AWS Secrets Manager

Accessing AWS services often involves the use of credentials, keys and other information (Usernames, passwords, etc) which need to be kept secure and protected from unauthorized access and distribution. In fact, AWS even has a name for such sensitive pieces of information: **Secrets** and a service called **AWS Secrets Manager** that helps us well, manage them.

To be more specific, AWS Secrets Manager is a service that helps securely store, manage, and retrieve **database credentials**, API keys, and other sensitive secrets. It allows **automatic rotation of credentials**, reducing the risk of exposure and ensuring robust security. By integrating seamlessly with AWS services such as RDS, Redshift, and Lambda, Secrets Manager simplifies managing access to sensitive information, enhancing the security of our AWS environment.

It also offers fine-grained access control using AWS Identity and Access Management (IAM), a cornerstone service for security in AWS (discussed in next section), ensuring that only authorized users or services can retrieve secrets. Additionally, Secrets Manager encrypts secrets using AWS KMS, providing an extra layer of protection.

Note however that AWS Secrets Manager is not the end-all be-all service for storing sensitive information and that certain other AWS services (some of which will be discussed later) may be better suited for specific types of secrets. When storing encryption keys for example, it might be better to use the AWS Key Management Service and when storing string parameters it might be better to use AWS Systems Manager Parameter Store.