

Module 2
AWS Foundational Services

aws training and certification

Module 2 Topics

aws training and certification

- Amazon Elastic Compute Cloud (EC2)
- Amazon Virtual Private Cloud (VPC)
  - Lab 1: Build your VPC and launch a web server
- Amazon Storage Services
  - Amazon Simple Storage Service (S3)
  - Amazon Elastic Block Store (EBS)

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

aws training and certification

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (EC2)

aws training and certification



Amazon EC2

- Resizable compute capacity
- Complete control of your computing resources
- Reduced time required to obtain and boot new server instances

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

Amazon EC2 Facts

aws training and certification

- **Scale capacity** as your computing requirements change
- Pay only for capacity that you actually use
- Choose **Linux** or **Windows**
- Deploy across AWS **Regions** and **Availability Zones** for reliability
- Use tags to help manage your Amazon EC2 resources

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

Choosing the Right Amazon EC2 Instance Type

aws training and certification

- Amazon EC2 provides a wide selection of instance types that are optimized for different use cases and workload requirements.
- Consider the following when choosing your instances:
  - Core count
  - Memory size
  - Storage size and type
  - Network performance
  - CPU technologies
- AWS uses Intel® Xeon® processors to provide customers with high performance and value.



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

Choosing the Right Amazon EC2 Instance Type

aws training and certification

Amazon EC2 Families:

- **General Purpose:** Balanced workloads
- **Compute-Optimized:** High-performance computing, data lakes, network appliances
- **Memory-Optimized:** High-performance databases, in-memory databases
- **Accelerated Computing:** GPU-intensive workloads (machine learning, 3D rendering)
- **Storage-Optimized:** High IOPS at low cost

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

Intel® Xeon Scalable Processors

aws training and certification

Latest generation of Intel Xeon processors (Skylake)

Available in latest generation Amazon EC2 instance types

Up to:

- 28 cores per CPU
- 6 memory channels
- 48 PCIe lanes of bandwidth/throughput
- 100 Gbps network bandwidth (C5n.16xlarge)

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

Intel® Xeon Family and EC2 Instances

aws training and certification

Scalable Processor Family	E5 Processor Family	E7 Processor Family
Memory-Optimized: z1d, R5, High Memory Compute-Optimized: C5/C5n General Purpose CPU: M5 General Purpose: T3	General Purpose: M4 Compute-Optimized: C4 Memory-Optimized: R4 GPU Intensive: P2/P3, G3, F1 Storage Optimized: H1, I3, D2	Memory Optimized: X1/X1e

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

Comparing Intel Xeon Generations

aws training and certification

C5n Instances

- 3.0 GHz Intel Xeon Platinum (Skylake) CPUs
- Up to 72 vCPUs
- Up to 192 GiB memory
- Up to 14k Mbps dedicated EBS bandwidth
- 25-100 Gbps network bandwidth

C4 Instances

- 2.9 GHz Intel Xeon E5-2666 v3 (Haswell) CPUs
- Up to 36 vCPUs
- Up to 60 GiB memory
- Up to 4k Mbps dedicated EBS bandwidth
- Up to 10 Gbps network bandwidth

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

C5n Instance Example Sizing Choices

aws training and certification

	vCPUs	Memory (GiB)	Network (Gbps)
large	2	5.25	Up to 25
xlarge	4	10.5	Up to 25
2xlarge	8	21	Up to 25
4xlarge	16	42	Up to 25
9xlarge	36	96	50
18xlarge	72	192	100

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

Choosing the Right Instance

aws training and certification

Newer generation instance types usually have a better price-to-performance ratio.

Examples*:

Instance Change	Costs Saved per Instance
T2.XLarge to T3.Large	47%
T2.Large to T3.Medium	44%
C4.8XLarge to C5.4XLarge	50%

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

* According to TSO Logic, November 2018 (link in notes)

Launching an Amazon EC2 Instance via the Management Console

aws training and certification

- Determine the **AWS Region** in which you want to launch the Amazon EC2 instance.
- Launch an Amazon EC2 instance from a pre-configured **Amazon Machine Image** (AMI).
- Choose an instance **type** based on CPU, memory, storage, and network requirements.
- Configure **network**, IP address, security groups, **storage** volume, tags, and **key pair**.

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

Amazon Machine Image (AMI) Details

aws training and certification

An AMI includes the following:

- A template for the **root volume** for the instance (for example, an operating system, an application server, and applications).
- **Launch permissions** that control which AWS accounts can use the AMI to launch instances.
- A block device mapping that specifies the **volumes to attach** to the instance when it is launched.

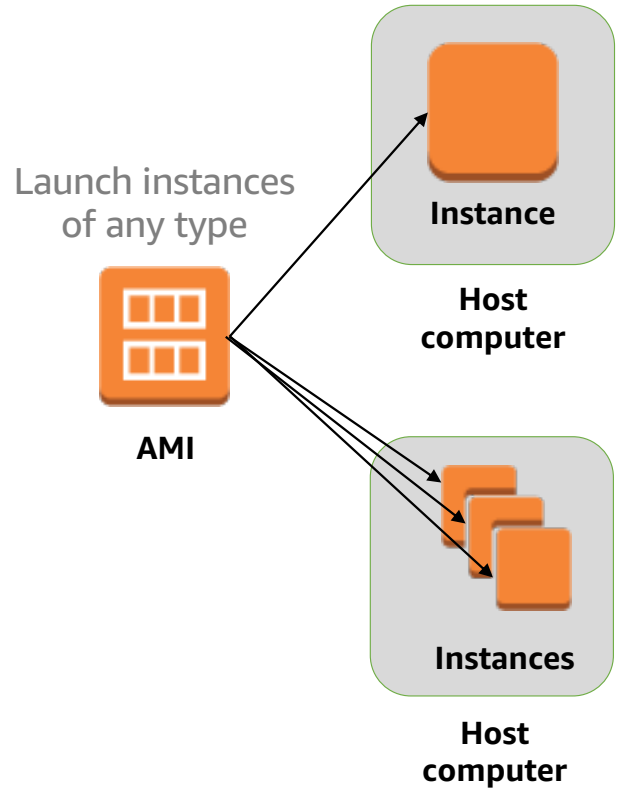
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Instances and AMIs

aws training and certification

Select an AMI based on:

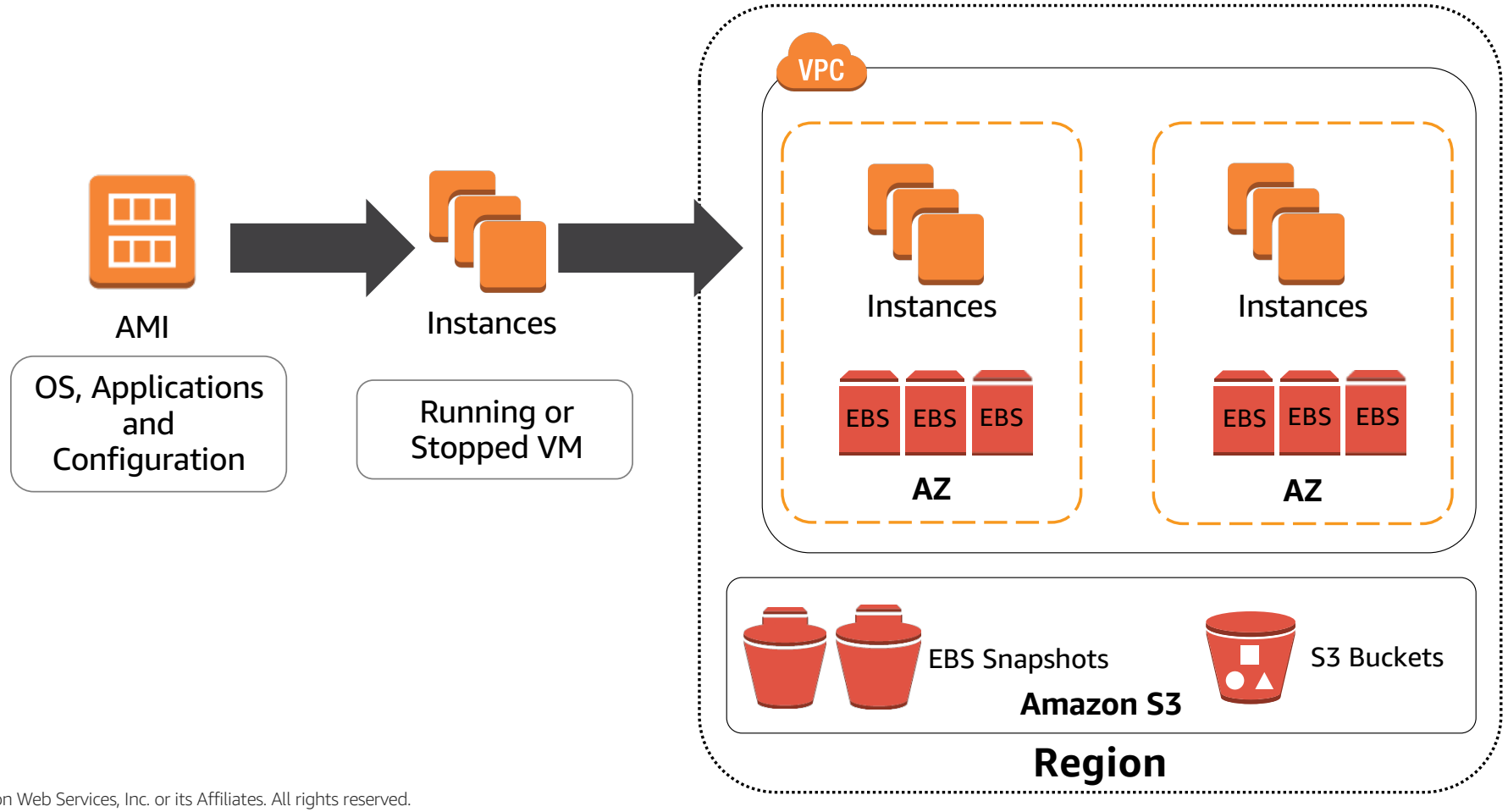
- Region
- Operating system
- Architecture (32-bit or 64-bit)
- Launch permissions
- Storage for the root device



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

Amazon EC2 Instances

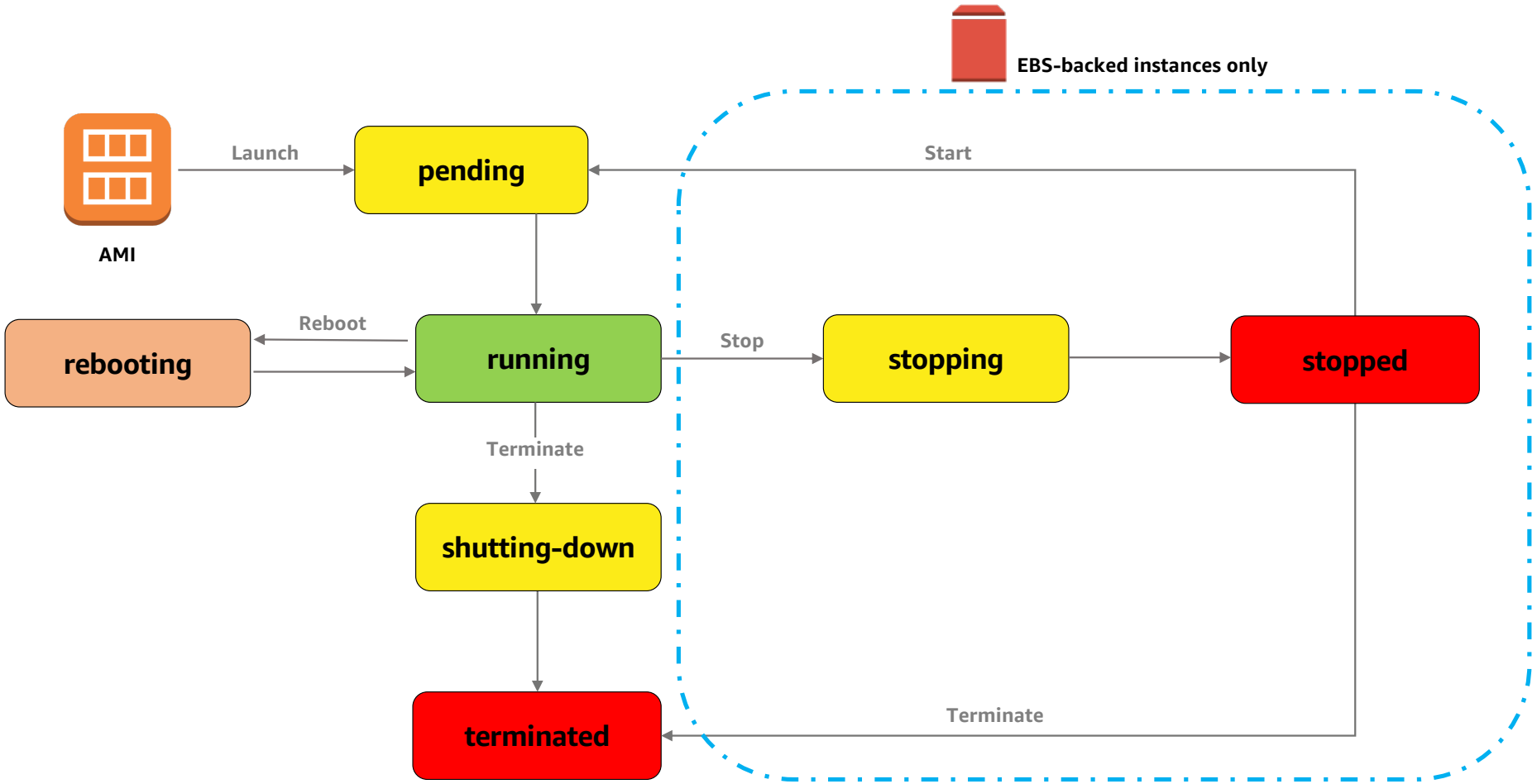
aws training and certification



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

Instance Lifecycle

aws training and certification



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

Instance Metadata

aws training and certification

- Is data about your instance.
- Can be used to configure or manage a running instance.

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

Retrieving Instance Metadata

aws training and certification

- To view all categories of instance metadata from within a running instance, use the following URI:

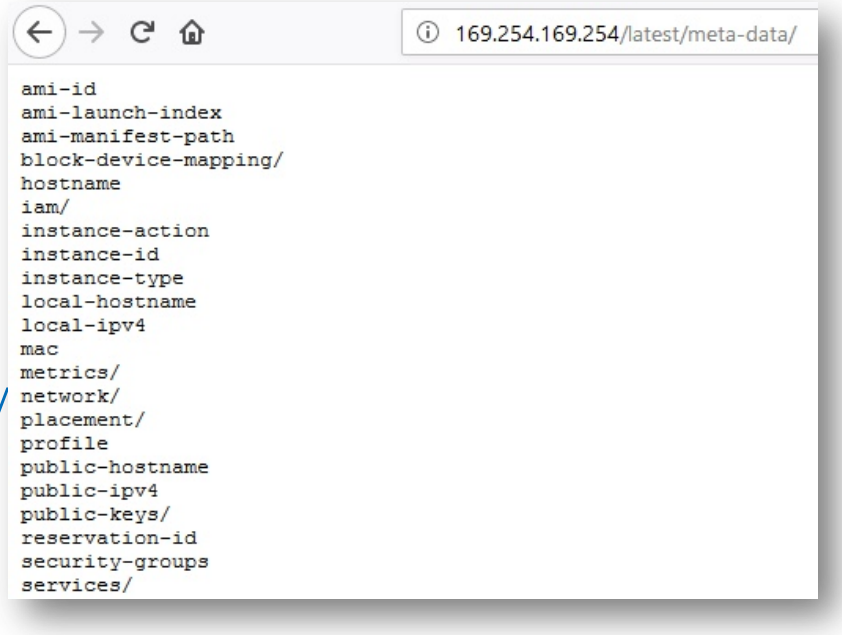
  http://169.254.169.254/latest/meta-data/

- On a Linux instance, you can use:

  $ curl http://169.254.169.254/latest/meta-data/

  $ GET http://169.254.169.254/latest/meta-data/

- All metadata is returned as text (content type text/plain).



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

Instance User Data

aws training and certification

- Can be passed to the instance **at launch**.
- Can be used to perform common automated configuration tasks.
- Runs scripts after the instance starts.

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

Adding User Data

aws training and certification

- You can specify user data when launching an instance.
- User data can be:
  - **Linux** script – executed by cloud-init
  - **Windows** batch or PowerShell scripts – executed by EC2Launch service
- User data scripts **run once** per instance ID by default.

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

User Data Example Linux

aws training and certification

```
#!/bin/sh
yum -y install httpd
chkconfig httpd on
/etc/init.d/httpd start
```

User data shell scripts must start with the #! characters and the path to the interpreter you want to read the script.

Install Apache web server
Enable the web server
Start the web server

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

User Data Example Windows

aws training and certification

```
<powershell>
Import-Module ServerManager

Install-WindowsFeature web-server, web-webserver
Install-WindowsFeature web-mgmt-tools
</powershell>
```

Import the Server Manager module for Windows PowerShell.

Install IIS
Install Web Management Tools

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

Retrieving User Data

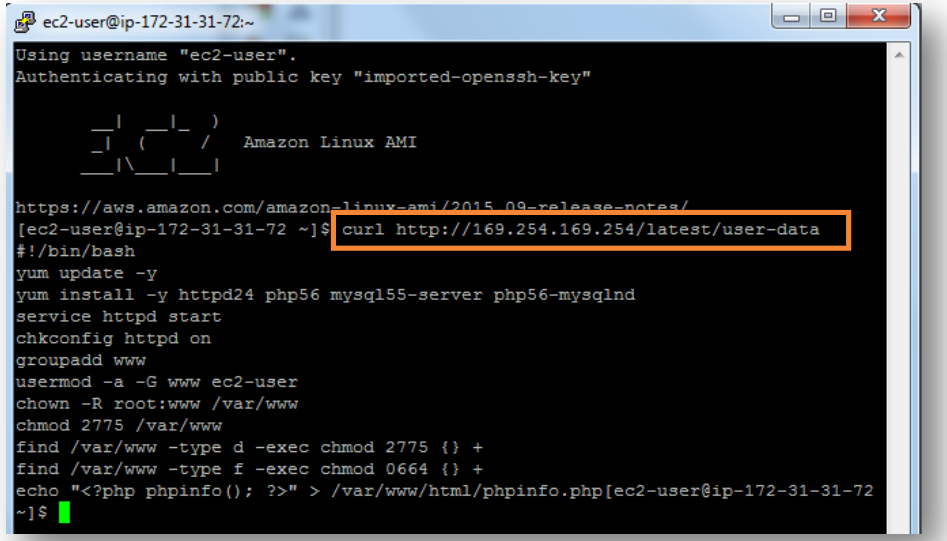
aws training and certification

- To retrieve user data, use the following URI:

```
http://169.254.169.254/latest/user-data
```

- On a Linux instance, you can use:

```
$ curl http://169.254.169.254/latest/user-data/
$ GET http://169.254.169.254/latest/user-data/
```



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

Amazon EC2 Purchasing Options

aws training and certification

On-Demand Instances

Pay by the **hour**.

Reserved Instances

Purchase, at a significant **discount**, instances that are **always available.**

1-year to 3-year terms.

Scheduled Instances

Purchase instances that are **always available** on the specified **recurring schedule**, for a one-year term.

Spot Instances

Bid on **unused instances**, which can run as long as they are available and your bid is above the Spot price.

Dedicated Instances

Pay, by the hour, for instances that run on **single-tenant hardware**.

Dedicated Hosts

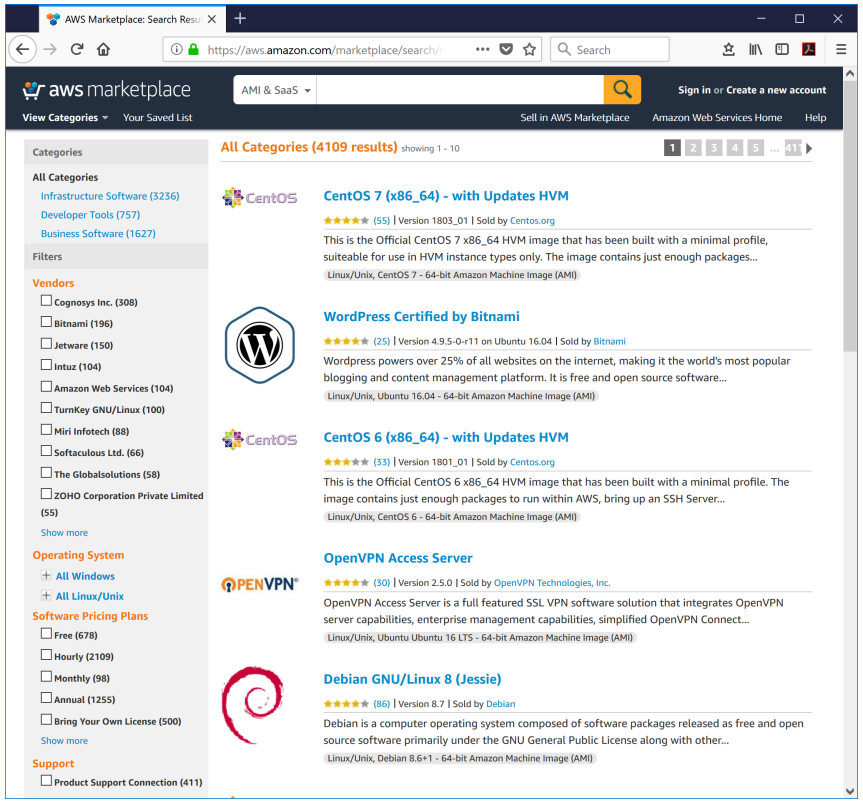
Pay for a physical host that is **fully dedicated** to running your instances.

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

AWS Marketplace: IT Software Optimized for the Cloud

aws training and certification

- Online store to discover, purchase, and deploy IT software on top of the AWS infrastructure.
- Catalog of 4100+ IT software solutions including Paid, BYOL, Open Source, SaaS, and free-to-try options.
- Pre-configured to operate on AWS.
  - Software checked by AWS for security and operability.
  - Deploys to AWS environment in minutes.
  - Flexible, usage-based billing models.
  - Software charges billed to AWS account.
- Includes AWS Test Drive/Quick Starts.
- https://aws.amazon.com/marketplace



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

aws training and certification

Networking: Amazon VPC

Amazon Virtual Private Cloud (VPC)

aws training and certification



Amazon VPC

- Provision **a private, isolated virtual network** on the AWS cloud.
- Have complete control over your virtual networking environment.

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

VPCs and Subnets

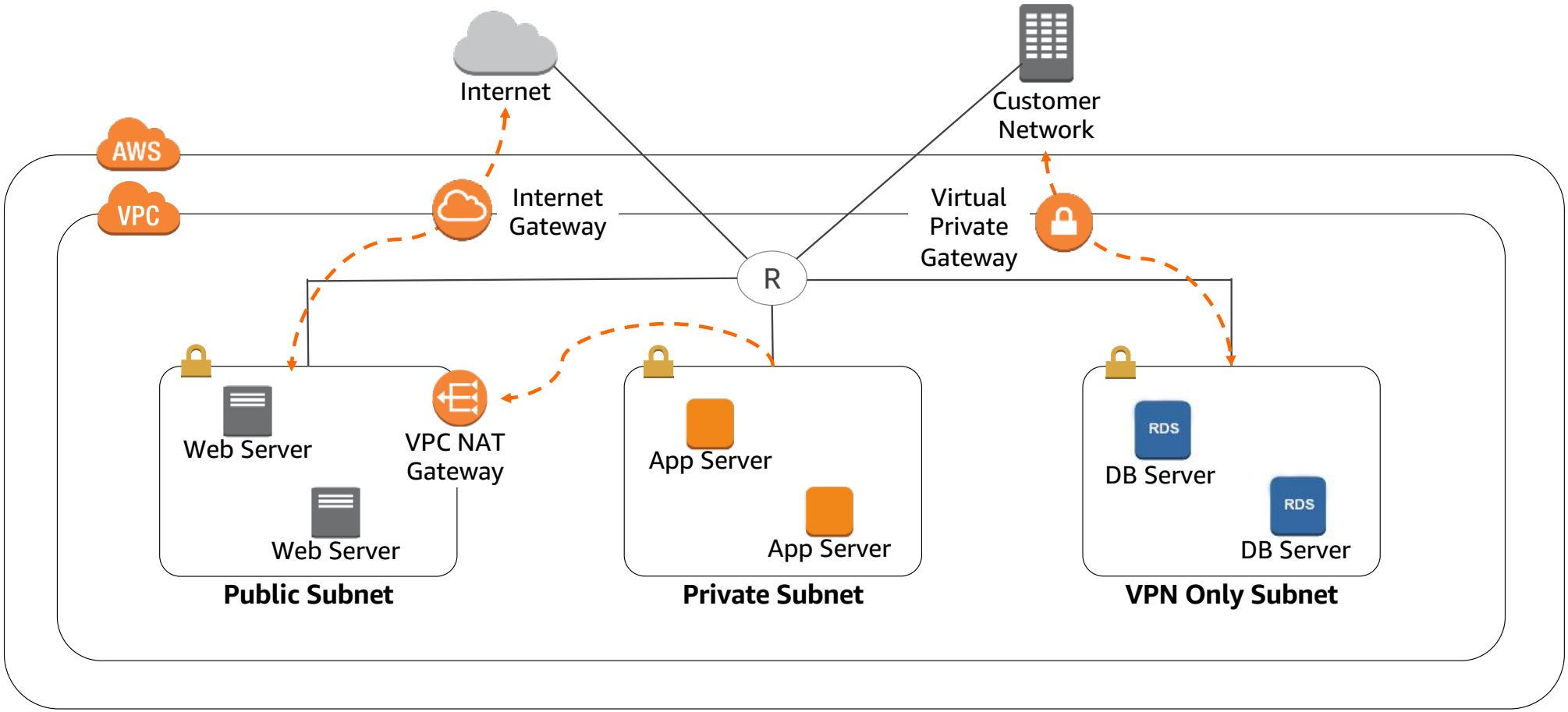
aws training and certification

- A subnet defines a range of IP addresses in your VPC.
- You can launch AWS resources into a subnet that you select.
- A **private subnet** should be used for resources that won't be accessible over the Internet.
- A **public subnet** should be used for resources that will be accessed over the Internet.
- Each subnet must reside entirely within one Availability Zone and cannot span zones.

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

Amazon VPC Example

aws training and certification

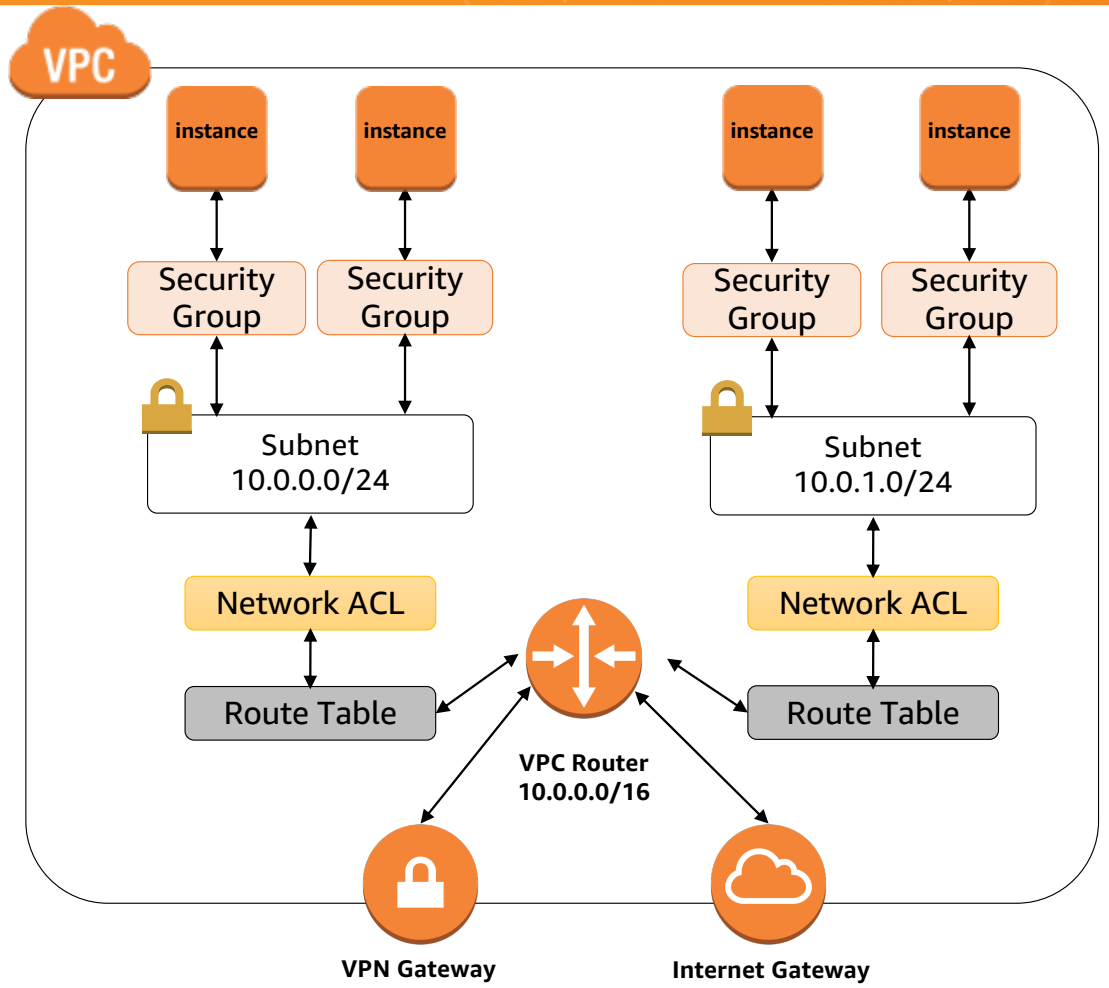


© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Security in Your VPC

aws training and certification

- Security groups
- Network access control lists (ACLs)
- Key Pairs



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

VPN Connections

aws training and certification

VPN Connectivity option	Description
AWS Hardware VPN	You can create an IPsec hardware VPN connection between your VPC and your remote network.
AWS Direct Connect	AWS Direct Connect provides a **dedicated** private connection from a remote network to your VPC.
AWS VPN CloudHub	You can create **multiple** AWS hardware VPN connections via your VPC to enable communications between various remote networks.
Software VPN	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a software **VPN appliance**.

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

aws training and certification

Lab 1: Build your VPC and Launch a Web Server



~ 40 minutes

Lab 1 Overview

aws training and certification

1

- **Create a VPC**
  - Two public subnets
  - Two private subnets
  - Across two Availability Zones

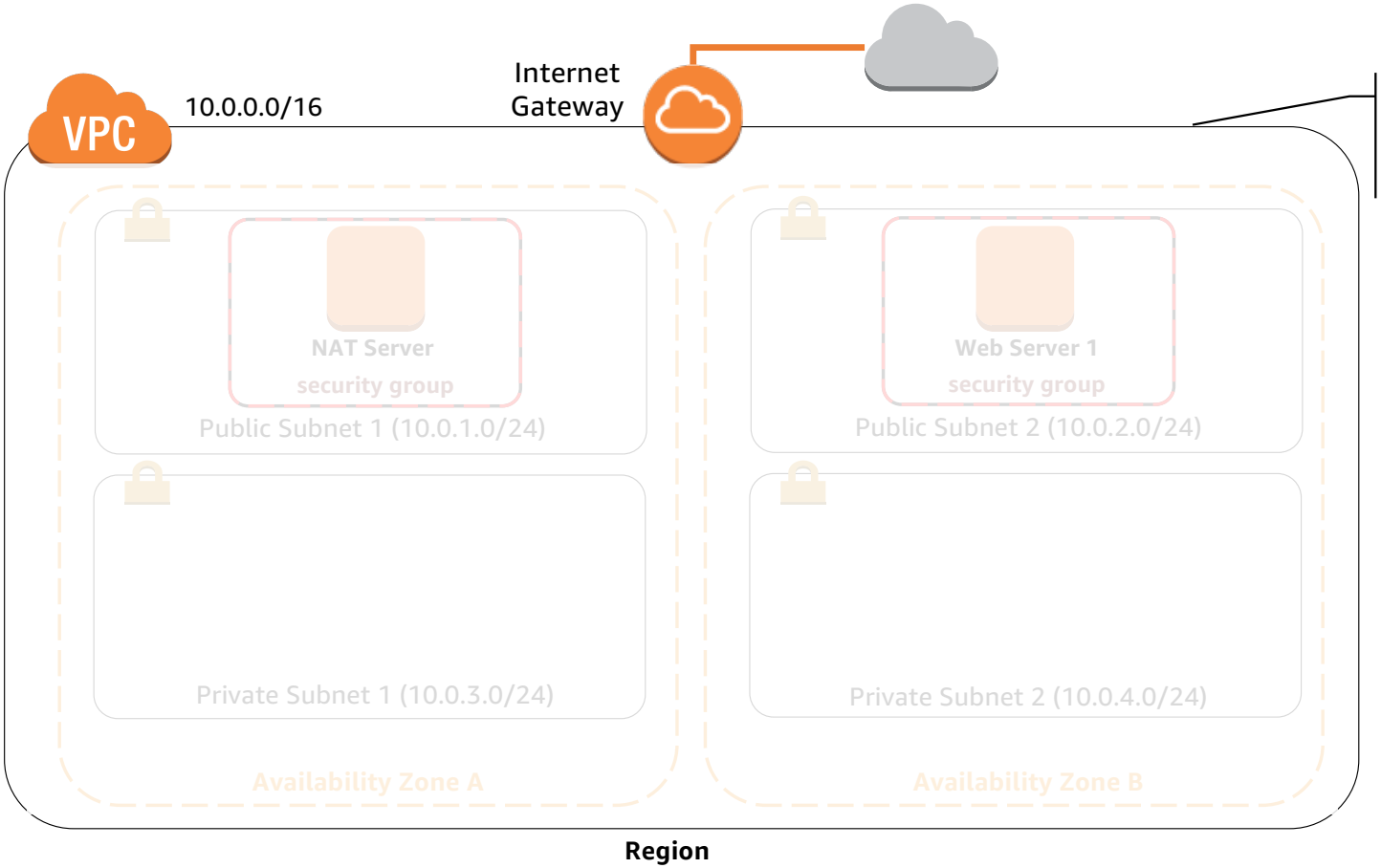
2

- **Create an Application Server**
  - Create a security group for your instance.
  - Launch your instance.

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

Lab 1 – Build your VPC and Launch a Web Server (1 of 8)

aws training and certification

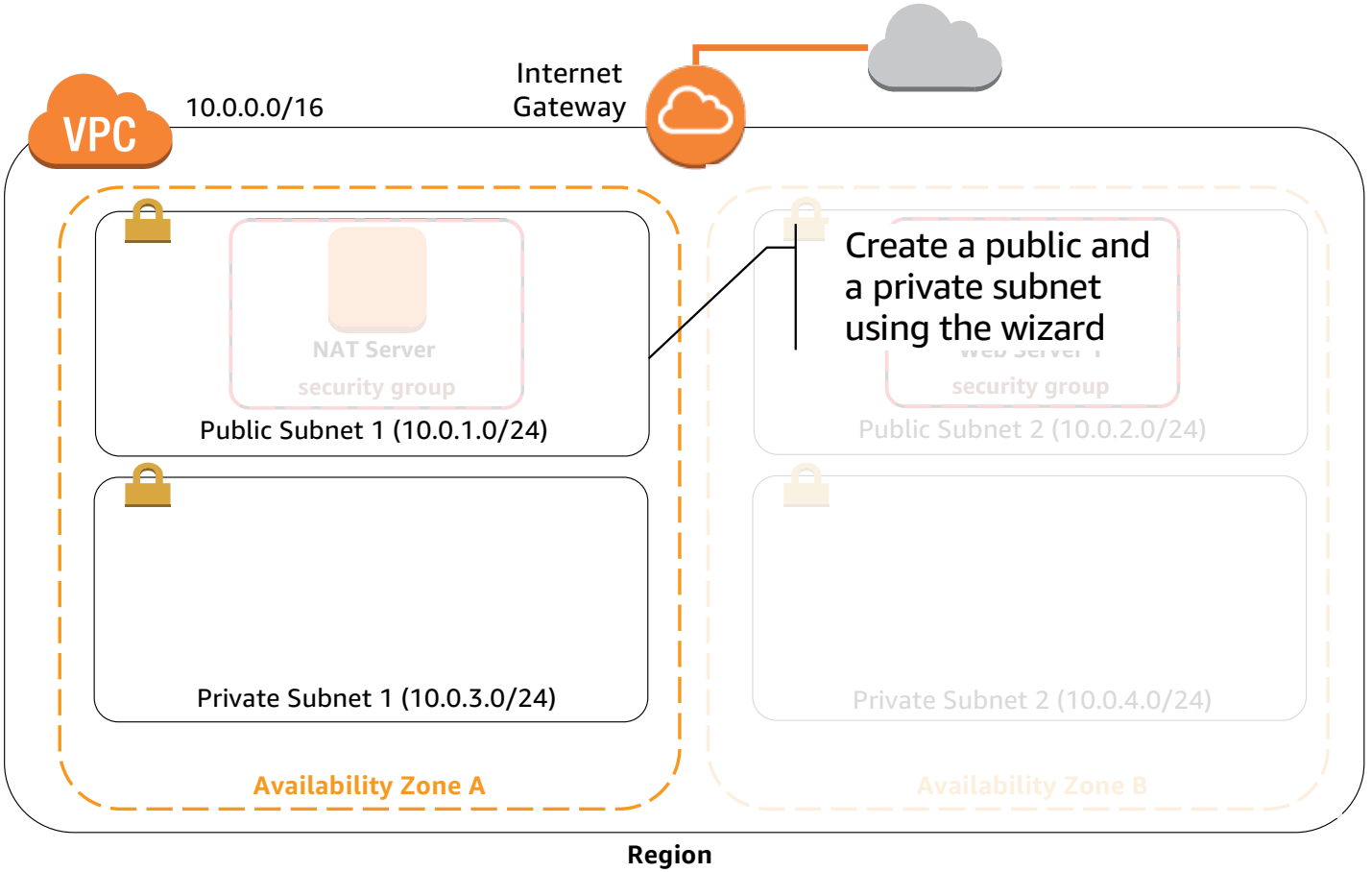


Create a VPC using the VPC Wizard

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

Lab 1 – Build your VPC and Launch a Web Server (2 of 8)

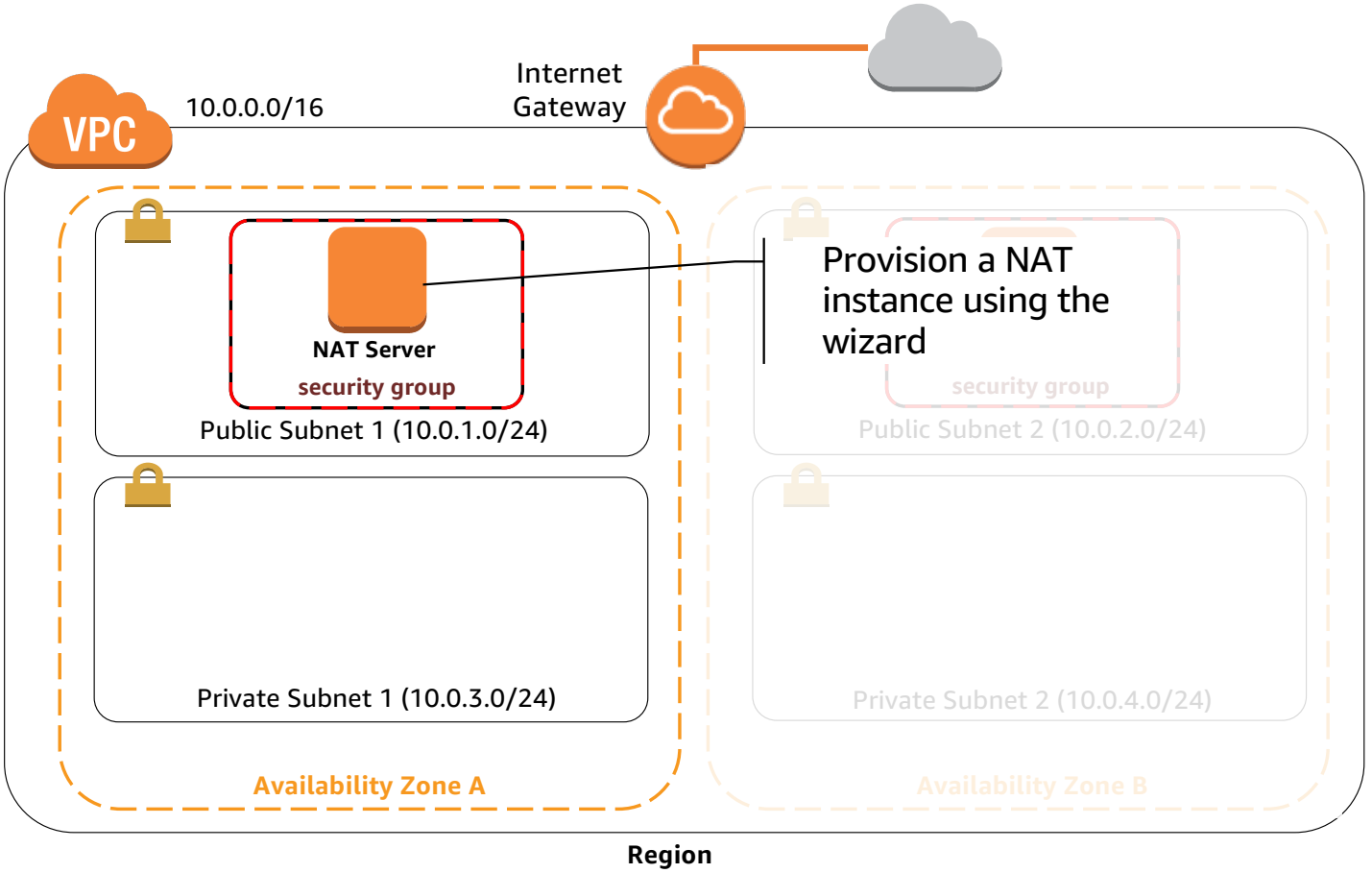
aws training and certification



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

Lab 1 – Build your VPC and Launch a Web Server (3 of 8)

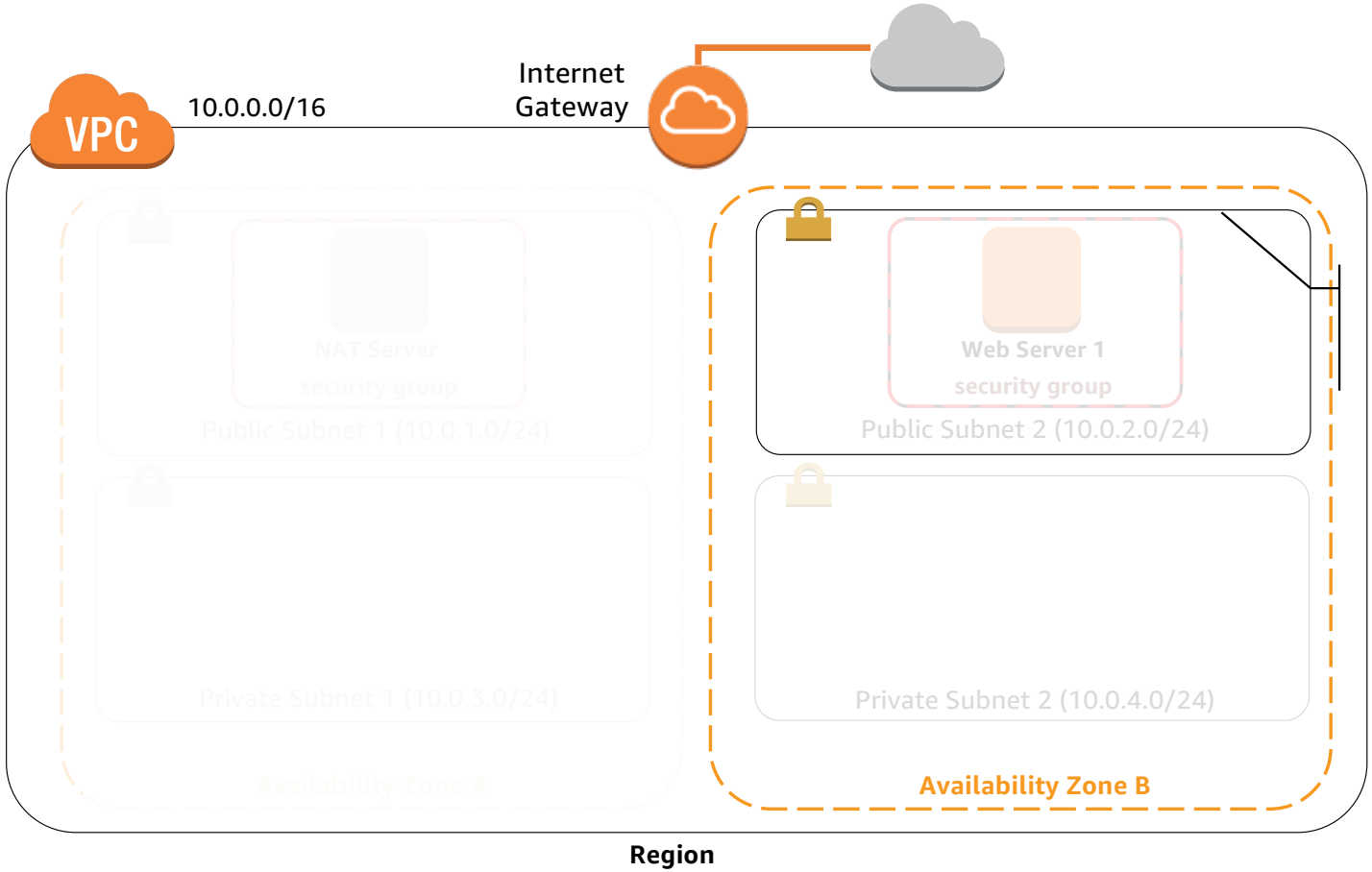
aws training and certification



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

Lab 1 – Build your VPC and Launch a Web Server (4 of 8)

aws training and certification

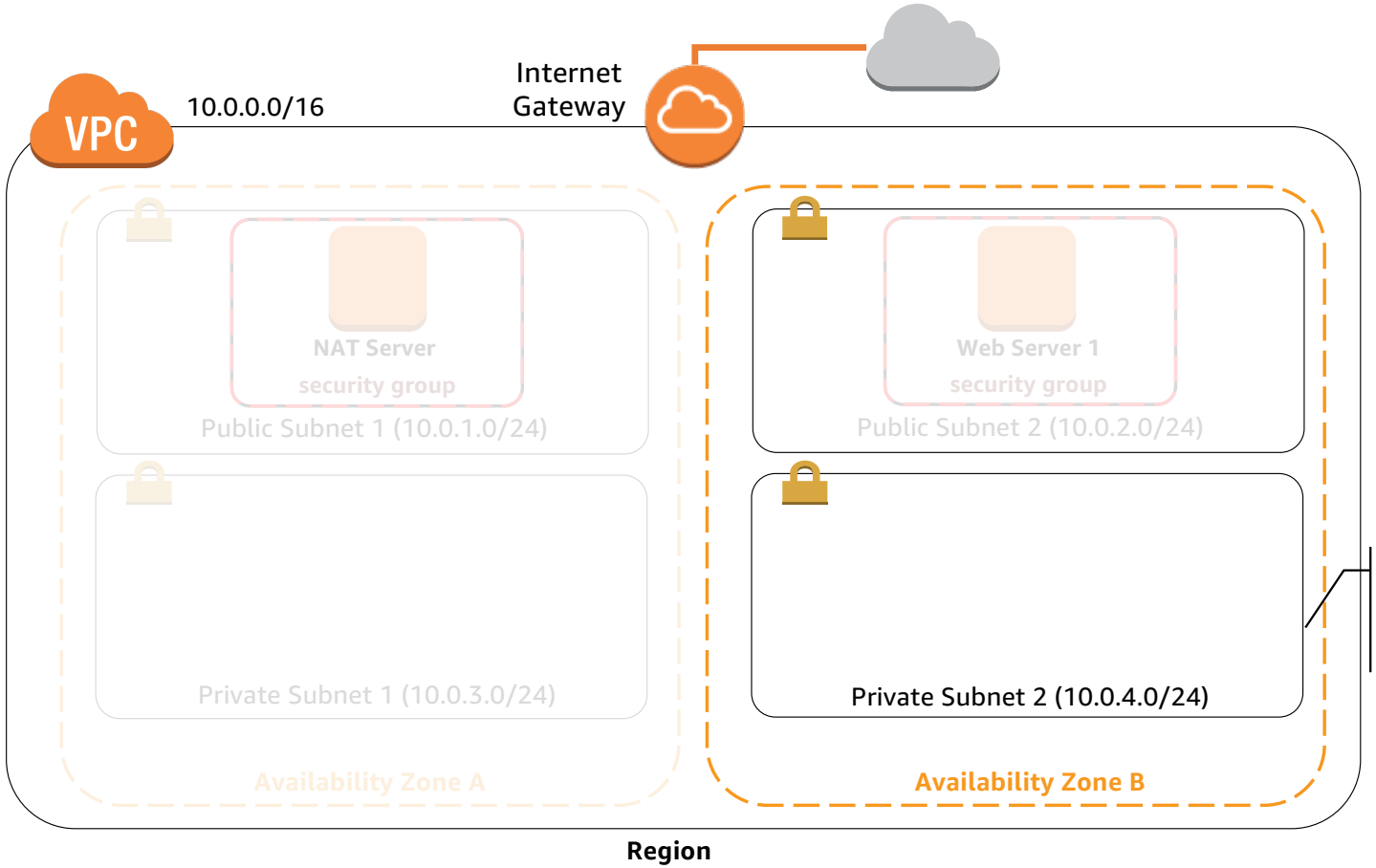


Create a public subnet in the second Availability Zone

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

Lab 1 – Build your VPC and Launch a Web Server (5 of 8)

aws training and certification

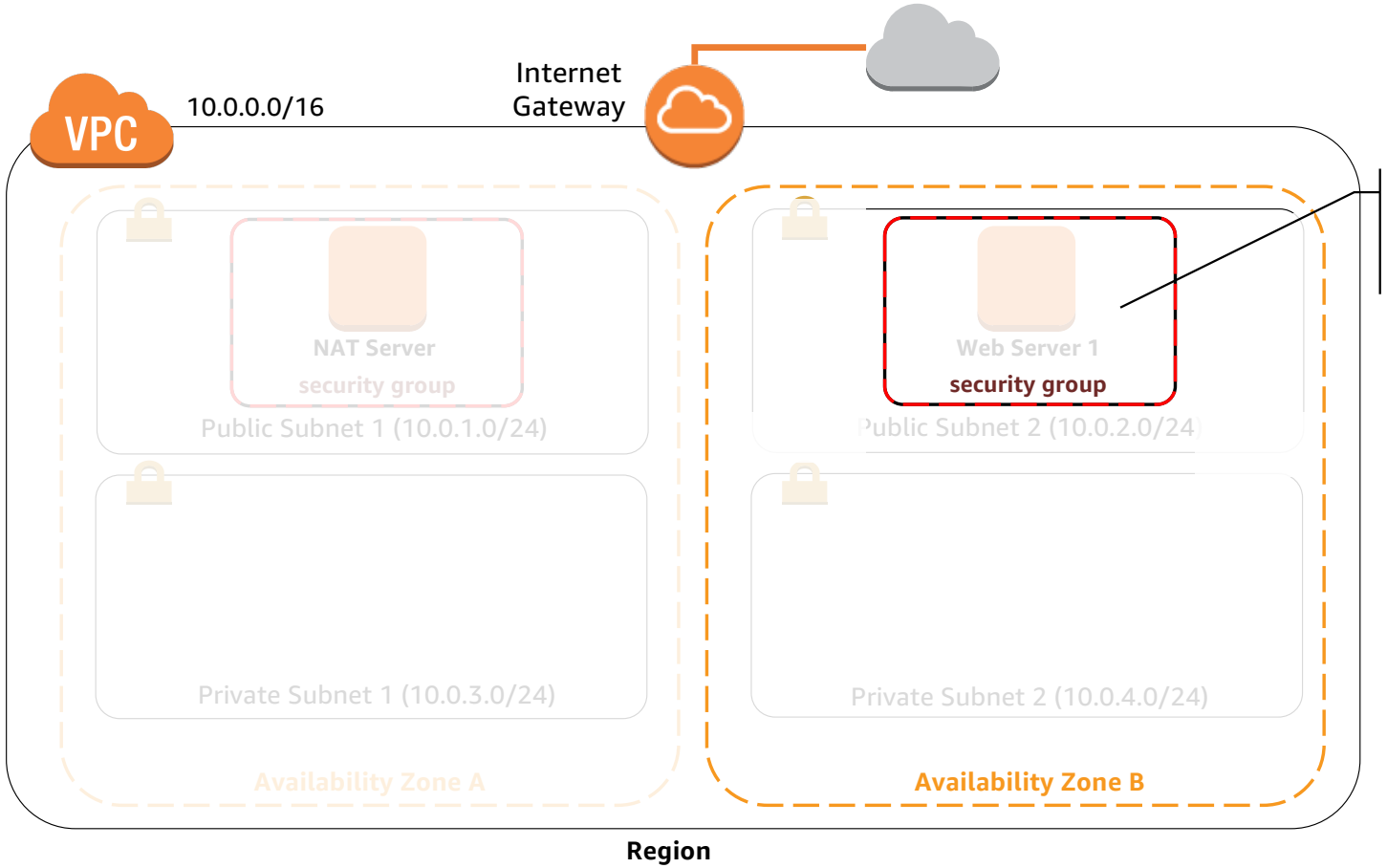


Create a private subnet in the second Availability Zone

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

Lab 1 – Build your VPC and Launch a Web Server (6 of 8)

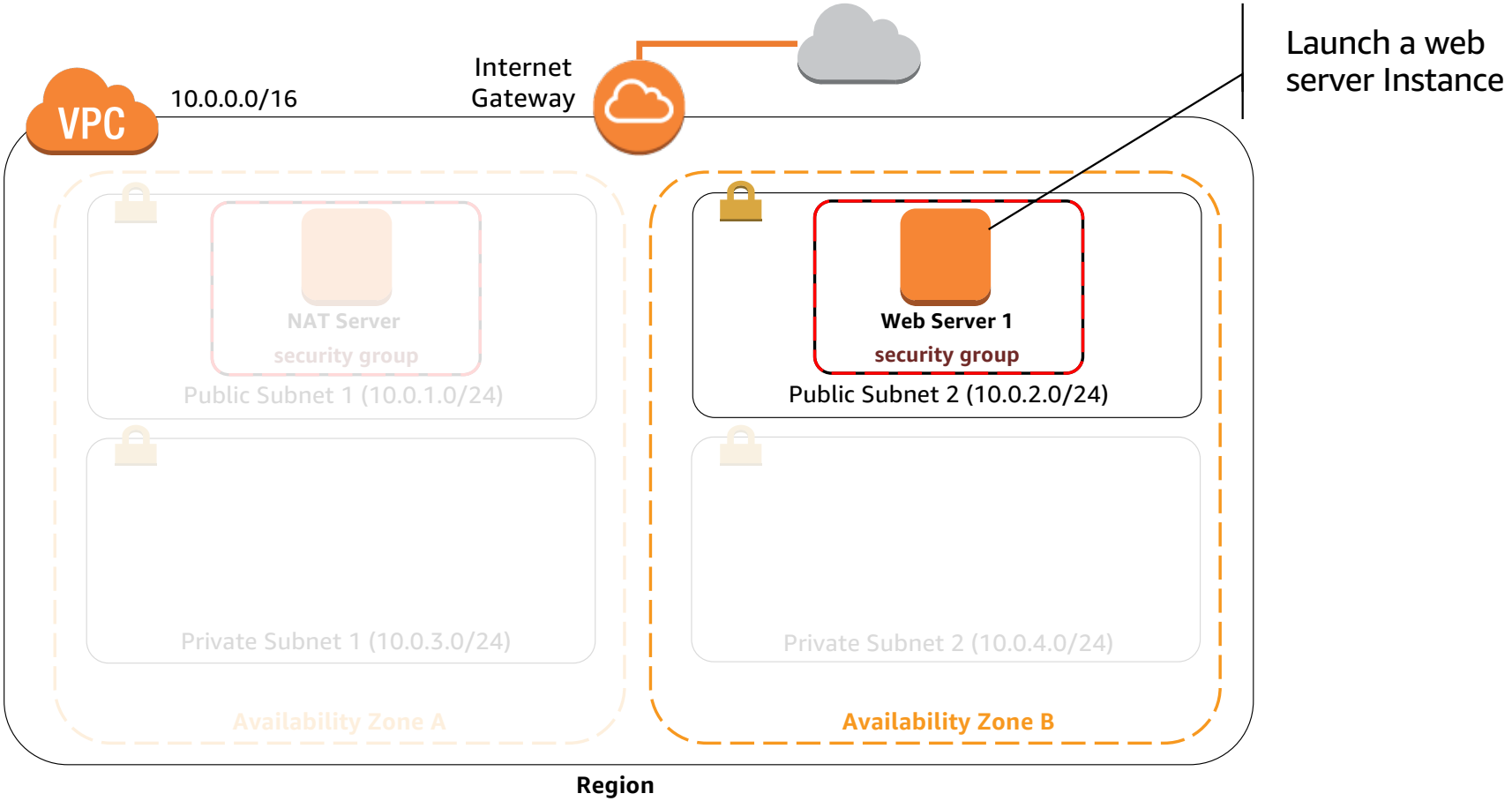
aws training and certification



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

Lab 1 – Build your VPC and Launch a Web Server (7 of 8)

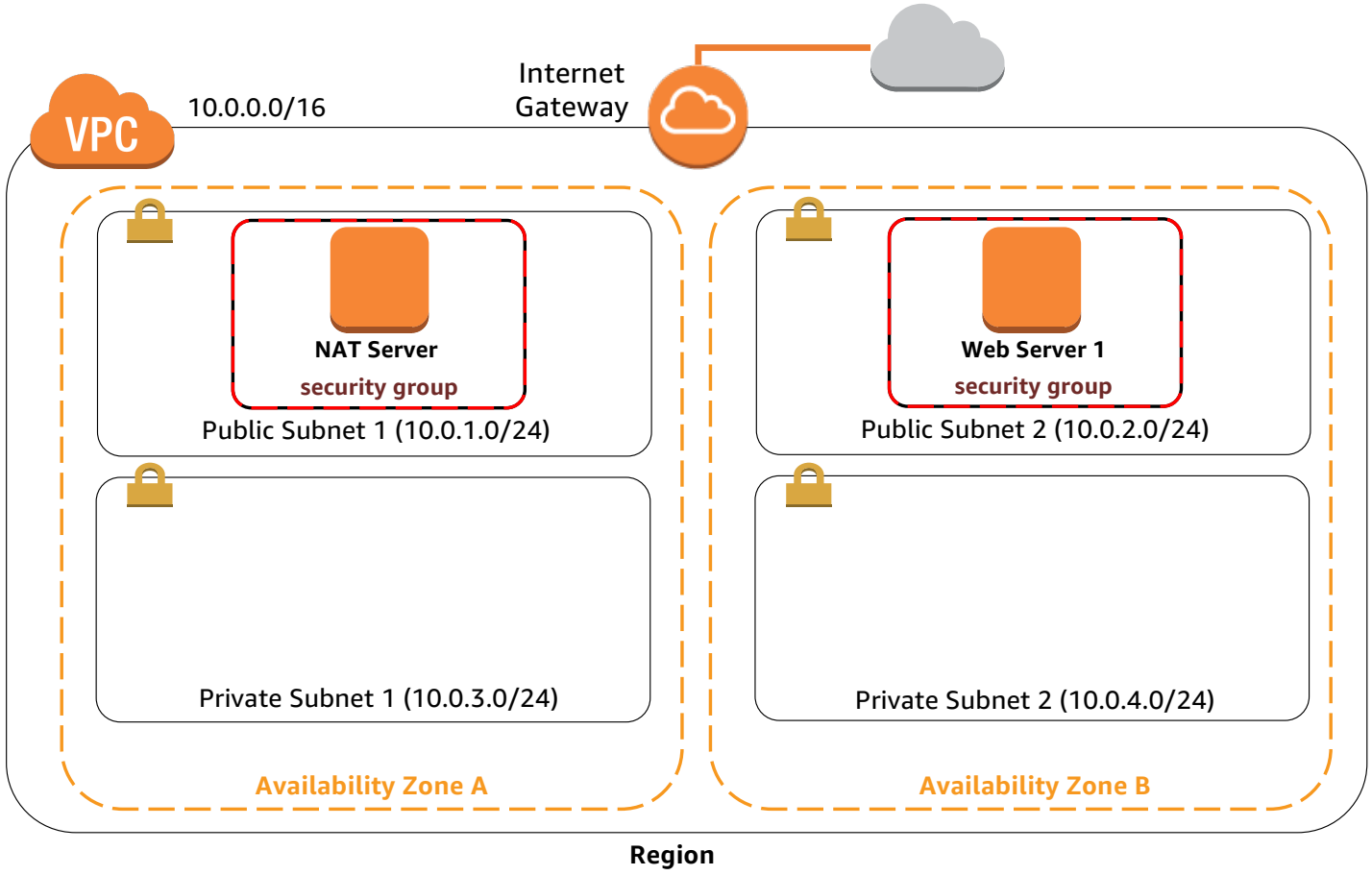
aws training and certification



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

Lab 1 – Build your VPC and Launch a Web Server (8 of 8)

aws training and certification



~ 40 minutes

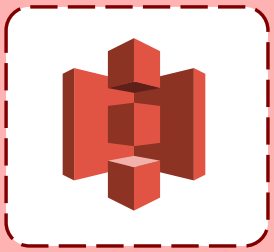
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws training and certification

Storage Services: Amazon S3 and Amazon EBS

Amazon Simple Storage Service (S3)

aws training and certification



Amazon S3

- Storage for the Internet
- Natively online, HTTP access
- Storage that allows you to store and retrieve any amount of data, any time, from anywhere on the web
- Highly scalable, reliable, fast and durable

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

Amazon S3 Facts

aws training and certification

- Can store an **unlimited** number of objects in a bucket
- Objects can be up to **5 TB**; no bucket size limit
- Designed for **99.999999999%** durability and **99.99%** availability of objects over a given year
- Can use **HTTP/S** endpoints to store and retrieve any amount of data, at any time, from anywhere on the web
- Highly scalable, reliable, fast, and inexpensive
- Can use optional server-side **encryption** using AWS or customer-managed provided client-side encryption
- Auditing is provided by access **logs**
- Provides standards-based **REST** and SOAP interfaces

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

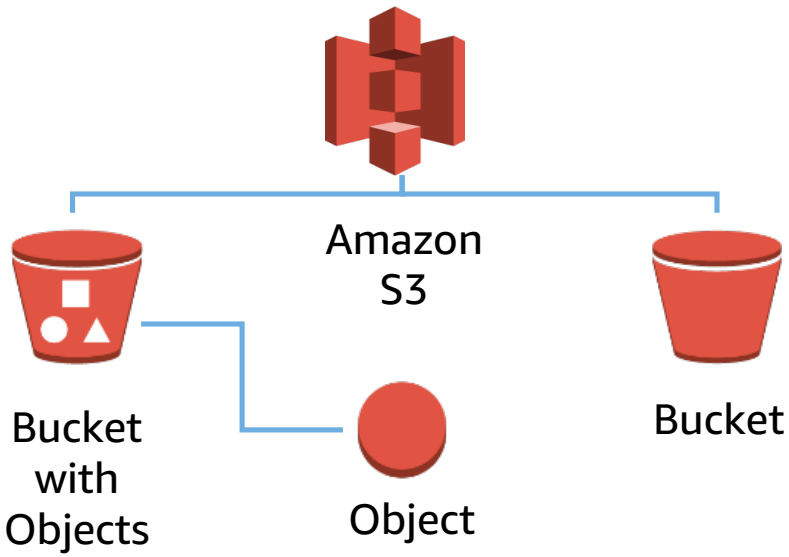
Common Use Scenarios

aws training and certification

- Storage and backup
- Application file hosting
- Media hosting
- Software delivery
- Store AMIs and snapshots

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

Amazon S3 Concepts



- Amazon S3 stores data as objects within buckets.
- An object is composed of a file and optionally any metadata that describes that file.
- You can have up to 100 buckets in each account.
- You can control access to the bucket and its objects.

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

Object Keys

aws training and certification

An object key is the unique identifier for an object in a bucket.

http://doc.s3.amazonaws.com/2006-03-01/AmazonS3.html



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

Amazon S3 Security

aws training and certification

- You can **control access** to buckets and objects with:
  - Access Control Lists (ACLs)
  - Bucket policies
  - Identity and Access Management (IAM) policies
- You can upload or download data to Amazon S3 via SSL **encrypted** endpoints.
- You can encrypt data using AWS SDKs.

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

Amazon S3 Versioning

aws training and certification

- Protects from accidental overwrites and deletes with no performance penalty.
- Generates a new version with every upload.
- Allows easily retrieval of deleted objects or roll back to previous versions.
- Three states of an Amazon S3 bucket
  - Un-versioned (default)
  - Versioning-enabled
  - Versioning-suspended



Versioning Enabled

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

Amazon S3 Object Lifecycle

aws training and certification

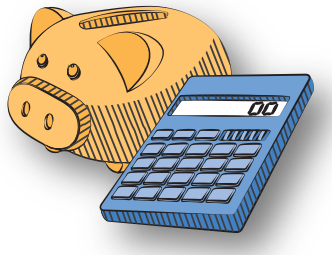
- Lifecycle management defines how Amazon S3 manages objects during their lifetime.
- Some objects that you store in an Amazon S3 bucket might have a well-defined lifecycle:
  - Log files
  - Archive documents
  - Digital media archives
  - Financial and healthcare records
  - Raw genomics sequence data
  - Long-term database backups
  - Data that must be retained for regulatory compliance

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

Amazon S3 Pricing

aws training and certification

- Pay only for what you use
- No minimum fee
- Prices based on location of your Amazon S3 bucket
- Estimate monthly bill using the **AWS Simple Monthly Calculator**
- Pricing is available as:
  - Storage Pricing
  - Request Pricing
  - Data Transfer Pricing: data transferred out of Amazon S3



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

Amazon Glacier

aws training and certification

- Long term low-cost **archiving** service
- Optimal for **infrequently accessed** data
- Designed for 99.999999999% durability
- Three to five hours' standard retrieval time
- Less than $0.01 per GB/month (depending on region)

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

Amazon S3 Storage Classes

aws training and certification

Storage Class	Durability	Availability	Other Considerations
Amazon S3 Standard	99.999999999 %	99.99%	
Amazon S3 Standard - Infrequent Access (IA)	99.999999999 %	99.9%	• Retrieval fee associated with objects • Most suitable for infrequently accessed data
Glacier	99.999999999 %	99.99% (once restored)	• Not available for real-time access • Must restore objects before you can access them • Restoring objects can take 1 minute - 12 hours

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

aws training and certification

Demo: Amazon S3

Amazon Elastic Block Store (EBS)



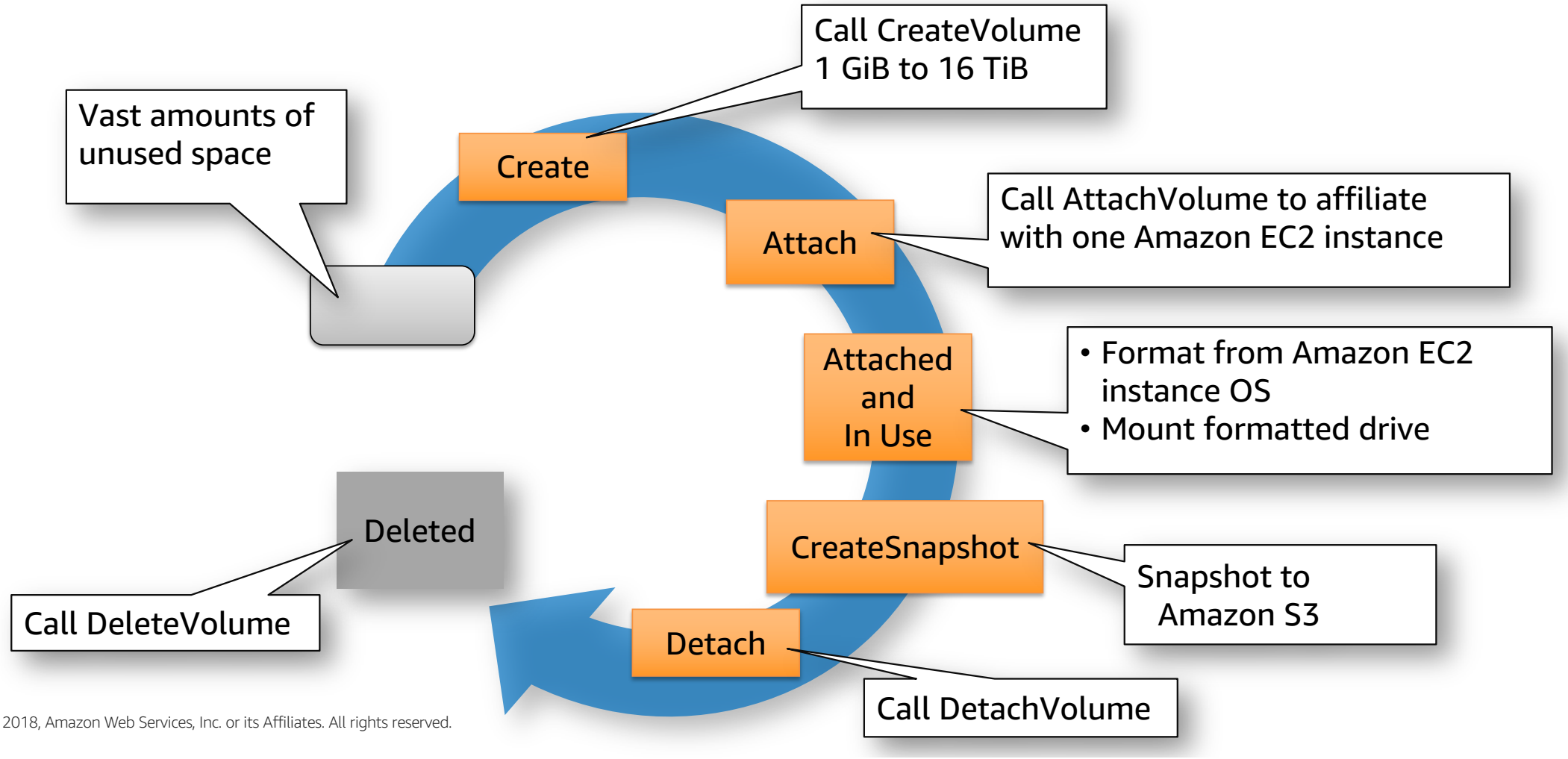
Amazon EBS

- Persistent block level storage volumes offer consistent and low-latency performance.
- Stored data is automatically replicated within its Availability Zone.
- Snapshots are stored durably in Amazon S3.

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

Amazon EBS Lifecycle

aws training and certification



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

Amazon EBS Volume Types

aws training and certification

- **SSD-backed** volumes are:
  - Optimized for transactional workloads that involve frequent read/write operations with small I/O size.
  - Dominant in IOPS performance.
- **HDD-backed** volumes are
  - Optimized for large streaming workloads.
  - Dominant in throughput (measured in MiB/s).

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

Amazon EBS Volume Types

aws training and certification

	SSD		HDD	
Volume Type	**General Purpose SSD (gp2)**	**Provisioned IOPS SSD (io1)**	**Throughput Optimized HDD (st1)**	**Cold HDD (sc1)**
Description	Balances price and performance for a wide variety of transactional loads.	Highest-performance SSD volume designed for mission-critical applications.	Low-cost HDD designed for frequently accessed, throughput-intensive workloads.	Lowest cost HDD designed for less frequently accessed workloads.
Volume Sizes	1 GiB – 16 TiB	4 GiB – 16 TiB	500 GiB – 16 TiB	500 GiB – 16 TiB
Dominant Performance Attribute	IOPS	IOPS	MiB/s	MiB/s

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

Amazon EBS Facts

aws training and certification

- EBS is recommended when data must be quickly accessible and requires long-term **persistence**.
- You can launch your EBS volumes as **encrypted** volumes. Data stored at rest on the volume, disk I/O, and snapshots created from the volume are all encrypted.
- You can create point-in-time **snapshots** of EBS volumes, which are persisted to Amazon S3.

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

Amazon EBS Use Cases

aws training and certification

- **OS**: Use for boot/root volume, secondary volumes
- **Databases**: Scales with your performance needs
- **Enterprise applications**: Provides reliable block storage to run mission-critical applications
- **Business continuity**: Minimize data loss and recovery time by regularly backing up using EBS Snapshots
- **Applications**: Install and persist any application

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

Amazon EBS Pricing

aws training and certification

Pay for what you provision:

- Pricing based on region
- Review Pricing Calculator online
- Pricing is available as:
  - Storage
  - IOPS

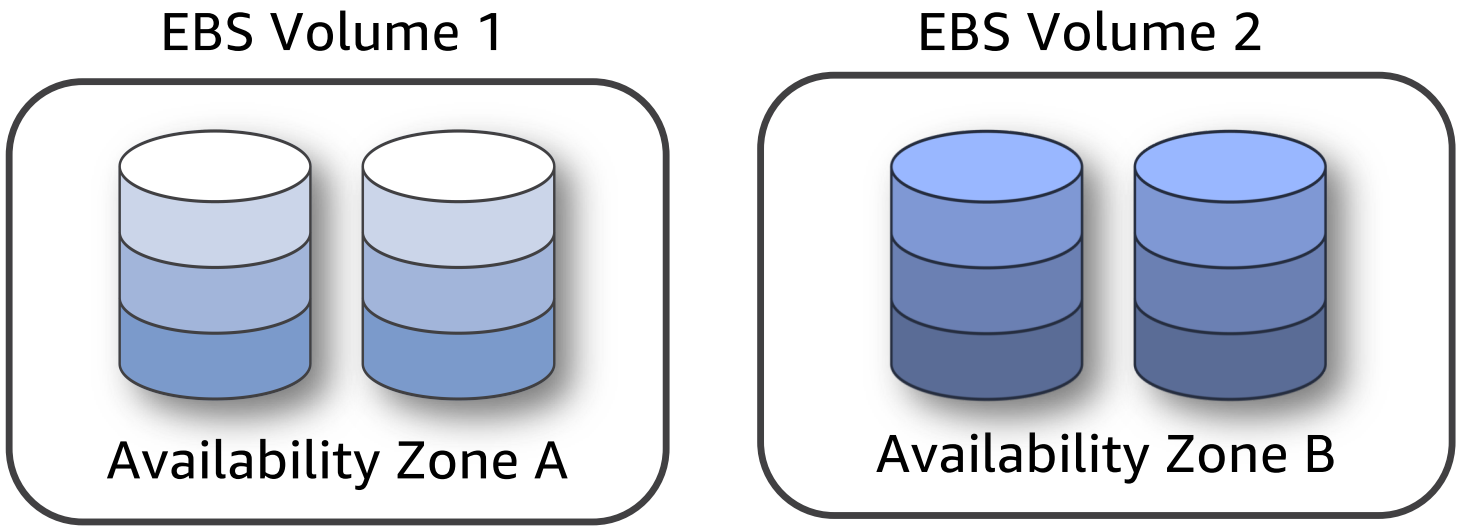
** Check Amazon EBS Pricing page for current pricing for all regions.*

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

Amazon EBS Scope

aws training and certification

Amazon EBS volumes are in a single Availability Zone



Volume data is replicated across multiple servers in an Availability Zone.

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

Amazon EBS and Amazon S3

aws training and certification

	Amazon EBS 	Amazon S3 
Paradigm	Block storage with file system	Object store
Performance	Very fast	Fast
Redundancy	Across multiple servers in an Availability Zone	Across multiple facilities in a Region
Security	EBS Encryption – Data volumes and Snapshots	Encryption
Access from the Internet?	No (1)	Yes (2)
Typical use case	It is a disk drive	Online storage

(1) Accessible from the Internet if mounted to server and set up as FTP, etc.
(2) Only with proper credentials, unless ACLs are world-readable

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

Amazon EC2 Instance Storage

aws training and certification

- Is local, complimentary direct attached block storage.
- Includes availability, number of disks, and size based on EC2 instance type.
- Is optimized for up to 365,000 Read IOPS and 315,000 First Write IOPS.
- Is SSD or magnetic.
- Has no persistence.
- Automatically deletes data when an EC2 instance stops, fails or is terminated.

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

Amazon EBS vs. Amazon EC2 Instance Store

aws training and certification

- Amazon EBS
  - Data stored on an Amazon EBS volume can persist independently of the life of the instance.
  - Storage is **persistent**.
- Amazon EC2 Instance Store
  - Data stored on a local instance store persists only as long as the instance is alive.
  - Storage is **ephemeral**.

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

Reboot vs. Stop vs. Terminate

aws training and certification

Characteristic	Reboot	Stop/Start (EBS-backed instances only)	Terminate
Host computer	The instance stays on the same host computer.	The instance runs on a new host computer.	
Public IP address	No change	New address assigned	
Elastic IP addresses (EIP)	EIP remains associated with the instance.	EIP remains associated with the instance.	EIP is disassociated from the instance.
Instance store volumes	Preserved	Erased	Erased
EBS volume	Preserved	Preserved	Boot volume is deleted by default.
Billing	Instance billing hour doesn't change.	You stop incurring charges as soon as state is changed to stopping.	You stop incurring charges as soon as state is changed to shutting-down.

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

Knowledge Check

aws training and certification

- Q: What AWS service would help support your web application by hosting static assets and storing user uploaded images and video off-instance?

  Amazon S3

- Q: How would an Amazon EC2 instance find its private and public IP addresses?

  Retrieve the instance metadata: http://169.254.169.254/latest/meta-data/

- Q: What acts as an additional layer of security at the subnet level in a VPC?

  Network ACLs

- True or False: Amazon S3 limits the total amount you can store.

  False (There is a 5TB limit per object)

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



Thanks for participating!

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: aws-course-feedback@amazon.com. For all other questions, contact us at: https://aws.amazon.com/contact-us/aws-training/. All trademarks are the property of their owners.

aws training and certification