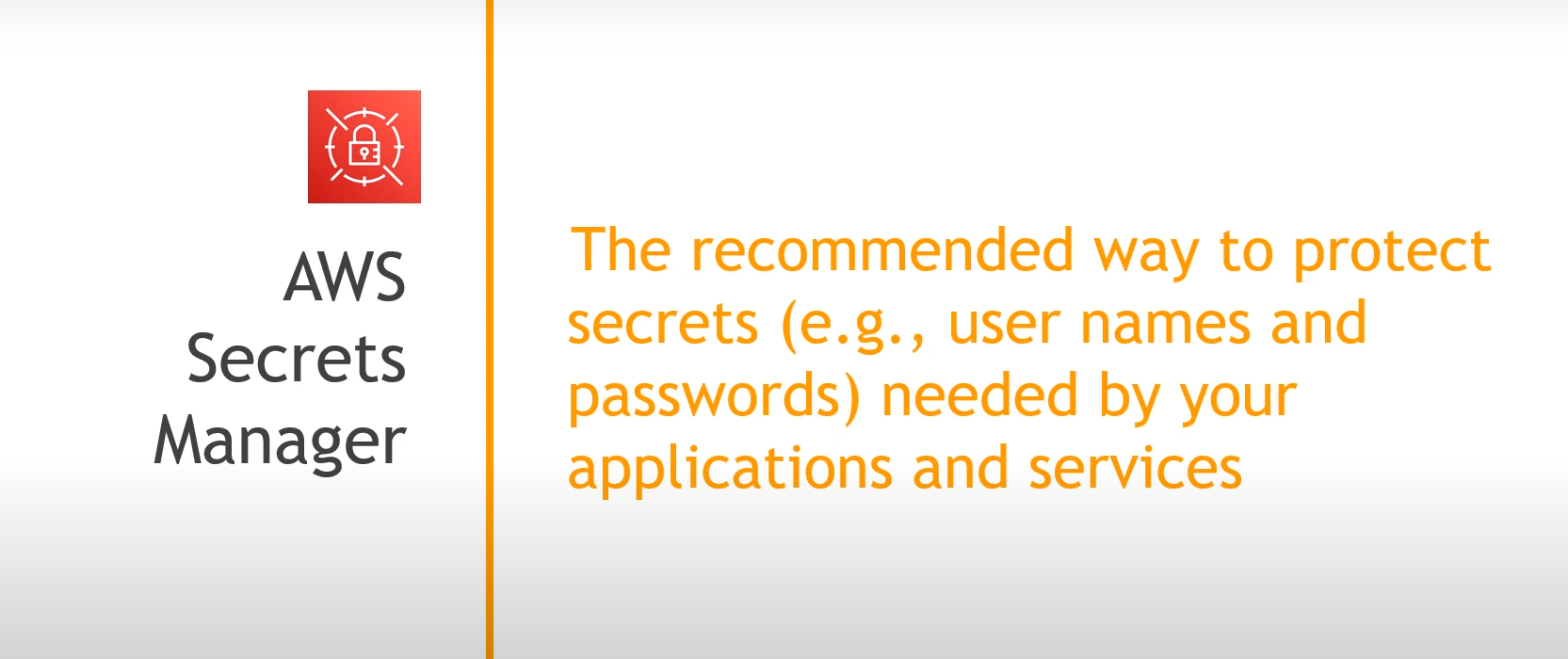
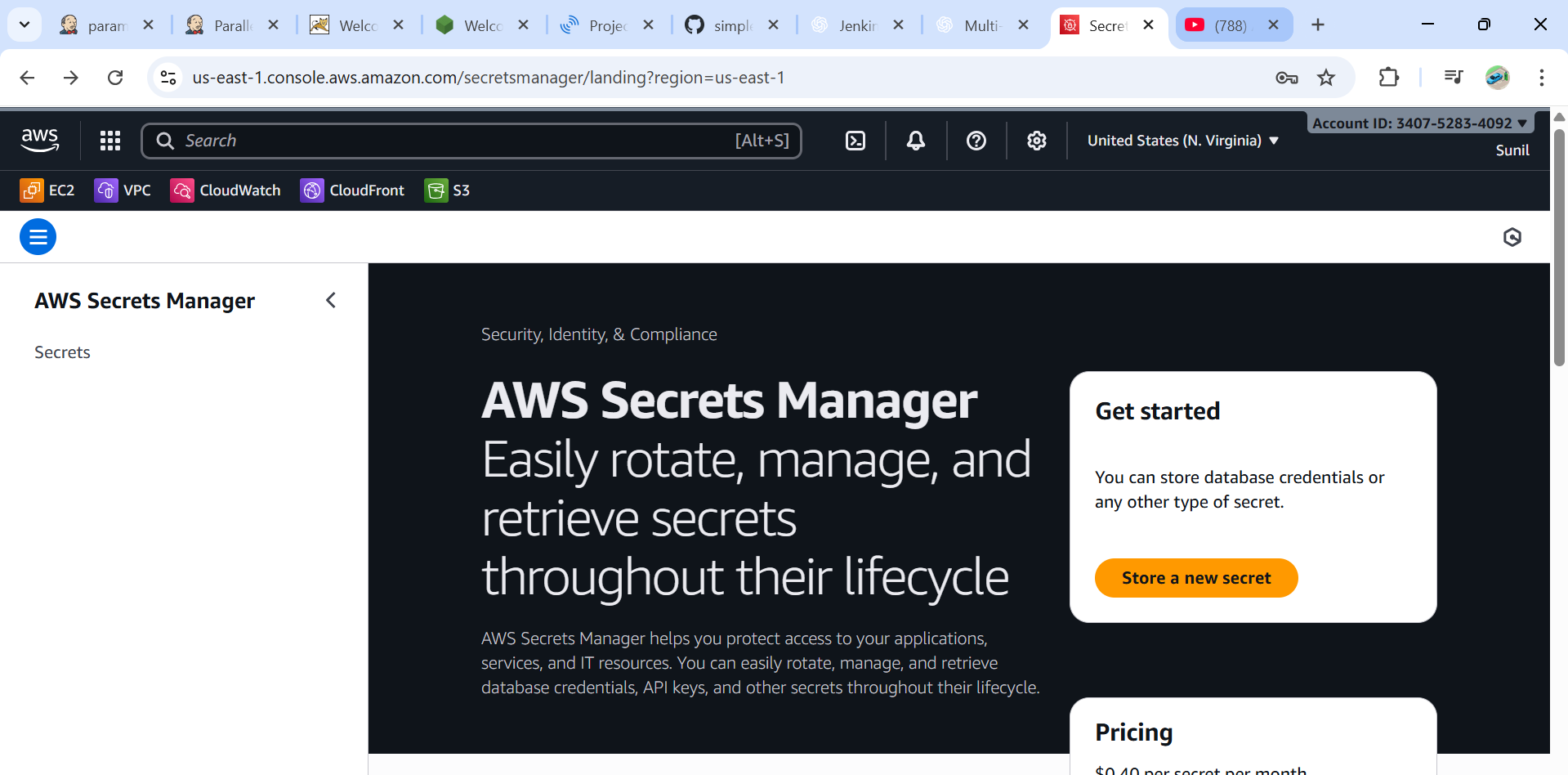
**AWS Secrets Manager**

AWS **Secrets Manager** is a fully managed service from AWS used to **store, manage, and retrieve secrets** securely.  
Secrets can be things like:

* Database credentials (username & password)
* API keys
* Access tokens
* SSH keys

Instead of hardcoding credentials in your code or configuration files, you store them in Secrets Manager and retrieve them securely when needed.





**⚙️ Key Features**

1. **Centralized secret storage** – Store all secrets in one place.
2. **Encryption by default** – Secrets are encrypted using AWS KMS keys.
3. **Automatic rotation** – You can configure secrets to rotate automatically (for example, rotate DB passwords every 30 days).
4. **Secure retrieval** – Applications can fetch secrets via AWS SDK, CLI, or API.
5. **Audit with CloudTrail** – Every access to a secret is logged.

**How It Works**

1. Store a secret (like DB password) in AWS Secrets Manager.
2. Grant IAM roles/policies permission to access the secret.
3. Your application uses AWS SDK/CLI to retrieve the secret securely at runtime.
4. (Optional) Set up **automatic rotation** with a Lambda function.

