Lección 4
Protección de Cuentas y Datos AWS

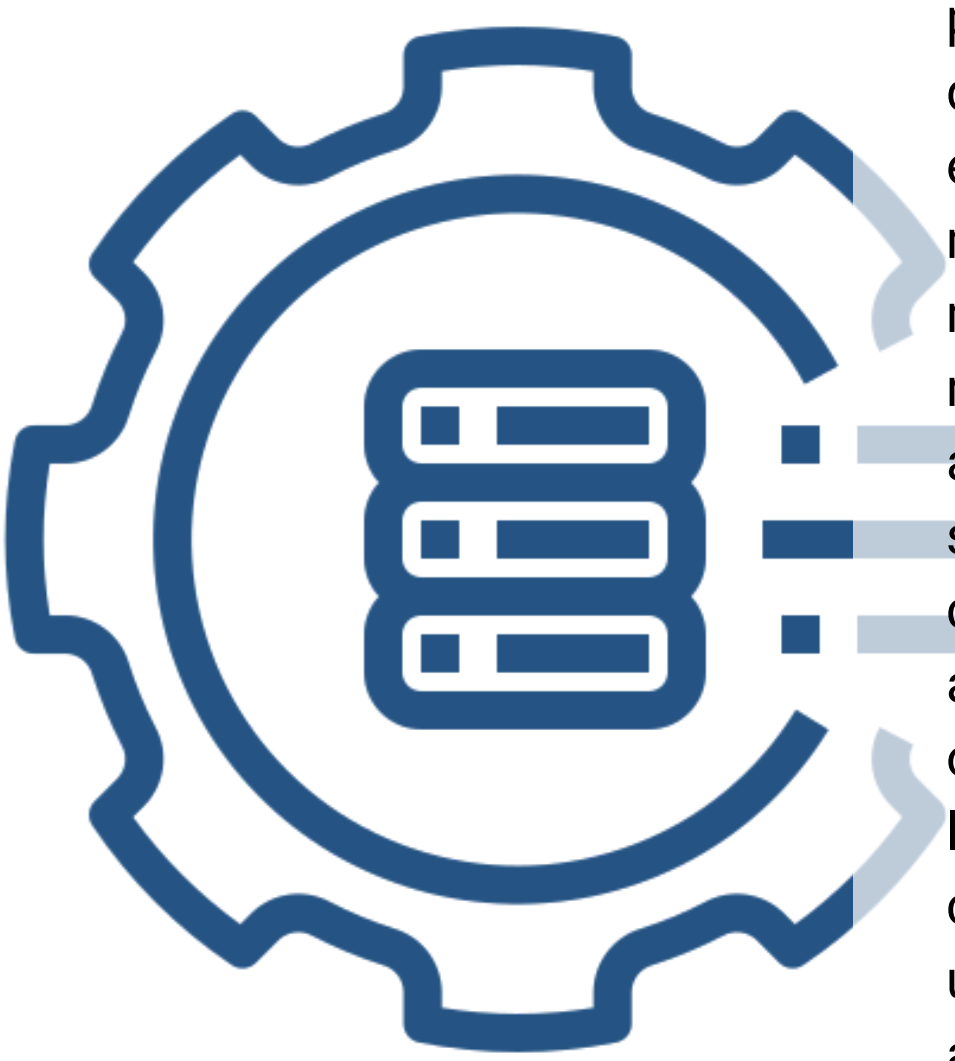
AWS Organizations

AWS Organizations le permite consolidar varias cuentas de AWS para que las administre de forma centralizada.
Características de seguridad de AWS Organizations:

- Agrupa las cuentas de AWS en unidades organizativas (OU) y asocian las difernetes políticas de acceso a cada una de ellas.
- Permite la integración de compatibilidad con IAM.
  - Los permisos para un usuario son la intersección de lo que AWS Organizations permite y lo que IAM concede en esa cuenta.
- Utiliza políticas de control de servicios para establecer el control sobre las acciones de API y los servicios de AWS a los que cada cuenta de AWS puede obtener acceso.

AWS Organizations es un servicio que facilita la gestión centralizada de múltiples cuentas de AWS. En términos de seguridad, ofrece características importantes.

Una característica es la capacidad de organizar cuentas en unidades organizativas (OU) y aplicar políticas de acceso específicas a cada una. Por ejemplo, puede agrupar cuentas con requisitos normativos similares en una OU y luego aplicar una política que restringe su acceso a ciertos servicios de AWS según esos requisitos.
Otra característica es la integración con IAM, lo que permite un control extendido a nivel de cuenta. Esto significa que puede definir qué pueden hacer los usuarios y roles en una cuenta o grupo de cuentas. Los permisos se determinan por la intersección entre las políticas de AWS Organizations y las políticas de IAM asignadas a los usuarios o roles.



Además, AWS Organizations proporciona políticas de control de servicios (SCP) que establecen los permisos máximos para las cuentas miembro. Con las SCP, puede restringir específicamente el acceso a acciones, recursos y servicios de AWS para cada cuenta. Estas restricciones anulan incluso los permisos otorgados explícitamente por los administradores de las cuentas miembro, garantizando un control más estricto sobre el acceso a recursos y servicios de AWS.

AWS Organizations: política de control de servicios

Las políticas de control de servicios (SCP) ofrecen control centralizado sobre las cuentas.
- Limita los permisos disponibles en una cuenta que forma parte de la organización.

Garantiza que las cuentas cumplan con las directrices de control de acceso.
Las SCP son similares a las políticas de permisos de IAM:
- Utilizan una sintaxis similar.
- Sin embargo, una SCP nunca concede permisos
- En su lugar, las SCP especifican los permisos máximos para una organización.

Aquí se ofrece un análisis más detallado de la característica de políticas de control de servicios (SCP) de AWS Organizations.

Las SCP ofrecen control central de los permisos máximos disponibles para todas las cuentas de la organización. De esta manera, le permite asegurarse de que sus cuentas cumplan en todo momento las directrices de control de acceso de la organización. Las SCP solo están disponibles en una organización que tiene todas las características habilitadas, incluida la facturación unificada. Las SCP no están disponibles si su organización ha habilitado únicamente las características de facturación unificada. Para obtener instrucciones sobre cómo habilitar las SCP, consulte Habilitación y deshabilitación de un tipo de política en un nodo raíz.

Las SCP son similares a las políticas de permisos de IAM y utilizan prácticamente la misma sintaxis. Sin embargo, una SCP nunca concede permisos. Las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). Asociar una SCP al nodo raíz de la organización o a una unidad organizativa (OU) establece una protección para las acciones que pueden realizar las cuentas del nodo raíz de la organización o la unidad organizativa. Sin embargo, no sustituye las configuraciones de IAM bien administradas dentro de cada cuenta. Además, tendrá que asociar políticas de IAM a los usuarios y a los roles de las cuentas de la organización para concederles realmente los permisos.

AWS Key Management Service (AWS KMS)

AWS Key Management Service (AWS KMS)

Responsabilidades de los clientes:

- Sistema operativo de la instancia de Amazon Elastic Compute Cloud (Amazon EC2)
  - Incluidos los parches y el mantenimiento
- Aplicaciones
  - Contraseñas, acceso basado en roles, etc.
- Configuración del grupo de seguridad
- SO o firewalls basados en host
  - Incluidos los sistemas de detección o prevención de instrucciones
- Configuraciones de red
- Administración de cuentas
  - Configuración de inicio de sesión y permisos para cada usuario

AWS Key Management Service (AWS KMS) es un servicio que le permite crear y administrar claves de cifrado, así como controlar el uso del cifrado en una amplia gama de servicios de AWS y sus aplicaciones. AWS KMS es un servicio seguro y resistente que utiliza módulos de seguridad de hardware (HSM) validados según el Estándar de procesamiento de la información federal (FIPS) 140-2 (o en proceso de validación) para proteger sus claves. AWS KMS también se integra AWS CloudTrail para ofrecerle los registros de uso de todas las claves a fin de que satisfagan sus necesidades vinculadas con asuntos normativos y de conformidad.

Las claves maestras de cliente (CMK) se utilizan para controlar el acceso a las claves de cifrado de datos que cifran y descifran los datos. Puede crear nuevas claves maestras cuando lo desee y puede administrar quién tiene acceso a estas claves y en qué servicios se pueden utilizar. Además, puede importar claves de su propia infraestructura de administración de claves en AWS KMS.

AWS KMS se integra a la mayoría de los servicios de AWS, lo que significa que puede utilizar claves maestras de AWS KMS para controlar el cifrado de los datos que almacena en estos servicios. Para obtener más información, consulte las características de AWS Key Management Service.

Amazon Cognito

Características de Amazon Cognito:

- Incorpora control de acceso, inicio de sesión y registro de usuarios a sus aplicaciones web y móviles.
- Escala a millones de usuarios.
- Admite el inicio de sesión con proveedores de identidad social, como Facebook, Google y Amazon; y proveedores de identidades empresariales, como Microsoft Active Directory a través del lenguaje de marcado para confirmaciones de seguridad (SAML) 2.0.

Amazon Cognito proporciona herramientas para administrar el acceso a los recursos de AWS desde su aplicación. Le permite definir roles y asignar usuarios a estos roles para que su aplicación solo pueda acceder a los recursos autorizados para cada usuario.

El servicio utiliza estándares comunes de gestión de identidades, como SAML 2.0. SAML es un estándar abierto que facilita el intercambio de información de identidad y seguridad entre aplicaciones y proveedores de servicios. Esto significa que puede utilizar las credenciales de su directorio corporativo, como el nombre de usuario y la contraseña de Microsoft Active Directory, para iniciar sesión en aplicaciones y servicios compatibles con SAML a través de un único inicio de sesión único (SSO).

Amazon Cognito es adecuado para cumplir una variedad de requisitos de seguridad y cumplimiento, incluidos los de sectores altamente regulados como la atención médica y el comercio. Puede utilizarse en entornos que requieren cumplimiento de normativas como HIPAA, PCI DSS, SOC (Control de Organizaciones), ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e ISO 9001.

AWS Shield

Características de AWS Shield:

- Es un servicio administrado de protección contra ataques de denegación de servicio distribuidos (DDoS).
- Protege las aplicaciones que se ejecutan en AWS.
- Proporciona detección permanente y mitigaciones directas automáticas.
- Se puede habilitar AWS Shield Standard sin costo adicional. AWS Shield Advanced es un servicio de pago opcional.

Utilícelo para minimizar el tiempo de inactividad y la latencia de la aplicación.

AWS Shield es un servicio administrado de protección contra ataques de denegación de servicio distribuidos (DDoS) que protege las aplicaciones ejecutadas en AWS. Ofrece detección permanente y mitigaciones directas automáticas que reducen el tiempo de inactividad y latencia de las aplicaciones, por lo que no hay necesidad de contar con AWS Support para disfrutar de la protección de DDoS.

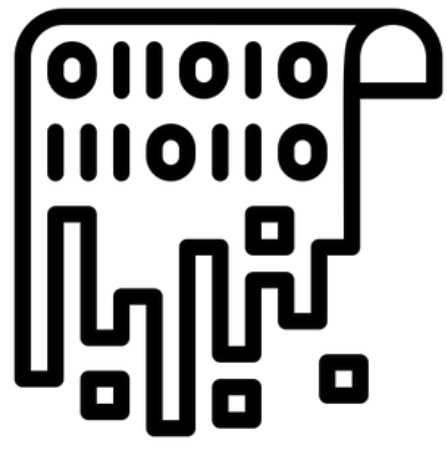
AWS Shield le ayuda a proteger su sitio web de todos los tipos de ataques DDoS, incluidos los ataques en la capa de la infraestructura (como las inundaciones del protocolo de datagramas de usuario o inundaciones [o UDP]), los ataques de agotamiento de estado (como las inundaciones TCP SYN) y los ataques en la capa de la aplicación (como las inundaciones HTTP GET o POST). Para ver ejemplos, consulte la guía para desarrolladores de AWS WAF y AWS Shield Advanced.

AWS Shield Standard se habilita automáticamente para todos los clientes de AWS sin costo adicional.
AWS Shield Advanced es un servicio de pago opcional. AWS Shield Advanced ofrece protecciones adicionales ante los ataques más grandes y sofisticados para las aplicaciones que se ejecutan en Amazon EC2, Elastic Load Balancing, Amazon CloudFront, AWS Global Accelerator y Amazon Route 53. AWS Shield Advanced está disponible para todos los clientes. Sin embargo, para ponerse en contacto con el equipo de respuesta de DDoS, los clientes necesitan contar con Enterprise Support o Business Support de AWS Support.

Cifrado de datos en reposo

El cifrado codifica los datos con una clave secreta, lo que hace que sean ilegibles.
- Solo aquellos que tienen la clave secreta pueden descodificar los datos.
- AWS KMS puede administrar sus claves secretas.

AWS admite el cifrado de datos en reposo.
- Datos en reposo = datos almacenados físicamente (en disco o en cinta)
- Puede cifrar los datos almacenados en cualquier servicio compatible con AWS KMS, como los siguientes:
  - Amazon S3
  - Amazon EBS
  - Amazon Elastic File System (Amazon EFS)
  - Bases de datos administradas de Amazon RDS



El cifrado de datos es una técnica fundamental para salvaguardar información digital. Funciona transformando los datos en un formato ilegible a menos que se disponga de una clave secreta para descifrarlos. De esta manera, incluso si un intruso logra acceder a los datos, no podrá comprender su contenido.

Los datos en reposo son aquellos que se almacenan físicamente en dispositivos de almacenamiento, como discos duros o cintas magnéticas.

Puede crear sistemas de archivos cifrados en AWS para que todos sus datos y metadatos se cifren en reposo mediante el algoritmo de cifrado estándar y abierto Advanced Encryption Standard (AES) de 256 bits. Cuando utiliza AWS KMS, el cifrado y el descifrado se gestionan de forma automática y transparente, por lo que no es necesario modificar sus aplicaciones. Si su organización está sujeta a políticas corporativas o normativas que requieren el cifrado de datos y metadatos en reposo, AWS recomienda que habilite el cifrado en todos los servicios que almacenan sus datos. Puede cifrar los datos almacenados en cualquier servicio compatible con AWS KMS. Consulte cómo los servicios de AWS utilizan AWS KMS para obtener una lista de los servicios admitidos.

Cifrado de datos en tránsito

Cifrado de datos en tránsito (datos que migran a través de una red)

- Transport Layer Security (TLS), anteriormente SSL, es un protocolo estándar abierto.
- AWS Certificate Manager ofrece una forma de administrar, implementar y renovar certificados TLS o SSL

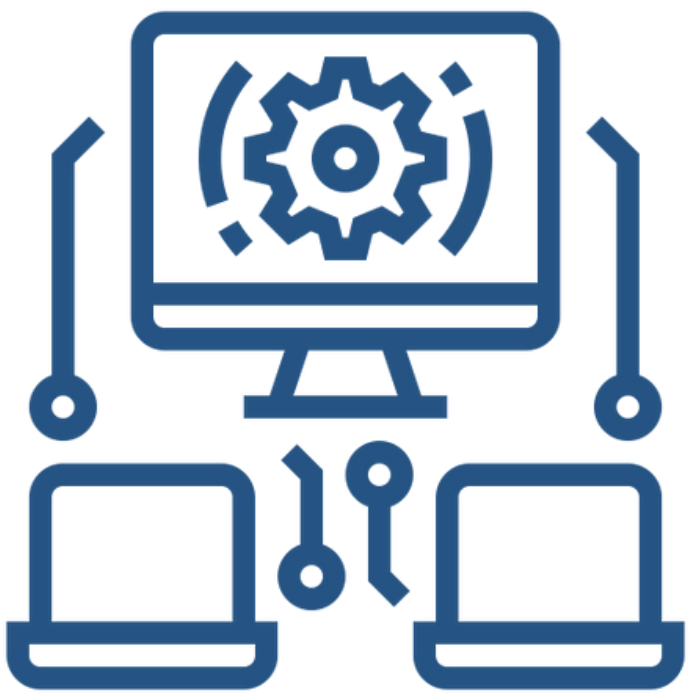
HTTP seguro (HTTPS) crea un túnel seguro.

- Utiliza TLS o SSL para el intercambio bidireccional de datos.

Los servicios de AWS admiten el cifrado de datos en tránsito.

- Dos ejemplos:

Los datos en tránsito se refieren a los datos que se mueven a través de la red. El cifrado de los datos en tránsito se realiza mediante el uso de la seguridad de Transport Layer Security (TLS) 1.2 con un cifrado AES de 256 bits estándar abierto. TLS anteriormente se denominaba capa de conexión segura (SSL).



AWS Certificate Manager es un servicio que le permite aprovisionar, administrar e implementar certificados SSL o TLS para su uso con los servicios de AWS y sus recursos internos conectados. Los certificados de SSL o TLS se usan para proteger las comunicaciones por red y para definir la identidad de sitios web mediante Internet y recursos en redes privadas. Con AWS Certificate Manager, puede solicitar un certificado y, luego, implementarlo en recursos de AWS (como balanceadores de carga o distribuciones de CloudFront). AWS Certificate Manager también se encarga de renovar certificados.

El tráfico web que se ejecuta a través de HTTP no es seguro. Sin embargo, el tráfico que se ejecuta a través de HTTP seguro (HTTPS) se cifra mediante TLS o SSL. El tráfico HTTPS está protegido contra ataques de acceso no autorizados y ataques de intermediario debido al cifrado bidireccional de la comunicación.
Los servicios de AWS admiten el cifrado de datos en tránsito. Se muestran dos ejemplos de cifrado para datos en tránsito. El primer ejemplo muestra una instancia EC2 que ha montado un sistema de archivos compartidos de Amazon EFS. Todo el tráfico de datos entre la instancia y Amazon EFS se cifra mediante TLS o SSL. Para obtener más información acerca de esta configuración, consulte Cifrado de datos de EFS en tránsito.

El segundo ejemplo muestra el uso de AWS Storage Gateway, un servicio de almacenamiento en la nube híbrida que proporciona acceso en las instalaciones al almacenamiento en la nube de AWS. En este ejemplo, la gateway de almacenamiento está conectada a través de Internet a Amazon S3 y la conexión cifra los datos en tránsito.

Protección de buckets y objetos de Amazon S3

Los buckets y objetos de S3 recientemente creados son privados y están protegidos de forma predeterminada.
Cuando los casos de uso requieren compartir objetos de datos en Amazon S3:

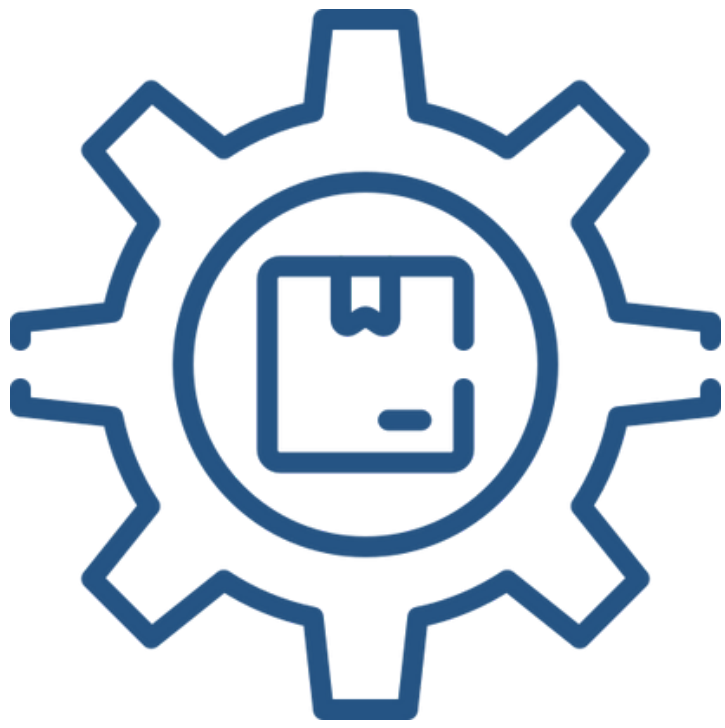
- Es fundamental administrar y controlar el acceso a los datos.
- Siga los permisos que siguen el principio de privilegio mínimo y considere la posibilidad de utilizar el cifrado de Amazon s3.

Entre las herramientas y opciones para controlar el acceso a los datos de S3 se incluyen las siguientes:

- Características de Amazon S3 Block Public Access: es fácil de usar.
- Políticas de IAM: son una buena opción cuando el usuario puede autenticarse en IAM.
- Políticas de buckets
- Listas de control de acceso (ACL): son un mecanismo de control de acceso heredado.

Comprobación de permisos del bucket de AWS Trusted Advisor: es una característica gratuita.

De forma predeterminada, todos los buckets de Amazon S3 son privados y solo pueden acceder los usuarios a los que se les concede acceso explícitamente. Es fundamental administrar y controlar el acceso a los datos de Amazon S3.



AWS proporciona muchas herramientas y opciones para controlar el acceso a sus buckets u objetos de S3, entre los que se incluyen los siguientes:

- El uso de Amazon S3 Block Public Access. Esta configuración anula cualquier otra política o permisos de objetos. Habilite Block Public Access para todos los buckets que no desee que sean accesibles públicamente. Esta característica proporciona un método sencillo para evitar la exposición no deseada de datos de Amazon S3.
- La escritura de políticas de IAM que especifiquen los usuarios o roles que pueden obtener acceso a buckets y objetos específicos. Este método se ha tratado en detalle anteriormente en este módulo.
- La escritura de políticas de bucket que definan el acceso a buckets u objetos específicos. Esta opción se suele utilizar cuando el usuario o el sistema no pueden autenticarse mediante IAM. Las políticas de bucket se pueden configurar para conceder acceso entre cuentas de AWS o para conceder acceso público o anónimo a los datos de Amazon S3. Si se utilizan políticas de bucket, deben escribirse detenidamente y probarse en su totalidad. Puede especificar una instrucción de denegación en una política de bucket para restringir el acceso. El acceso estará restringido incluso si los usuarios tienen permisos concedidos en una política basada en identidad asociada a los usuarios.
- Configuración de listas de control de acceso (ACL) en sus buckets y objetos. Las ACL se utilizan con menos frecuencia (las ACL preceden a la IAM). Si utiliza ACL, no establezca un acceso demasiado abierto o permisivo.
- AWS Trusted Advisor proporciona una característica de comprobación de permisos de buckets, que es una herramienta útil para descubrir si alguno de los buckets de su cuenta tiene permisos que conceden acceso global.