



# HI-TECH INSTITUTION

CORPORATE CAREER ENHANCEMENT TRAININGS

OUR ROOT LEVEL  
TRAINING WILL  
GIVE YOU BETTER  
GROWTH





## ABOUT US

### Our Vision:

To provide better training by full filling the requirements of our trainee.

### Our Mission:

We always ensure to give practical based training. And we make the candidates to get good hands-on experience on any platform.

### Philosophy:

Our Root Level Training Will give you Better Growth.

We successfully survived around 5 years in the IT field. Started this is as small Training room. But now we are having 5 branches across India.

Certified Trainers taking the session on various domain with any level of doubts clarification.

For More Details: [www.hitechins.in](http://www.hitechins.in)

Write feedback to [operations@hitechins.in](mailto:operations@hitechins.in)

## Creating an Amazon EBS Snapshot

A point-in-time snapshot of an EBS volume, can be used as a baseline for new volumes or for data backup. If you make periodic snapshots of a volume, the snapshots are incremental—only the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the entire volume.

Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is `pending` until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume.

### Important

Although you can take a snapshot of a volume while a previous snapshot of that volume is in the `pending` status, having multiple `pending` snapshots of a volume may result in reduced volume performance until the snapshots complete.

Snapshots that are taken from encrypted volumes are automatically encrypted. Volumes that are created from encrypted snapshots are also automatically encrypted. The data in your encrypted volumes and any associated snapshots is protected both at rest and in motion.

By default, only you can create volumes from snapshots that you own. However, you can share your unencrypted snapshots with specific AWS accounts, or you can share them with the entire AWS community by making them public.

You can share an encrypted snapshot only with specific AWS accounts. For others to use your shared, encrypted snapshot, you must also share the CMK key that was used to encrypt it. Users with access to your encrypted snapshot must create their own personal copy of it and then use that copy to restore the volume. Your copy of a shared, encrypted snapshot can also be re-encrypted with a different key.

When a snapshot is created from a volume with an AWS Marketplace product code, the product code is propagated to the snapshot.

You can take a snapshot of an attached volume that is in use. However, snapshots only capture data that has been written to your Amazon EBS volume at the time the snapshot command is issued. This might exclude any data that has been cached by any applications or the operating system. If you can pause any file writes to the volume long enough to take a snapshot, your snapshot should be complete. However, if you can't pause all file writes to the volume, you should Unmount the volume from within the instance, issue the snapshot command, and then remount the volume to ensure a consistent and complete snapshot. You can remount and use your volume while the snapshot status is `pending`.

To create a snapshot for an Amazon EBS volume that serves as a root device, you should stop the instance before taking the snapshot.

To Unmount the volume in Windows, open Disk Management, right-click the volume to unmount, and select **Change Drive Letter and Path**. Select the mount point to remove, and then click **Remove**.

To make snapshot management easier, you can tag your snapshots during creation or add tags afterward. For example, you can apply tags describing the original volume from which the snapshot was created, or the device name that was used to attach the original volume to an instance.

### To create 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. Choose **Create Snapshot**.
4. On the **Create Snapshot** page, select the volume to create a snapshot for.
5. (Optional) Choose **Add tags to your snapshot**. For each tag, provide a tag key and a tag value.
6. Choose **Create Snapshot**.

### Deleting an Amazon EBS Snapshot

When you delete a snapshot, only the data referenced exclusively by that snapshot is removed. Deleting previous snapshots of a volume does not affect your ability to restore volumes from later snapshots of that volume.

Deleting a snapshot of a volume has no effect on the volume. Deleting a volume has no effect on the snapshots made from it.

### To delete 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 a snapshot and then choose **Delete** from the **Actions** list.
4. Choose **Yes, Delete**.

### Restoring an Amazon EBS Volume from a Snapshot

You can restore an Amazon EBS volume with data from a snapshot stored in Amazon S3. You need to know the ID of the snapshot you want to restore your volume from and you need to have access permissions for the snapshot.

New volumes created from existing EBS snapshots load lazily in the background. This means that after a volume is created from a snapshot, there is no need to wait for all of the data to



transfer from Amazon S3 to your EBS volume before your attached instance can start accessing the volume and all its data. If your instance accesses data that hasn't yet been loaded, the volume immediately downloads the requested data from Amazon S3, and continues loading the rest of the data in the background.

EBS volumes that are restored from encrypted snapshots are automatically encrypted. Encrypted volumes can only be attached to selected instance types.

Because of security constraints, you cannot directly restore an EBS volume from a shared encrypted snapshot that you do not own. You must first create a copy of the snapshot, which you will own. You can then restore a volume from that copy.

New EBS volumes receive their maximum performance the moment that they are available and do not require initialization (formerly known as pre-warming). However, storage blocks on volumes that were restored from snapshots must be initialized (pulled down from Amazon S3 and written to the volume) before you can access the block. This preliminary action takes time and can cause a significant increase in the latency of an I/O operation the first time each block is accessed. Performance is restored after the data is accessed once.

For most applications, amortizing the initialization cost over the lifetime of the volume is acceptable. To ensure that your restored volume always functions at peak capacity in production, you can force the immediate initialization of the entire volume using **dd** or **fio**.

### 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](#).
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.

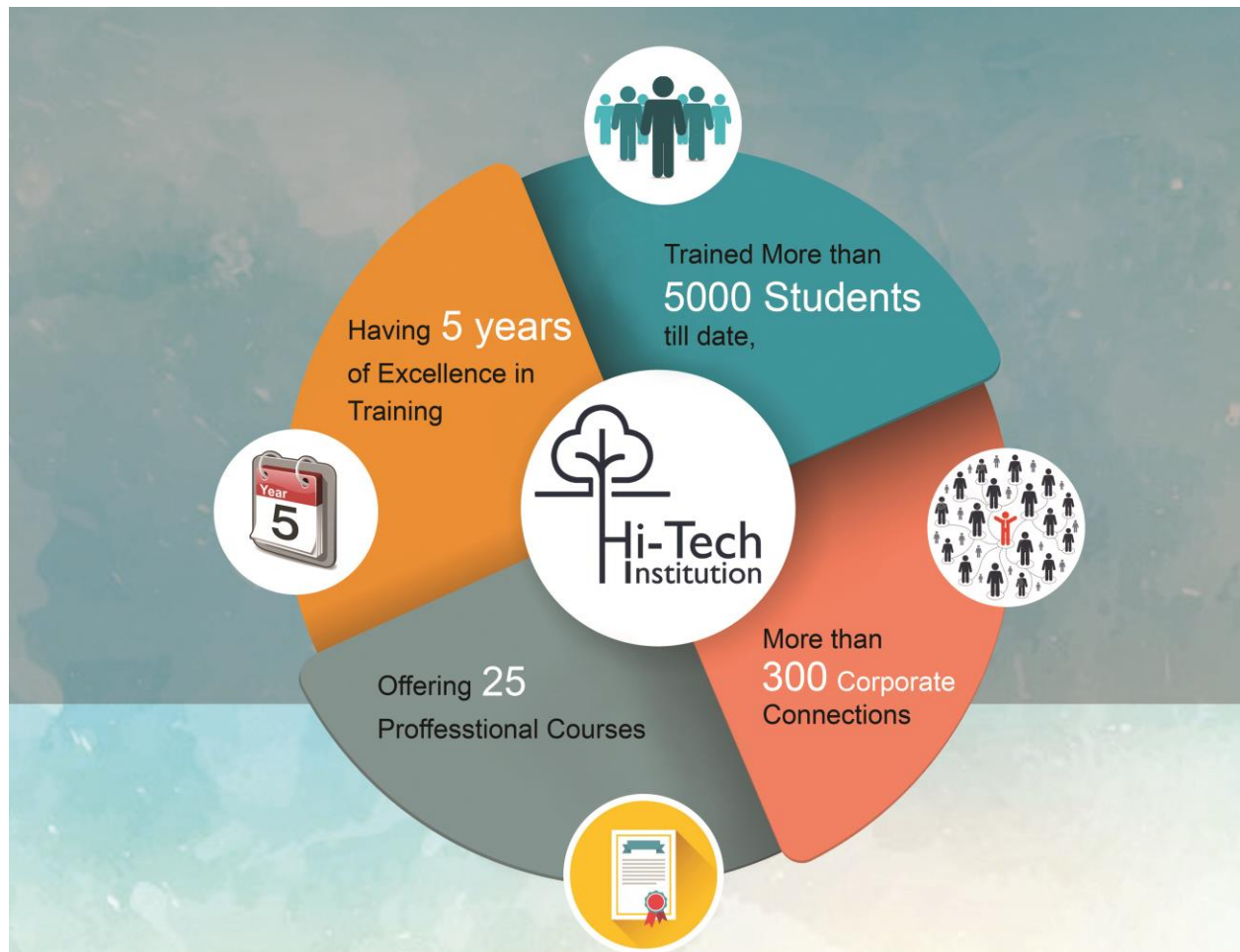
## Note

The following Amazon EBS volume considerations apply to Windows boot volumes:

- Windows boot volumes must use an MBR partition table, which limits the usable space to 2 TiB, regardless of volume size.
- Windows boot volumes of 2 TiB (2048 GiB) that have been converted to use a dynamic MBR partition table display an error when examined with Disk Manager.

The following Amazon EBS volume considerations apply to Windows data (non-boot) volumes:

- Windows volumes 2 TiB (2048 GiB) or greater must use a GPT partition table to access the entire volume.
  - Amazon EBS volumes over 2048 GiB that are attached to Windows instances at launch are automatically formatted with a GPT partition table.
  - Amazon EBS volumes attached to Windows instances after launch must be manually initialized with a GPT partition table.
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.
  10. (Optional) Choose **Create additional tags** to add tags to the volume. For each tag, provide a tag key and a tag value.
  11. Choose **Create Volume**.
  12. After you've restored a volume from a snapshot, you can attach it to an instance to begin using it.
  13. If you restored a snapshot to a larger volume than the default for that snapshot, you must extend the file system on the volume to take advantage of the extra space.



## TOP RECRUITERS





**offer for School or College students**

**30% offer for IT Employees**

Above offer applicable only technical courses. Terms and conditions apply



[operations@hitechins.in](mailto:operations@hitechins.in)



[www.hitechins.in](http://www.hitechins.in)



**7092 90 91 92 / 82 20 21 7640**

#### PONDICHERRY

No.32, 100 feet road,  
Ellaipillaichavady,  
Pondicherry – 605 005,  
Nearby Rajiv Gandhi Hospital

#### TAMBARAM

No.24, Chithi Vinayagar Kovil street,  
KamarajNagar, Tambaram Sanatorium,  
Chennai – 600 047,  
Nearby Sanatorium Railway Station

#### VELACHERRY

No: 21, Officer Colony,  
100 feet road, VijayaNagar,  
Velacherry – 600 042,  
Nearby Sathya Home Appliances

**Locations**

**Chennai & Pondicherry**