AMAZON EBS - QUIZ

Attempt	1	**Completed on**	Saturday , 12 January 2019 , 08:37 PM
Marks Obtained	4 / 10	**Time Taken**	00 H 11 M 35 S
Your score is	40%	**Result**	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	10	4	6	0

10 Questions	4 Correct	6 Incorrect	0 Unattempted

Show Answers: All

QUESTION 1 CORRECT

Which of the following statements are correct with respect to instance store and EBS volume? Please select 2 correct options.

- [ ] **A.** Instance store backed EC2 instances will persist storage across instance stop, terminate and failures.
- [x] **B.** EBS backed EC2 instances will persist storage across instance stop, terminate and failures. ✔
- [ ] **C.** Instance store backed EC2 instance will persist storage only during instance stop and start.
- [x] **D.** You cannot add instance store volumes once EC2 instance is launched. ✔
- [ ] **E.** All available EC2 instance types support instance store and EBS volumes.

Explanation :

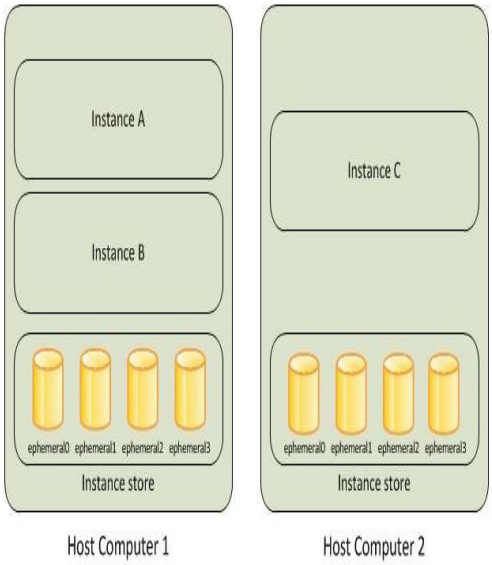
Answer: B, D

Amazon EC2 Instance Store

An *instance store* provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.

An instance store consists of one or more instance store volumes exposed as block devices. The size of an instance store as well as the number of devices available varies by instance type. While an instance store is dedicated to a particular instance, the disk subsystem is shared among instances on a host computer.

The virtual devices for instance store volumes are `ephemeral[0-23]`. Instance types that support one instance store volume have `ephemeral0`. Instance types that support two instance store volumes have `ephemeral0` and `ephemeral1`, and so on.



- https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/InstanceStorage.html (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/InstanceStorage.html)

Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. EBS volumes that are attached to an EC2 instance are exposed as storage volumes that persist independently from the life of the instance.

- https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEBS.html (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEBS.html)

- Option A is not correct.

Instance Store Lifetime

You can specify instance store volumes for an instance only when you launch it. You can't detach an instance store volume from one instance and attach it to a different instance.

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data in the instance store is lost under any of the following circumstances:

- The underlying disk drive fails
- The instance stops
- The instance terminates

- Option B is correct.

- **Data persistence**

  An EBS volume is off-instance storage that can persist independently from the life of an instance. You continue to pay for the volume usage as long as the data persists.

  By default, EBS volumes that are attached to a running instance automatically detach from the instance with their data intact when that instance is terminated. The volume can then be reattached to a new instance, enabling quick recovery. If you are using an EBS-backed instance, you can stop and restart that instance without affecting the data stored in the attached volume. The volume remains attached throughout the stop-start cycle. This enables you to process and store the data on your volume indefinitely, only using the processing and storage resources when required. The data persists on the volume until the volume is deleted explicitly. The physical block storage used by deleted EBS volumes is overwritten with zeroes before it is allocated to another account. If you are dealing with sensitive data, you should consider encrypting your data manually or storing the data on a volume protected by Amazon EBS encryption. For more information, see Amazon EBS Encryption.

  By default, EBS volumes that are created and attached to an instance at launch are deleted when that instance is terminated. You can modify this behavior by changing the value of the flag `DeleteOnTermination` to `false` when you launch the instance. This modified value causes the volume to persist even after the instance is terminated, and enables you to attach the volume to another instance.

- Option C is not correct.

Instance store persists during reboots, not during stop and start of the instance.

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data in the instance store is lost under any of the following circumstances:

- The underlying disk drive fails
- The instance stops
- The instance terminates

- Option D is correct.

You can specify the instance store volumes for your instance only when you launch an instance. You can't attach instance store volumes to an instance after you've launched it.

- https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/add-instance-store-volumes.html (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/add-instance-store-%20volumes.html)

- Option E is not correct.

The number and size of available instance store volumes for your instance varies by instance type. Some instance types do not support instance store volumes. For more information about the instance store volumes support by each instance type, see Instance Store Volumes. If the instance type you choose for your instance supports instance store volumes, you must add them to the block device mapping for the instance when you launch it. After you launch the instance, you must ensure that the instance store volumes for your instance are formatted and mounted before you can use them. The root volume of an instance store-backed instance is mounted automatically.

- https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/InstanceStorage.html#instance-store-volumes (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/InstanceStorage.html#instance-%20store-volumes)

Ask our Experts

QUESTION 2 CORRECT

Your organization is planning to build a BigData project on AWS. They need high data transfer rates for huge workloads to stream through with better performance. They are also looking for a solution which is cost effective. Which EBS storage type would you choose in this scenario?

- A. General Purpose SSD
- B. Provisioned IOPS SSD
- C. Throughput Optimized HDD ✔
- D. Cold HDD

Explanation :

Answer: C
Amazon EBS provides the following volume types, which differ in performance characteristics and price, so that you can tailor your storage performance and cost to the needs of your applications. The volumes types fall into two categories:

- SSD-backed volumes optimized for transactional workloads involving frequent read/write operations with small I/O size, where the dominant performance attribute is IOPS
- HDD-backed volumes optimized for large streaming workloads where throughput (measured in MiB/s) is a better performance measure than IOPS

	Solid-State Drives (SSD)		Hard disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	• Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments	• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume • Large database workloads, such as: o MongoDB o Cassandra o Microsoft SQL Server o MySQL o PostgreSQL o Oracle	• Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume
API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS/Volume**	10,000	32,000***	500	250
Max. Throughput/Volume	160 MiB/s****	500 MiB/s†	500 MiB/s	250 MiB/s
Max. IOPS/Instance	80,000	80,000	80,000	80,000
Max. Throughput/Instance††	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s
Dominant Performance Attribute	IOPS	IOPS	MiB/s	MiB/s

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/EBSVolumeTypes.html (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/EBSVolumeTypes.html)

Ask our Experts

QUESTION 3 INCORRECT

You are working for a data management company which uses AWS platform to manage the data for various customers. They are using AWS EBS backed EC2 instance with “Delete EBS volume on termination” checked. EC2 instances are used

to run data streaming application which generates logs and are stored on EBS volumes. The log files are critical for auditing purposes. How would you protect the data stored on EBS volumes from accidental terminations of EC2 instances?

- A. Every EBS volume will have a daily EBS snapshot created automatically by AWS.
- B. Setup a Data LifeCycle Manager policy scheduler to create EBS snapshots for your EBS volumes. ✔
- C. When EC2 instance is terminated, it automatically creates a snapshot of EBS volume and then deletes the EBS volume.
- D. Write a custom script on your EC2 instance and schedule it to back up the data onto AWS S3. ✖

Explanation :

Answer: B

Deleting an Amazon EBS Volume

After you no longer need an Amazon EBS volume, you can delete it. After deletion, its data is gone and the volume can't be attached to any instance. However, before deletion, you can store a snapshot of the volume, which you can use to re-create the volume later.

To delete a volume, it must be in the `available` state (not attached to an instance). For more information, see Detaching an Amazon EBS Volume from an Instance.

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved

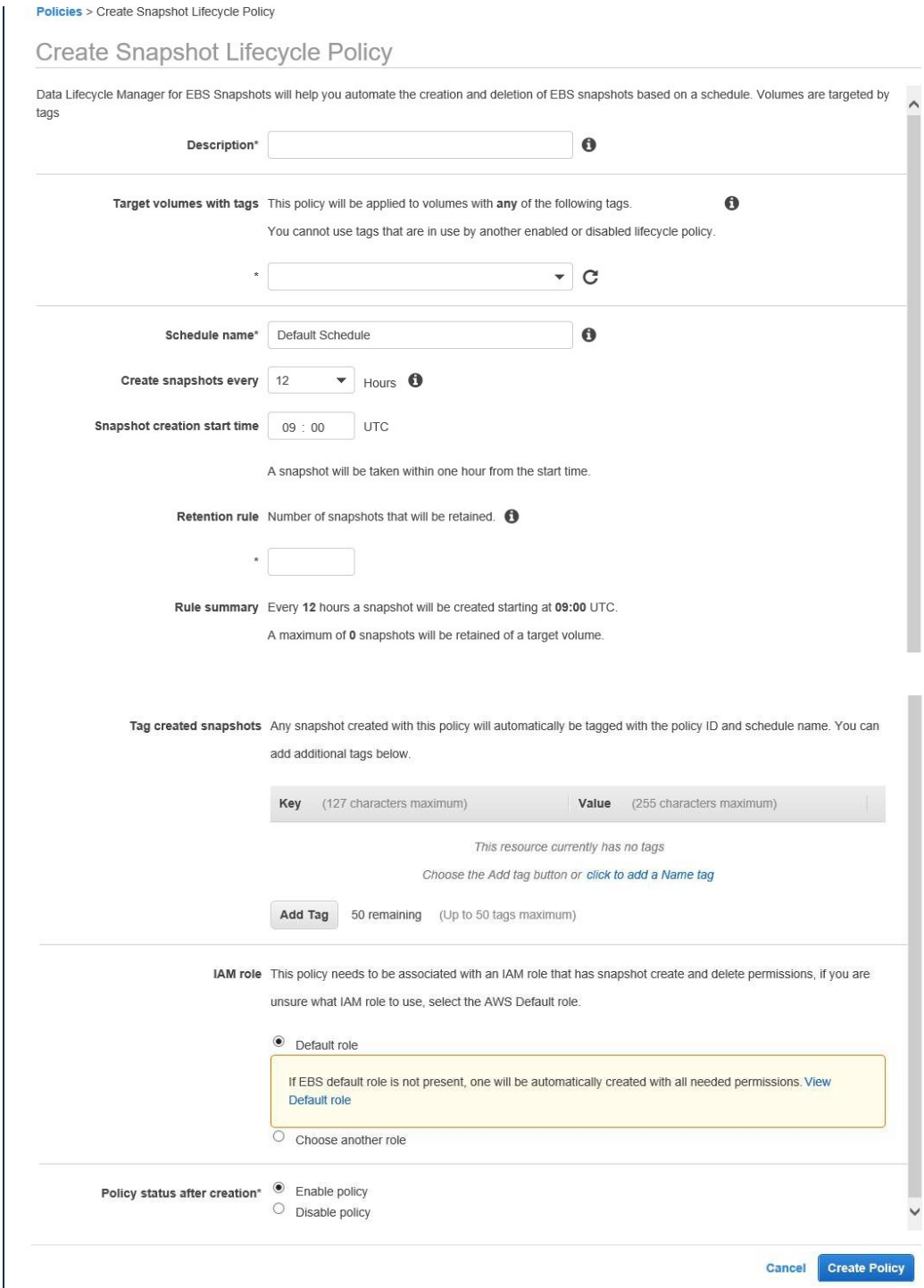
Automating the Amazon EBS Snapshot Lifecycle

You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes. Automating snapshot management helps you to:

- Protect valuable data by enforcing a regular backup schedule.
- Retain backups as required by auditors or internal compliance.
- Reduce storage costs by deleting outdated backups.

Combined with the monitoring features of Amazon CloudWatch Events and AWS CloudTrail, Amazon DLM provides a complete backup solution for EBS volumes at no additional cost.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html)



Ask our Experts

QUESTION 4 INCORRECT

Which of the following is an action you cannot perform on an EBS snapshot?

- A. Create Image from snapshot. ✖
- B. Create EBS volume from snapshot.
- C. Share a snapshot with another AWS account.
- D. Make unencrypted copy of an encrypted snapshot. ✔

Explanation :

Answer: D

Option A is a snapshot action.

To create an AMI from your root volume using the console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Elastic Block Store**, **Snapshots**.
3. Choose **Create Snapshot**.
4. For **Volumes**, start typing the name or ID of the root volume, and then select it from the list of options.
5. Choose the snapshot that you just created, and then choose **Actions**, **Create Image**.
6. In the **Create Image from EBS Snapshot** dialog box, provide the following information and then choose **Create**. If you're re-creating a parent instance, then choose the same options as the parent instance.
   - **Architecture**: Choose **i386** for 32-bit or **x86_64** for 64-bit.
   - **Root device name**: Enter the appropriate name for the root volume. For more information, see Device Naming on Linux Instances.
   - **Virtualization type**: Choose whether instances launched from this AMI use paravirtual (PV) or hardware virtual machine (HVM) virtualization. For more information, see Linux AMI Virtualization Types.
   - (PV virtualization type only) **Kernel ID** and **RAM disk ID**: Choose the AKI and ARI from the lists. If you choose the default AKI or don't choose an AKI, you are required to specify an AKI every time you launch an instance using this AMI. In addition, your instance may fail the health checks if the default AKI is incompatible with the instance.
   - (Optional) **Block Device Mappings**: Add volumes or expand the default size of the root volume for the AMI. For more information about resizing the file system on your instance for a larger volume, see Extending a Linux File System after Resizing the Volume.

Option B is a snapshot action.

To restore an EBS volume from a snapshot using the console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the navigation bar, select the region that your snapshot is located in.

   To restore the snapshot to a volume in a different region, you can copy your snapshot to the new region and then restore it to a volume in that region. For more information, see Copying an Amazon EBS Snapshot.
3. In the navigation pane, choose **ELASTIC BLOCK STORE**, **Volumes**.
4. Choose **Create Volume**.
5. For **Volume Type**, choose a volume type. For more information, see Amazon EBS Volume Types.

   Note

   Some AWS accounts created before 2012 might have access to Availability Zones in us-west-1 or ap-northeast-1 that do not support Provisioned IOPS SSD (`io1`) volumes. If you are unable to create an `io1` volume (or launch an instance with an `io1` volume in its block device mapping) in one of these regions, try a different Availability Zone in the region. You can verify that an Availability Zone supports `io1` volumes by creating a 4 GiB `io1` volume in that zone.
6. For **Snapshot**, start typing the ID or description of the snapshot from which you are restoring the volume, and choose it from the list of suggested options.

   Volumes that are restored from encrypted snapshots can only be attached to instances that support Amazon EBS encryption. For more information, see Supported Instance Types.
7. For **Size (GiB)**, type the size of the volume, or verify that the default size of the snapshot is adequate.

   Note

   If you specify both a volume size and a snapshot, the size must be equal to or greater than the snapshot size. When you select a volume type and a snapshot, the minimum and maximum sizes for the volume are shown next to **Size**. Any AWS Marketplace product codes from the snapshot are propagated to the volume.
8. With a Provisioned IOPS SSD volume, for **IOPS**, type the maximum number of input/output operations per second (IOPS) that the volume should support.
9. For **Availability Zone**, choose the Availability Zone in which to create the volume. EBS volumes can only be attached to EC2 instances in the same Availability Zone.

Option C is a snapshot action.

Sharing an Unencrypted Snapshot

To share a snapshot using the console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Choose **Snapshots** in the navigation pane.
3. Select the snapshot and then choose **Actions**, **Modify Permissions**.
4. Make the snapshot public or share it with specific AWS accounts as follows:
   - To make the snapshot public, choose **Public**.

     This option is not valid for encrypted snapshots or snapshots with an AWS Marketplace product code.
   - To share the snapshot with one or more AWS accounts, choose **Private**, type the AWS account ID (without hyphens) in **AWS Account Number**, and choose **Add Permission**. Repeat for any additional AWS accounts.
5. Choose **Save**.

To use an encrypted snapshot that was shared with me

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Choose **Snapshots** in the navigation pane.
3. Choose the **Private Snapshots** filter.
4. Locate the snapshot by ID or description. You can use this snapshot as you would any other; for example, you can create a volume from the snapshot or copy the snapshot to a different region.

Sharing an Encrypted Snapshot

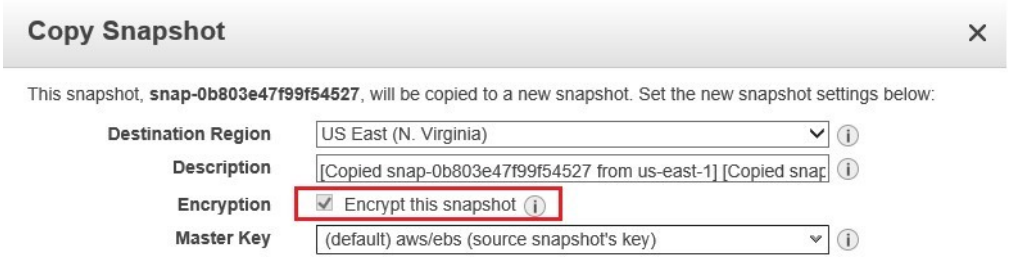
To share an encrypted snapshot using the console

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. Choose **Encryption keys** in the navigation pane.
3. Choose the alias of the custom key that you used to encrypt the snapshot.
4. For each AWS account, choose **Add External Accounts** and type the AWS account ID where prompted. When you have added all AWS accounts, choose **Save Changes**.
5. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
6. Choose **Snapshots** in the navigation pane.
7. Select the snapshot and then choose **Actions**, **Modify Permissions**.
8. For each AWS account, type the AWS account ID in **AWS Account Number** and choose **Add Permission**. When you have added all AWS accounts, choose **Save**.

To use an encrypted snapshot that was shared with me

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Choose **Snapshots** in the navigation pane.
3. Choose the **Private Snapshots** filter. Optionally add the **Encrypted** filter.
4. Locate the snapshot by ID or description.
5. We recommend that you re-encrypt the snapshot with a different key that you own. This protects you if the original key is compromised, or if the owner revokes the key, which could cause you to lose access to any encrypted volumes you create from the snapshot.
   a. Select the snapshot and choose **Actions**, **Copy**.
   b. (Optional) Select a destination region.
   c. Select a custom CMK that you own.
   d. Choose **Copy**.

Option D is correct answer. We cannot disable encryption while performing copy of an encrypted snapshot.



Ask our Experts

QUESTION 5 CORRECT

You are working as an AWS architect in your organization. An application is being developed on AWS EC2 instance and would need a local volume with low latency to handle database workloads. They figured out Provisioned IOPS SSD volume type suits best. However, when the application team is launching an EC2 instance, they found an option named "EBS-optimized". They reached out to you asking the purpose of EBS optimized instances. What do you suggest?

- **A.** Amazon EBS–optimized instance provides additional, dedicated capacity for Amazon EBS I/O. ✔
- **B.** Amazon EBS-optimized instance comes with instance store ephemeral storage which provides faster throughput.
- **C.** EBS-optimized is a configuration on the EBS volume, not an option on EC2 instance.
- **D.** Amazon EBS-optimized instances cannot have Provisioned IOPS SSD volume types. They only work with General Purpose SSD, Throughput optimized HDD, Cold HDD

Explanation :

Answer: A
An Amazon EBS–optimized instance uses an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance. EBS–optimized instances deliver dedicated bandwidth to Amazon EBS, with options between 425 Mbps and 14,000 Mbps, depending on the instance type you use. When attached to an EBS–optimized instance, General Purpose SSD (gp2) volumes are designed to deliver within 10% of their baseline and burst performance 99% of the time in a given year, and Provisioned IOPS SSD (io1) volumes are designed to deliver within 10% of their provisioned performance 99.9% of the time in a given year. Both Throughput Optimized HDD (st1) and Cold HDD (sc1) guarantee performance consistency of 90% of burst throughput 99% of the time in a given year. Non- compliant periods are approximately uniformly distributed, targeting 99% of expected total throughput each hour.
For more information on EBS-optimized instances, refer documentation here.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html)

Ask our Experts

QUESTION 6 CORRECT

Which of the following is not true with respect to EBS volume encryption?

- A. Encrypts data at rest inside the volume.
- B. Encrypts all data moving between the volume and the instance.
- C. Encrypts all snapshots created from the volume.
- D. Encrypted EBS volumes are supported on all instance types. ✔

Explanation :

Answer: D

Options A, B, C are correct statements.

Amazon EBS Encryption

Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

- Data at rest inside the volume
- All data moving between the volume and the instance
- All snapshots created from the volume
- All volumes created from those snapshots

Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html)

option D is correct answer

Amazon EBS encryption is only available on certain instance types. You can attach both encrypted and unencrypted volumes to a supported instance type. For more information, see Supported Instance Types.

Supported Instance Types

Amazon EBS encryption is available on the current-generation instance types listed below. These instance types leverage the Intel AES New Instructions (AES-NI) instruction set to provide faster and simpler data protection. You can attach both encrypted and unencrypted volumes to these instance types simultaneously.

- General purpose: T2, T3, M4, M5, M5d
- Compute optimized: C4, C5, C5d
- Memory optimized: R4, R5, R5d, X1, X1e, z1d, `cr1.8xlarge`
- Storage optimized: D2, I3, `h1.2xlarge`, `h1.4xlarge`, `i3.metal`
- Accelerated computing: F1, G3, P2, P3

For more information about these instance types, see Amazon EC2 Instance Types.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#EBSEncryption_supported_instances (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html%23EBSEncryption_s%20upported_ins

Ask our Experts

QUESTION 7 INCORRECT

Which of the following statements is true with respect to encryption?

- A. Enable encryption when creating a snapshot from unencrypted volume. ✖
- B. Enable encryption while copying snapshot from an unencrypted snapshot. ✔
- C. Disable encryption while creating a snapshot from encrypted volume.
- D. Disable encryption while copying snapshot from an encrypted snapshot.

Explanation :

Answer: B

Changing the Encryption State of Your Data

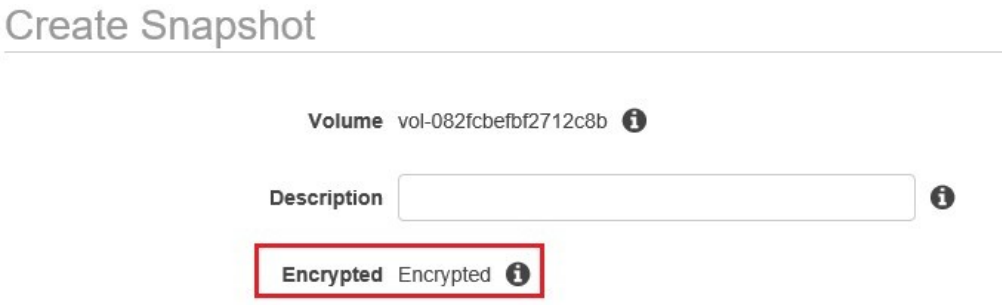
There is no direct way to encrypt an existing unencrypted volume, or to remove encryption from an encrypted volume. However, you can migrate data between encrypted and unencrypted volumes. You can also apply a new encryption status while copying a snapshot:

- While copying an unencrypted snapshot of an unencrypted volume, you can encrypt the copy. Volumes restored from this encrypted copy are also encrypted.
- While copying an encrypted snapshot of an encrypted volume, you can associate the copy with a different CMK. Volumes restored from the encrypted copy are only accessible using the newly applied CMK.

You cannot remove encryption from an encrypted snapshot.

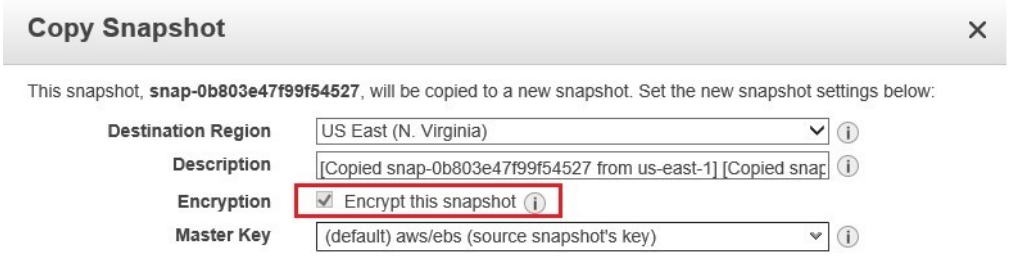
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#EBSEncryption_considerations

Option C is not correct.



Option D is not correct.

We cannot disable encryption while performing copy of a snapshot.



Ask our Experts

QUESTION 8 INCORRECT

You are working as an architect in your organization. An application team is using EBS volume for their database workloads which would need a high throughput, low latency and maximum I/O. They chose Provisioned IOPS EBS volume for better performance. However, after setting up the entire application, they notice the performance is not up to the mark. Which performance tuning mechanisms would you suggest? Please choose 3 correct options.

- [x] **A.** Use EBS-Optimized Instances. ✔
- [ ] **B.** Use Throughput optimized HDD volume types for low latency and maximum I/O.
- [ ] **C.** Use a Modern Linux Kernel. ✔
- [x] **D.** Use RAID 0 to Maximize Utilization of Instance Resources. ✔
- [x] **E.** Performance of Provisioned IOPS SSD volume increase with volume size. Increase EBS volume size. ✖

Explanation :

Answer: A, C, D
Option A is correct.

Amazon EBS Performance Tips

These tips represent best practices for getting optimal performance from your EBS volumes in a variety of user scenarios.

Use EBS-Optimized Instances

On instances without support for EBS-optimized throughput, network traffic can contend with traffic between your instance and your EBS volumes; on EBS-optimized instances, the two types of traffic are kept separate. Some EBS-optimized instance configurations incur an extra cost (such as C3, R3, and M3), while others are always EBS-optimized at no extra cost (such as M4, C4, C5, and D2). For more information, see Amazon EC2 Instance Configuration.

Option B is not correct. Provisioned IOPS SSD volume type is more suitable for database workloads.

	Solid-State Drives (SSD)		Hard disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	• Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments	• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume • Large database workloads, such as: ◦ MongoDB ◦ Cassandra ◦ Microsoft SQL Server ◦ MySQL ◦ PostgreSQL ◦ Oracle	• Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume

Option C is correct.

Use a Modern Linux Kernel

Use a modern Linux kernel with support for indirect descriptors. Any Linux kernel 3.11 and above has this support, as well as any current-generation EC2 instance. If your average I/O size is at or near 44 KiB, you may be using an instance or kernel without support for indirect descriptors. For information about deriving the average I/O size from Amazon CloudWatch metrics, see I/O Characteristics and Monitoring.

To achieve maximum throughput on `st1` or `sc1` volumes, we recommend applying a value of 256 to the `xen_blkfront.max` parameter (for Linux kernel versions below 4.6) or the `xen_blkfront.max_indirect_segments` parameter (for Linux kernel version 4.6 and above). The appropriate parameter can be set in your OS boot command line.

Option D is correct.

Use RAID 0 to Maximize Utilization of Instance Resources

Some instance types can drive more I/O throughput than what you can provision for a single EBS volume. You can join multiple `gp2`, `io1`, `st1`, or `sc1` volumes together in a RAID 0 configuration to use the available bandwidth for these instances. For more information, see RAID Configuration on Linux.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html#tips (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html#tips)

Option E is not correct. The statement is applicable to General Purpose SSD, not for Provisioned IOPS SSD.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_gp2

(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_gp2)
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_piops
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_piops)

Ask our Experts

QUESTION 9 INCORRECT

Which of the following is not an AWS CloudWatch metric for EBS Volumes?

- A. VolumeReadBytes
- B. VolumeWriteOps
- C. VolumeThroughputPercentage ✖
- D. VolumeRemainingSize ✔

Explanation :

Answer: D

Metric	Description
VolumeReadBytes VolumeWriteBytes	Provides information on the I/O operations in a specified period of time. The Sum statistic reports the total number of bytes transferred during the period. The Average statistic reports the average size of each I/O operation during the period, except on volumes attached to a Nitro instance, where the average represents the average over the specified period. The SampleCount statistic reports the total number of I/O operations during the period, except on volumes attached to a Nitro instance, where the sample count represents the number of data points used in the statistical calculation. Data is reported to CloudWatch only when the volume is active. The Minimum and Maximum statistics on this metric are supported only by volumes attached to the following instances: C5, C5d, i3.metal, M5, M5d, R5, R5d, T3, and z1d. Units: Bytes
VolumeReadOps VolumeWriteOps	The total number of I/O operations in a specified period of time. To calculate the average I/O operations per second (IOPS) for the period, divide the total operations in the period by the number of seconds in that period. The Minimum and Maximum statistics on this metric are supported only by volumes attached to the following instances: C5, C5d, i3.metal, M5, M5d, R5, R5d, T3, and z1d. Units: Count

VolumeTotalReadTime VolumeTotalWriteTime	The total number of seconds spent by all operations that completed in a specified period of time. If multiple requests are submitted at the same time, this total could be greater than the length of the period. For example, for a period of 5 minutes (300 seconds): if 700 operations completed during that period, and each operation took 1 second, the value would be 700 seconds. The Average statistic on this metric is not relevant for volumes attached to the following instances: C5, C5d, i3.metal, M5, M5d, R5, R5d, T3, and z1d. The Minimum and Maximum statistics on this metric are supported only by volumes attached to the following instances: C5, C5d, i3.metal, M5, M5d, R5, R5d, T3, and z1d. Units: Seconds
VolumeIdleTime	The total number of seconds in a specified period of time when no read or write operations were submitted. The Average statistic on this metric is not relevant for volumes attached to the following instances: C5, C5d, i3.metal, M5, M5d, R5, R5d, T3, and z1d. The Minimum and Maximum statistics on this metric are supported only by volumes attached to the following instances: C5, C5d, i3.metal, M5, M5d, R5, R5d, T3, and z1d. Units: Seconds

VolumeQueueLength	The number of read and write operation requests waiting to be completed in a specified period of time. The Sum statistic on this metric is not relevant for volumes attached to the following instances: C5, C5d, i3.metal, M5, M5d, R5, R5d, T3, and z1d. The Minimum and Maximum statistics on this metric are supported only by volumes attached to the following instances: C5, C5d, i3.metal, M5, M5d, R5, R5d, T3, and z1d. Units: Count
VolumeThroughputPercentage	Used with Provisioned IOPS SSD volumes only. The percentage of I/O operations per second (IOPS) delivered of the total IOPS provisioned for an Amazon EBS volume. Provisioned IOPS SSD volumes deliver within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year. During a write, if there are no other pending I/O requests in a minute, the metric value will be 100 percent. Also, a volume's I/O performance may become degraded temporarily due to an action you have taken (for example, creating a snapshot of a volume during peak usage, running the volume on a non-EBS-optimized instance, or accessing data on the volume for the first time). Units: Percent

VolumeConsumedReadWriteOps	Used with Provisioned IOPS SSD volumes only. The total amount of read and write operations (normalized to 256K capacity units) consumed in a specified period of time. I/O operations that are smaller than 256K each count as 1 consumed IOPS. I/O operations that are larger than 256K are counted in 256K capacity units. For example, a 1024K I/O would count as 4 consumed IOPS. Units: Count
BurstBalance	Used with General Purpose SSD (gp2), Throughput Optimized HDD (st1), and Cold HDD (sc1) volumes only. Provides information about the percentage of I/O credits (for gp2) or throughput credits (for st1 and sc1) remaining in the burst bucket. Data is reported to CloudWatch only when the volume is active. If the volume is not attached, no data is reported. The Sum statistic on this metric is not relevant for volumes attached to the following instances: C5, C5d, i3.metal, M5, M5d, R5, R5d, T3, and z1d. Units: Percent

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-volume-status.html#using_cloudwatch_ebs (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-volume-%20status.html%23using_cloudwatch_ebs)

Ask our Experts

QUESTION 10 INCORRECT

You are using AWS EC2 linux instance for log processing which would require high throughput. You chose Throughput optimized HDD storage with 500 GB in size. You deployed your application to production mode and it is running as expected. After a month, you see an increase in log files and you are fast approaching the 500 GB size and running out of space on the EBS volume. Which of the following is a best approach to mitigate the situation with minimal configuration?

- A. Add a new EBS volume, mount on EC2 instance and configure your application accordingly. ✖
- B. Increase the size of the existing EBS volume. ✔
- C. EBS volume size cannot be changed. Build purging logic for your old log files
- D. You can have only one EBS volume per instance. Snapshot existing EBS volume, detach current volume, create a new volume from snapshot with bigger size and attached to EC2 instance.

Explanation :

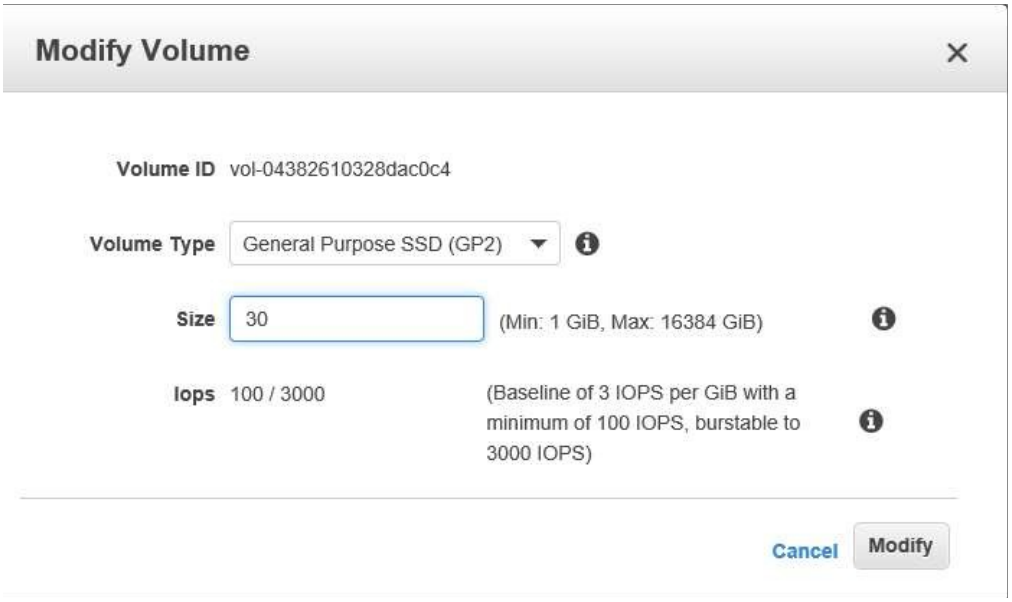
Answer: B

Although option A looks correct, it is not the best approach since it involves more configuration and

changes to the application to point to new EBS mount point.

Option B is correct.

You can modify the volume and increase volume size.



https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modify-volume.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modify-volume.html)

Option C is not a correct solution.

Option D is not correct. You can attach multiple EBS volumes to the single EC2 instances.

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14818)

Certification

- Cloud Certification (https://www.whizlabs.com/cloud-certification-training-courses/)
- Java Certification (https://www.whizlabs.com/oracle-java-certifications/)
- PM Certification (https://www.whizlabs.com/project-management-certifications/)

Company

- Support (https://help.whizlabs.com/hc/en-us)
- Discussions (http://ask.whizlabs.com/)
- Blog (https://www.whizlabs.com/blog/)

- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Mobile App

- Android Coming Soon
- iOS Coming Soon

Follow us

(https://www.facebook.com/whizlabs.software/)

(https://in.linkedin.com/company/whizlabs-software)

(https://twitter.com/whizlabs?lang=en)

(https://plus.google.com/+WhizlabsSoftware)