**Day 11**





**“CLOUD SECURITY”**

**Amazon CloudFront Security:**

1. **Secure Content Delivery & Access Control**

* Delivers content with low latency via global edge locations.
* Supports HTTPS/TLS encryption, signed URLs, geo-restriction, and Origin Access Identity (OAI) to control who can access content.
* Private content feature protects S3-origin files and prevents unauthorized downloads.

1. **Authentication & Encryption**

* All API calls require HMAC-SHA1 authentication and SSL encryption.
* Uses Perfect Forward Secrecy (ECDHE) to prevent decryption even if long-term keys are compromised.
* Supports custom SSL via SNI or dedicated IP for secure HTTPS delivery using customer domains.

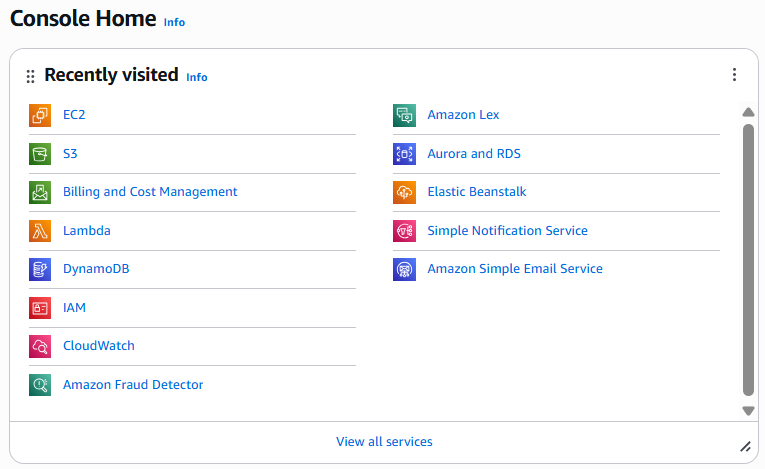
1. **Logging & Monitoring**

* CloudFront access logs track requests, IPs, edge locations, referrers, and user agents.
* Customers can configure S3 to store logs and monitor usage securely.

**Create Security Group to Secure EC2 Instances:**

Steps:

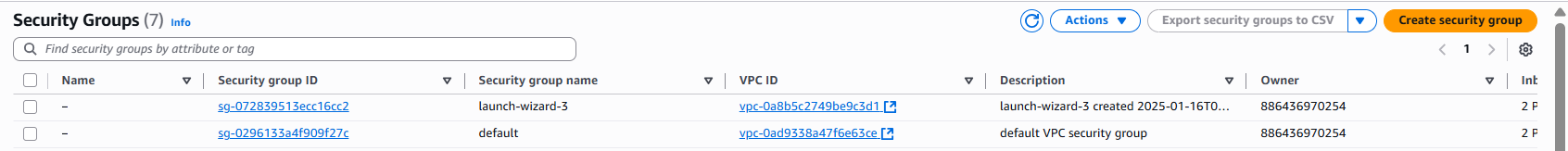
Open the AWS, and click on the EC2 instance option:



Under the “Network and Security” option in the menu click on the “Security Groups” option:



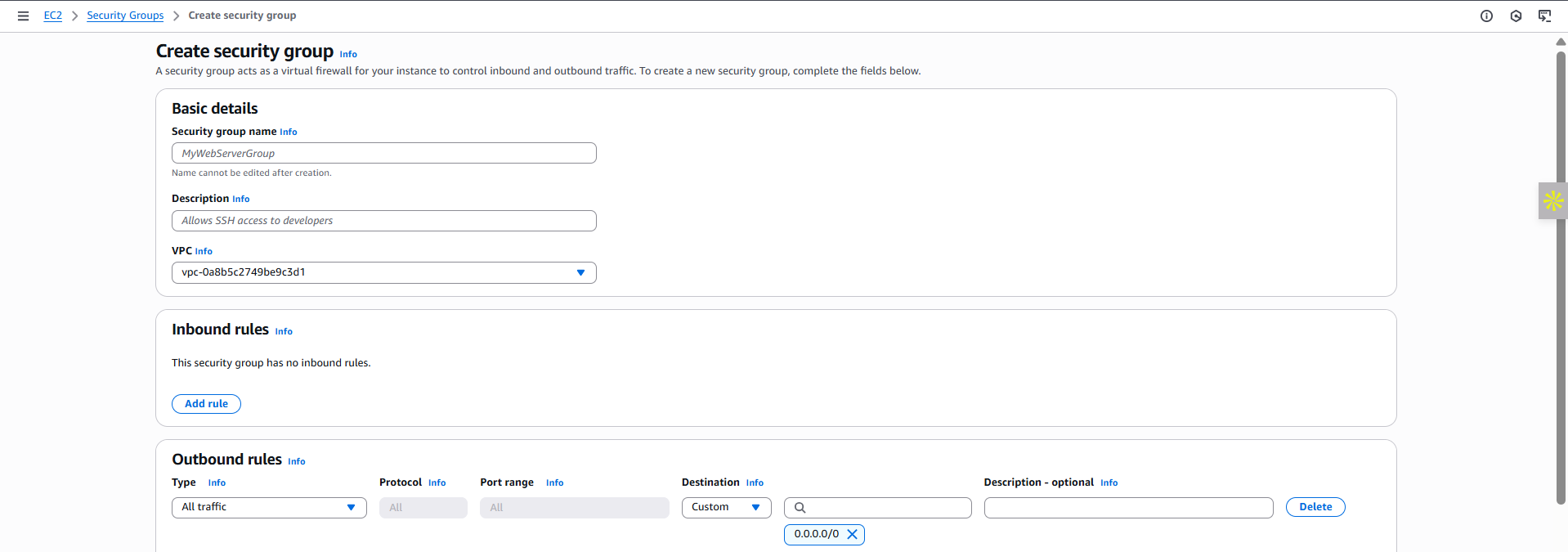
Following list of security groups will appear:



Click on the “Create security group” button:



Following screen will appear:



Specify the details and click on the orange button at the right bottom corner.

--The End--