Encryption in Transit and at Rest

Encryption in Transit and at Rest

In this section, Rudy and Hong discussed data encryption in transit and at rest.

Encryption of Data in Transit

You can mount a file system so all NFS traffic is encrypted in transit using Transport Layer Security 1.2 (TLS, formerly called Secure Sockets Layer [SSL]) with an industry-standard AES-256 cipher. TLS is a set of industry-standard cryptographic protocols used for encrypting information that is exchanged over the wire. AES-256 is a 256-bit encryption cipher used for data transmission in TLS. If your organization is subject to corporate or regulatory policies that require encryption of data and metadata in transit, we recommend setting up encryption in transit on every client accessing the file system. More information on Encryption of data in transit can be found at: https://docs.aws.amazon.com/whitepapers/latest/efs-encrypted-file-systems/encryption-of-data-in-transit.html

Encryption of Data at Rest

You can create an encrypted file system so all your data and metadata is encrypted at rest using an industry-standard AES-256 encryption algorithm. Encryption and decryption is handled automatically and transparently, so you don't have to modify your applications. If your organization is subject to corporate or regulatory policies that require encryption of data and metadata at rest, we recommend creating an encrypted file system.

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs. More details on AWS KMS can be found at:https://aws.amazon.com/kms/

AWS CloudHSM

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries. CloudHSM is standards-compliant and enables you to export all of your keys to most other commercially-available HSMs, subject to your configurations. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs. More information on AWS CloudHSM can be found at:https://aws.amazon.com/cloudhsm/