PROTECCIÓN Y ENCRIPTACIÓN DE DATOS EN AWS

CONTENIDO

PROTECCIÓN Y ENCRIPTACIÓN DE DATOS EN AWS

Para comprender otros servicios de seguridad de AWS, vamos a continuar con la analogía de la cafetería, usada en la clase anterior.

Con todo el movimiento que ocurre en la cafetería, querrá aumentar la seguridad de los granos de café, el equipamiento (computadores, cajas registradoras, etc.) e incluso el dinero en la caja. En el caso de los granos, esto podría ser cuando están almacenados en la despensa, o incluso cuando los transporta de una tienda a otra. Después de todo, no queremos visitantes no deseados que accedan a nuestros granos de café, o incluso que huyan con el equipo valioso.
Para empezar, hablemos sobre cómo puede proteger sus granos de café o sus datos, ya sea que estén en reposo o en tránsito. Para los granos de café, la forma más sencilla de hacerlo sería cerrando la puerta cuando salgamos por la noche. Esa es la noción de cifrado, que es proteger un mensaje o datos de forma tal que sólo pueden acceder las partes autorizadas. Por lo tanto, es menos probable que las partes no autorizadas puedan acceder al mensaje o no puedan acceder a él en absoluto. Piense en ello como ese ejemplo de la llave y la puerta, si tiene la llave, puede abrir la puerta, pero si no, entonces no puede abrirla.

En AWS, esto viene en dos variantes: Cifrado en reposo y cifrado en tránsito. En reposo, cuando los datos están inactivos, solo se los almacenan y no se mueven. Por ejemplo, el cifrado en reposo del lado del servidor está habilitado en todos los datos de las tablas de DynamoDB y eso ayuda a evitar el acceso no autorizado.

DATOS SIN CRIFRAR

DATOS CIFRADOS

El cifrado en reposo de DynamoDB también se integra con AWS Key Management Service, o KMS para administrar la clave de cifrado que se utiliza para cifrar las tablas. Esa es la llave de la puerta, ¿lo recuerda? Y sin ella no podrá acceder a sus datos, así que asegúrese de mantenerla en un lugar seguro.

Del mismo modo, en tránsito significa que los datos están viajando entre, digamos, A y B, donde A es el servicio de AWS y B podría ser un cliente que accede al servicio, o incluso otro servicio de AWS.

Por ejemplo, supongamos que tenemos una instancia de Redshift en ejecución, y queremos conectarla con un cliente SQL. Usamos Secure Sockets Layer, o conexiones de SSL para cifrar datos, y podemos usar certificados de servicio para validar y autorizar a un cliente. Esto significa que los datos están protegidos cuando pasan entre Redshift y nuestro cliente.

Esta funcionalidad existe en muchos otros servicios de AWS como SQS, S3, RDS y muchos más.

Pero hablando de otros servicios de encriptación y protección de datos, el siguiente servicio que queremos destacar se llama AWS Secrets Manager. Secrets Manager permite alternar, administrar y recuperar credenciales de bases de datos, claves de API y otros datos confidenciales durante su ciclo de vida.

Otra oferta de AWS es el Parameter Store (almacén de parámetros) de Systems Manager de AWS, el cual proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y administrar las claves o secretos. Puede almacenar datos como contraseñas, cadenas de base de datos y códigos de licencia como valores de parámetros. No obstante, el almacén de parámetros no proporciona servicios de rotación automática para los secretos almacenados. En su lugar, Parameter Store le permite almacenar el secreto en Secrets Manager y, a continuación, hacer referencia al secreto como parámetro de Parameter Store.

AWS KEY MANAGEMENT SERVICE (AWS KMS)

AWS Key Management Service (AWS KMS) es un servicio administrado que le permite crear y controlar fácilmente las claves de cifrado que se utilizan para proteger sus datos.

La cafetería tiene muchos artículos, como cafeteras, pastelillos, dinero en las cajas registradoras, etc. Puede considerar estos elementos como datos. Los propietarios de la cafetería quieren asegurarse de que todos estos artículos estén seguros, tanto si están almacenados como si los están transportando entre tiendas.

Del mismo modo, debe asegurarse de que los datos de las aplicaciones estén seguros mientras están almacenados (cifrado en reposo) y mientras se transmiten, lo que se conoce como cifrado en tránsito.

AWS Key Management Service (AWS KMS) le permite realizar operaciones de cifrado mediante el uso de llaves criptográficas. Una llave criptográfica es una cadena aleatoria de dígitos que se utiliza para bloquear (cifrar) y desbloquear (descifrar) datos. Puede utilizar AWS KMS para crear, administrar y utilizar llaves criptográficas. También puede controlar el uso de claves en una amplia gama de servicios y en sus aplicaciones.

Con AWS KMS obtiene más control sobre el acceso a los datos que cifra. Puede utilizar las características criptográficas y administración de claves directamente en sus aplicaciones o a través de los servicios de AWS que están integrados con AWS KMS. Tanto si escribe aplicaciones para AWS como si usa los servicios de AWS, AWS KMS le permite mantener el control sobre quién puede usar sus AWS KMS keys y obtener acceso a sus datos cifrados.

Con AWS KMS, puede elegir los niveles específicos de control de acceso que necesita para sus claves. Por ejemplo, puede especificar qué usuarios y roles de IAM pueden administrar claves. Alternativamente, puede deshabilitar temporalmente las claves para que nadie las pueda utilizar. Las claves nunca salen de AWS KMS y siempre tiene el control de ellas.

AWS KMS está integrado con la mayoría de los demás servicios de AWS que cifran sus datos. Está integrado con AWS CloudTrail para registrar el uso de sus claves KMS para las necesidades de auditoría, regulación y cumplimiento. Al usarlo con CloudTrail, puede monitorear e investigar cómo y cuándo se usaron sus claves KMS y quién las usó.

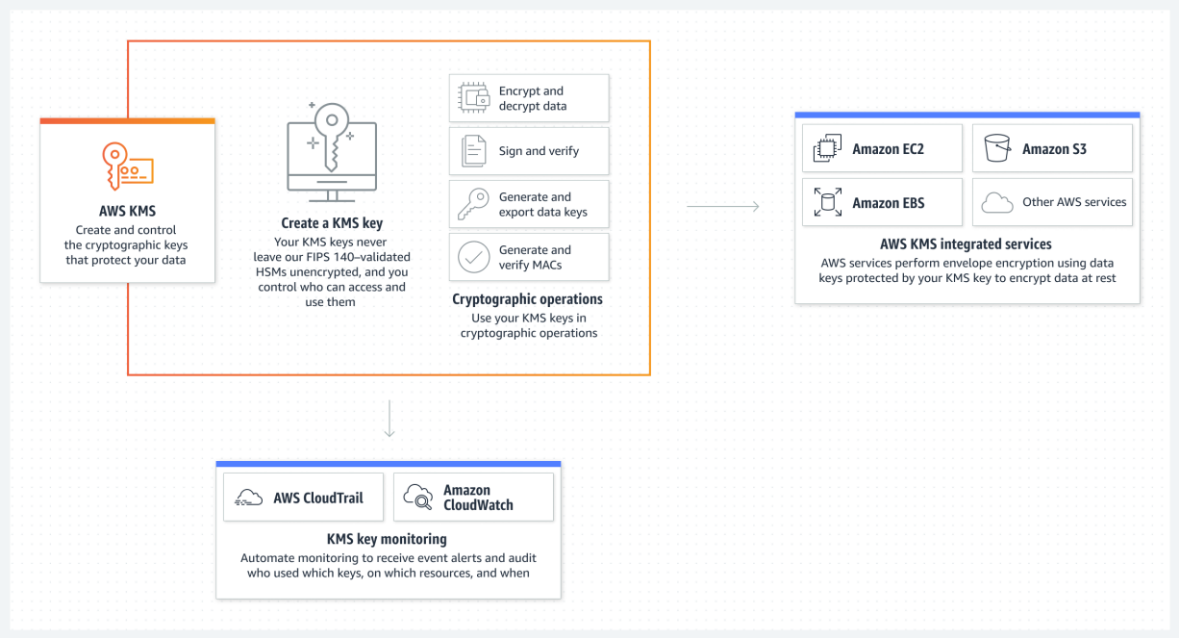
FUNCIONAMIENTO DE AWS KMS

En el diagrama se muestran las características clave de AWS Key Management Service y las integraciones disponibles con otros servicios de AWS. Se muestran tres secciones.

La primera sección se titula “AWS KMS”, con una ilustración del icono de arquitectura de AWS KMS y el texto “Cree y controle las claves criptográficas que protegen sus datos”. A la derecha, aparece un cuadro titulado “Crear una clave de KMS” con el texto “Sus claves de KMS nunca dejan nuestros HSM validados con FIPS 140 sin cifrar; además, usted controla quién puede acceder a ellas y utilizarlas”. A la derecha, aparece otro encabezado, “Operaciones criptográficas”, con el texto explicativo “Utilice sus claves de KMS en operaciones criptográficas”. La primera sección, además, enumera las características clave de AWS KMS. Estas son las características: “Cifrar y descifrar datos”, “Firmar y verificar”, “Generar y exportar claves de datos” y “Generar y verificar MAC”.

Debajo de la primera sección se encuentra el título “Monitoreo de claves de KMS” con el texto explicativo “Automatice el monitoreo para recibir alertas de eventos y auditar quién utilizó cuáles claves, en qué recursos y cuándo”. Se enumeran dos servicios con sus respectivos íconos de arquitectura: AWS CloudTrail y Amazon CloudWatch.

A la derecha de estas dos secciones se encuentra la tercera y última sección. El título es “Servicios integrados de AWS KMS” con el siguiente texto: “Los servicios de AWS realizan un cifrado de sobre con claves de datos protegidas por sus claves de KMS para cifrar datos en reposo”. Estos son los servicios enumerados: Amazon EC2, Amazon S3, Amazon EBS y otros servicios de AWS.



CASOS DE USO DE AWS KMS

Proteja los datos en reposo: Active el cifrado del lado del servidor mediante AWS KMS con claves de KMS que puede controlar y administrar.

Cifrar y descifrar datos: Utilice SDK de cifrado de AWS para administrar de manera segura operaciones criptográficas con sus aplicaciones.

Firmar y verificar firmas digitales: Proteja operaciones de firma con AWS KMS mediante claves KMS asimétricas.

Crear bases de datos seguras para múltiples usuarios: Utilice el SDK de cifrado de bases de datos de AWS para cifrar de forma sencilla y buscar de forma segura los registros confidenciales de sus bases de datos.

AWS SECRETS MANAGER

AWS Secrets Manager ayuda a gestionar, recuperar y rotar las credenciales de las bases de datos, las credenciales de las aplicaciones, los tokens de OAuth, las claves de API y otros datos secretos a lo largo de sus ciclos de vida. Muchos AWS servicios almacenan y utilizan secretos en Secrets Manager.

Secrets Manager ayuda a mejorar la posición de seguridad, ya que ya no necesita credenciales de codificación rígida en el código fuente de la aplicación. El almacenamiento de las credenciales en Secrets Manager ayuda a evitar una posible concesión por parte de cualquier persona que pueda inspeccionar la aplicación o sus componentes. El usuario reemplaza las credenciales de codificación rígida con una llamada de tiempo de ejecución al servicio de Secrets Manager para recuperar las credenciales de forma dinámica cuando las necesita.

Con Secrets Manager, puede configurar un programa de rotación automática para sus secretos. Esto le permite reemplazar secretos a largo plazo con secretos a corto plazo, reduciendo significativamente el riesgo de peligro. Dado que las credenciales ya no se almacenan con la aplicación, su rotación ya no requiere la actualización de las aplicaciones ni la implementación de cambios en los clientes de la aplicación.

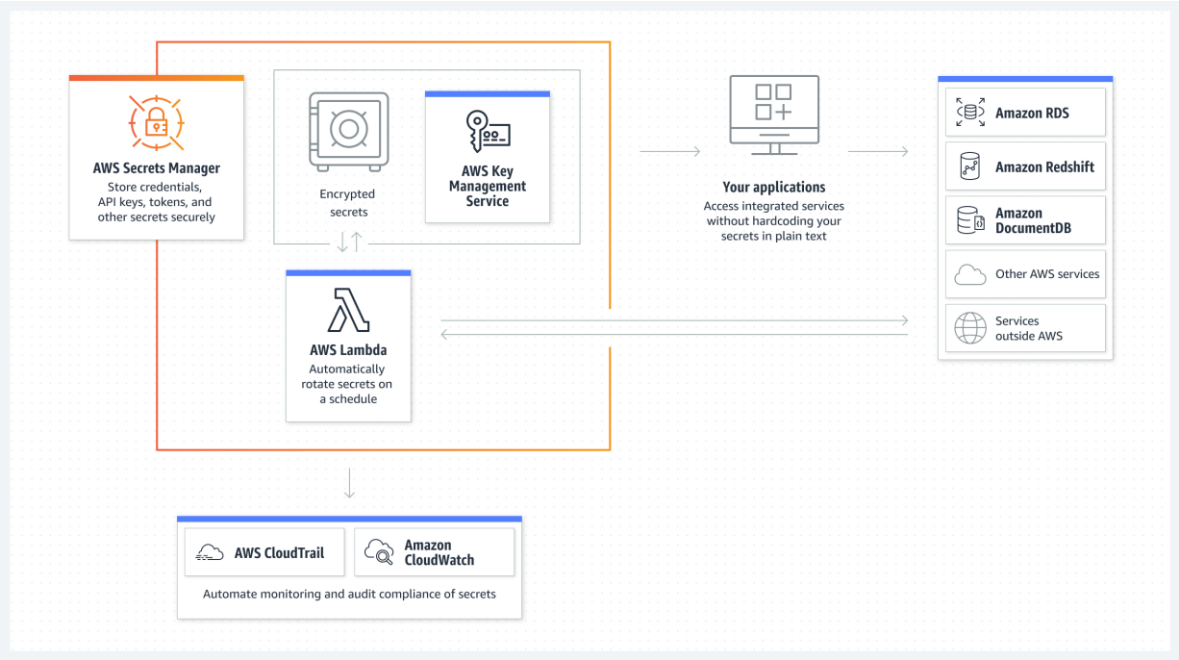
FUNCIONAMIENTO DE AWS SECRETS MANAGER

En el diagrama se muestra el funcionamiento de AWS Secrets Manager.

La primera sección tiene el título «AWS Secrets Manager», con una ilustración del icono arquitectónico de AWS Secrets Manager y el texto «Almacene credenciales, claves de API, tokens y otros secretos de forma segura». En el cuadro de la derecha hay una pequeña ilustración de «Secretos cifrados» junto al icono arquitectónico de AWS Key Management Service. «Secretos cifrados» tiene flechas de doble cara que apuntan a otro icono arquitectónico de AWS Lambda, con un texto explicativo que dice «Rote automáticamente los secretos según un cronograma». El icono de AWS Lambda apunta hacia abajo a dos servicios adicionales y sus respectivos íconos arquitectónicos, AWS CloudTrail y Amazon CloudWatch, y al texto «Automatice el monitoreo y la auditoría del cumplimiento de los secretos».

A la derecha, una ilustración cercana de un escritorio apunta de la primera a la segunda sección. El texto adjunto dice: «Acceda a los servicios integrados sin necesidad de codificar sus secretos en texto plano».

La segunda sección tiene íconos que muestran los servicios de AWS que se integran con AWS Secrets Manager. Los servicios que se enumeran son: Amazon RDS, Amazon Redshift, Amazon DocumentDB, otros servicios de AWS y servicios externos a AWS.



CARACTERÍSTICAS DE AWS SECRETS MANAGER

Proteja el almacenamiento de datos confidenciales: AWS Secrets Manager cifra datos confidenciales en reposo mediante claves de cifrado que posee y almacena en AWS Key Management Service (AWS KMS).

- Cuando recupera un dato confidencial, Secrets Manager lo descifra y lo transmite de forma segura a través de TLS a su entorno local.
- Secrets Manager se integra con AWS Identity and Access Management (AWS IAM) para controlar el acceso al dato confidencial a través de las políticas minuciosas de IAM y de políticas basadas en recursos.

Rotación automática de datos confidenciales sin interrumpir las aplicaciones: Con AWS Secrets Manager, puede rotar datos confidenciales en forma programada o bajo demanda con la consola de Secrets Manager, AWS SDK o la CLI de AWS.

- Secrets Manager admite de forma nativa credenciales rotativas para bases de datos alojadas en Amazon RDS y Amazon DocumentDB y clústeres alojados en Amazon Redshift.
- Puede ampliar Secrets Manager para rotar datos confidenciales que se usan con otros servicios al modificar las funciones de muestra de Lambda.

Replicación automática de datos confidenciales a varias regiones de AWS: Con AWS Secrets Manager, puede replicar automáticamente datos confidenciales a varias regiones de AWS para satisfacer sus requisitos únicos de recuperación de desastres y redundancia entre regiones. Especifique las regiones de AWS en las que se tiene que replicar un dato confidencial para que Secrets Manager cree réplicas de lectura regionales de forma segura, lo que elimina la necesidad de mantener una solución compleja para esta funcionalidad. Puede dar a sus aplicaciones de varias regiones acceso a datos confidenciales replicados en las regiones requeridas y confiar en Secrets Manager para mantener las réplicas sincronizadas con el dato confidencial principal.

Recuperación de datos confidenciales mediante programas: Cree aplicaciones priorizando la seguridad de los datos confidenciales.

- Secrets Manager proporciona ejemplos de código para llamar a las API de Secrets Manager desde lenguajes de programación comunes. Hay dos tipos de API para recuperar secretos:
    - Recupere un único secreto por nombre o ARN.
    - Recupere un grupo de secretos mediante una lista de nombres o ARN, o al filtrar criterios, como etiquetas.
- Configure los puntos de conexión de Amazon Virtual Private Cloud (Amazon VPC) para que mantengan el tráfico entre su VPC y Secrets Manager en la red de AWS.
- También puede usar las bibliotecas de almacenamiento en caché por parte del cliente de AWS Secrets Manager para mejorar la disponibilidad y reducir la latencia durante la recuperación de datos confidenciales.

Audite y supervise el uso de datos confidenciales: AWS Secrets Manager le permite auditar y supervisar datos confidenciales a través de la integración en los servicios de registro, supervisión y notificación de AWS. Por ejemplo, después de habilitar AWS CloudTrail para una región de AWS, puede auditar cuándo se crea o rota un dato confidencial viendo los registros de AWS CloudTrail. Del mismo modo, puede configurar Amazon CloudWatch para recibir mensajes de correo electrónico con el servicio de notificación simple de Amazon cuando los datos confidenciales permanezcan sin usar durante un tiempo, o puede configurar eventos de Amazon CloudWatch para recibir notificaciones automáticas cuando Secrets Manager los rota.

Conformidad: Puede usar AWS Secrets Manager para cumplir con los requisitos de conformidad.

- Use las reglas de AWS Config para poder verificar que los datos confidenciales se configuran según los requisitos de conformidad y seguridad de su organización.
- Administre los datos confidenciales de las cargas de trabajo que están sujetas a la Guía de Requisitos de Seguridad para la Computación en la Nube del Departamento

de Defensa (DoD CC SRG IL2, DoD CC SRG IL4 y DoD CC SRG IL5), el Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP), la Ley de Responsabilidad y Portabilidad de Seguros de Salud (HIPAA) de Estados Unidos, el Programa de Asesores Registrados para la Seguridad de la Información (Information Security Registered Assessors Program, IRAP), el Informe de auditoría de proveedores de servicios externos (Outsourced Service Provider's Audit Report, OSPAR), las normas ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 9001, el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS) o los Controles de Sistemas y Organizaciones (System and Organization Controls, SOC).

Integración de Secrets Manager: Los servicios de AWS se integran con Secrets Manager para administrar de manera segura las credenciales. Estas integraciones le ayudan a intercambiar credenciales con varios servicios de AWS. Las credenciales almacenadas en Secrets Manager se cifran mediante las claves de KMS administradas por AWS o las claves administradas por el cliente. Secrets Manager rota los datos confidenciales de manera periódica con el fin de mantener elevada la seguridad. Una vez que los datos confidenciales se almacenen con Secrets Manager, podrá proporcionar el ARN de uno de estos en lugar de la credencial en texto sin formato cuando lo requiera un servicio de AWS.

CASOS DE USO DE AWS SECRETS MANAGER

Almacene datos confidenciales de manera segura: Almacene y administre las credenciales, llaves API y otros datos confidenciales de manera centralizada.

Administre el acceso con políticas específicas: Utilice las políticas de permisos de AWS Identity and Access Management (IAM) para administrar el acceso a sus datos confidenciales.

Automatice la rotación de los datos confidenciales: Rote los datos confidenciales bajo demanda o de manera programada, sin re implementar o interrumpir aplicaciones que ya estén activas.

Audite y monitorice el uso de datos confidenciales: Integre los datos confidenciales con los servicios de registro, supervisión y notificaciones de AWS.

AWS SYSTEMS MANAGER PARAMETER STORE

AWS Systems Manager Parameter Store es un servicio que proporciona almacenamiento seguro y jerárquico para la administración de datos de configuración y secretos. Puede guardar datos como contraseñas, cadenas de base de datos, ID de Amazon Machine Image

(AMI) y códigos de licencia como valores de parámetros. Además, puede almacenar estos valores como texto sin formato o datos cifrados. Parameter Store permite hacer referencia a estos parámetros en scripts, comandos y documentos de SSM, facilitando la gestión centralizada y segura de los datos. Es una excelente forma de separar secretos y datos de configuración del código y mejorar la seguridad en tus aplicaciones.

También se integra con Secrets Manager, lo que permite recuperar secretos cuando se utiliza otros servicios de AWS que admiten referencias a los parámetros de Parameter Store. Es una herramienta útil para mantener los secretos seguros en la nube de AWS.

¿QUÉ ES UN PARÁMETRO?

Un parámetro de Parameter Store es cualquier dato guardado en Parameter Store, como un bloque de texto, una lista de nombres, una contraseña, un ID de AMI, una clave de licencia, etc. Puede hacer referencia a estos datos de forma centralizada y segura en sus scripts, comandos y documentos SSM.

Cuando se hace referencia a un parámetro, se debe especificar el nombre del parámetro utilizando la siguiente convención.

{{ssm:parameter-name}}

Parameter Store permite usar tres tipos de parámetros: String, StringList y SecureString.

BENEFICIOS DE PARAMETER STORE

Parameter Store ofrece las siguientes ventajas:

- Utilice un servicio de administración de secretos alojado seguro y escalable, sin servidores que administrar.
- Mejore el nivel de seguridad separando los datos del código.
- Almacene datos de configuración y cadenas seguras en jerarquías y realice un seguimiento de las versiones.
- Controle y audite el acceso granular de forma detallada.
- Almacene los parámetros de forma fiable porque Parameter Store se aloja en varias zonas de disponibilidad en una Región de AWS.

CARACTERÍSTICAS DE PARAMETER STORE

Notificación de cambio: Puede configurar las notificaciones de cambios y active las acciones automatizadas, tanto para los parámetros como para sus políticas correspondientes.

Organización de parámetros: Puede etiquetar los parámetros de manera individual para facilitar la identificación de uno o varios parámetros en función de las etiquetas que les haya asignado. Por ejemplo, puede etiquetar los parámetros de etiqueta para departamentos o entornos específicos.

Versiones de etiquetas: Puede asociar un alias para las versiones del parámetro mediante la creación de etiquetas. Las etiquetas pueden ayudarlo a recordar el propósito de una versión de un parámetro cuando hay varias versiones.

Validación de datos: Puede crear parámetros que apunten a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) y Parameter Store valida estos parámetros para asegurarse de que hace referencia al tipo de recurso esperado, que el recurso existe y que el cliente tiene permiso para usar el recurso. Por ejemplo, puede crear un parámetro con el ID de una Amazon Machine Image (AMI) como un valor con tipo de datos aws:ec2:image, y Parameter Store realiza una operación de validación asíncrona para asegurarse de que el valor del parámetro cumple los requisitos de formato para un ID de AMI y que la AMI específica está disponible en su Cuenta de AWS.

Secretos de referencia: Parameter Store está integrado con AWS Secrets Manager, lo que permite recuperar secretos de Secrets Manager cuando utiliza otros Servicios de AWS que admiten las referencias a los parámetros de Parameter Store.

Compartir parámetros con otras cuentas: Si lo desea, puede centralizar los datos de configuración en una sola cuenta de AWS y compartir los parámetros con otras cuentas que necesiten acceder a ellos.

Accesible desde otros Servicios de AWS: Puede utilizar parámetros de Parameter Store con otras capacidades de Systems Manager y otros Servicios de AWS para recuperar secretos y datos de configuración del almacén central. Los parámetros funcionan con otras funciones de Systems Manager, como Run Command, Automation y State Manager, capacidades de AWS Systems Manager.

Integración con otros Servicios de AWS: Configure la integración con los siguientes Servicios de AWS para el cifrado, la notificación, la supervisión y la auditoría: AWS Key Management Service (AWS KMS), Amazon Simple Notification Service (Amazon SNS), Amazon CloudWatch, Amazon EventBridge y AWS CloudTrail.

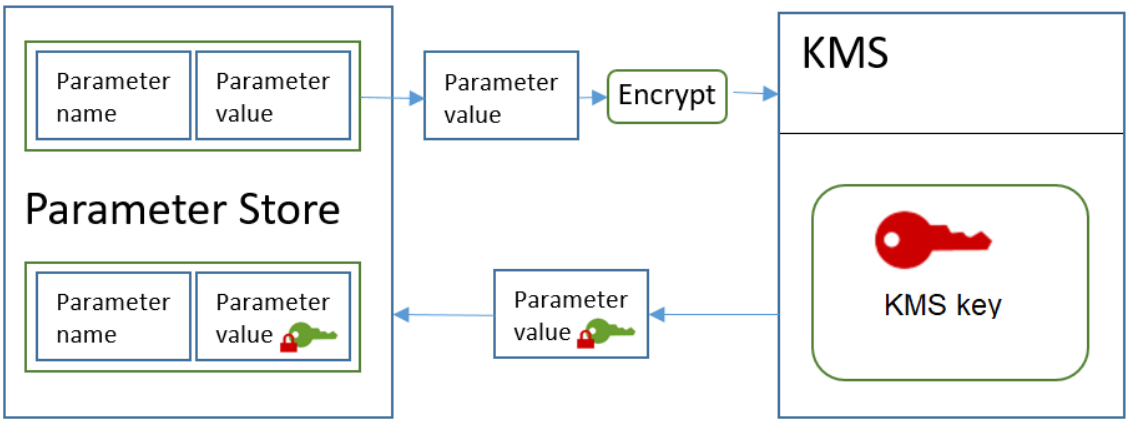
FUNCIONAMIENTO DE PARAMETER STORE

El siguiente flujo de trabajo muestra cómo Parameter Store utiliza una clave KMS para cifrar y descifrar un parámetro de cadena segura estándar.

Cifrar un parámetro estándar:

1. Cuando utiliza PutParameter para crear un parámetro de cadena segura, Parameter Store envía una solicitud Encrypt a AWS KMS. Dicha solicitud incluye el valor del parámetro en texto no cifrado, la clave KMS que ha elegido y el contexto de cifrado de Parameter Store. Durante la transmisión a AWS KMS, el valor en texto no cifrado del parámetro de cadena segura está protegido por seguridad de la capa de transporte (TLS).

2. AWS KMS cifra el valor del parámetro con la clave KMS y el contexto de cifrado especificados. Devuelve el texto cifrado a Parameter Store, que almacena el nombre del parámetro y su valor cifrado.



Descifrar un parámetro estándar

1. Cuando se incluye el parámetro WithDecryption en una solicitud GetParameter, Parameter Store envía una solicitud Decrypt a AWS KMS con el valor del parámetro de cadena segura cifrado y el contexto de cifrado de Parameter Store.

2. AWS KMS utiliza la misma clave KMS y el contexto de cifrado proporcionado para descifrar el valor cifrado. Devuelve el valor del parámetro en texto no cifrado (descifrado) a Parameter Store. Durante la transmisión, los datos en texto no cifrado están protegidos por TLS.

3. Parameter Store devuelve el valor del parámetro en texto no cifrado en la respuesta de GetParameter.

CONCLUSIONES

- El cifrado de datos es esencial para mantener la confidencialidad, la integridad y la privacidad de la información, así como para generar confianza entre las marcas y sus clientes.

- AWS Key Management Service (AWS KMS) permite crear, administrar y controlar claves criptográficas en las aplicaciones y en servicios de AWS.

- AWS Secrets Manager protege el acceso a tus aplicaciones y recursos de TI sin la inversión inicial y los costos de mantenimiento continuos de operar tu propia infraestructura. Es una excelente opción para mantener tus secretos seguros.

- Si deseas una forma centralizada de administrar datos de configuración y secretos, AWS Parameter Store es una excelente opción.

- AWS ofrece varias opciones para cifrar datos en reposo y en tránsito, para garantizar la confidencialidad e integridad de la información, evitando que terceros no autorizados accedan o alteren los datos.