Separación lógica

Una evaluación de los Requisitos de seguridad para la informática en la nube para cargas de trabajo confidenciales del Departamento de Defensa (DoD, por sus siglas en inglés) de EE. UU.

Mayo de 2018

aws

[Series del Manual de AWS para el gobierno]

Avisos

Este documento se suministra únicamente con fines informativos. Representa los actuales productos y prácticas de AWS en el momento de la publicación de este documento que pueden modificarse sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece “tal cual”, sin garantía de ningún tipo, ya sea explícita o implícita. Mediante este documento no genera ninguna garantía, declaración, compromiso contractual, condición ni certeza por parte de AWS, sus filiales, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Contenido

Finalidad

Este artículo examina la equivalencia de seguridad de la separación lógica para clientes que utilizan la infraestructura de Amazon Web Services (AWS) como servicio (IaaS) para el cumplimiento de los requisitos de separación establecidos en la Guía de requisitos de seguridad (SRG) para la informática en la nube del Departamento de Defensa (DoD). El artículo analiza un enfoque de tres pilares, aprovechamiento de la virtualización, cifrado e implementación de capacidad informática a hardware dedicado, que los gobiernos de todo el mundo pueden aprovechar para migrar con confianza cargas de trabajo no clasificadas confidenciales (p. ej., alto impacto) a la nube sin tener que contar con una infraestructura dedicada físicamente.

Introducción

La tecnología en la nube aprovecha las técnicas de transformación en la tecnología de la información (TI). Los clientes que aprovechan la nube pueden beneficiarse de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes del mundo. Los nuevos modelos operativos y las nuevas abstracciones que proporcionan las tecnologías en la nube contribuyen a crear un entorno de TI más seguro. Los CSP como AWS utilizan la nube para innovar, entregando a los clientes características de seguridad nuevas y mejoradas. AWS proporciona servicios disponibles inmediatamente y respalda capacidades de "defensa en profundidad" y "defensa en amplitud" con mecanismos de seguridad intrínsecos de las operaciones y diseños de servicios de la nube.

AWS proporciona a los clientes propiedad y control sobre el contenido mediante el diseño a través de herramientas que permiten a los clientes determinar donde se almacenará su contenido. Las características de AWS permiten a los clientes asegurar su contenido en tránsito y en reposo, así como administrar el acceso de sus usuarios a recursos y servicios de AWS. Los clientes de AWS mantienen el control absoluto sobre el acceso a su contenido lo que evita que clientes y usuarios no autorizados accedan a las cuentas de otros clientes. AWS proporciona servicios para múltiples inquilinos con la mejor seguridad de separación de inquilinos del sector. Esta separación lógica entre entornos de clientes ofrecida por AWS proporciona una seguridad más efectiva y de confianza que la de una infraestructura física dedicada.

Antecedentes

En diciembre de 2011, el director de sistemas de información federal estadounidense estableció una política gubernamental en la que se exigía que las agencias federales utilizaran el Programa federal de administración de riesgos y autorizaciones (FedRAMP, por sus siglas en inglés), un programa federal estandarizado para la autorización de seguridad de servicios en la nube. El enfoque de FedRAMP “de hacer una vez, utilizar muchas veces” se diseñó para ofrecer beneficios significativos, como por ejemplo aumentar la coherencia y la fiabilidad en la evaluación de controles de seguridad, reducir costos para proveedores de servicio y clientes de la agencia y agilizar evaluaciones de autorización duplicadas entre agencias que adquirieran el mismo servicio. El principal organismo para la toma de decisiones y de gobierno del FedRAMP es la Junta de Autorización Conjunta (JAB) formada por los directores de información (CIO) de la Administración de Servicios Generales, el Departamento de Seguridad Nacional y el DoD.

FedRAMP cuenta en la actualidad con tres referencias de seguridad estandarizadas: impactos bajo, moderado y alto, basados en las clasificaciones de la Publicación 199 del Federal Information Processing Standards Publication (FIPS) . Estas referencias se desarrollaron mediante la colaboración con expertos de ciberseguridad del sector privado y el gobierno estadounidense (incluido el DoD). Si bien el DoD ha establecido reciprocidad con la referencia moderada del FedRAMP, no ha establecido reciprocidad con la referencia alta del FedRAMP. En su lugar, el DoD ha desarrollado e implementado lo que es efectivamente un conjunto “FedRAMP plus” de requisitos y controles de seguridad a través de la Guía de requisitos de seguridad (SRG) para la informática en la nube del Departamento de Defensa (DoD).

En particular, el DoD a través de la SRG exige la separación entre el DoD y los inquilinos/misiones del gobierno Federal ya sea mediante métodos físicos o lógicos. De manera más específica, la SRG establece que los "proveedores de servicios en la nube tienen que ofrecer pruebas de monitoreo y controles de separación virtual sólidos, y la capacidad de dar respuesta a solicitudes de registro e incautación sin divulgar información y datos del DoD". Es más, para sistemas de nivel de impacto 5 (IL5),[1] el DoD exige "separación física (p. ej., infraestructura dedicada) de inquilinos ajenos al DoD/al gobierno Federal". Estos requisitos del DoD se centran en la preocupación del DoD con respecto a la mezcla de los datos del DoD con los datos de otros inquilino ante el vertido o la filtración de datos y el acceso no autorizado o la manipulación de datos del DoD por parte de un inquilino ajeno al DoD.

Para implementar una práctica recomendada centrada en los resultados, la SRG reconoció el uso de la separación lógica como enfoque viable para el cumplimiento de los requisitos de separación del IL5 del DoD:

> "Un CSP puede ofrecer soluciones alternativas que proporcionan seguridad equivalente a los requisitos establecidos. La aprobación se evaluará individualmente durante el proceso de evaluación de autorización provisional (AP)".

---

1 5.2.2.2 Requisitos de separación y ubicación de nivel de impacto 5

La información que debe procesarse y almacenarse en el nivel de impacto 5 solo puede procesarse en una infraestructura dedicada, en las instalaciones o fuera de las instalaciones en cualquier modelo de implementación de la nube que restrinja la ubicación física de la información tal y como se describe en la sección 5.2.1 relativa a los requisitos relacionados con la jurisdicción/ubicación, Esto excluye las ofertas de servicios públicos.

Se aplicará lo siguiente:

- Tan solo las nubes comunitaria del gobierno federal, comunitaria del DoD o privada del DoD son elegibles para el nivel de impacto 5.
- Cada modelo de implementación puede admitir varias misiones o inquilinos/misiones para cada organización de clientes.
- Se permite la separación virtual/lógica entre inquilinos/misiones del DoD y el gobierno Federal.
- Se exige como mínimo la separación virtual/lógica entre inquilinos/sistemas de misiones.
- Se exige la separación física (p. ej., infraestructura dedicada) de inquilinos ajenos al DoD/al gobierno Federal.

NOTA: Un proveedor de servicios en la nube (CSP) puede ofrecer soluciones alternativas que proporcionan seguridad equivalente a los requisitos establecidos. La aprobación se evaluará individualmente durante el proceso de evaluación de autorización provisional (AP).

https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf

¿Cuáles son las limitaciones de los requisitos de separación física?

Los requisitos de los productos de nube dedicados físicamente se rigen principalmente por la preocupación en torno al acceso de terceros u otro acceso no autorizado a aplicaciones, contenido o datos, incluido el acceso obligado de las fuerzas de seguridad y el acceso no autorizado de terceros. No obstante, para los sistemas a los que se puede acceder a través de una red o de Internet, la separación física de esos sistemas, como por ejemplo su colocación en una jaula bajo llave o en una instalación de centro de datos separada, no proporciona seguridad añadida o control sobre el acceso. Dicho de manera sencilla, todos los controles de acceso para sistemas conectados se administran a través de controles de acceso lógico, la administración de permisos, el enrutamiento del tráfico de red y el cifrado. AWS aborda cualquier preocupación relativa a la separación física a través de las capacidades de seguridad lógica que proporcionamos a todos nuestros clientes y los controles de seguridad con los que contamos para proteger los datos de los clientes que se describen en más detalle en el enfoque de separación lógica de tres pilares a continuación.

Los entornos más pequeños separados físicamente no tienen paridad con los entornos de la nube disponibles con carácter general; de ahí que cualquier requisito de separación física pueda limitar o retrasar la capacidad del cliente para aprovechar inversiones innovadoras (incluidas innovaciones de características de seguridad) realizadas en nombre de todos los clientes que utilizan servicios de AWS. Entre las ventajas también se incluyen una estructura de costo superior y menor utilización derivada del uso menos eficiente del espacio así como características y opciones de redundancia limitadas en comparación con la diversidad geográfica de regiones de centros de datos comerciales.

¿En qué medida es la separación lógica más efectiva que la separación física?

Los clientes pueden aprovechar el enfoque de tres pilares siguiente para alcanzar con éxito los resultados de seguridad equivalentes a la separación física, necesarios para el nivel de impacto 5 del Departamento de Defensa (DoD IL5).

1. Virtual Private Cloud (VPC): demostración suficiente de que la VPC crea el equivalente de dominios de redes completamente separadas para cada inquilino;
2. Cifrado de datos en reposo y en tránsito: aprovechando capacidades de cifrado intrínsecas o proporcionadas por el usuario de servicios en la nube de AWS como EBS, S3 y DynamoDB, con claves de cifrado generadas y almacenadas por AWS Key Management Service (KMS) o por AWS Cloud Hardware Security Module (CloudHSM); y
3. Hosts dedicados, instancias dedicadas y Bare Metal: los propietarios de misiones del DoD pueden aprovisionar hosts físicos de AWS completos para procesar instancias de máquinas con y sin hipervisor que asignan y las cargas de trabajo asociadas.

1. Virtual Private Cloud (VPC)

AWS VPC permite la creación de un enclave de red separado lógicamente dentro de la red de AWS Elastic Cloud Compute (Amazon EC2) que puede albergar recursos de computación y almacenamiento. Este entorno puede conectarse a la infraestructura existente del cliente a través de una conexión de red virtual privada (VPN) a través de Internet o a través de AWS Direct Connect, un servicio que proporciona conectividad privada a la nube de AWS. El uso de una VPC proporciona a los propietarios de la misión flexibilidad, seguridad y control completo de su presencia de red en la nube. Permite una transición controlada a la nube utilizando un modelo de centro de datos existente del cliente y un esquema de administración. El cliente controla el entorno privado, incluidas las direcciones IP, subredes, listas de control de acceso a la red, grupos de seguridad, firewalls del sistema operativo, tablas de ruteo, VPN o gateways de Internet. Amazon VPC proporciona el aislamiento lógico sólido de todos los recursos del cliente. Por ejemplo, cada flujo de paquetes en la red se autoriza individualmente para validar el origen y el destino correctos antes de su transmisión y entrega. No es posible que la información pase entre múltiples inquilinos si no están autorizados específicamente por los clientes transmisores y receptores. Si se dirige un paquete a un destino sin la regla correspondiente, se descarta el paquete. Es más, si bien los paquetes del protocolo de resolución de direcciones (ARP) disparan una búsqueda autenticada en la base de datos, los paquetes ARP nunca llegan a la red ya que no son necesarios para el descubrimiento de la topología de red virtual, por lo que es imposible que se produzca la suplantación del ARP. Además, el modo promiscuo no revela ningún tráfico salvo el que va hacia el sistema operativo del cliente y desde este. Estos conjuntos precisos de reglas de entrada y salida de tráfico establecidos por el cliente no solo permiten una mayor flexibilidad de conexión, sino que también permite un mayor control por parte del cliente de la segmentación de tráfico y del enrutamiento.

Por ejemplo, las opciones de conectividad de VPC[2] incluyen la capacidad para que el cliente pueda:

- Conectarse a Internet mediante traducción de direcciones de red (subredes privadas): las subredes privadas pueden usarse para instancias que no deberían tener acceso directo a Internet o desde Internet. Las instancias en una subred privada pueden acceder a Internet sin exponer su dirección IP privada dirigiendo su tráfico a través de una gateway de traducción de direcciones de red (NAT) en una subred pública.
- Conectarse de manera segura a su centro de datos corporativo: todo el tráfico hacia y desde instancias en su VPC puede dirigirse a su centro de datos corporativo a través de una conexión de VPN de hardware IPsec cifrada estándar del sector.
- Conectarse de manera privada a otras VPC: interconecte las VPC para compartir recursos entre varias redes virtuales propiedad de sus cuentas AWS.
- Conectar de manera privada sus servicios internos a través de diferentes cuentas y VPC dentro de su propia organización, simplificando de manera significativa su arquitectura de red interna.

---

2 Nota: El uso de VPC con una gateway privada a un punto de accceso a la nube (CAP) aprobado o arquitectura de informática en la nube segura (SCCA) del DoD es obligatorio para todos los clientes que utilizan cargas de trabajo de IL5 de la Guía de requisitos de seguridad (SRG) en la región AWS GovCloud (EE. UU) salvo que sean eximidos por circunstancias especiales por el director de información del DoD.

2. Cifrado de datos en reposo y en tránsito

Para aquellos datos que los propietarios de la misión están almacenando en servicios de almacenamiento de AWS o que transitan en nuestras redes, recomendamos encarecidamente el cifrado para datos en reposo y en tránsito. Para que sea sencillo y seguro para nuestros clientes, proporcionamos una serie de herramientas y características que les permiten cifrar datos, así como varias opciones de infraestructuras de administración de claves de cifrado. Estas características de control de acceso de datos y cifrado ya están integradas en servicios de base como Amazon Simple Storage Service (Amazon S3), un servicio de almacenamiento de objetos muy escalable, Amazon Elastic Block Store (Amazon EBS), que proporciona almacenamiento asociado a la red a instancias EC2 y Amazon Relational Database Service (Amazon RDS), que proporciona motores de bases de datos administradas. Estas características son llave en mano y proporcionan abundante documentación para ayudar a los clientes a comprender cómo se están protegiendo sus datos y las opciones de configuración que pueden controlar para personalizar quién puede acceder a los sistemas. Los servicios nativos de AWS están evolucionando las capacidades de seguridad que, en entornos de legado, solo podían alcanzarse agregando proveedores de terceros. Estas capacidades están ahora cada vez más disponibles lo que permite a los clientes centrarse en la innovación del servicio.

La combinación de AWS Key Management Service (KMS) y AWS CloudHSM son la pieza clave de una solución de cifrado rigurosa. AWS KMS es un servicio regional altamente disponible y completamente administrado que utiliza módulos de seguridad de hardware (HSM) (seguridad física) validados por FIPS 140-2 de nivel 3[3] en su base, con sofisticado software para escalar en horizontal que puede gestionar cientos de miles de solicitudes de API por segundo. Proporciona a los clientes la capacidad de realizar funciones de administración clave de una manera que está totalmente integrada con otros servicios de AWS. AWS CloudHSM proporciona un HSM validado por FIPS 140-2 de nivel 3 (general) dedicado bajo su control exclusivo, directamente en su Amazon Virtual Private Cloud (VPC).[4] El servicio CloudHSM proporciona disponibilidad automatizada, replicación y backup de los HSM de clientes individuales dedicados entre zonas de disponibilidad. Se integra en aplicaciones propiedad del cliente mediante API criptográficas estándares del sector. Si bien son aplicables en diferentes contextos, ambos servicios trabajan para garantizar que el algoritmo de cifrado sea lo suficientemente sólido como para hacer que los datos sean ininteligibles y las claves estén lo suficientemente protegidas como para que personas no autorizadas no puedan leer el texto cifrado. En otras palabras, el almacenamiento de datos cifrados de manera apropiada con claves seguras y administradas correctamente garantiza que los datos están totalmente protegidos. Este enfoque es igual de relevante, aplicable y efectivo independientemente de si se implementa en un entorno de nube comercial aislado de manera física o lógica.

3 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3139

4 https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3108

Con el cifrado, la confidencialidad de las claves criptográficas del propietario de la misión es crucial. La seguridad depende de dónde se cifraron los datos y quién tiene acceso y protege las claves. Si el propietario de la misión cifra los datos antes de su introducción a la nube, no existe motivo alguno por el que el CSP tenga acceso a las claves, el control y la responsabilidad recaen en su totalidad en el propietario de la misión. Por otro lado, si los datos se cifran utilizando servicios inherentes al CSP, entonces tanto el CSP como el propietario de los datos forman parte de la cadena de custodia de las claves. AWS KMS se ha diseñado de manera que nadie, ni siquiera los empleados de AWS, puedan recuperar sus claves de texto no cifrado del servicio. El servicio utiliza los HSM validados por FIPS 140-2 para proteger la confidencialidad y la integridad de sus claves independientemente de si solicita a KMS que cree claves en su nombre o las importa al servicio. Sus claves de texto no cifrado no se escriben nunca en el disco y solo se utilizan en la memoria volátil de los HSM durante el tiempo necesario para realizar la operación criptográfica solicitada. Las claves de KMS no se transmiten nunca fuera de las regiones de AWS en las que se han creado. Las actualizaciones al firmware de KMS HSM se controlan mediante el control de acceso basado en el cuórum auditado y revisado por un grupo independiente dentro de Amazon. Estas políticas, procesos y procedimientos se han auditado y acreditado de manera independiente en virtud del FedRAMP y por parte del Departamento de Defensa (DoD). La sección a continuación resume las capacidades de AWS KMS y AWS CloudHSM. Los clientes pueden remitirse a los enlaces incrustados para obtener recursos adicionales sobre AWS KMS y AWS CloudHSM.

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) proporciona a los clientes control centralizado sobre las claves de cifrado que se utilizan para proteger sus datos. Con AWS KMS, los clientes pueden crear, rotar, inhabilitar, eliminar, definir políticas de uso para el uso de claves de cifrado utilizadas para cifrar los datos de los clientes y realizar auditorías. AWS KMS se integra con servicios de AWS lo cual facilita el cifrado de datos almacenados en estos servicios con claves de cifrado administradas por el cliente (o mediante claves de cifrado predeterminadas que un servicio de AWS administra en nombre del cliente). Este servicio se incluye junto con cinco servicios esenciales que se ha acreditado que cumplen los requisitos del Departamento de Defensa de nivel de impacto 5 (DoD IL5) para habilitar el cifrado de datos en reposo y en tránsito, y proporciona suficiente separación de los datos del DoD que transitan en la infraestructura de AWS y coubicados en hardware con datos del cliente ajenos al DoD. Por ejemplo, en el caso de los datos en reposo, el uso de sólidos algoritmos criptográficos para la separación lógica de los datos del cliente es la base para el establecimiento de equivalencia con la separación física de los datos en reposo, un requisito del IL5.

El límite de seguridad interior de AWS KMS es el módulo de seguridad de hardware (HSM). El HSM tiene una API basada en web interna limitada y ninguna otra interfaz física activa en su estado operativo. Un HSM operativo se configura y carga con claves criptográficas apropiadas durante la inicialización. Los materiales criptográficos confidenciales del HSM solo se almacenan en la memoria volátil y se borran cuando el HSM sale del estado operativo, lo que incluye los cierres o los restablecimientos previstos o no previstos. Cuando se encuentra en estado operativo, ningún operador humano puede acceder al HSM. Solo los hosts de servicio que gestionan las solicitudes de los clientes pueden realizar conexiones a través de la API limitada. Las API de HSM están disponibles a través de una sesión confidencial autenticada mutuamente establecida por operadores humanos (cuando no está operativo) o hosts de servicio (cuando está operativo).

El sistema se ha diseñado de manera que se necesitan varios operadores humanos que utilizan autenticación de dos factores mediante un proceso basado para actualizar la configuración de software o firmware en cualquier KMS HSM pero incluso en ese caso solo después de que se pone en un estado no operativo y no contiene material clave.

> **Nota:** AWS Key Management Service (KMS) utiliza ahora módulos de seguridad de hardware (HSM) validados por FIPS 140-2 y admite puntos de enlace validados por FIPS 140-2, que proporcionan garantías independientes sobre la confidencialidad y la integridad de sus claves.

AWS CloudHSM

AWS CloudHSM ofrece la administración efectiva de claves mediante hardware a escala de la nube para cargas de trabajo confidenciales y reguladas. CloudHSM permite a los propietarios de la misión aprovisionar y aprovechar claves criptográficas para cifrar sus datos dentro de los servicios de AWS y sus aplicaciones residentes. Con CloudHSM, los clientes administran sus propias claves de cifrado mediante un HSM validado por FIPS 140-2 de nivel 3, y ofrece la flexibilidad necesaria para realizar la integración con las aplicaciones que utilizan API estándar del sector como PKCS#11, extensiones de criptografía de Java (JCE) y bibliotecas Microsoft CryptoNG (CNG). También cumple con los estándares y permite a los propietarios de la misión exportar todas las claves a la mayoría de los demás HSM a la venta. CloudHSM es un servicio administrado que automatiza las arduas tareas administrativas, como el aprovisionamiento de hardware, los parches de software, la alta disponibilidad y los backups. Para proteger y aislar su CloudHSM de otros clientes de Amazon, debe aprovisionarse CloudHSM dentro de una VPC.

La separación de obligaciones y el control de acceso basado en roles es inherente al diseño de CloudHSM. AWS tiene acceso limitado al HSM que nos permite monitorear y mantener el estado y la disponibilidad del HSM, realizar backups cifrados, y extraer y publicar registros de auditoría de sus CloudWatch Logs. AWS no puede ver, acceder ni utilizar sus claves ni hacer que su HSM realice operaciones criptográficas con ellas.

3. Hosts dedicados, instancias dedicadas y Bare Metal

Además de proporcionar servicios informáticos para varios inquilinos, aislados lógicamente y muy seguros, AWS también proporciona tres maneras de implementar capacidad informática a hardware dedicado utilizando instancias dedicadas, hosts dedicados y Bare Metal. Estas opciones de implementación se pueden usar para lanzar instancias Amazon EC2 en servidores físicos que están dedicados para su uso. Las instancias dedicadas son instancias Amazon EC2 con hipevisor que se ejecutan en una nube virtual privada (VPC) en hardware dedicado para un único cliente. Las instancias dedicadas están físicamente aisladas en el nivel de hardware de host de las instancias que pertenecen a otras cuentas de AWS. Las instancias dedicadas pueden compartir hardware con otras instancias de la misma cuenta de AWS que no son instancias dedicadas. Un host dedicado también es un servidor físico dedicado para su uso. Con un host dedicado, tiene visibilidad y control sobre el modo en el que las instancias con hipervisor se colocan en el servidor. Las instancias Bare Metal son dispositivos de hardware de host sin hipervisor. El uso de la tecnología AWS Nitro para la descarga de la red y de almacenamiento, así como el chip de seguridad Nitro para eliminar los riesgos asociados con una sola tenencia de serie en Bare Metal, los clientes tienen acceso directo al hardware de Amazon EC2. Estas instancias de Bare Metal son miembros de pleno derecho del servicio Amazon EC2 y tienen acceso a servicios como Amazon VPC y Amazon Elastic Block Store (EBS).[5]

5 En la actualidad, es posible experimentar Amazon EC2 Bare Metal en la familia de instancias I3, dentro del tipo de instancia “i3.metal”.

No hay diferencias de desempeño, seguridad o físicas entre las instancias dedicadas e instancias implementadas en hosts dedicados. No obstante, los hosts dedicados ofrecen a los propietarios de la misión control adicional sobre el modo en el que las instancias se colocan en un servidor físico y cómo se utiliza ese servidor. Cuando usa hosts dedicados, tiene control sobre la ubicación de las instancias en el host mediante los valores de configuración de ubicación automática de instancias y afinidad de hosts. Si su organización desea usar AWS y tiene una licencia de software existente que exige que el software se ejecute en una pieza en particular de hardware durante una cantidad mínima de tiempo. Los hosts dedicados permiten tener visibilidad del hardware del host, lo que posibilita que cumpla esos requisitos para la obtención de la licencia.

¿De qué manera respalda la nube para varios inquilinos las solicitudes de datos por parte de los organismos encargados del cumplimiento de la ley sin divulgar datos del DoD?

AWS cumple las solicitudes de datos de los organismos encargados del cumplimiento de la ley legales. Si bien los sistemas locales suelen permitir a las autoridades incautar o acceder a hardware físico del propietario de los datos, la informática en la nube introduce un modelo diferente desde que los datos se alojan en un entorno para varios inquilinos. La incautación física o el acceso a hardware físico en AWS no es posible porque los datos de un cliente se distribuyen entre diferentes dispositivos físicos, forzando que todas las solicitudes de datos pasen por un proceso de recuperación lógico aprobado y autorizado. A través de nuestra acreditación FedRAMP, AWS cumple con los controles de NIST 800-53 que comprende el marco de referencia moderado de FedRAMP, incluidos los controles de seguridad “Information Handling and Retention” (Gestión y retención de information) y “System and Information Integrity” (Integridad de los sistemas y la información). Esto significa, entre otras cosas, que los servicios de AWS se encuentran entre los límites de diferentes cuentas de los clientes, evitan que se mezclen las cuentas de los clientes y hace que los clientes tengan control absoluto sobre el contenido y las operaciones de sus cuentas de AWS individuales. Los clientes del DoD, al igual que todos los clientes, pueden tener la certeza de que cualquier solicitud legal de los organismos encargados del cumplimiento de la ley se aplicará tan solo a los datos dentro de la cuenta de un cliente objeto de la solicitud. También cumplimos con los controles de "integridad de los sistemas y la información" que exigen que los CSP conformes proporcionen a los clientes acceso a sus datos y exige que las agencias conformes mantengan sus propios datos de conformidad con la legislación aplicable. Además, los controles de "auditoría y responsabilidad" exigen que las organizaciones conserven los registros de auditorías para apoyar las investigaciones de las incidencias de seguridad una vez que se han producido, y para cumplir los requisitos normativos y de la organización para la retención de información. Los clientes pueden recuperar informes y registros de auditorías de la nube aprovechando CloudTrail y CloudWatch Logs, que podrán entregar a continuación a las autoridades correspondientes. Estas soluciones permiten al Departamento de Defensa (DoD) responder directamente a las peticiones de información de los organismos encargados del cumplimiento de la ley y del inspector general, posibilitando que los funcionarios gubernamentales tengan acceso directo a información que podrían necesitar sin tener que decomisar hardware.

AWS también aplica controles y políticas robustas en torno al saneamiento y la destrucción. Por ejemplo, AWS hace un seguimiento, documenta y verifica las acciones de saneamiento y destrucción. El cliente no tiene en ningún momento acceso físico a los medios asignados a su objeto o volumen lógico. Toda retirada y desecho de medios es realizada por personal de AWS designado. El contenido en unidades se trata con el mayor nivel de clasificación de acuerdo con la política de clasificación de datos de AWS. Todos los medios quedan ilegibles y se destruyen al final del ciclo de vida de los medios antes de abandonar una sala del centro de datos de AWS de conformidad con los estándares de seguridad de AWS como parte del proceso de retirada.

¿De qué manera se protege la nube para varios inquilinos frente al acceso no autorizado de terceros, incluido el acceso de los empleados de los proveedores de servicios en la nube, a datos del DoD?

Una preocupación relacionada con la amplitud de la capacidad de los organismos encargados del cumplimiento de la ley para solicitar legalmente datos del cliente es la posibilidad de que un tercero no autorizado acceda al contenido del cliente y la idoneidad de las medidas de control de acceso para prevenir el acceso no autorizado del personal del proveedor de servicios en la nube. No obtenemos acceso a contenido del cliente ni lo utilizamos para ningún fin distinto al exigido legalmente. Lo hacemos para mantener los servicios de AWS y proporcionarlos a nuestros clientes y a sus usuarios finales.

El acceso de los empleados a sistemas de AWS se asigna en función del principio de privilegio mínimo, aprobado por una persona autorizada antes de acceder al aprovisionamiento y supervisado por un empleado de AWS. Las obligaciones y los ámbitos de responsabilidad (por ejemplo, solicitud de acceso y aprobación, solicitud de administración de cambio y aprobación, etc.) deben repartirse entre diferentes personas para reducir las probabilidades de que se produzca una modificación no autorizada o no intencionada, o un uso indebido de sistemas de AWS. El personal de AWS que por motivos de negocio tenga que obtener acceso al plano administrativo tiene que pasar primero una autenticación multifactor, que es diferente de sus credenciales corporativas normales de Amazon, para obtener acceso a hosts administrativos creados expresamente. Estos hosts administrativos son sistemas diseñados, creados, configurados y robustecidos a propósito para proteger el plano administrativo. Todo este acceso está sujeto a registros y auditorías. Cuando un empleado ya no necesite obtener acceso por motivos de negocio al plano administrativo, se le revocan los privilegios y el acceso a estos hosts y a los sistemas pertinentes. AWS ha implementado una política de bloqueo de sesión que se aplica sistemáticamente. El bloqueo de sesión se conserva hasta que se han realizado procedimientos de identificación y autenticación establecidos.

Los clientes administran el acceso al contenido de sus clientes y a los recursos y servicios de AWS. Proporcionamos un conjunto avanzado de características de acceso, cifrado y registro que le ayudarán a llevar esto a cabo de forma eficaz (como AWS CloudTrail, CloudWatch, CloudHSM y AWS KMS según se describe más arriba).

¿Cuáles son las recomendaciones de AWS a los gobiernos que están considerando los requisitos de separación física?

A través del proceso de autorización de Guía de requisitos de seguridad (SRG) para la informática en la nube del Departamento de Defensa (DoD), AWS demostró la suficiencia de la separación lógica para cumplir la intención tras una solicitud de infraestructura dedicada aislada físicamente para las cargas de trabajo no clasificadas más confidenciales del DoD. Nuestro enfoque confirma que los entornos separados lógicamente para múltiples inquilinos que cumplen robustos controles de seguridad pueden proporcionar un nivel de seguridad superior a implementaciones dedicadas en la nube privada, al tiempo que se proporcionan ventajas significativas en disponibilidad, escalabilidad y menor costo. La moderna tecnología para la nube de proveedores establecidos ofrece soluciones novedosas que pueden cumplir el objetivo de seguridad de la tecnología tradicional siempre y cuando los enfoques de acreditación sean lo suficientemente flexibles como para dar cabida a implementaciones alternativas.

Si bien revisar los controles de seguridad puede ser valioso para demostrar la conformidad, nuestra experiencia ha demostrado que las organizaciones que se centran principalmente (y en algunos casos de manera exclusiva) en la implementación de controles tradicionales pueden limitar de manera inadvertida su acceso a excelentes soluciones de seguridad. A medida que los gobiernos evalúan si los proveedores de servicios en la nube cumplen los requisitos en función de conceptos de legado, deberían articular claramente cuál es el resultado de seguridad deseado y permitir que los proveedores de servicios en la nube desarrollen las técnicas óptimas para cumplir (si no superar) dichos resultados. Centrarse en el objetivo de seguridad deseado tras un requisito específico puede ayudar a las agencias federales a centrarse debidamente en los resultados que desean alcanzar en lugar de en los detalles de la implementación.

A medida que los programas de garantía de seguridad maduran y escalan para mantener el rápido ritmo de innovación de la seguridad y las características de la nube, los detalles de la implementación de controles serán cada vez más irrelevantes con respecto a las capacidades con las que cuentan los proveedores de servicios en la nube. El estado final deseado, seguridad en la nube robusta, basada en un marco definido por los desenlaces de seguridad del cliente y las técnicas de seguridad determinadas por los proveedores de servicios en la nube para cumplir esos desenlaces, solo puede producirse como consecuencia del diálogo continuado dentro de la comunidad de partes interesadas de garantías de la nube. Creemos que este enfoque proporcionaría mejoras significativas a la hora de mantener la garantía de la postura de seguridad de un proveedor de seguridad en la nube (CSP).

Además de proporcionar una solución alternativa equivalente desde el punto de vista lógico, AWS utilizó un enfoque integral y participó en sesiones de profundización para abordar plenamente las principales preocupaciones de seguridad del DoD. Empezando por las necesidades del cliente manifestadas en la Guía de requisitos de seguridad (SRG) para la informática en la nube del Departamento de Defensa (DoD), AWS celebró varias sesiones informativas para mostrar a DoD la manera en que nuestro enfoque de tres pilares cumplía la intención de requisito de separación física. El evaluador que validó nuestros servicios también participó en estas sesiones para corroborar la exactitud de nuestras afirmaciones y ofrecer su evaluación basada en riesgos. Estas sesiones de colaboración actuaron como un método valioso y eficiente de asegurar la garantía de seguridad, acelerar la acreditación y, en última instancia, avanzar los objetivos de modernización de TI del DoD.

Nos anima la evolución del DoD hacia la aceptación de innovadoras soluciones que se adaptan a la nube para alcanzar la intención tras los requisitos de separación física en la nube. Estamos comprometidos con la colaboración continuada con los gobiernos de todo el mundo que están evaluando los méritos y prácticas recomendadas del enfoque de equivalencia de separación lógica del DoD.