you preserve application availability and lets you automatically add or remove EC2 instances according to conditions that you describe
- You can use the fleet management features of EC2 Auto Scaling to maintain the health and availability of your fleet
- You can also use the dynamic and predictive scaling features of EC2 Auto Scaling to add or remove EC2 instances

Auto-Scaling Groups



Core Compute Services

- **Amazon Elastic Container Registry (Amazon ECR)** is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images
 - Amazon ECR is integrated with **Amazon Elastic Container Service (Amazon ECS)**
- Amazon ECS is a highly scalable, high-performance container orchestration service that supports Docker containers and allows you to easily run and scale containerized applications on AWS

Core Compute Services

- **Amazon Lightsail** is one of the easiest ways to launch and manage a virtual private server with AWS
- Lightsail plans include everything necessary to jumpstart a project for a low, predictable price:
 - A virtual machine
 - SSD- based storage
 - Data transfer
 - DNS management
 - A static IP address



@iconshock.com

Core Compute Services

- **AWS Elastic Beanstalk** is an easy-to-use service for deploying, monitoring and scaling web applications and services developed on several different platforms and applications
 1. Choose your platform (Generic Docker, Preconfigured, Preconfigured Docker)
 2. Upload an application or use a sample code from AWS
 3. Run it
- **AWS Batch** enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS

Elastic Beanstalk

Application information

Application name

Up to 100 Unicode characters, not including forward slash (/).

Base configuration

Platform

– Choose a platform –

- Choose a platform –
- Generic
 - Docker
 - Multi-container Docker
- Preconfigured
 - Elastic Beanstalk Packer Builder
 - Go
 - .NET (Windows/IIS)
 - Java
 - Node.js
 - Ruby
 - PHP
 - Python
 - Tomcat
- Preconfigured – Docker
 - GlassFish
 - Go
 - Python

...n configuration options.

...r copy one from Amazon S3.

Cancel

Configure more options

Create application

Core Compute Services

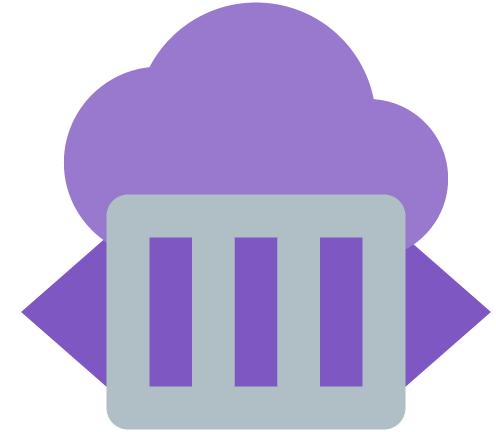
- **AWS Lambda** lets you run code without deploying or managing servers
 - You pay only for the compute time you consume and there is no charge when your code is not running
 - You can run code for virtually any type of application or backend service—all with zero administration
- <https://aws.amazon.com/serverless/#usecases>



@iconshock.com

Core Compute Services

- **AWS Outposts** bring native AWS services, infrastructure, and operating models to virtually any data center, co-location space, or on-premises facility
- You can use the same APIs, tools, hardware, and the same functionality across on-premises and the cloud to deliver a truly consistent hybrid experience
- aws.amazon.com/outposts



@iconshock.com

A large, light gray circular icon containing a white right-pointing triangle, resembling a play button or a start symbol.

AWS Cloud Practitioner

Michael J.
Shannon

See You
Tomorrow!

