**Day 17**





**“CLOUD SECURITY”**

**Amazon EBS Snapshots for Data Backup:**

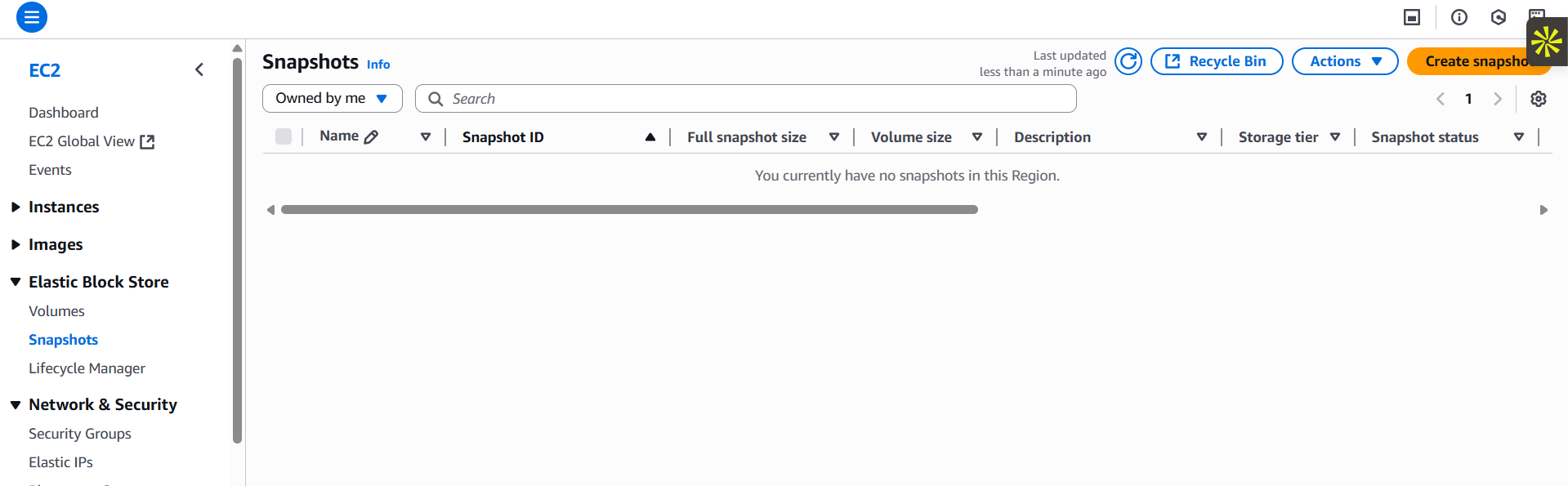
* Amazon EBS Snapshots are point-in-time backups of EBS volumes, offering secure, incremental data protection for disaster recovery, migration, and compliance.
* They support encryption by default, integrate with Amazon Data Lifecycle Manager for automation, and protect data both in transit and at rest.
* Snapshots can be shared across AWS accounts (with proper CMK permissions) and support multi-volume backups for EC2 instances.

**Some basic info:**

* EBS (Elastic Block Store): A block-level storage service used with EC2 instances to store data persistently, such as OS, application files, and databases.
* EBS Snapshot: A point-in-time, incremental backup of an EBS volume. It captures only the data that has changed since the last snapshot.
* Incremental Backup: Only modified blocks (since the last snapshot) are stored, making snapshots efficient in storage and faster.
* Encrypted Snapshot: A snapshot taken from an encrypted EBS volume. It stays encrypted at rest and in transit. It can be shared only with authorized AWS accounts via CMK (Customer Master Key).
* Data Lifecycle Manager (DLM): An AWS service used to automate creation, retention, and deletion of EBS snapshots based on policies.
* Multi-Volume Snapshot: Allows simultaneous backup of all EBS volumes attached to an EC2 instance to ensure data consistency.

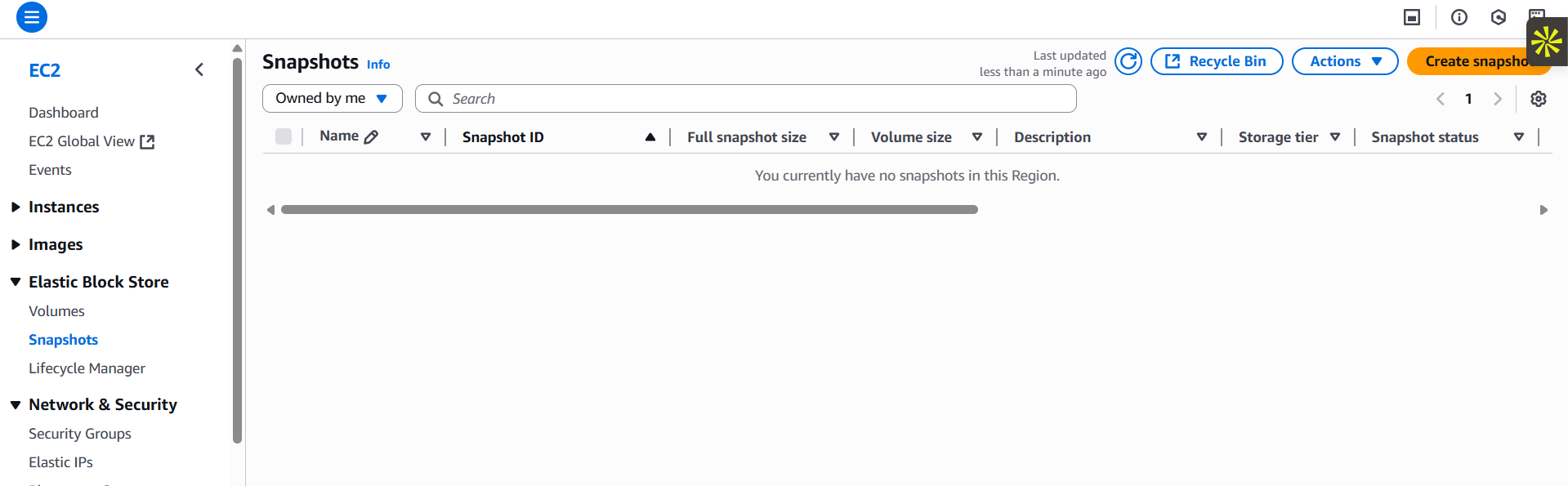
**Where can we find the option for EBS?**

It can be found under the “EBS” section in EC2 instance page:

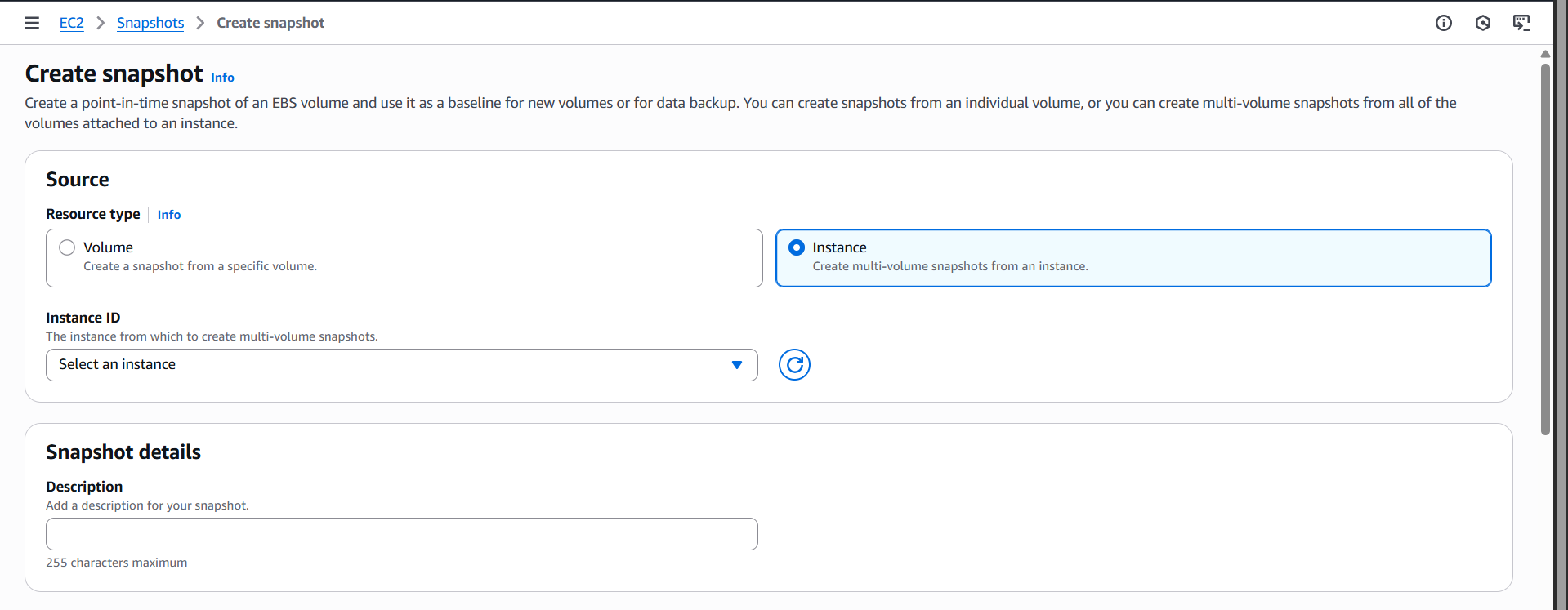


**Creating a snapshot:**

Steps:

Under the EBS submenu, click on the “snapshot” section: following screen will appear.   


Click on the “orange button” following screen will appear:



Fill it as required, and click on the orange button at the bottom right corner for creating it.

**Best Practices for keeping Snapshots safe and secure:**

**1. Enable Encryption**

* Always use EBS encryption when creating volumes or snapshots.
* Snapshots of encrypted volumes are automatically encrypted.
* Encryption protects data both at rest and in transit using AWS-managed or customer-managed CMKs.

**2. Control Snapshot Sharing**

* Never make snapshots public unless absolutely necessary.
* If sharing is required, share encrypted snapshots only with trusted AWS accounts and also share the corresponding CMK.
* Regularly audit shared snapshots using AWS CLI or AWS Config.

**3. Use IAM Policies and Permissions**

* Implement strict IAM policies to control who can:
  + Create snapshots
  + Delete snapshots
  + Share snapshots
  + Restore snapshots
* Always follow the principle of least privilege.

**4. Enable AWS CloudTrail**

* Use AWS CloudTrail to log snapshot-related actions, such as:
  + Who created or deleted snapshots
  + Who shared them and with whom
* These logs help in auditing and identifying unauthorized access.

**5. Automate with Lifecycle Policies**

* Use Amazon Data Lifecycle Manager (DLM) to:
  + Automate snapshot creation and deletion
  + Reduce the risk of forgotten or outdated snapshots containing sensitive data

**6. Avoid Unused or Orphan Snapshots**

* Periodically review and delete old or unused snapshots to minimize risk exposure.
* Orphaned snapshots may cause data leakage if mistakenly accessed or shared.

**7. Use CMK Rotation and Access Logging**

* When using customer-managed keys (CMKs):
  + Rotate the keys regularly
  + Enable CloudWatch Logs to track key usage and ensure transparency

--The End--