LECCIÓN 4: CÓMO SE PROTEGEN LOS DATOS EN TRÁNSITO

¿POR QUÉ SE DEBEN PROTEGER LOS DATOS EN TRÁNSITO?

• Sus comunicaciones pueden pasar por la Internet pública.

• ¿Cuáles son los riesgos a los que están expuestos los datos en tránsito?

• Divulgaciones de información accidentales
• Peligros para la integridad de los datos
• Peligros relacionados con Ia identidad
• Ataques de intermediario (MITM)
• Suplantación de identidad

Los datos en tránsito son datos que se mueven activamente de una ubicación a otra, por ejemplo, a través de Internet o de una red privada. Para asegurar los datos en tránsito, estos se protegen mientras se mueven de una red a otra o se transfieren de un dispositivo de almacenamiento local a uno de almacenamiento en la nube.
Dondequiera que se muevan los datos, las medidas de protección son críticas, ya que a menudo se consideran menos seguros mientras están en movimiento.

Las aplicaciones en la nube suelen comunicarse a través de enlaces públicos, como Internet, por lo que es importante proteger los datos en tránsito cuando ejecuta aplicaciones en la nube. Esto supone proteger el tráfico de red entre clientes y servidores, y el tráfico de red entre servidores.

Mientras se transfieren a través de varias aplicaciones y redes, los datos en tránsito están expuestos a los siguientes riesgos:

Divulgaciones de información accidentales

Peligros para la integridad de los datos

Peligros relacionados con la identidad

Ataques de intermediario (MITM)

Suplantación de identidad

Un ataque de intermediario (MITM) es una forma de ataque cibernético en el que los delincuentes explotan protocolos basados en la web que son débiles para insertarse entre entidades en un canal de comunicación a fin de robar datos. El atacante está en medio de una comunicación en curso entre dos entidades. Este tipo de ataque hace que la red sea vulnerable al análisis y la modificación de paquetes.

PROTECCIÓN DE DATOS EN TRÁNSITO

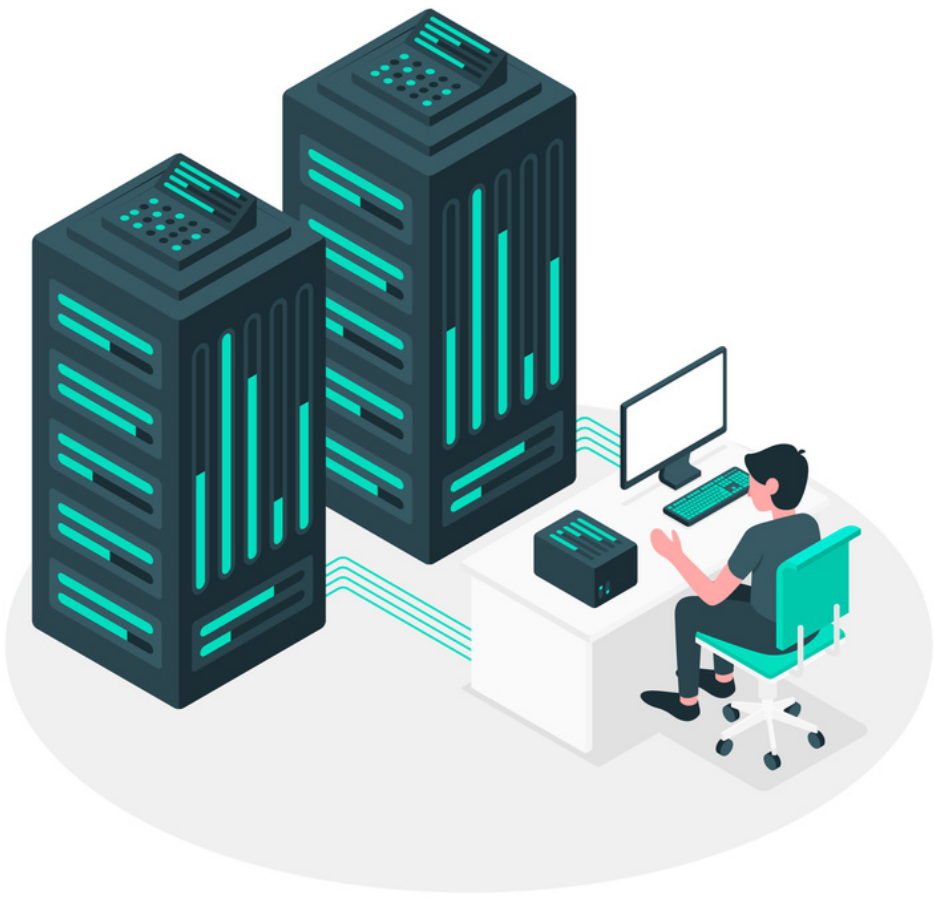
UTILICE PUNTOS DE ENLACE DE SECURE SOCKETS LAYER (SSL) EN LUGAR DE TRANSPORT LAYER SECURITY (TLS) (HTTPS).	UTILICE CIFRADO	UTILICE LOS PUNTOS DE ENLACE DE AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC) PARA LIMITAR EL ACCESO A SU BUCKET.

Puede proteger los datos en tránsito con Secure Sockets Layer (SSL) o el cifrado del lado del cliente. Puede cargar o descargar sus datos de forma segura desde Amazon S3 a través de puntos de enlace SSL utilizando el protocolo HTTPS. El cifrado del lado del cliente protegerá sus datos en tránsito ya que los datos se cifran antes de enviarlos a Amazon S3.

También puede limitar el acceso a un bucket de S3 desde un punto de enlace específico de Amazon Virtual Private Cloud (Amazon VPC) o un conjunto de puntos de enlace mediante el uso de políticas de bucket de S3.

Para proteger los datos en tránsito, AWS recomienda a los clientes que utilicen un enfoque de varios niveles. Todo el tráfico de red entre los centros de datos de AWS se cifra de forma transparente en la capa física. Todo el tráfico dentro de una VPC y entre VPC interconectadas en las regiones de AWS se cifra de forma transparente en la capa de red cuando se utilizan tipos de instancias de EC2 compatibles. En la capa de aplicación, los clientes pueden determinar si usarán el cifrado y cómo lo utilizarán con un protocolo como Transport Layer Security (TLS). Todos los puntos de enlace de servicios de AWS admiten TLS para crear una conexión HTTPS segura para realizar solicitudes de API.

PROTECCIÓN DE CONEXIONES REMOTAS A SERVIDORES



El protocolo de escritorio remoto (RDP) se usa normalmente para servidores de Windows.

- El RDP establece una conexión SSL/TLS subyacente.
- Para mayor seguridad, emita un certificado X.509 de confianza.
- No utilice los certificados autofirmados predeterminados.

Secure Shell (SSH) se usa normalmente para servidores de Linux.

- SSH establece un canal de comunicación seguro.
- Utilice la tunelización para proteger la sesión de la aplicación en tránsito.
- No permita que el usuario raíz use un terminal SSH.
- Asegúrese de que todos los usuarios inicien sesión con un par de claves SSH y luego desactive la autenticación con contraseña.

Los usuarios que acceden a los Servicios de Terminal de Windows en la nube pública suelen utilizar el protocolo de escritorio remoto (RDP) de Microsoft. De forma predeterminada, las conexiones RDP establecen una conexión SSL/TLS subyacente. Para una protección óptima, el servidor de Windows al que se accede debe recibir un certificado X.509 de confianza para protegerlo de la suplantación de identidad o los ataques de intermediario. De forma predeterminada, los servidores RDP de Windows usan certificados autofirmados, que no son de confianza y deben evitarse.

Secure Shell (SSH) es el enfoque preferido para establecer conexiones administrativas a servidores de Linux. SSH es un protocolo que, al igual que SSL, proporciona un canal de comunicación seguro entre el cliente y el servidor. SSH admite la tunelización, que debe usar para ejecutar aplicaciones como X-Windows sobre SSH y proteger la sesión de la aplicación en tránsito. De forma predeterminada, las imágenes de máquina de Amazon (AMI) que proporcionan AWS y la mayoría de los proveedores de AWS Marketplace no permiten que el usuario raíz inicie sesión desde un terminal SSH. La configuración predeterminada para las AMI proporcionadas por AWS es iniciar sesión con un par de claves SSH y la autenticación con contraseña desactivada.

AWS CERTIFICATE MANAGER (ACM)

Proporciona una única interfaz para administrar certificados públicos y privados.

Facilita la implementación de certificados.

Protege y almacena certificados privados.

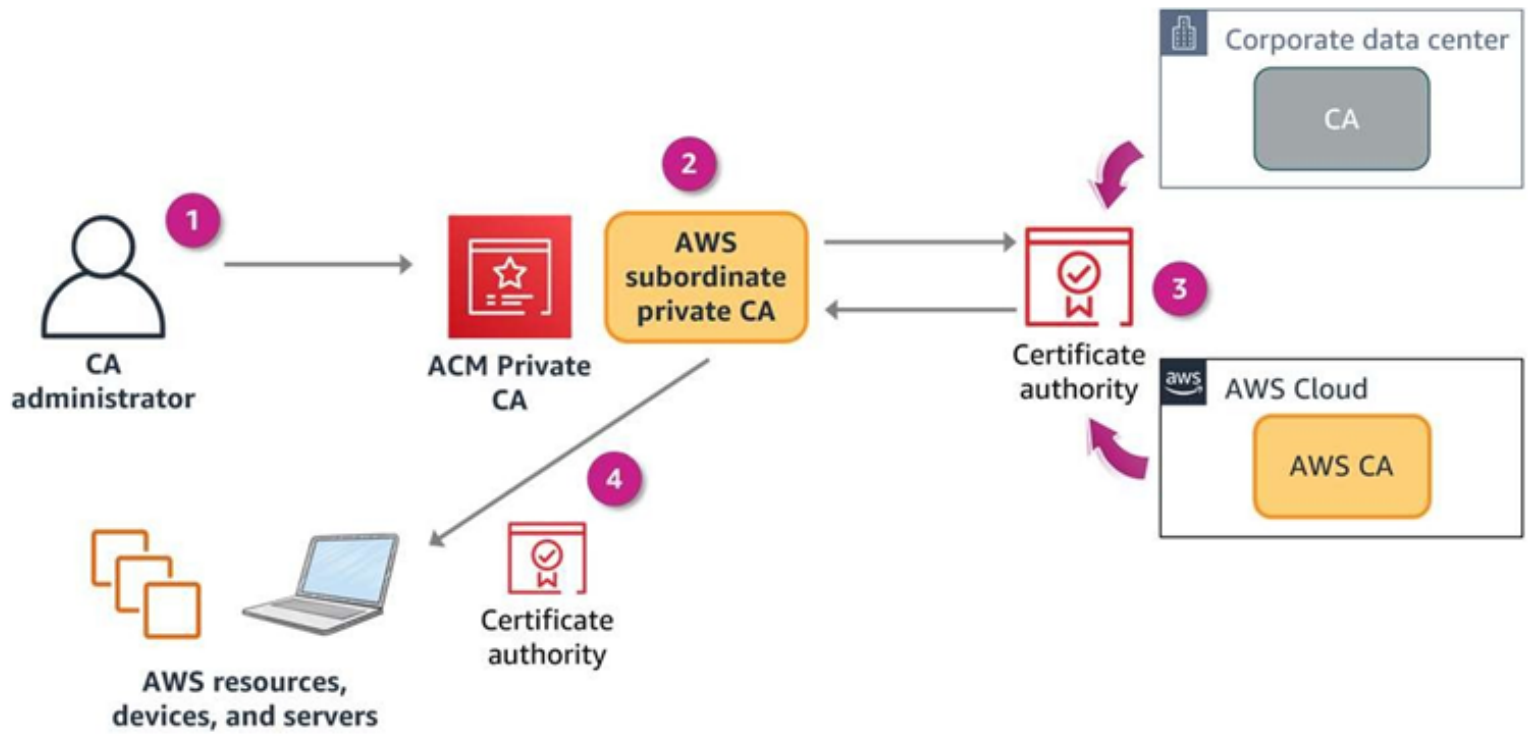
Minimiza el tiempo de inactividad y las interrupciones con renovaciones automáticas.

Al facilitar la habilitación de SSL/TLS, AWS Certificate Manager (ACM) ayuda a las organizaciones a cumplir con los requisitos normativos y de cumplimiento para el cifrado de datos en tránsito. ACM se encarga de la compleja tarea de crear y administrar los certificados SSL/TLS públicos para sus aplicaciones y sitios web basados en AWS. También puede utilizar ACM para emitir certificados SSL/TLS X.509 privados que identifican internamente a los usuarios, equipos, aplicaciones, servicios, servidores y otros dispositivos.

ACM proporciona una única interfaz para administrar certificados públicos y privados. Con ACM, puede crear e implementar certificados públicos y privados de forma sencilla para sus recursos en las instalaciones, como servidores internos y dispositivos de Internet de las cosas (IoT). También puede implementar certificados privados o públicos en recursos de AWS, como equilibradores de carga, distribuciones de Amazon CloudFront y puntos de enlace de Amazon API Gateway mediante la consola de administración de AWS o la API de ACM.

ACM también está diseñado para proteger y administrar certificados privados. El servicio también puede ayudar a minimizar el tiempo de inactividad debido a certificados mal configurados o vencidos. ACM ayuda a resolver los desafíos de mantener certificados, incluidas las renovaciones de certificados, para que no tenga que preocuparse por sus vencimientos. Los certificados renovados se implementan en los recursos de AWS de forma automática.

AWS CERTIFICATE MANAGER PRIVATE CERTIFICATE AUTHORITY

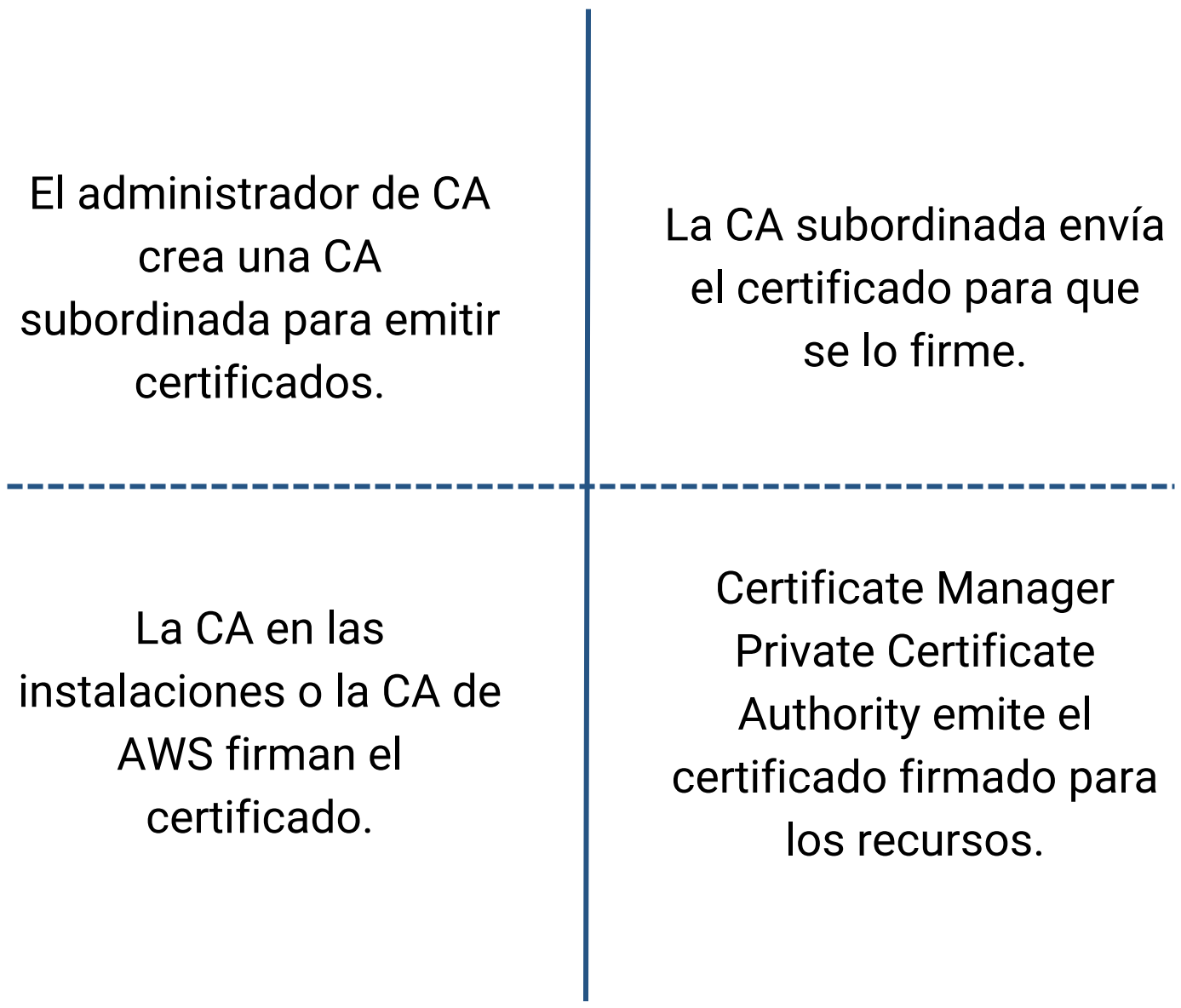


Mediante el uso de AWS Certificate Manager Private Certificate Authority, puede crear jerarquías de autoridades de certificación (CA) privadas, incluidas las CA raíz y subordinadas, sin los costos de inversión y mantenimiento de operar una CA en las instalaciones. Sus CA privadas pueden emitir certificados X.509 de entidad final, que son útiles en escenarios como los siguientes:

Creación de canales de comunicación TLS cifrados	Autenticación de usuarios, equipos, puntos de enlace de API y dispositivos de IoT
Código de firma criptográfica	Implementación del protocolo de estado de certificado en línea (OCSP) para obtener el estado de revocación del certificado

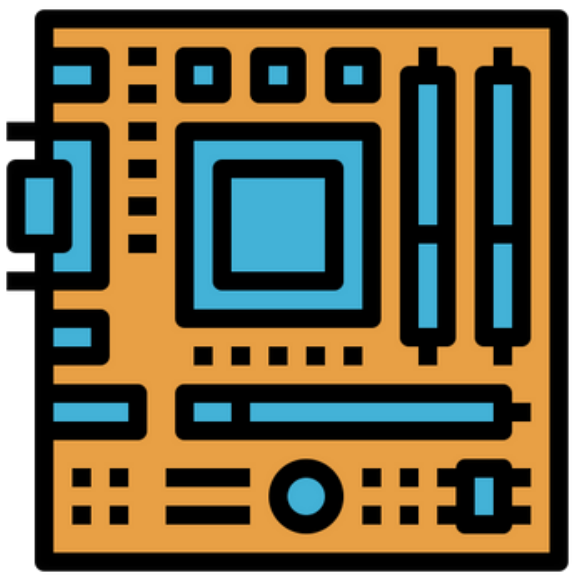
ACM Private CA es para clientes empresariales que crean una infraestructura de clave pública (PKI) dentro de la nube de AWS. El servicio está destinado al uso privado dentro de una organización. Con Certificate Manager Private Certificate Authority, puede crear su propia jerarquía de CA y emitir certificados con ella para autenticar usuarios internos, equipos, aplicaciones, servicios, servidores y otros dispositivos, y para firmar el código de un equipo. Los certificados que emite una CA privada son de confianza solo dentro de su organización, no en Internet. Después de crear una CA privada, tiene la capacidad de emitir certificados directamente (es decir, sin obtener la validación de una CA de terceros) y personalizarlos para satisfacer las necesidades internas de su organización.

El diagrama muestra a Certificate Manager Private Certificate Authority en acción:



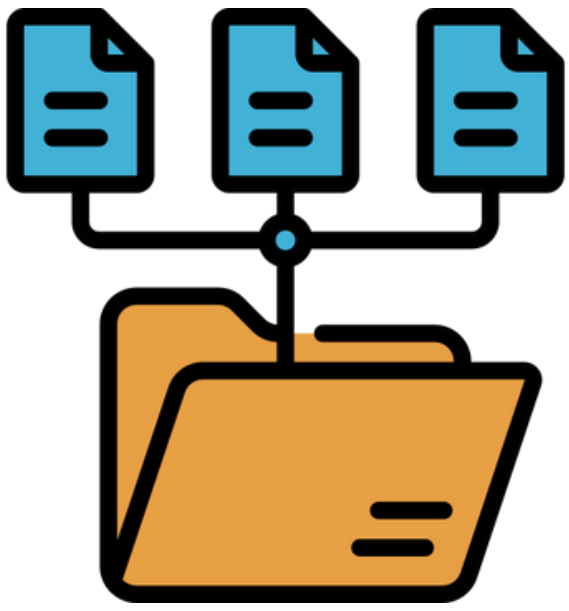
CONSIDERACIONES SOBRE CERTIFICATE MANAGER PRIVATE CERTIFICATE AUTHORITY

MÓDULOS DE SEGURIDAD DE HARDWARE (HSM)



POLÍTICAS DE IAM PARA EL CONTROL DE ACCESO

LISTA DE REVOCACIÓN DE CERTIFICADOS



INFORMES DE AUDITORÍA GENERADOS

Certificate Manager Private Certificate Authority está protegido por HSM. Estos HSM cumplen con los estándares de seguridad establecidos por FIPS 140-2 nivel 3 para ayudar a proteger su CA privada contra peligros relacionados con la clave. Los administradores de CA también pueden controlar el acceso al servicio por medio de políticas de IAM. Certificate Manager Private Certificate Authority publica y actualiza listas de revocación de certificados en un bucket de S3 de manera automática a fin de evitar que se usen certificados revocados. Por ejemplo, una aplicación de IoT puede verificar si el certificado privado de un sensor es válido antes de aceptar los datos procedentes de dicho sensor. Certificate Manager Private Certificate Authority también crea otro bucket de S3 que brinda la capacidad de generar informes de auditoría.

Proteger los servicios internos es un caso práctico frecuente para Certificate Manager Private Certificate Authority. Por ejemplo, un certificado privado resulta útil para proteger las conexiones a sus equilibradores de carga, puntos de enlace de API, aplicaciones y Wi-Fi interno. Este servicio también es un componente de la infraestructura de ACM, que presenta una amplia variedad de usos propios. Los ejemplos incluyen la administración de certificados privados con el beneficio de renovaciones administradas y vinculación de certificados, y la emisión de certificados privados para identificar recursos de AWS, como instancias de EC2, mensajes de Amazon Simple Notification Service (Amazon SNS) o dispositivos de IoT. Certificate Manager Private Certificate Authority también funciona bien para aquellos clientes que quieren obtener un reemplazo para los certificados autofirmados y la automatización por medio de API.