Amazon Web Services: Información general acerca de los procesos de seguridad

Marzo de 2020

Avisos

Los clientes son responsables de hacer su propia evaluación independiente de la información en este documento. Este documento: (a) solo tiene fines informativos, (b) representa las prácticas y las ofertas de productos de AWS actuales, las cuales están sujetas a cambios sin aviso previo, y (c) no crea compromisos ni promesas de parte de AWS y sus empresas afiliadas, proveedores o licenciantes. Los servicios o los productos de AWS se ofrecen “como son”, sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS frente a sus clientes se rigen por los acuerdos celebrados con AWS, y este documento no forma parte de ningún acuerdo entre AWS y sus clientes, ni lo modifica.

This paper has been archived

For the latest Security, Identity and Compliance content, refer to:

https://aws.amazon.com/architecture/security-identity-compliance/

Contenido

Resumen

Este documento tiene como objetivo responder preguntas, por ejemplo: *¿de qué forma AWS ayuda a garantizar que mis datos estén protegidos?* En concreto, en este documento se describen los procesos de seguridad física y operativa de AWS para la infraestructura de redes y servidores administrada con AWS.

Introducción

Amazon Web Services (AWS) ofrece una plataforma escalable, altamente disponible y confiable de servicios tecnológicos, que proporciona herramientas que permiten a los clientes construir y albergar una gran variedad de aplicaciones. Para AWS, es sumamente importante proteger la confidencialidad, la integridad y la disponibilidad de los sistemas y los datos de los clientes, al igual que conservar su confianza.

Modelo de responsabilidad compartida en torno a la seguridad

Antes de analizar en detalle la forma en que AWS protege los recursos, es importante entender de qué manera la seguridad en la nube difiere un poco de la seguridad en los centros de datos en las instalaciones. Cuando traslada los sistemas informáticos y los datos a la nube, la responsabilidad en torno a la seguridad se empieza a compartir entre el proveedor de servicios en la nube y usted. En este caso, AWS se hace cargo de proteger la infraestructura subyacente que respalda la nube y usted se hace responsable de todo lo que coloque en la nube o conecte a ella. Este modelo de responsabilidad compartida en torno a la seguridad puede reducir la carga operativa de muchas maneras y, en algunos casos, incluso puede mejorar su posición de seguridad predeterminada sin que deba encargarse de tareas adicionales.

F efer to:

ht npliance/

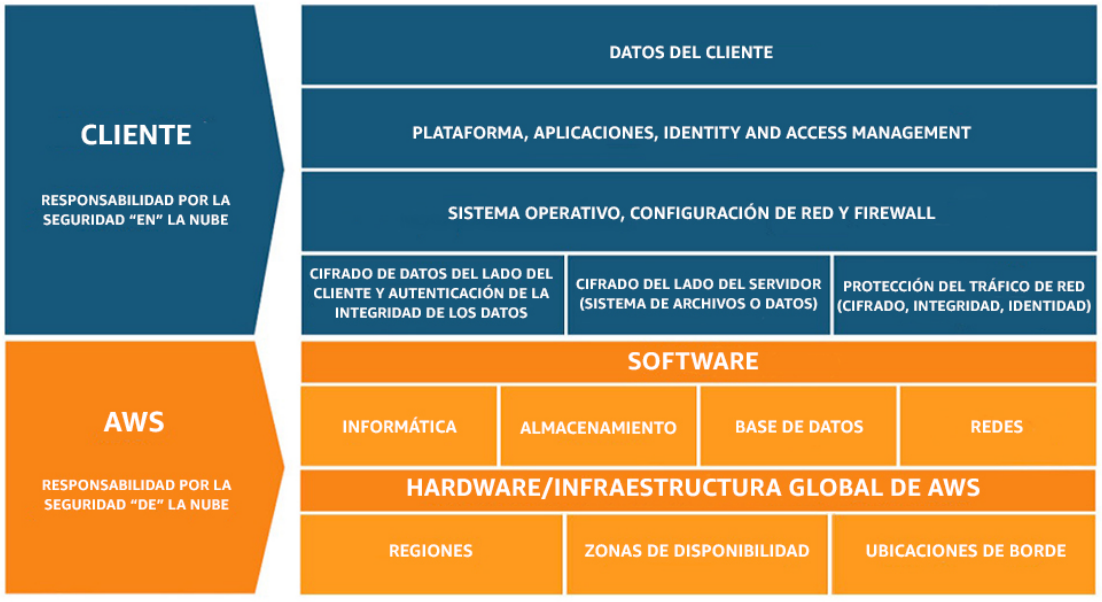


Imagen 1: Modelo de responsabilidad compartida en torno a la seguridad de AWS

La cantidad de tareas de configuración de la seguridad que debe realizar varía según los servicios que seleccione y el grado de confidencialidad de los datos. Sin embargo, hay ciertas características de seguridad (como las credenciales y las cuentas de los usuarios individuales, los protocolos SSL o TLS para las transmisiones de datos, y el registro de la actividad del usuario) que debe configurar sin importar el servicio de AWS que utilice. Para obtener más información sobre estas características de seguridad, consulte la sección Características de seguridad de las cuentas de AWS.

Responsabilidades en torno a la seguridad de AWS

Amazon Web Services se hace cargo de proteger la infraestructura global que ejecuta todos los servicios que se ofrecen en la nube de AWS. Esta infraestructura está compuesta por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de AWS. Proteger esta infraestructura es la principal prioridad de AWS. Aunque no pueda visitar nuestros centros de datos o nuestras oficinas para verlo de primera mano, ofrecemos varios informes de auditores externos que han verificado que cumplimos una serie de estándares y normas para la seguridad informática. Para obtener más información, consulte Conformidad de AWS.

Tenga en cuenta que, además de proteger la infraestructura global, AWS se hace cargo de la configuración de la seguridad en sus productos, los cuales se consideran servicios administrados. Entre los ejemplos de estos tipos de servicios se incluyen Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon EMR, Amazon WorkSpaces y varios otros servicios. Estos servicios proporcionan la plataforma y el cliente, los recursos basados en la nube con el beneficio adicional de que están administrados. En estos servicios, AWS administra las tareas de seguridad básicas, como la implementación de parches en las bases de datos y el sistema operativo huésped, la configuración del firewall y la recuperación de desastres. En la mayoría de estos servicios administrados, todo lo que tiene que hacer es configurar controles de acceso lógicos para los recursos y proteger las credenciales de su cuenta. Algunos de ellos pueden necesitar otras tareas, como configurar las cuentas de usuario en la base de datos, pero, en general, el servicio se encarga de las tareas de configuración de la seguridad.

Responsabilidades en torno a la seguridad del cliente

Con la nube de AWS, puede aprovisionar servidores virtuales, almacenamiento, bases de datos y escritorios en cuestión de minutos en lugar de semanas. También puede utilizar herramientas de flujo de trabajo y analítica basadas en la nube para

procesar los datos según los necesite y, luego, almacenarlos en sus propios centros de datos o en la nube. Los servicios de AWS que utilice determinarán la cantidad de tareas de configuración que tendrá que realizar como parte de sus responsabilidades en torno a la seguridad.

Los productos de AWS que forman parte de la categoría conocida de infraestructura como servicio (IaaS), tales como Amazon EC2, Amazon VPC y Amazon S3, están completamente bajo su control y necesitan que realice todas las tareas necesarias de administración y configuración de la seguridad. Por ejemplo, en las instancias EC2, usted se encarga de la administración del sistema operativo huésped (incluidas las actualizaciones y los parches de seguridad), todo el software de aplicación o las utilidades que instale en las instancias, y la configuración del firewall proporcionado por AWS (denominado grupo de seguridad) en cada instancia. Son básicamente las mismas tareas de seguridad que acostumbra realizar, sin importar dónde se encuentren sus servidores.

Los servicios de AWS administrados, como Amazon RDS o Amazon Redshift, proporcionan todos los recursos necesarios para realizar una tarea específica, pero no incluyen las tareas de configuración que esta conlleva. Con los servicios administrados, no tiene que preocuparse por lanzar o mantener instancias, ni aplicar parches en el sistema operativo huésped o la base de datos, ni replicar las bases de datos. AWS se encarga de todo ello por usted. Pero, como con todos los servicios, debe proteger las credenciales de cada uno de sus cuentas de usuario individuales con Amazon Identity and Access Management (IAM) para que cada uno de los usuarios tenga sus propias credenciales y pueda aplicar la fundamental de distribución de tareas. También se recomienda utilizar la autenticación multifactor (MFA) en cada cuenta, lo que requiere el uso de SSL o TLS para establecer la comunicación con sus recursos de AWS. Además, se recomienda configurar el registro de la actividad del usuario o la API con AWS CloudTrail. Para obtener más información sobre las medidas adicionales que puede tomar, consulte el documento técnico Prácticas recomendadas para la seguridad de AWS y la lectura recomendada en la página web Recursos de seguridad de AWS.

Seguridad de la infraestructura global de AWS

AWS opera la infraestructura global en la nube que utiliza para aprovisionar una serie de recursos informáticos básicos, como el procesamiento y el almacenamiento. La infraestructura global de AWS incluye las instalaciones, la red, el hardware y el

software operativo (por ejemplo, el sistema operativo host, el software de virtualización, etc.) que permiten el aprovisionamiento y el uso de estos recursos. La infraestructura global de AWS está diseñada y se administra en función de las prácticas recomendadas para la seguridad, así como también una serie de estándares de conformidad en torno a la seguridad. Como cliente de AWS, puede estar seguro de que construye arquitecturas web sobre algunas de las infraestructuras informáticas más seguras del mundo.

Programa de conformidad de AWS

La conformidad de AWS permite a los clientes comprender los controles sólidos establecidos en AWS para mantener la seguridad y la protección de los datos en la nube. Como se crean sistemas a partir de la infraestructura en la nube de AWS, la responsabilidad relacionada con la conformidad se debe compartir. Mediante la combinación de características de servicio centradas en la gobernanza y compatibles con la auditoría con los estándares aplicables de conformidad o auditoría, los habilitadores de conformidad de AWS crean a partir de programas tradicionales, lo que ayuda a los clientes a establecerse y trabajar en un entorno de control de la seguridad de AWS. La infraestructura de TI que AWS ofrece a sus clientes está diseñada y se administra en función de las prácticas recomendadas para la seguridad y una serie de estándares de seguridad de TI, entre los que se incluyen los siguientes:

- SOC 1/SSAE 16/ISAE 3402 (anteriormente SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP y FedRAMP
- CSM del DOD Niveles 1 a 5
- PCI DSS Nivel 1
- ISO 9001/ISO 27001/ISO 27017/ISO 27018
- ITAR
- FIPS 140-2
- MTCS Nivel 3
- HITRUST

Además, la flexibilidad y el control que ofrece la plataforma de AWS permiten a los clientes implementar soluciones que cumplan estándares específicos de diferentes sectores, incluidos los siguientes:

- Servicios de Información de Justicia Penal (CJIS)
- Cloud Security Alliance (CSA)
- Ley de Derechos Educativos y Privacidad Familiar (FERPA)
- Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA)
- Asociación Cinematográfica de Estados Unidos (MPAA)

AWS ofrece una gran variedad de información acerca del entorno de control de la TI a los clientes a través de documentos técnicos, informes, certificaciones y otras declaraciones de terceros. Para obtener más información, consulte Conformidad de AWS.

Seguridad física y del entorno

Los centros de datos de AWS cuentan con tecnología de vanguardia y utilizan enfoques innovadores para la arquitectura y la ingeniería. Amazon tiene muchos años de experiencia en el diseño, la creación y el manejo de centros de datos a gran escala. Esta experiencia se aplicó a la plataforma y la infraestructura de AWS. Los centros de datos de AWS se encuentran en instalaciones que no están catalogadas como pertenecientes a AWS. El acceso físico se controla de forma estricta, tanto en el perímetro como en los puntos de entrada del edificio, con personal de seguridad profesional que utiliza vigilancia por video, sistemas de detección de intrusos y otros medios electrónicos.

El personal autorizado debe atravesar un sistema de autenticación de dos factores como mínimo dos veces para acceder a los pisos del centro de datos. Todos los visitantes deben presentar una identificación, y el personal autorizado los registra y acompaña de forma permanente.

AWS solo ofrece acceso a los centros de datos e información a los empleados y los contratistas cuyas necesidades empresariales sean legítimas para tales privilegios. Cuando las necesidades empresariales de un empleado ya no exigen esos privilegios, su acceso se revoca de inmediato, incluso si continúa siendo un empleado de Amazon o Amazon Web Services. Todo acceso físico a los centros de datos ejercido por los empleados de AWS se registra y audita de forma rutinaria.

Detección y extinción de incendios

Se han instalado equipos automáticos de detección y extinción de incendios para reducir los riesgos. El sistema de detección de incendios utiliza sensores de detección de humo en todos los entornos de centros de datos, espacios de infraestructura mecánica y eléctrica, salas de refrigeración y salas de equipos generadores. Estas áreas están protegidas por sistemas de rociadores de tubería húmeda, de acción preventiva con doble bloqueo o de gases.

Energía

Los sistemas de energía eléctrica en los centros de datos están diseñados para que sean completamente redundantes y se puedan mantener sin perjudicar a las operaciones, las 24 horas del día, los siete días de la semana. Las unidades del sistema de alimentación ininterrumpida (SAI) proporcionan energía de respaldo en caso de una falla eléctrica para cargas críticas y esenciales en la instalación. Los centros de datos utilizan generadores para proporcionar energía de respaldo a todas las instalaciones.

Clima y temperatura

Se debe controlar el clima a fin de mantener una temperatura operativa uniforme para los servidores y otros dispositivos, lo que evita el sobrecalentamiento y reduce la posibilidad de interrupciones en el servicio. Los centros de datos están preparados para mantener las condiciones atmosféricas en niveles óptimos. El personal y los sistemas monitorean y controlan la temperatura y la humedad en niveles apropiados.

Administración

AWS monitorea los sistemas y los equipos eléctricos, mecánicos y esenciales para que todos los problemas se identifiquen de inmediato. Se realiza un mantenimiento preventivo para sostener la operatividad continua de los equipos.

Retiro de dispositivos de almacenamiento

Cuando se termina la vida útil de un dispositivo de almacenamiento, los procedimientos de AWS incluyen un proceso de retiro diseñado para evitar que los datos del cliente se expongan a personas no autorizadas. AWS utiliza las técnicas detalladas en la publicación NIST 800-88 (“Pautas para el saneamiento de contenido multimedia”) como parte del proceso de retiro.

Administración de la continuidad del negocio

La infraestructura de Amazon tiene un alto nivel de disponibilidad y ofrece a los clientes las características necesarias para implementar una arquitectura de tecnología informática resiliente. Los sistemas de AWS se han diseñado para tolerar errores en el sistema o el hardware con un nivel de impacto mínimo sobre el cliente. La Administración de la continuidad empresarial de los centros de datos en AWS está a cargo del Grupo de infraestructura de Amazon.

Disponibilidad

Los centros de datos se encuentran repartidos en grupos entre distintas regiones de todo el mundo. Todos los centros de datos se encuentran en línea y a disposición los clientes; ninguno de ellos está “inactivo”. En caso de error, los procesos automatizados alejan el tráfico de datos del cliente del área afectada. Las aplicaciones centrales se implementan en una configuración N+1, de forma que, en el caso de que se produzca un error en el centro de datos, haya capacidad suficiente como para permitir que se equilibre la carga de tráfico entre los demás sitios.

AWS le brinda la flexibilidad necesaria para colocar instancias y almacenar datos en varias regiones geográficas, así como en varias zonas de disponibilidad dentro de cada región. Cada zona de disponibilidad está diseñada como una zona con independencia ante errores.

Esto significa que las zonas de disponibilidad se encuentran separadas físicamente dentro de una región metropolitana típica y se ubican en los terrenos con menor riesgo de inundación (la clasificación específica de las zonas de inundación varía según la región). Además de contar con un sistema de alimentación ininterrumpida (SAI), instalaciones de generación de energía de respaldo en el sitio con independencia entre sí, cada uno de ellos se alimenta a través de diferentes redes correspondientes a servicios independientes para reducir aún más la posibilidad de errores en componentes individuales. Todas las zonas de disponibilidad están conectadas de forma redundante a varios proveedores de tránsito de nivel 1.

Debe diseñar el uso de AWS a partir del objetivo de aprovechar las múltiples regiones y zonas de disponibilidad. La distribución de aplicaciones entre varias zonas de disponibilidad brinda la capacidad de resistir la mayoría de los modos de error, incluidos los desastres naturales o las fallas en el sistema.

Respuesta ante incidentes

El equipo de Administración de Incidentes de Amazon emplea procedimientos de diagnóstico estándar de la industria para impulsar la resolución de eventos que afectan al negocio. Los operadores de personal brindan cobertura las 24 horas del día, los 7 días de la semana, durante los 365 días del año para detectar los incidentes y administrar el efecto y la resolución.

Revisión ejecutiva en toda la empresa

El grupo de Auditoría Interna de Amazon ha revisado recientemente los planes de resiliencia de los servicios de AWS, los cuales también se someten a la revisión periódica de los miembros del equipo sénior de administración ejecutiva y el Comité de Auditoría de la Junta directiva.

Comunicación

AWS ha implementado distintos métodos de comunicación interna a nivel global para ayudar a los empleados a comprender sus roles y responsabilidades individuales, y a comunicar eventos importantes de manera oportuna. Entre estos métodos, se incluyen programas de orientación y capacitación para empleados recién contratados, reuniones periódicas de administración para dar a conocer las novedades sobre el rendimiento empresarial y otros asuntos, y recursos electrónicos, como las videoconferencias, los mensajes de correo electrónico y la publicación de información a través de la intranet de Amazon.

AWS también ha implementado diferentes métodos de comunicación externa para respaldar a su base de clientes y la comunidad. Existen mecanismos que permiten notificar al equipo de atención al cliente sobre los problemas operativos que afectan a la experiencia del cliente. El equipo de atención al cliente dispone de un Panel de estado del servicio y se encarga de su mantenimiento para avisar a los clientes sobre cualquier problema que pueda tener un gran impacto. El Centro de seguridad en la nube de AWS está disponible para brindarle detalles sobre la seguridad y la conformidad en AWS. También puede suscribirse a las ofertas de AWS Support que incluyen comunicación directa con el equipo de atención al cliente y alertas proactivas sobre todo tipo de problema que afecte al cliente.

Seguridad de la red

La red de AWS ha sido diseñada con el fin de permitirle seleccionar el nivel de seguridad y resiliencia adecuado para su carga de trabajo. AWS ha implementado una infraestructura de red de primera clase cuidadosamente monitoreada y administrada para permitirle diseñar arquitecturas tolerantes a errores y geográficamente dispersas con recursos en la nube.

Arquitectura de red protegida

Los dispositivos de red, incluidos el firewall y otros dispositivos de frontera, se han implementado para monitorear y controlar las comunicaciones en el límite externo de la red y en los límites internos importantes dentro de ella. Estos dispositivos de frontera emplean conjuntos de reglas, listas de control de acceso (ACL) y configuraciones para forzar el flujo de información hacia servicios específicos del sistema de información.

Las ACL o, políticas de flujo de tráfico, se establecen en cada interfaz administrada, que se encargan de administrar y dirigir el flujo de tráfico. Seguridad de la Información de Amazon aprueba las políticas de la ACL. Estas políticas se envían automáticamente mediante la herramienta de administración de la ACL de AWS para asegurarse de que estas interfaces administradas apliquen las ACL más actualizadas.

Puntos de acceso protegidos

AWS ha colocado de forma estratégica una cantidad limitada de puntos de acceso a la nube para que se pueda realizar un monitoreo más completo de las comunicaciones entrantes y salientes, y del tráfico de red. Estos puntos de acceso de los clientes se denominan puntos de enlace de la API y habilitan el acceso HTTP seguro (HTTPS), lo que le permite establecer una sesión de comunicación segura con sus instancias de almacenamiento o cómputo dentro de AWS. Para admitir a los clientes con requisitos criptográficos de FIPS, los balanceadores de carga con terminación SSL en AWS GovCloud (EE. UU.) cumplen los requisitos del estándar FIPS 140-2.

Además, AWS ha implementado dispositivos de red que se dedican a administrar las comunicaciones de interfaz con los proveedores de servicios de Internet (ISP). AWS se conecta de forma redundante a más de un servicio de comunicación en cada extremo de la red de AWS con conexión a Internet. Cada una de estas conexiones tiene dispositivos de red dedicados.

Protección de la transmisión

Puede conectarse a un punto de acceso de AWS a través de HTTP o HTTPS con capa de conexión segura (SSL), un protocolo criptográfico diseñado para ofrecer protección frente a escuchas, manipulaciones y falsificaciones de mensajes.

Para los clientes que necesitan capas adicionales de seguridad de red, AWS ofrece Amazon Virtual Private Cloud (VPC), que proporciona una subred privada dentro de la nube de AWS y la capacidad de utilizar un dispositivo de red privada virtual (VPN) con IPsec, que proporciona un túnel cifrado entre la VPC de Amazon y su centro de datos. Para obtener más información sobre las opciones de configuración de la VPC, consulte la sección Seguridad de Amazon Virtual Private Cloud (Amazon VPC).

Segregación corporativa de Amazon

Como se podría esperar, la red de producción de AWS se encuentra separada de la red corporativa de Amazon mediante un complejo conjunto de dispositivos de seguridad y segregación de red. Los desarrolladores y los administradores de AWS de la red corporativa que necesitan acceder a los componentes de la nube de AWS para hacerles mantenimiento deben solicitar el acceso de forma explícita a través del sistema de tratamiento de incidencias de AWS. El propietario del servicio correspondiente se encarga de revisar y aprobar todas las solicitudes.

El personal de AWS autorizado luego se conecta a la red de AWS a través de un host bastión que restringe el acceso a los dispositivos de red y otros componentes de la nube, y además registra toda la actividad para una revisión de seguridad. Para obtener acceso a los hosts bastión, se requiere autenticación de clave pública SSH para todas las cuentas a nivel de usuario del host. Si desea obtener más información sobre el acceso lógico de desarrolladores y administradores de AWS, consulte “Acceso de AWS” a continuación.

Diseño tolerante a errores

La infraestructura de Amazon tiene un alto nivel de disponibilidad y le ofrece la capacidad de implementar una arquitectura de TI resiliente. Los sistemas de AWS se han diseñado para tolerar errores en el sistema o el hardware con un nivel de impacto mínimo sobre el cliente.

Los centros de datos se encuentran repartidos en grupos entre distintas regiones de todo el mundo. Todos los centros de datos se encuentran en línea y a disposición los

clientes; ninguno de ellos está “inactivo”. En caso de error, los procesos automatizados alejan el tráfico de datos del cliente del área afectada. Las aplicaciones centrales se implementan en una configuración N+1, de forma que, en el caso de que se produzca un error en el centro de datos, haya capacidad suficiente como para permitir que se equilibre la carga de tráfico entre los demás sitios.

AWS le brinda la flexibilidad necesaria para colocar instancias y almacenar datos en varias regiones geográficas, así como en varias zonas de disponibilidad dentro de cada región. Cada zona de disponibilidad está diseñada como una zona con independencia ante errores. Esto significa que las zonas de disponibilidad se encuentran separadas físicamente dentro de una región metropolitana típica y se ubican en los terrenos con menor riesgo de inundación (la clasificación específica de las zonas de inundación varía según la región). Además de emplear un sistema de alimentación ininterrumpida (SAI) y generadores de respaldo en el sitio con independencia entre sí, cada uno de ellos se alimenta a través de diferentes redes correspondientes a servicios independientes para reducir aún más la posibilidad de errores en componentes individuales. Todas las zonas de disponibilidad están conectadas de forma redundante a varios proveedores de tránsito de nivel 1.

Debe diseñar el uso de AWS a partir del objetivo de aprovechar las múltiples regiones y zonas de disponibilidad. La distribución de aplicaciones entre varias zonas de disponibilidad brinda la capacidad de resistir la mayoría de las situaciones de error, incluidos los desastres naturales o las fallas en el sistema. Sin embargo, debe tener en cuenta los requisitos jurisdiccionales de privacidad específicos de cada ubicación, como la Directiva de Protección de Datos de la UE. Los datos no se replican entre regiones a menos que el cliente lo haga de manera explícita. AWS proporciona a los clientes con este tipo de requisitos de ubicación y privacidad de datos la capacidad de establecer entornos que los cumplan. Cabe destacar que todas las comunicaciones entre las regiones se realizan a través de la infraestructura pública de Internet, por lo que deben usarse métodos de cifrado adecuados para proteger los datos confidenciales.

Los centros de datos se encuentran repartidos en grupos en distintas regiones de todo el mundo, incluidas las siguientes: EE. UU. Este (Norte de Virginia), EE. UU. Oeste (Oregón), EE. UU. Oeste (Norte de California), AWS GovCloud (EE. UU.) (Oregón), UE (Fráncfort), UE (Irlanda), Asia-Pacífico (Seúl), Asia-Pacífico (Singapur), Asia-Pacífico (Tokio), Asia-Pacífico (Sídney), China (Pekín) y América del Sur (São Paulo). Para ver la lista completa de regiones de AWS, consulte la página Infraestructura global de AWS.

AWS GovCloud (EE. UU.) es una región de AWS aislada que se diseñó para permitir

que los clientes y las agencias gubernamentales de EE. UU. trasladen cargas de trabajo a la nube al permitir que cumplan ciertos requisitos normativos y de conformidad. El marco de AWS GovCloud (EE. UU.) permite a las agencias gubernamentales de EE. UU. y a sus contratistas cumplir el Reglamento Internacional de Tráfico de Armas (ITAR) de EE. UU, así como los requisitos del Programa Federal de Administración de Autorizaciones y Riesgo (FedRAMP). AWS GovCloud (EE. UU.) ha recibido la autorización para operar (ATO) de la agencia del Departamento de Salud y Servicios Sociales (HHS) de EE. UU. a través de una organización evaluadora externa independiente (3PAO) acreditada por FedRAMP para varios servicios de AWS.

La región AWS GovCloud (EE. UU.) ofrece el mismo diseño tolerante a errores que otras regiones, con dos zonas de disponibilidad. Además, la región AWS GovCloud (EE. UU.) es un servicio de Virtual Private Cloud (VPC) de AWS obligatorio de forma predeterminada para crear una parte aislada de la nube de AWS y lanzar instancias de Amazon EC2 que tengan direcciones privadas (RFC 1918). Para obtener más información, consulte AWS GovCloud (EE. UU.).

Monitoreo y protección de la red

AWS utiliza una gran variedad de sistemas de monitoreo automatizado para ofrecer un elevado nivel de rendimiento y disponibilidad en los servicios. Las herramientas de monitoreo de AWS se han diseñado para detectar actividades y condiciones inusuales o no autorizadas en los puntos de comunicación de entrada y salida. Estas herramientas monitorean el uso de los servidores y la red, las actividades de escaneo de puertos, el uso de las aplicaciones y los intentos de intrusión no autorizados. Las herramientas pueden definir límites personalizados en las métricas de rendimiento relativas a la actividad inusual.

Los sistemas en AWS disponen de una gran variedad de recursos para monitorear las métricas operativas principales. Las alarmas se configuran para notificar automáticamente al personal de operaciones y administración cuando las métricas operativas clave superan los límites de advertencia anticipada. Se utiliza un horario de guardia a fin de que el personal esté siempre disponible para solucionar los problemas operativos. Esto incluye un sistema de localización para que las alarmas se comuniquen al personal de operaciones de forma rápida y fiable.

La documentación se mantiene actualizada para ayudar e informar al personal de operaciones sobre el tratamiento de incidentes o problemas. En caso de que se necesite colaboración para solucionar algún problema, se utiliza un sistema de

conferencia que admite capacidades de comunicación y registro. Los coordinadores de las llamadas cualificados facilitan la comunicación y el progreso durante el tratamiento de los problemas operativos que precisan de colaboración. Los análisis *post mortem* se realizan después de cualquier problema operativo importante, independientemente del impacto externo. Además, se elaboran documentos sobre la causa del error (COE) para identificar la causa raíz y adoptar medidas preventivas en el futuro. Se hace un seguimiento de la implementación de las medidas preventivas durante reuniones semanales de operaciones.

Acceso de AWS

La red de producción de AWS está separada de la red corporativa de Amazon y requiere un conjunto de credenciales diferente para el acceso lógico. La red corporativa de Amazon emplea ID de usuarios, contraseñas y Kerberos, mientras que la red de producción de AWS requiere la autenticación de claves públicas SSH a través de un host bastión.

Los desarrolladores y los administradores de AWS en la red corporativa de Amazon que necesitan acceder a los componentes de la nube de AWS deben solicitar el acceso explícitamente a través del sistema de administración de acceso de AWS. El propietario o el administrador pertinentes deben revisar y aprobar todas las solicitudes.

Auditoría y revisión de cuentas

Las cuentas se revisan cada 90 días. Se necesita la renovación explícita de la aprobación; de lo contrario, se revocará el acceso al recurso automáticamente. El acceso también se revoca de manera automática cuando se cierra el historial de un empleado en el sistema de Recursos Humanos de Amazon. Se desactivan las cuentas de Windows y UNIX. Además, el sistema de administración de permisos de Amazon elimina al usuario de todos los sistemas.

Las solicitudes de cambios en el acceso se capturan en el registro de auditoría de la herramienta de administración de permisos de Amazon. Cuando se produce un cambio en la función laboral de un empleado, se debe aprobar de forma explícita el acceso continuo al recurso; de lo contrario, dicho acceso se revocará automáticamente.

Comprobaciones de antecedentes

AWS ha establecido políticas y procedimientos formales para definir estándares mínimos de acceso lógico a los hosts de la plataforma y la infraestructura de AWS. AWS verifica los antecedentes penales, según lo permitido por la ley, como parte de las prácticas de preselección de empleados y de acuerdo con el cargo y el nivel de acceso del empleado. Las políticas también identifican responsabilidades funcionales para la administración de la seguridad y del acceso lógico.

Política de credenciales

El sector de seguridad en AWS ha establecido una política de credenciales con las configuraciones y los intervalos de caducidad necesarios. Las contraseñas tienen que ser complejas y es obligatorio cambiarlas cada 90 días.

Principios de diseño protegidos

El proceso de desarrollo de AWS aplica las prácticas recomendadas para el desarrollo de software seguro, las cuales incluyen las revisiones formales del diseño por parte del equipo de seguridad de AWS, el modelado de amenazas y la evaluación de riesgos. Las herramientas de análisis de código estático se ejecutan como parte de un proceso de compilación estándar y todo el software implementado se somete a pruebas de intrusión regulares realizadas por expertos del sector seleccionados de forma minuciosa. Las revisiones de la evaluación de riesgos para la seguridad que realizamos comienzan en la fase de diseño y el compromiso se extiende desde el lanzamiento hasta las operaciones en curso.

Administración de los cambios

Los cambios rutinarios, de emergencia y de configuración en la infraestructura existente de AWS están sujetos a autorización, registro, prueba, aprobación y documentación de conformidad con las normas del sector establecidas para sistemas similares. Se realizan actualizaciones de la infraestructura de AWS para minimizar cualquier efecto sobre el cliente y su uso de los servicios. AWS se comunicará con los clientes, ya sea por email o a través del Panel de estado del servicio de AWS cuando es probable que el uso del servicio se vea afectado negativamente.

Software

AWS aplica un enfoque sistemático para administrar los cambios a fin de revisar minuciosamente, probar, aprobar y comunicar los cambios introducidos en los servicios que repercutan en los clientes. El proceso de administración de cambios de AWS está diseñado para evitar interrupciones involuntarias del servicio y mantener la integridad del servicio que se presta al cliente. Los cambios implementados en los entornos de producción se someten a los siguientes procesos:

- **Revisión:** se requieren revisiones entre pares de los aspectos técnicos de los cambios.
- **Prueba:** los cambios que se aplican se prueban para asegurarse de que se comportarán según lo previsto sin afectar negativamente el rendimiento.
- **Aprobación:** se deben autorizar todos los cambios para ofrecer la supervisión y el conocimiento adecuados sobre el impacto empresarial.

Los cambios suelen introducirse en la fase de producción con una implementación gradual, empezando por áreas con el menor nivel de impacto. Las implementaciones se prueban en un único sistema y se monitorean con cuidado a fin de poder evaluar los efectos. Los propietarios del servicio cuentan con una serie de métricas configurables que miden el estado de las dependencias ascendentes del servicio. Estas métricas se controlan cuidadosamente mediante límites y alarmas. Los procedimientos de restauración se registran en el boleto de administración de cambios.

Cuando es posible, los cambios se programan durante periodos de cambio regulares. Los cambios de emergencia en los sistemas de producción que requieren desviaciones de los procedimientos estándar de administración de cambios se asociarán a un incidente y se registrarán y aprobarán según corresponda.

De forma periódica, AWS realiza auditorías por su cuenta de los cambios introducidos en los servicios clave para monitorear la calidad, mantener estándares altos y facilitar la mejora constante del proceso de administración de cambios. Todas las excepciones se analizan para determinar la causa raíz y se toman las medidas adecuadas para que los cambios cumplan los requisitos o para que se reviertan si es necesario. Luego, se toman medidas para abordar y solucionar el proceso o el problema del usuario.

Infraestructura

El equipo Aplicaciones Corporativas de Amazon desarrolla y administra el software a fin de automatizar los procesos de TI para los hosts de UNIX/Linux en los ámbitos de entrega de software de terceros, de software desarrollado internamente y de administración de la configuración. El equipo de infraestructuras mantiene y opera un marco de administración de la configuración de UNIX/Linux para gestionar la escalabilidad, la disponibilidad, la auditoría y la administración de seguridad del hardware. Amazon puede alcanzar sus objetivos de alta disponibilidad, repetibilidad, escalabilidad, seguridad y recuperación de desastres gracias a una administración centralizada de los hosts mediante la utilización de procesos automatizados que gestionan los cambios.

Los ingenieros de sistemas y redes monitorean el estado de estas herramientas automatizadas de forma continua a través de la revisión de los informes para atender a los hosts que no pueden obtener ni actualizar su configuración y el software.

Cuando se incorpora hardware nuevo, se instala un software de administración de la configuración que se ha desarrollado internamente. Estas herramientas se ejecutan en todos los hosts de UNIX para validar que estén configurados y que el software esté instalado de conformidad con los estándares determinados por el rol asignado al host. Este software de administración de la configuración también permite actualizar con regularidad los paquetes que ya están instalados en el host. Solo el personal autorizado a través del servicio de permisos puede acceder a los servidores centrales de administración de la configuración.

AWS ofrece diversas herramientas y características para que mantenga su cuenta de AWS y sus recursos a salvo del uso no autorizado. Entre estas se incluyen las credenciales para el control del acceso, los puntos de enlace HTTPS para la transmisión de datos cifrados, la creación de cuentas de usuario de IAM distintas, el registro de la actividad del usuario para monitorear la seguridad y las comprobaciones de seguridad de Trusted Advisor. Puede aprovechar todas estas herramientas de seguridad independientemente de los servicios de AWS que seleccione.

Credenciales de AWS

Para ayudarlo a asegurarse de que solo los usuarios y los procesos autorizados tengan acceso a su cuenta de AWS y sus recursos, AWS utiliza varios tipos de

credenciales para la autenticación. Entre ellos se incluyen contraseñas, claves criptográficas, firmas digitales y certificados. También ofrecemos la opción de solicitar autenticación multifactor (MFA) para iniciar sesión en su cuenta de AWS o en las cuentas de usuario de IAM. En la siguiente tabla, se destacan las distintas credenciales de AWS y sus usos.

Tabla 1: Tipos de credenciales y usos

Tipo de credencial	Uso	Descripción
Contraseñas	Inicio de sesión con la cuenta raíz de AWS o la cuenta de usuario de IAM en la consola de administración de AWS	Una cadena de caracteres utilizada para iniciar sesión en su cuenta de AWS o su cuenta de IAM. Las contraseñas de AWS deben tener un mínimo de 6 caracteres y un máximo de 128.
Multi-Factor Authentication (MFA)	Inicio de sesión con la cuenta raíz de AWS o la cuenta de usuario de IAM en la consola de administración de AWS	Un código de seis dígitos de un solo uso obligatorio, además de la contraseña para iniciar sesión en la cuenta de AWS o la cuenta de usuario de IAM
Claves de acceso	Solicitudes firmadas digitalmente a las API de AWS (mediante el SDK de AWS, la CLI o las API REST/consulta)	Incluye un ID de clave de acceso y una clave de acceso secreta. Las claves de acceso se utilizan para firmar digitalmente las solicitudes de programación que presenta a AWS.
Pares de claves	URL firmadas por CloudFront para inicio de sesión SSH a instancias EC2	Se requiere un par de claves para conectarse a una instancia EC2 lanzada desde una AMI pública. Los tamaños que se admiten son 1024, 2048 y 4096. Si se conecta mediante SSH a la vez que usa la API de conexión a una instancia EC2, los tamaños que se admiten son 2048 y 4096. Puede indicar que se genere un par de claves automáticamente en su nombre cuando lance la instancia o puede cargar su propio par.

Tipo de credencial	Uso	Descripción
Certificados X.509	Solicitudes SOAP firmadas digitalmente a las API de AWS Certificados de servidor SSL para HTTPS	Los certificados X.509 solo se utilizan para firmar solicitudes basadas en SOAP (que actualmente solo se utilizan con Amazon S3). Puede pedir a AWS que cree un certificado X.509 y una clave privada que pueda descargar, o puede cargar su propio certificado a través de la página de credenciales de seguridad.

Puede descargar un informe de credenciales de su cuenta en cualquier momento desde dicha página. En este informe, se indican todos los usuarios de su cuenta y el estado de sus credenciales. La información incluye si utilizan una contraseña, si la contraseña caduca y debe cambiarse periódicamente, la última vez que cambiaron la contraseña, la última vez que cambiaron sus claves de acceso y si tienen activada la MFA.

Por motivos de seguridad, si sus credenciales se pierden o ya no las recuerda, no puede recuperarlas ni volver a descargarlas. Sin embargo, puede crear credenciales nuevas y después desactivar o eliminar el conjunto anterior de credenciales.

De hecho, AWS recomienda que cambie (rote) sus claves de acceso y certificados periódicamente. Para permitirle hacerlo sin que se vea afectada la disponibilidad de la aplicación, AWS admite varias claves de acceso y certificados a la vez. Esta característica le permite activar y desactivar con regularidad el uso de las claves y los certificados, sin que la aplicación sufra periodos de inactividad. Esto ayuda a mitigar los riesgos derivados de situaciones en las que los certificados o las claves de acceso se han perdido o se ha comprometido su integridad. La API de AWS IAM le permite rotar las claves de acceso de la cuenta de AWS y las de las cuentas de usuario de IAM.

Contraseñas

Las contraseñas son necesarias para obtener acceso a la cuenta de AWS, las cuentas de usuario de IAM individuales, los foros de debate de AWS y el Centro de soporte de AWS. La contraseña se especifica la primera vez que se crea la cuenta y puede cambiarla en cualquier momento desde la página de credenciales de seguridad. Las contraseñas de AWS pueden tener hasta 128 caracteres y pueden contener caracteres especiales, por lo que le recomendamos que cree una contraseña segura que no sea fácil de adivinar.

Puede definir una política de contraseñas para las cuentas de usuario de IAM con el fin de garantizar que se utilicen contraseñas seguras y que se cambien a menudo. Una política de contraseñas es un conjunto de reglas que definen el tipo de contraseña que puede configurar un usuario de IAM. Para obtener más información sobre las políticas de contraseñas, consulte Administración de las contraseñas de los usuarios de IAM.

AWS Multi-Factor Authentication (MFA)

AWS Multi-Factor Authentication (MFA) es una capa de seguridad adicional para obtener acceso a los servicios de AWS. Si habilita esta característica opcional, tiene que proporcionar un código de seis dígitos de un solo uso, además de sus credenciales estándar de nombre de usuario y contraseña, para que se le conceda acceso a la configuración de su cuenta de AWS o a los servicios y los recursos de AWS. Obtiene este código de un solo uso de un dispositivo de autenticación que tiene en su posesión. Esto se denomina autenticación multifactor porque se comprueban más de un factor para poder obtener acceso: una contraseña (algo que conoce) y el código exacto de su dispositivo de autenticación (algo que tiene). Puede habilitar dispositivos de MFA para su cuenta de AWS, así como para los usuarios que haya creado con AWS IAM para dicha cuenta de AWS. Además, cuando quiera permitir a un usuario que haya creado en una cuenta de AWS que adopte un rol de IAM para obtener acceso a los recursos que se encuentran en otra cuenta de AWS, puede agregar protección de MFA para tener acceso entre cuentas de AWS. Puede exigir que el usuario utilice MFA antes de asumir el rol como una capa de seguridad adicional.

AWS MFA es compatible con el uso de tokens de hardware y dispositivos de MFA virtuales. Los dispositivos de MFA virtuales utilizan los mismos protocolos que los dispositivos de MFA físicos, pero se pueden ejecutar en cualquier dispositivo de hardware móvil, incluso un teléfono inteligente. Un dispositivo de MFA virtual utiliza una aplicación de software que genera códigos de autenticación de seis dígitos compatibles con el estándar para contraseñas temporales de un solo uso (TOTP), tal como se describe en RFC 6238. La mayoría de las aplicaciones de MFA virtuales le permiten alojar más de un dispositivo de MFA virtual, por lo que resultan más cómodas que los dispositivos de MFA físicos. Sin embargo, debe tener en cuenta que como es posible que una aplicación de MFA virtual se ejecute en un dispositivo menos seguro, como un teléfono inteligente, podría no proporcionar el mismo nivel de seguridad que un dispositivo de MFA físico.

También puede aplicar la autenticación MFA para las API de servicios de AWS si desea proporcionar una capa adicional de protección en torno a acciones más

comprometidas o con mayor nivel de privilegios, como terminar instancias de Amazon EC2 o leer datos confidenciales almacenados en Amazon S3. Para esto, agregue un requisito de autenticación MFA a una política de acceso de IAM. Puede asociar estas políticas de acceso a usuarios de IAM, grupos de IAM o recursos que admitan listas de control de acceso (ACL), como buckets de Amazon S3, colas de SQS y temas de SNS.

Es fácil obtener tokens de hardware de un proveedor externo participante o aplicaciones de MFA virtuales de una tienda de aplicaciones, y configurarlos para utilizarlos a través del sitio web de AWS. Puede obtener más información en AWS Multi-Factor Authentication (MFA).

Claves de acceso

AWS requiere que todas las solicitudes de API estén firmadas, es decir, que incluyan una firma digital que AWS pueda usar para verificar la identidad del solicitante. La firma digital se calcula mediante una función hash criptográfica. La entrada de la función hash, en este caso, incluye el texto de la solicitud y la clave de acceso secreta. Si utiliza alguno de los SDK de AWS para generar solicitudes, el cálculo de la firma digital se realiza por usted; en caso contrario, puede hacer que su aplicación la calcule e incluir la firma en las solicitudes REST o de consulta siguiendo las instrucciones en Realizar solicitudes con los SDK de AWS.

El proceso de firma no solo ayuda a proteger la integridad de los mensajes porque impide la manipulación de la solicitud mientras está en tránsito, sino que también ofrece protección frente a posibles ataques de reproducción. Las solicitudes deben llegar a AWS en un plazo de 15 minutos que se cuenta a partir de la marca temporal que figura en ellas. De lo contrario, AWS rechaza la solicitud.

La versión más reciente del proceso de cálculo de firmas digitales es Signature Version 4, el cual, para calcular la firma, utiliza el protocolo HMAC-SHA256. Version 4 proporciona una medida de protección adicional frente a versiones anteriores al exigir que el mensaje se firme con una clave derivada de la clave de acceso secreta en lugar de utilizar la propia clave de acceso secreta. Además, la clave de firma se obtiene en función del ámbito de credenciales, que ofrece aislamiento criptográfico de la clave de firma.

Como es posible que se haga uso indebido de las claves de acceso si estas terminan en las manos incorrectas, le aconsejamos que las guarde en un lugar seguro y que no las incruste en su código. Para los clientes con grandes flotas de instancias EC2 de

escalado elástico, el uso de roles de IAM puede representar una forma más segura y conveniente de administrar la distribución de las claves de acceso. Los roles de IAM proporcionan credenciales temporales, las cuales no solo se cargan automáticamente en la instancia de destino, sino que también se rotan de manera automática varias veces a lo largo del día.

Pares de claves

Las instancias de Amazon EC2 creadas a partir de una AMI pública utilizan un par de claves públicas y privadas en lugar de una contraseña para iniciar sesión a través de Secure Shell (SSH). La clave pública está incrustada en la instancia y la clave privada se utiliza para iniciar sesión de forma segura sin una contraseña. Después de crear sus propias AMI, puede elegir otros mecanismos para iniciar sesión de forma segura en sus instancias nuevas.

Puede indicar que se genere un par de claves automáticamente en su nombre cuando lance la instancia o puede cargar su propio par. Guarde la clave privada en un lugar seguro del sistema y anote la ubicación donde la ha guardado.

En el caso de Amazon CloudFront, utilizará pares de claves a fin de crear URL firmadas para contenido privado, como cuando desee distribuir contenido restringido por el que alguien ha pagado. Los pares de claves de Amazon CloudFront se crean con la página de credenciales de seguridad. Solo se pueden crear con la cuenta raíz y no los pueden crear los usuarios de IAM.

Certificados X.509

Los certificados X.509 se utilizan para firmar solicitudes basadas en SOAP. Contienen una clave pública y metadatos adicionales (como una fecha de vencimiento que AWS verifica cuando carga el certificado), y están asociados a una clave privada. Cuando se crea una solicitud, se crea una firma digital con la clave privada y luego se incluye esa firma en la solicitud junto con el certificado. AWS descifra la firma con la clave pública que figura en su certificado para verificar que usted sea el remitente. AWS también verifica que el certificado enviado concuerde con el que ha cargado en AWS.

Para su cuenta de AWS, puede pedir a AWS que cree un certificado X.509 y una clave privada que pueda descargar, o puede cargar su propio certificado a través de la página de credenciales de seguridad. Para los usuarios de IAM, debe crear el certificado X.509 (certificado de firma) con software de otro proveedor. A diferencia de lo que ocurre con las credenciales de la cuenta raíz, AWS no puede crear un

certificado X.509 para los usuarios de IAM. Después de crear el certificado, deberá asociarlo a un usuario de IAM a través de ese servicio.

Además de las solicitudes SOAP, los certificados X.509 se utilizan como certificados de servidor SSL/TLS para los clientes que desean utilizar HTTPS para cifrar sus transmisiones. Si desea utilizarlos para HTTPS, puede emplear una herramienta de código abierto, como OpenSSL, para crear una clave privada única. Necesitará la clave privada a fin de crear la solicitud de firma de certificado (CSR) que envía a una entidad de certificación (CA) para obtener el certificado de servidor. Luego, utilizará la CLI de AWS para cargar el certificado, la clave privada y la cadena de certificados en IAM.

También necesitará un certificado X.509 para crear una AMI Linux personalizada para las instancias EC2. El certificado solo es necesario para crear una AMI respaldada por una instancia (en lugar de una AMI respaldada por EBS). Puede pedir a AWS que cree un certificado X.509 y una clave privada que pueda descargar, o puede cargar su propio certificado a través de la página de credenciales de seguridad.

Cuentas de usuario individuales

AWS proporciona un mecanismo centralizado llamado AWS Identity and Access Management (IAM) para crear y administrar usuarios individuales en su cuenta de AWS. Un usuario puede ser cualquier individuo, sistema o aplicación que interactúe con recursos de AWS, ya sea mediante programación o a través de la consola de administración de AWS o la interfaz de línea de comandos (CLI) de AWS. Cada usuario tiene un nombre único dentro de la cuenta de AWS y un conjunto exclusivo de credenciales de seguridad que no se comparte con otros usuarios. AWS IAM elimina la necesidad de compartir las contraseñas o las claves, y le permite minimizar el uso de las credenciales de su cuenta de AWS.

Con IAM, se definen políticas que controlan a cuáles servicios de AWS pueden acceder los usuarios y qué pueden realizar con ellos. Puede otorgar a los usuarios solo los permisos mínimos que necesitarán para llevar a cabo sus trabajos. Consulte la sección AWS Identity and Access Management (AWS IAM) para obtener más información.

Puntos de acceso HTTPS protegidos

Para lograr una mayor seguridad en las comunicaciones cuando se acceda a los recursos de AWS, debería utilizar HTTPS en lugar de HTTP para las transmisiones de datos. HTTPS utiliza el protocolo SSL/TLS, el cual usa la criptografía de clave pública a

fin de evitar el espionaje, la manipulación y la falsificación. Todos los servicios de AWS proporcionan puntos de acceso de clientes seguros (también llamados puntos de enlace de la API) que le permiten establecer sesiones de comunicación HTTPS seguras.

Varios servicios ahora también ofrecen paquetes de cifrado más avanzados que utilizan el protocolo Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). El protocolo ECDHE permite a los clientes SSL/TLS proporcionar confidencialidad directa total, la cual usa claves de sesión efímeras que no se almacenan en ningún lugar. Eso contribuye a impedir que terceros sin autorización decodifiquen los datos recopilados, incluso si la propia clave secreta configurada para el largo plazo se haya visto comprometida.

Registros de seguridad

Así como las credenciales y los puntos de enlace cifrados son importantes para evitar los problemas de seguridad, los registros son igual de esenciales para entender los eventos después de un problema. Para ser efectivo como una herramienta de seguridad, un registro no solo debe incluir una lista de lo que sucedió y de cuándo sucedió, sino que también debe identificar el origen. A fin de ayudarlo con las investigaciones posteriores al problema y la detección de intrusos casi en tiempo real, AWS CloudTrail ofrece un registro de eventos dentro de su cuenta. Para cada evento, puede ver a qué servicio se accedió, qué acción se llevó a cabo y quién efectuó la solicitud.

CloudTrail registra las llamadas a las API, así como otras actividades, por ejemplo, los eventos de inicio de sesión en la consola. Una vez que habilita CloudTrail, los registros de eventos se entregarán cada 5 minutos aproximadamente. Puede configurar CloudTrail para que agrupe los archivos de registros provenientes de varias regiones o cuentas en un único bucket de Amazon S3. De forma predeterminada, un único registro de seguimiento registrará y entregará eventos de todas las regiones actuales y futuras. Además de S3, puede enviar eventos a CloudWatch Logs para establecer métricas y alarmas personalizadas, o puede cargar los registros en sus soluciones de administración y análisis de registros favoritas a fin de llevar a cabo análisis de seguridad y detectar patrones de comportamiento de los usuarios. A fin de obtener una respuesta rápida, puede crear reglas de CloudWatch Events para tomar acciones oportunas respecto de eventos específicos. De forma predeterminada, los archivos de registros se almacenan de manera segura en Amazon S3, pero también es posible guardarlos en Amazon S3 Glacier a fin de cumplir los requisitos de auditoría y conformidad.

Además de los registros de CloudTrail respecto de las actividades de los usuarios, puede utilizar la característica de Amazon CloudWatch Logs para recopilar y monitorear el sistema, las aplicaciones y los archivos de registros personalizados de las instancias EC2 y otros orígenes casi en tiempo real. Por ejemplo, puede monitorear los archivos de registros del servidor web para buscar los mensajes de usuarios no válidos a fin de detectar los intentos de inicio de sesión sin autorización en su sistema operativo huésped.

Comprobaciones de seguridad de AWS Trusted Advisor

El servicio AWS Trusted Advisor no solo monitorea la resiliencia y el rendimiento en la nube, sino también su seguridad. Trusted Advisor inspecciona su entorno de AWS y efectúa recomendaciones cuando existe la posibilidad de ahorrar dinero, mejorar el rendimiento del sistema o solucionar puntos vulnerables de la seguridad. Proporciona alertas sobre varios de los errores más comunes que se pueden producir en la configuración de la seguridad, lo que incluye dejar ciertos puertos abiertos que lo vuelven vulnerable a hackeos y accesos sin autorización, descuidar la creación de cuentas de IAM para sus usuarios internos, permitir el acceso público a los buckets de Amazon S3, no activar el registro de la actividad de los usuarios (AWS CloudTrail) o no utilizar MFA en la cuenta de AWS raíz. También tiene la opción de disponer de un contacto de seguridad en su organización a fin de recibir de forma automática un email semanal con el estado actualizado de las comprobaciones de seguridad de Trusted Advisor.

El servicio AWS Trusted Advisor proporciona cuatro comprobaciones a todos los usuarios sin cargos adicionales y, adicionales, comprobaciones de seguridad importantes: los puertos específicos sin restricción, el uso de IAM y la MFA en la cuenta raíz. Con la inscripción en los niveles Business o Enterprise de AWS Support, recibe acceso total a todas las comprobaciones de Trusted Advisor.

Comprobaciones de seguridad de AWS Config

AWS Config es un servicio continuo de monitoreo y evaluación que registra los cambios en la configuración de sus recursos de AWS. Puede ver las configuraciones actuales e históricas de un recurso y utilizar esta información para resolver los problemas de interrupción, efectuar análisis de ataques a la seguridad y mucho más. Puede ver la configuración definida para cualquier momento y usar esa información para volver a configurar los recursos y llevarlos a un estado estable durante una situación de interrupción del servicio.

Mediante el uso de las reglas de AWS Config, puede ejecutar comprobaciones de evaluación continua en sus recursos a fin de verificar que cumplan sus propias políticas de seguridad, prácticas recomendadas del sector y sistemas de conformidad, como PCI/HIPAA. Por ejemplo, AWS Config proporciona reglas de AWS Config administradas para garantizar que se active el cifrado de todos los volúmenes de EBS en su cuenta. También puede escribir una regla de AWS Config personalizada a fin de, en esencia, "codificar" sus propias políticas de seguridad corporativas. AWS Config le envía una alerta en tiempo real si un recurso no está configurado de manera correcta o si un recurso infringe una política de seguridad determinada.

Seguridad de AWS para servicios específicos

No solo se incorpora seguridad en cada capa de la infraestructura de AWS, sino también en cada uno de los servicios disponibles en dicha infraestructura. Los servicios de AWS están diseñados para funcionar de manera eficiente y segura con todas las redes y las plataformas de AWS. Cada servicio proporciona amplias características de seguridad que le permiten proteger los datos confidenciales y las aplicaciones.

Servicios informáticos

Amazon Web Services ofrece una serie de servicios informáticos basados en la nube que incluyen una amplia selección de instancias de cómputo que pueden ampliar o reducir su capacidad de forma automática a fin de satisfacer las necesidades de su aplicación o empresa.

Seguridad de Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Compute Cloud (Amazon EC2) es un componente clave de la infraestructura como servicio (IaaS) de Amazon, el cual proporciona capacidad de cómputo que puede cambiar de tamaño a través de instancias de servidor en los centros de datos de AWS. Amazon EC2 está diseñado para facilitar la informática a escala de la Web al permitirle obtener y configurar la capacidad con un nivel mínimo de fricción. Se crean y lanzan instancias, las cuales son colecciones de hardware y software de plataforma.

Múltiples niveles de seguridad

La seguridad dentro de Amazon EC2 se proporciona en varios niveles: el sistema operativo de la plataforma de alojamiento, el sistema operativo de la instancia virtual o el sistema operativo huésped; el firewall; y las llamadas a la API firmadas. Cada uno de estos elementos se basa en las capacidades de los demás. El objetivo es evitar que sistemas o usuarios no autorizados intercepten los datos dentro de Amazon EC2, y ofrecer las propias instancias de Amazon EC2 con el mayor nivel de seguridad posible, sin sacrificar la flexibilidad en la configuración que exigen los clientes.

Hipervisor

Amazon EC2 actualmente utiliza una versión del hipervisor Xen con un alto grado de personalización, por lo que aprovecha la paravirtualización (en el caso de los huéspedes Linux). Dado que los huéspedes paravirtualizados dependen del hipervisor para que se admitan las operaciones que, por lo general, necesitan accesos de privilegio, el sistema operativo huésped no cuenta con acceso elevado a la CPU. La CPU proporciona cuatro modos de privilegio diferentes, los cuales se denominan anillos: de 0 a 3. El anillo 0 es el que posee mayor privilegio y el 3 es el que cuenta con menos privilegio. El sistema operativo host se ejecuta en el anillo 0. Sin embargo, el sistema operativo huésped, en vez de ejecutarse en el anillo 0 como lo hace la mayoría de los sistemas operativos, se ejecuta en el anillo 1, el cual tiene menos privilegios, y las aplicaciones, en el anillo 3, que es el que menos privilegios tiene. Esta virtualización explícita de los recursos físicos lleva a una separación evidente entre el huésped y el hipervisor, lo que resulta en la separación de seguridad adicional entre ambos.

Tradicionalmente, los hipervisores protegen el hardware físico y los dispositivos, virtualizan la CPU, el almacenamiento y las redes; y ofrecen un conjunto completo de capacidades de administración. Con Nitro System, podemos desarmar esas funciones, descargarlas en hardware y software dedicados, y reducir los costos al entregar todos los recursos de un servidor a las instancias.

El hipervisor Nitro proporciona un rendimiento constante y recursos informáticos y de memoria mejorados para las instancias EC2 virtualizadas, ya que elimina los componentes de software del sistema de alojamiento. Permite a AWS ofrecer tamaños de instancias más grandes (como c5.18xlarge), los cuales proporcionan a los clientes prácticamente todos los recursos del servidor. Antes, las instancias C3 y C4 eliminaban los componentes de software trasladando las funcionalidades de VPC y EBS al hardware diseñado y creado por AWS. Este hardware permite que el hipervisor Nitro sea muy pequeño y no participe en las tareas de procesamiento de datos de las redes y el almacenamiento.

Sin embargo, mientras AWS expanda su infraestructura global en la nube, el uso que Amazon EC2 haga de su hipervisor basado en Xen también seguirá creciendo. Xen continuará siendo un componente principal de las instancias EC2 por ahora.

Aislamiento de instancias

Las diferentes instancias que se ejecutan en la misma máquina física se aíslan unas de otras por medio del hipervisor Xen. Amazon es un miembro activo de la comunidad Xen, lo que permite le mantenerse actualizado sobre los desarrollos más recientes. Además, el firewall de AWS está ubicado dentro de la capa del hipervisor, entre la interfaz física de la red y la interfaz virtual de la instancia. Todos los paquetes deben atravesar esta capa, por lo que los vecinos de una instancia no tienen más acceso a dicha instancia que cualquier otro host de Internet, y se pueden tratar como si estuviesen ubicados en hosts físicos diferentes. La RAM física se separa por medio de mecanismos similares.

Las instancias de los clientes no tienen acceso a los dispositivos del disco sin procesar, pero, en cambio, se les otorgan discos virtualizados. La capa de virtualización de discos con patente de AWS restablece de forma automática todos los bloques de almacenamiento utilizados por los clientes, de manera que los datos de cada uno de ellos nunca se expongan por accidente ante los demás. Además, el hipervisor borra (establece en cero) la memoria asignada a los huéspedes cuando se anula la asignación. La memoria no se devuelve al grupo de memoria libre disponible para nuevas asignaciones antes de que la acción de borrar esté completa.

Además, AWS recomienda a los clientes proteger sus datos con medios adecuados. Una solución común es ejecutar un sistema de archivos cifrados encima del dispositivo de disco virtualizado.

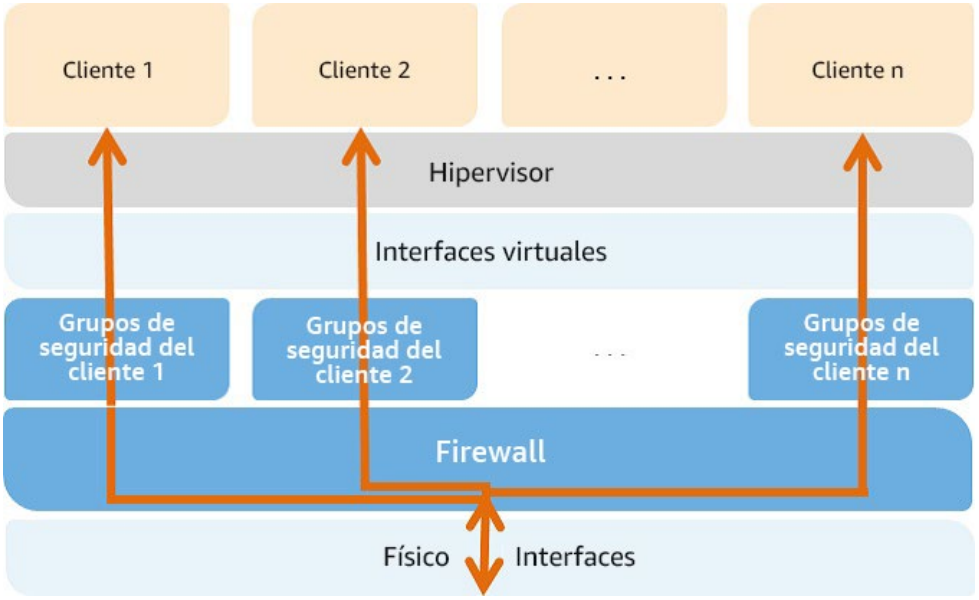


Imagen 2: Las múltiples capas de seguridad de Amazon EC2

Sistema operativo host: se requiere que los administradores que tengan la necesidad empresarial de acceder al plano de la administración utilicen la autenticación multifactor para obtener acceso a los hosts de administración especialmente diseñados. Estos hosts administrativos son sistemas que se han diseñado, creado, configurado y fortalecido con el propósito específico de proteger el plano de la administración en la nube. Todos estos tipos de acceso se registran y auditan. Cuando un empleado deja de tener la necesidad empresarial de acceder al plano de la administración, se pueden revocar los privilegios para poder acceder a estos hosts y a los sistemas pertinentes.

Sistema operativo huésped: el cliente, usted, controla las instancias virtuales completamente. Cuenta con el acceso raíz o de control administrativo completos sobre las cuentas, los servicios y las aplicaciones. AWS no posee ningún derecho de acceso a sus instancias o al sistema operativo huésped. AWS sugiere contar con un conjunto básico de prácticas recomendadas para la seguridad que incluyan desactivar el acceso que requiere solo contraseñas para los huéspedes y utilizar alguna forma de autenticación multifactor a la hora de obtener acceso a sus instancias (o, como mínimo, un acceso SSH versión 2 basado en certificados). Además, debería utilizar un mecanismo de ampliación de los privilegios con registros por usuario. Por ejemplo, si el sistema operativo huésped es Linux, después de fortalecer su instancia, debería utilizar el protocolo SSHv2 basado en certificados para acceder a la instancia virtual, desactivar el inicio de sesión raíz remoto, utilizar el registro de línea de comandos y usar “sudo” para la ampliación de los privilegios.

Debería generar su propio par de claves con el fin de garantizar que sean únicas y no se compartan con otros clientes o con AWS.

AWS también admite el uso del protocolo de red Secure Shell (SSH) para que poder iniciar sesión de forma segura en sus instancias EC2 de UNIX/Linux. La autenticación para SSH utilizada con AWS se realiza a través de un par de claves públicas o privadas a fin de reducir el riesgo de accesos sin autorización a su instancia. También puede conectarse de forma remota a sus instancias de Windows por medio del protocolo de escritorio remoto (RDP) utilizando un certificado RDP generado para su instancia.

También tiene control sobre la actualización de su sistema operativo huésped, incluidas las actualizaciones de seguridad, y sobre la aplicación de parches en él. Las AMI basadas en Windows y Linux que proporciona Amazon se actualizan con regularidad con los últimos parches, por lo que, si no necesita conservar los datos ni las personalizaciones de sus instancias de las AMI de Amazon en ejecución, puede simplemente volver a lanzar instancias nuevas con la AMI que se actualizó hace menos tiempo. Además, las actualizaciones se proporcionan para la AMI de Amazon Linux a través de los repositorios yum de Amazon Linux.

Firewall: Amazon EC2 ofrece una solución de firewall completa. Este firewall de entrada obligatorio está configurado de forma predeterminada con un modo de denegación de todo, por lo que los clientes de Amazon EC2 deben abrir de forma explícita los puertos necesarios para permitir el tráfico entrante. El tráfico puede restringirse por el protocolo, por el puerto de servicio, así como por la dirección IP de origen (IP individual o bloque de direccionamiento entre dominios sin clases [CIDR]).

El firewall se puede configurar en grupos que permitan que las diferentes clases de instancias tengan reglas distintas. Por ejemplo, consideremos el caso de una aplicación web tradicional de tres capas. El grupo de los servidores web tendría abierto a Internet el puerto 80 (HTTP), el puerto 443 (HTTPS) o ambos. El grupo de los servidores de la aplicación tendría accesible el puerto 8000 (específico de la aplicación) solo para el grupo del servidor web. El grupo de los servidores de la base de datos tendría abierto el puerto 3306 (MySQL) solo para el grupo del servidor de la aplicación. Los tres grupos permitirían el acceso administrativo en el puerto 22 (SSH), pero esto solo se admitiría desde la red corporativa del cliente. Las aplicaciones con un alto nivel de seguridad se pueden implementar con este mecanismo de expresión. Observe la siguiente imagen.

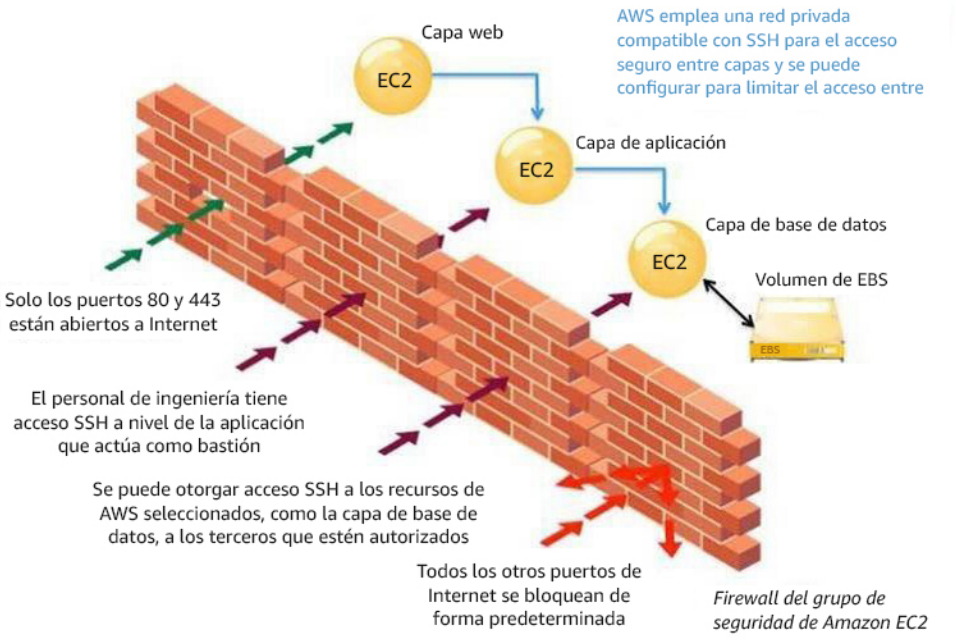


Imagen 3: Firewall del grupo de seguridad de Amazon EC2

El firewall no se controla a través del sistema operativo huésped, sino que requiere su certificado X.509 y la clave para autorizar los cambios, lo que implica una capa de seguridad adicional. AWS admite la posibilidad de otorgar acceso detallado a las diferentes funciones administrativas de las instancias y del firewall, por lo que le permite implementar seguridad adicional a través de la separación de tareas. El nivel de seguridad que brinda el firewall depende de los usuarios que lo operan, durante cuánto tiempo y con qué propósito. El estado predeterminado es el de negación de todo el tráfico entrante. Deberá planificar cuidadosamente cómo creará grupos de sus aplicaciones y defina el nivel de protección en ellas. La administración del tráfico y el diseño de seguridad basados en información adecuada siguen siendo necesarios para cada instancia. Además, AWS recomienda aplicar filtros adicionales por instancia con firewall basado en el alojamiento, como IPtables o el firewall de Windows y las VPN. Esto puede restringir tanto el tráfico entrante como el saliente.

Acceso a la API: todas las llamadas a la API para lanzar y terminar instancias, cambiar los parámetros del firewall y llevar a cabo otras funciones se firman con su clave de acceso secreta de Amazon, la cual puede ser la clave de acceso secreta de las cuentas de AWS o la clave de acceso secreta de un usuario creada con AWS IAM. Sin contar con acceso a la clave de acceso secreta, las llamadas a la API de Amazon EC2 no pueden realizarse en su nombre. Además, las llamadas a la API se pueden cifrar con SSL a fin de mantener la confidencialidad. Amazon recomienda utilizar siempre puntos de enlace de la API protegidos con SSL.

Permisos: AWS IAM también le permite controlar hasta a qué API tiene permiso un usuario para efectuar llamadas.

Seguridad de Elastic Block Storage (Amazon EBS)

Amazon Elastic Block Storage (Amazon EBS) le permite crear volúmenes de almacenamiento desde 1 GB hasta 16 TB, que las instancias de Amazon EC2 pueden montar como dispositivos.

Los volúmenes de almacenamiento se comportan como dispositivos de bloque sin procesar y sin formato, con nombres de dispositivos proporcionados por el usuario y una interfaz de dispositivos de bloque. Puede crear un sistema de archivos sobre los volúmenes de Amazon EBS o utilizarlos de cualquier otra manera en la que utilizaría un dispositivo de bloque (como un disco duro). El acceso a los volúmenes de Amazon EBS está restringido a la cuenta de AWS que creó el volumen y a los usuarios de la cuenta de AWS creados con AWS IAM, si se les otorgó acceso a las operaciones de EBS. Por consiguiente, se niega a todas las demás cuentas y usuarios de AWS el permiso de ver el volumen o acceder a él.

Los datos almacenados en los volúmenes de Amazon EBS se guardan de forma redundante en múltiples ubicaciones físicas, como parte del funcionamiento normal de esos servicios y sin cargos adicionales. Sin embargo, la replicación de Amazon EBS se almacena dentro de la misma zona de disponibilidad, no en diferentes zonas, por lo que es muy recomendable que genere instantáneas con regularidad y las guarde en Amazon S3 para preservar los datos a largo plazo. En el caso de los clientes que han diseñado bases de datos transaccionales complejas con EBS, se recomienda que las copias de seguridad en Amazon S3 se lleven a cabo a través del sistema de administración de bases de datos, de manera que se puedan analizar las transacciones y los registros distribuidos. AWS no efectúa copias de seguridad de los datos que se mantengan en discos virtuales asociados a las instancias en ejecución de Amazon EC2.

Puede generar instantáneas de los volúmenes de Amazon EBS que estén disponibles de forma pública para que otras cuentas de AWS las usen como la base para crear sus propios volúmenes. Compartir las instantáneas de los volúmenes de Amazon EBS no proporciona a las otras cuentas de AWS el permiso necesario para modificar o eliminar la instantánea original, dado que ese derecho está explícitamente reservado para la cuenta de AWS que creó el volumen. Una instantánea de EBS es una vista de nivel de bloques de un volumen de EBS completo. Tenga en cuenta que los datos que no estén visibles a través del sistema de archivos del volumen, como los archivos que

se eliminaron, pueden aparecer en la instantánea de EBS. Si desea crear instantáneas compartidas, debería hacerlo con cuidado. Si un volumen ha contenido datos confidenciales o si se han eliminado algunos de sus archivos, se debería crear un nuevo volumen de EBS. Los datos que se incluirán en la instantánea compartida deberían copiarse en el nuevo volumen y, luego, se debería crear la instantánea a partir del volumen nuevo.

Los volúmenes de Amazon EBS se presentan como dispositivos de bloque sin procesar y sin formato cuyo contenido se ha eliminado antes de ponerse a disposición para su uso. La eliminación se produce inmediatamente antes de que se pueda volver a usar, de manera que pueda estar seguro de que el proceso de eliminación se completó. Si tiene procedimientos que requieren que todos los datos se eliminen mediante un método específico, como los detallados en NIST 800-88 (“Pautas para el saneamiento de contenido multimedia”), cuenta con la posibilidad de hacerlo en Amazon EBS. Debería llevar a cabo un procedimiento de eliminación de datos especializado antes de eliminar el volumen a fin de cumplir los requisitos de conformidad que haya establecido.

Por lo general, el cifrado de datos confidenciales es una práctica recomendada para la seguridad, y AWS ofrece la posibilidad de cifrar los volúmenes de EBS y sus instantáneas con AES-256. El cifrado se produce en los servidores que alojan las instancias EC2, lo que brinda el cifrado de datos a medida que estos se mueven entre las instancias EC2 y el almacenamiento de EBS. Con el objetivo de llevar a cabo este proceso de manera eficiente y con baja latencia, el cifrado de EBS solo está disponible en los tipos de instancias más potentes de EC2 (p. ej., M3, C3, R3, G2).

Seguridad de Auto Scaling

Auto Scaling le permite ampliar o reducir de forma automática la capacidad en Amazon EC2 en función de las condiciones que usted defina. De esta manera, la cantidad de instancias de Amazon EC2 que utilice se amplía con facilidad durante los picos de demanda a fin de mantener el rendimiento y se reduce automáticamente durante los periodos de tranquilidad en la demanda para minimizar los costos.

Como todos los servicios de AWS, Auto Scaling requiere la autenticación de cada una de las solicitudes que se hagan a su API de control a fin de que solo los usuarios autenticados puedan obtener acceso a Auto Scaling y administrarlo. Las solicitudes llevan una firma HMAC-SHA1 que se calcula a partir de la solicitud y la clave privada que tiene el usuario. Sin embargo, obtener credenciales para las nuevas

instancias EC2 lanzadas con Auto Scaling puede ser un desafío para las flotas grandes o de escalado elástico. A fin de simplificar este proceso, puede utilizar los roles dentro de IAM para que cualquier instancia nueva que se lance con un rol reciba las credenciales de forma automática. Cuando lanza una instancia EC2 con un rol de IAM, se aprovisionan en ella de forma segura las credenciales de seguridad de AWS temporales con los permisos especificados por el rol y se ponen a disposición de su aplicación a través del servicio de metadatos de instancias de Amazon EC2. El servicio de metadatos pone a disposición nuevas credenciales de seguridad temporales antes de que se venzan las credenciales activas actuales, de manera que siempre haya credenciales válidas disponibles en la instancia. Además, las credenciales de seguridad temporales se rotan automáticamente varias veces por día, lo que potencia la seguridad.

También puede controlar el acceso a Auto Scaling mediante la creación de usuarios en su cuenta de AWS con AWS IAM y a través del control de qué API de Auto Scaling pueden llamar esos usuarios. Para obtener más información sobre cómo usar los roles al momento de lanzar instancias, consulte Identity and Access Management para Amazon EC2.

Servicios de red

Amazon Web Services ofrece una gama de servicios de redes que le permiten crear y definir una red aislada de forma lógica, establecer una conexión dedicada privada con la nube de AWS, usar un servicio de DNS de alta escalabilidad y disponibilidad, y entregar contenido a los usuarios finales con un servicio web de entrega de contenido a altas velocidades de transferencia y con baja latencia.

Seguridad de Elastic Load Balancing

Elastic Load Balancing se utiliza para administrar el tráfico de una flota de instancias de Amazon EC2 mediante la distribución del tráfico a las instancias de todas las zonas de disponibilidad dentro de una región. Elastic Load Balancing ofrece todas las ventajas de un balanceador de carga en las instalaciones, además de varios beneficios en materia de seguridad:

- Se encarga de las tareas de cifrado y descifrado desde las instancias de Amazon EC2 y las administra de forma centralizada en el balanceador de carga.
- Ofrece a los clientes un punto de contacto único y también puede operar como la primera línea de defensa de su red contra los ataques.

- Cuando se utiliza en una Amazon VPC, admite la creación y la administración de los grupos de seguridad asociados a su Elastic Load Balancing a fin de proporcionar más opciones de redes y seguridad.
- Admite el cifrado del tráfico de extremo a extremo con TLS (anteriormente, SSL) en las redes que utilicen conexiones HTTP seguras (HTTPS). Cuando se utiliza TLS, el certificado del servidor TLS utilizado para terminar las conexiones del cliente se puede administrar de manera centralizada en el balanceador de carga, en lugar de hacerlo en cada instancia individual.

HTTPS/TLS utiliza una clave secreta de largo plazo para generar una clave de sesión de corto plazo que se utilizará entre el servidor y el navegador a fin de crear el mensaje cifrado. Elastic Load Balancing configura su balanceador de carga con un conjunto de cifrado predefinido que se utiliza para la negociación de TLS cuando se establece una conexión entre un cliente y el balanceador de carga. El conjunto de cifrado predefinido ofrece compatibilidad con una amplia variedad de clientes y utiliza algoritmos criptográficos potentes. Sin embargo, es posible que algunos clientes tengan requisitos para permitir solo cifrados y protocolos específicos (como PCI, SOX, etc.) de los clientes a fin de asegurar que se cumplan los estándares. En estos casos, Elastic Load Balancing ofrece opciones para seleccionar diferentes configuraciones de los cifrados y los protocolos TLS. Puede elegir habilitar o deshabilitar el cifrado en función de sus requisitos específicos.

A fin de garantizar el uso de paquetes de cifrado más nuevos y potentes a la hora de establecer una conexión segura, puede configurar el balanceador de carga para que tenga la palabra final en cuanto a la selección del paquete de cifrado durante la negociación entre el cliente y el servidor. Cuando se selecciona la opción de Preferencia de orden del servidor, el balanceador de carga selecciona un paquete de cifrado basado en las prioridades del servidor en lugar de las del cliente en relación con los paquetes de cifrado. Esto le brinda mayor control sobre el nivel de seguridad que usan los clientes para conectarse a su balanceador de carga.

Para lograr un nivel de privacidad incluso más alto en las comunicaciones, Elastic Load Balancing permite el uso de la confidencialidad directa total, la cual utiliza claves de sesión efímeras que no se almacenan en ningún lugar. Esto impide que se decodifiquen los datos recopilados, incluso si la propia clave secreta de largo plazo se ha visto comprometida.

Elastic Load Balancing le permite identificar la dirección IP de origen de un cliente que se conecta a sus servidores, ya sea que esté usando balanceo de carga TCP o

HTTPS. Por lo general, la información de conexión de los clientes, como las direcciones IP y los puertos, se pierde cuando las solicitudes se procesan con un balanceador de carga como proxy. Esto se debe a que el balanceador de carga envía solicitudes al servidor en nombre del cliente, lo que hace que el balanceador de carga aparezca como si fuera el cliente solicitante. Tener la dirección IP del cliente de origen resulta útil si se necesita más información acerca de los visitantes de sus aplicaciones a fin de recopilar estadísticas de conexión, analizar registros de tráfico o administrar listas blancas de direcciones IP.

Los registros de accesos de Elastic Load Balancing contienen información acerca de cada solicitud HTTP y TCP procesada por su balanceador de carga. Esto incluye la dirección IP y el puerto del cliente solicitante, la dirección IP del backend de la instancia que procesó la solicitud, el tamaño de la solicitud y la respuesta, y la línea de solicitud real del cliente (por ejemplo, GET http://www.ejemplo.com:80/HTTP/1.1). Todas las solicitudes que se envían al balanceador de carga se registran, incluidas las solicitudes que nunca llegaron a las instancias del backend.

Seguridad de Amazon Virtual Private Cloud (Amazon VPC)

Por lo general, cada instancia de Amazon EC2 que se lanza se asigna de forma aleatoria a una dirección IP pública en el espacio de direcciones de Amazon EC2. Amazon VPC le permite crear una porción aislada de la nube de AWS y lanzar instancias de Amazon EC2 que tengan direcciones privadas (RFC 1918) en el rango de su elección (por ejemplo, 10.0.0.0/16). Puede definir las subredes dentro de su VPC y agrupar las instancias de tipos similares en función del rango de direcciones IP para luego configurar el direccionamiento y la seguridad a fin de controlar el flujo de tráfico que entra y sale de las instancias y las subredes.

AWS ofrece una variedad de plantillas de arquitectura para las VPC con configuraciones que proporcionan niveles variables de acceso público:

- **VPC con solo una subred pública.** Sus instancias se ejecutan en una sección privada y asilada de la nube de AWS con acceso directo a Internet. Las listas de control de acceso (ACL) de red y los grupos de seguridad se pueden utilizar para proporcionar un control estricto sobre el tráfico de red entrante y saliente de las instancias.
- **VPC con subredes públicas y privadas.** Además de contar con una subred pública, esta configuración agrega una subred privada cuyas instancias no son accesibles desde Internet. Las instancias de la subred privada pueden

establecer conexiones salientes hacia Internet a través de la subred pública usando la traducción de direcciones de red (NAT).

- **VPC con subredes públicas y privadas, y acceso a VPN mediante hardware.** Esta configuración agrega una conexión IPsec VPN entre su Amazon VPC y su centro de datos. De esta manera, extiende de forma efectiva el centro de datos a la nube, a la vez que proporciona acceso directo a Internet para las instancias de la subred pública de su Amazon VPC. En esta configuración, los clientes agregan un dispositivo de VPN del lado de sus centros de datos corporativos.
- **VPC con solo subred privada y acceso a VPN mediante hardware.** Sus instancias se ejecutan en una sección privada y aislada de la nube de AWS con una subred privada cuyas instancias no son accesibles desde Internet. Puede conectar esta subred privada a su centro de datos corporativo a través de un túnel IPsec VPN.

También puede conectar dos VPC usando una dirección IP privada, lo que permite a las instancias de las dos VPC comunicarse entre sí como si estuvieran dentro de la misma red. Puede crear una interconexión de VPC entre sus propias VPC o con una VPC de otra cuenta de AWS dentro de una única región.

Las características de seguridad dentro de Amazon VPC incluyen los grupos de seguridad, las ACL de red, las tablas de enrutamiento y las gateways externas. Cada uno de estos elementos se complementa con proporcionar una red aislada y segura que se puede extender a través de la habilitación selectiva de acceso directo a Internet o de la conectividad privada a otra red.

Las instancias de Amazon EC2 que se ejecutan dentro de la Amazon VPC heredan todos los beneficios que se describen a continuación en relación con el sistema operativo huésped y la protección contra el análisis de paquetes.

Sin embargo, tenga en cuenta que debe crear grupos de seguridad de VPC específicamente para su Amazon VPC, dado que cualquier grupo de seguridad de Amazon EC2 que haya creado no funcionará dentro de la Amazon VPC. Además, los grupos de seguridad de Amazon VPC cuentan con capacidades adicionales que los grupos de seguridad de Amazon EC2 no tienen, como la capacidad de cambiar el grupo de seguridad luego de lanzar la instancia y de especificar cualquier protocolo con un número de protocolo estándar (en lugar de solo TCP, UDP o ICMP).

Cada Amazon VPC es una red distinta y aislada dentro de la nube. El tráfico de red dentro de cada Amazon VPC está aislado del de todas las demás Amazon VPC. Al

momento de la creación, se selecciona un rango de direcciones IP para cada Amazon VPC. Es posible crear y asociar una gateway de Internet, una gateway virtual privada o ambas a fin de establecer una conectividad externa, sujeto a los controles que se indican a continuación.

Acceso a la API: todas las llamadas para crear y eliminar las Amazon VPC; para cambiar los parámetros del direccionamiento, el grupo de seguridad y la ACL de red; y para llevar a cabo otras funciones se firman con su clave de acceso secreta de Amazon, la cual puede ser la clave de acceso secreta de la cuenta de AWS o la clave de acceso secreta de un usuario creada con AWS IAM. Sin el acceso a la clave de acceso secreta, las llamadas a la API de Amazon VPC no pueden realizarse en su nombre. Además, las llamadas a la API se pueden cifrar con SSL a fin de mantener la confidencialidad. Amazon recomienda utilizar siempre puntos de enlace de la API protegidos con SSL. AWS IAM también permite a los clientes controlar hasta a qué API tiene permisos de llamar un usuario recién creado.

Subredes y tablas de enrutamiento: puede crear una o más subredes dentro de cada Amazon VPC. Cada instancia que se lanza en la Amazon VPC se conecta a una subred. Los ataques tradicionales a la capa 2 de seguridad, incluidas las suplantaciones de MAC y ARP, están bloqueados.

Cada subred de una Amazon VPC está asociada a una tabla de enrutamiento, y todo el tráfico de red que deja la subred se procesa a través de la tabla de enrutamiento a fin de determinar el destino.

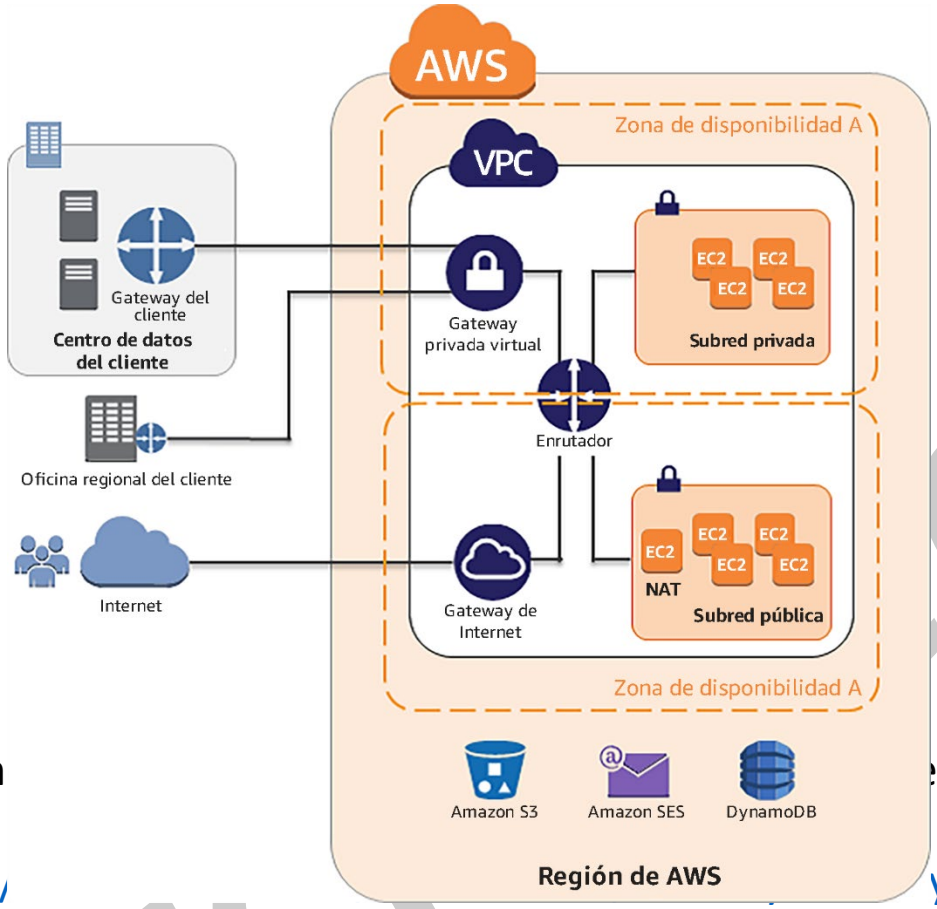
Firewall (grupos de seguridad): como Amazon EC2, la Amazon VPC admite una solución completa de firewall que permite filtrar tanto el tráfico entrante como el saliente de una instancia. El grupo predeterminado permite la comunicación entrante que provenga de otros miembros del mismo grupo y la comunicación saliente hacia cualquier destino.

El tráfico puede restringirse por cualquier protocolo de IP, por el puerto de servicio, así como por la dirección IP de origen o destino (IP individual o bloque de direccionamiento entre dominios sin clases [CIDR]).

El firewall no se controla a través del sistema operativo huésped sino que se puede modificar solo mediante la invocación de las API de Amazon VPC. AWS admite la posibilidad de otorgar acceso detallado a las diferentes funciones administrativas de las instancias y del firewall, por lo que le permite implementar seguridad adicional a través de la separación de tareas. El nivel de seguridad que brinda el firewall depende

de los puertos que se abran, durante cuánto tiempo y con qué propósito. La administración del tráfico y el diseño de seguridad basados en información adecuada siguen siendo necesarios para cada instancia.

Además, AWS recomienda aplicar filtros adicionales por instancia con firewall basado en el alojamiento, como iptables en Linux o el firewall de Windows.



For th ent, refer to:

https:/ y-compliance/

Imagen 4: Arquitectura de red de Amazon VPC

Listas de control de acceso de red: a fin de agregar una capa de seguridad más dentro de Amazon VPC, puede configurar listas de control de acceso (ACL) de red. Estas listas consisten en filtros de tráfico sin estado que se aplican a todo el tráfico entrante y saliente de una subred dentro de Amazon VPC. Estas ACL pueden contener reglas ordenadas para permitir o denegar el tráfico según el protocolo de IP, tanto por puerto de servicio como por dirección IP de origen o destino.

Al igual que los grupos de seguridad, las ACL de red se administran a través de las API de Amazon VPC, lo que agrega una capa más de protección y habilita seguridad

adicional a través de la separación de tareas. El diagrama que aparece a continuación muestra cómo los controles de seguridad anteriores se interrelacionan a fin de habilitar topologías de redes flexibles, a la vez que brindan control total sobre los flujos de tráfico de la red.

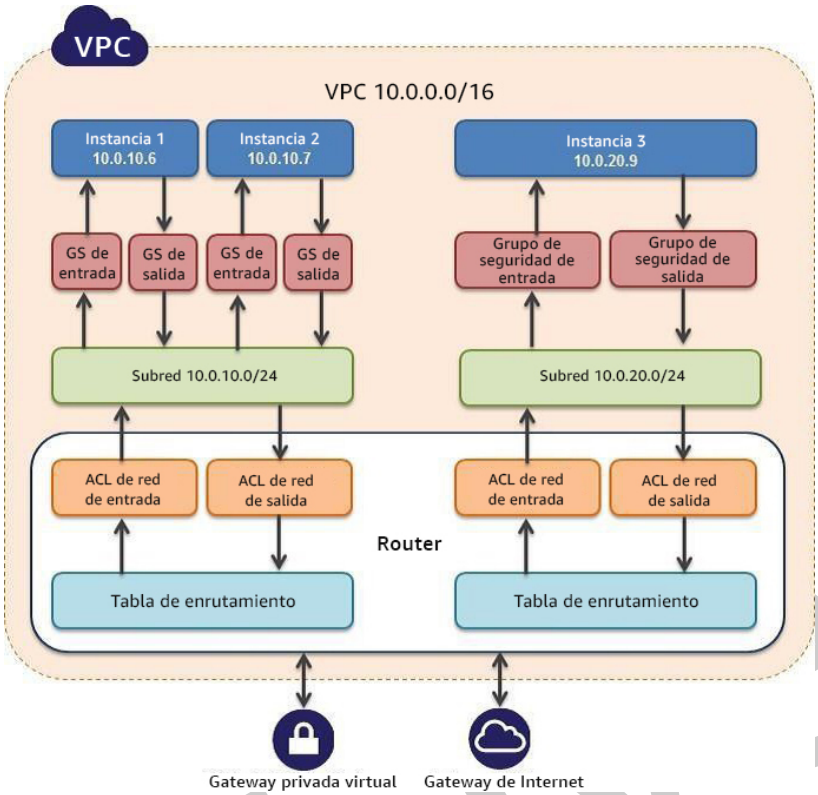


Imagen 5: Topología de redes flexibles

Gateway privada virtual: este tipo de gateway permite establecer conectividad privada entre la Amazon VPC y otra red. El tráfico de red dentro de una gateway privada virtual está aislado del tráfico de red dentro de todas las otras gateways privadas virtuales. Puede establecer conexiones de VPN a la gateway privada virtual desde los dispositivos de gateway en sus instalaciones. Cada conexión se protege con una clave compartida previamente junto con la dirección IP del dispositivo de gateway del cliente.

Gateway de Internet: se puede asociar una gateway de Internet a una Amazon VPC con el fin de permitir la conectividad directa con Amazon S3, otros servicios de AWS e Internet. Todas las instancias que deseen este acceso deben contar con una IP elástica asociada o dirigir el tráfico a través de una instancia NAT. Además, las rutas de red se configuran (consulte la información anterior) para dirigir el tráfico a la

gateway de Internet. AWS ofrece AMI NAT de referencia que se pueden ampliar para que lleven registros de la red, efectúen inspecciones de paquetes profundas, apliquen filtros a la capa de aplicaciones o lleven a cabo otros controles de seguridad.

Este acceso solo se puede modificar a través de la invocación de las API de Amazon VPC. AWS admite la posibilidad de otorgar acceso detallado a las diferentes funciones administrativas de las instancias y de la gateway de Internet, por lo que le permite implementar seguridad adicional a través de la separación de tareas. Puede utilizar una gateway con traducción de direcciones de red (NAT) a fin de permitir que las instancias de una subred privada se conecten a Internet o a otros servicios de AWS, pero evitar que Internet inicie una conexión con esas instancias.

Instancias dedicadas: dentro de una VPC, se pueden lanzar instancias de Amazon EC2 que estén físicamente aisladas en el nivel del hardware de alojamiento (es decir, que se ejecutarán en hardware de tenencia exclusiva). Las Amazon VPC se pueden crear con tenencia "dedicada" a fin de que todas las instancias que se lancen en la Amazon VPC utilicen esta característica. De forma alternativa, las VPC de Amazon se pueden crear con tenencia "predeterminada", pero se puede especificar la tenencia dedicada para instancias individuales que se lancen en la VPC.

Interfaces de red elásticas: todas las instancias de Amazon EC2 tienen una interfaz de red predeterminada que se asigna a una dirección IP privada en la red de Amazon VPC.

Puede crear una interfaz de red adicional, conocida como una interfaz de red elástica, y asociarla a cualquier instancia de Amazon EC2 de su Amazon VPC para tener un total de dos interfaces de red por instancia. Asociar más de una interfaz de red a una instancia resulta útil cuando se desea crear una red de administración, usar dispositivos de red y seguridad en su Amazon VPC, o crear instancias de doble alojamiento con cargas de trabajo o roles en subredes diferentes. Los atributos de la interfaz de red, incluidas la dirección IP privada, las direcciones IP elásticas y la dirección MAC, siguen la interfaz de red a medida que se conecta o desconecta de una instancia y se vuelve a conectar a otra instancia. Para obtener más información acerca de Amazon VPC, consulte Amazon Virtual Private Cloud.

Control de acceso a la red adicional con EC2-VPC

Si lanza instancias en una región en la cual no tenía instancias antes de que AWS lanzara la nueva característica EC2-VPC (también llamada VPC predeterminada), todas las instancias se aprovisionarán de forma automática en una VPC

predeterminada lista para usar. Puede elegir crear VPC adicionales o puede crear VPC para las instancias de las regiones en las que ya tenía instancias antes de que lanzáramos EC2-VPC.

Si crea una VPC más tarde, con una VPC regular, deberá especificar un bloque CIDR, crear subredes, escribir el direccionamiento y la seguridad para dichas subredes, y aprovisionar una gateway de Internet o una instancia NAT si desea que una de sus subredes sea capaz de acceder a Internet. Cuando lance instancias EC2 en una EC2-VPC, la mayoría de este trabajo se llevará a cabo automáticamente.

Cuando lance una instancia en una VPC predeterminada usando EC2-VPC, haremos lo siguiente a fin de configurarla por usted:

- Crearemos una subred predeterminada en cada zona de disponibilidad.
- Crearemos una gateway de Internet y la conectaremos a la VPC predeterminada.
- Crearemos una tabla de enrutamiento principal para la VPC predeterminada con una regla que envíe todo el tráfico destinado a Internet a la gateway de Internet.
- Crearemos un grupo de seguridad predeterminado y lo asociaremos a su VPC predeterminada.
- Crearemos una lista de control de acceso (ACL) de red y la asociaremos a la VPC predeterminada.
- Asociaremos las opciones de DHCP predeterminadas que se establecieron para su cuenta de AWS con la VPC predeterminada.

Además de que la VPC predeterminada tiene su propio rango de direcciones IP privadas, las instancias EC2 que se lanzan en una VPC predeterminada también pueden recibir una dirección IP pública.

La siguiente tabla resume las diferencias entre las instancias que se lanzan en EC2-Classic, las que se lanzan en una VPC predeterminada y las que se lanzan en una VPC no predeterminada.

Tabla 2: Diferencias entre las distintas instancias EC2

Característica	EC2-Classic	EC2-VPC (VPC predeterminada)	VPC regular
		Dirección IP de forma predeterminada, salvo que especifique lo contrario durante el lanzamiento.	Salvo que especifique lo contrario durante el lanzamiento.
Dirección IP privada	Su instancia recibe una dirección IP privada del rango EC2-Classic cada vez que se inicia.	Su instancia recibe una dirección IP privada estática del rango de direcciones de su VPC predeterminada.	Su instancia recibe una dirección IP privada estática del rango de direcciones de su VPC.
Múltiples direcciones IP privadas	Seleccionamos una sola dirección IP para su instancia. No admiten múltiples direcciones IP.	Puede asignar múltiples direcciones IP privadas a su instancia.	Puede asignar múltiples direcciones IP privadas a su instancia.
Dirección IP elástica	Se anula la asociación de la dirección IP elástica con la instancia cuando se detiene.	La dirección IP elástica sigue asociada a la instancia cuando se detiene.	La dirección IP elástica sigue asociada a la instancia cuando se detiene.
Nombres de host DNS	Los nombres de host DNS se habilitan de forma predeterminada.	Los nombres de host DNS se habilitan de forma predeterminada.	Los nombres de host DNS se deshabilitan de forma predeterminada.

Característica	EC2-Classic	EC2-VPC (VPC predeterminada)	VPC regular
Grupos de seguridad	Los grupos de seguridad pueden hacer referencia a grupos de seguridad que pertenezcan a otras cuentas de AWS.	Los grupos de seguridad pueden hacer referencia solo a grupos de seguridad de su VPC.	Los grupos de seguridad pueden hacer referencia solo a grupos de seguridad de su VPC.
Asociación de grupos de seguridad	Debe terminar la instancia para cambiar su grupo de seguridad.	Puede cambiar el grupo de seguridad de su instancia en ejecución.	Puede cambiar el grupo de seguridad de su instancia en ejecución.
Reglas de los grupos de seguridad	Puede agregar reglas solo para el tráfico entrante.	Puede agregar reglas para el tráfico entrante y el saliente.	Puede agregar reglas para el tráfico entrante y el saliente.
Tenencia	La instancia se ejecuta en hardware compartido. No puede ejecutar instancias en hardware de tenencia exclusiva.	Puede ejecutar la instancia en hardware compartido o en hardware de tenencia exclusiva.	Puede ejecutar la instancia en hardware compartido o en hardware de tenencia exclusiva.

Nota: Los grupos de seguridad para las instancias de EC2-Classic presentan algunas diferencias en comparación con los grupos de seguridad para las instancias de EC2-VPC. Por ejemplo, puede agregar reglas para el tráfico entrante de EC2-Classic, pero puede agregar reglas para el tráfico entrante y saliente de EC2-VPC. En EC2-Classic, no puede cambiar los grupos de seguridad asignados a una instancia después de su lanzamiento, pero, en EC2-VPC, sí puede hacerlo. Además, no puede usar los grupos de seguridad que haya creado para usar en EC2-Classic con instancias de su VPC. Debe crear grupos de seguridad para usarlos específicamente con instancias de su VPC. Las reglas que crea para usar con un grupo de seguridad de una VPC no pueden referirse a los grupos de seguridad de EC2-Classic, y viceversa.

Seguridad de Amazon Route 53

Amazon Route 53 es un servicio de sistema de nombres de dominio (DNS) de alta disponibilidad y escalabilidad que responde a las consultas de DNS mediante la traducción de los nombres de dominio en direcciones IP a fin de que los equipos puedan comunicarse entre sí. Route 53 se puede utilizar para conectar las solicitudes de los usuarios a la infraestructura que se ejecuta en AWS (como una instancia de Amazon EC2 o un bucket de Amazon S3) o a una infraestructura fuera de AWS.

Amazon Route 53 le permite administrar las direcciones IP (registros) enumeradas para sus nombres de dominio. Además, responde las solicitudes (consultas) para traducir los nombres de dominio específicos y convertirlos en las direcciones IP correspondientes. Las consultas para su dominio se dirigen automáticamente a un servidor DNS cercano por medio del uso de anycast a fin de proporcionar la latencia más baja posible. Route 53 le permite administrar el tráfico de forma global a través de distintos tipos de direccionamiento, incluidos el direccionamiento basado en la latencia (LBR), el DNS geográfico y el turno rotativo ponderado (WRR), los cuales se pueden combinar con la conmutación por error a nivel de DNS con el fin de crear distintas arquitecturas tolerantes a los errores y de baja latencia. Los algoritmos de conmutación por error implementados por Amazon Route 53 están diseñados no solo para dirigir el tráfico hacia los puntos de enlace que estén en buen estado, sino también para ayudar a evitar que se empeoren las situaciones de desastre debido a las aplicaciones y las comprobaciones de estado mal configuradas, a las sobrecargas en los puntos de enlace y a los errores de partición.

Route 53 también ofrece el registro de nombres de domino, por lo que puede comprar y administrar nombres de dominio, como ejemplo.com, y Route 53 configurará de manera automática los ajustes de DNS predeterminados de sus dominios. Puede comprar, administrar y transferir (tanto dentro como fuera) dominios desde una amplia selección de dominios genéricos y de nivel superior (TLD) específicos de cada país. Durante el proceso de registro, tiene la opción de habilitar la protección de la privacidad para su dominio. Con esta opción, la mayor parte de su información personal no será visible en la base de datos pública Whois a fin de que sea más difícil que le envíen spam o rastreen sus datos.

Amazon Route 53 se creó a partir de la infraestructura de AWS que cuenta con un alto nivel de disponibilidad y fiabilidad. El carácter distribuido de los servidores DNS de AWS contribuye a velar por que sus usuarios finales siempre se puedan dirigir a su aplicación. Route 53 contribuye también a garantizar la disponibilidad de su sitio web gracias a las comprobaciones de estado y las capacidades de conmutación por error a nivel de DNS. Es sencillo configurar Route 53 para que compruebe el estado de su sitio web periódicamente (incluso los sitios web seguros a los que se puede acceder solo mediante SSL) y para que se cambie a un sitio de respaldo si el principal no funciona.

Como todos los servicios de AWS, Amazon Route 53 requiere la autenticación de cada una de las solicitudes que se hagan a su API de control a fin de que solo los usuarios autenticados puedan obtener acceso a Amazon Route 53 y administrarlo. Las solicitudes a la API llevan una firma HMAC-SHA1 o HMAC-SHA256 que se calcula a partir de la solicitud y la clave de acceso secreta de AWS que tiene el usuario. Además, la única vía de acceso a la API de control de Amazon Route 53 son los puntos de enlace cifrados mediante SSL. Es compatible con los direccionamientos IPv4 e IPv6.

Puede controlar el acceso a las funciones de administración del DNS de Amazon Route 53 mediante la creación de usuarios en su cuenta de AWS con el servicio AWS IAM y a través del control de qué operaciones de Route 53 pueden ejecutar esos usuarios.

Seguridad de Amazon CloudFront

Amazon CloudFront ofrece a los clientes una forma sencilla de distribuir contenido entre los usuarios finales con un nivel de latencia bajo y una velocidad alta para la transferencia de datos. Entrega contenido dinámico, estático y de streaming a través de una red mundial de ubicaciones de borde. Las solicitudes de objetos de clientes se dirigen automáticamente a la ubicación de borde más cercana para que el contenido se entregue con el mejor rendimiento posible. Amazon CloudFront está optimizado

para que funcione con otros servicios de AWS, como Amazon S3, Amazon EC2, Elastic Load Balancing y Amazon Route 53. También funciona sin inconvenientes con cualquier servidor que no sea de AWS y en el que se almacenen las versiones originales y definitivas de sus archivos.

Amazon CloudFront requiere la autenticación de todas las solicitudes que se hagan a su API de control a fin de que los usuarios autorizados sean los únicos que puedan crear, modificar o eliminar el contenido que se pretende distribuir mediante Amazon CloudFront. Las solicitudes llevan una firma HMAC-SHA1 que se calcula a partir de la solicitud y la clave privada que tiene el usuario. Además, la única vía de acceso a la API de control de Amazon CloudFront son los puntos de enlace habilitados con SSL.

No se garantiza la durabilidad de los datos que se almacenen en las ubicaciones de borde de Amazon CloudFront. Es posible que, de vez en cuando, el servicio quite objetos de las ubicaciones de borde si no se los solicita con frecuencia. La durabilidad la ofrece Amazon S3, que funciona como el servidor de origen de Amazon CloudFront, ya que almacena las copias originales y definitivas de los objetos entregados con Amazon CloudFront.

Si quiere controlar quiénes podrán descargar contenido de Amazon CloudFront, puede habilitar la característica de contenido privado del servicio. Esta característica tiene dos componentes. El primer componente controla la manera en que se entrega el contenido de la ubicación de borde de Amazon CloudFront a los usuarios de Internet. El segundo componente controla la manera en que las ubicaciones de borde de Amazon CloudFront acceden a los objetos en Amazon S3. CloudFront también es compatible con la restricción geográfica, que restringe el acceso a su contenido en función de la ubicación geográfica de sus lectores.

Amazon CloudFront le permite crear una o más "identidades de acceso de origen" y asociarlas al contenido que distribuya para que controle el acceso a las copias originales de los objetos en Amazon S3. Si una identidad de acceso de origen se asocia al contenido que se distribuye mediante Amazon CloudFront, la distribución usará esa identidad para recuperar objetos de Amazon S3. Después puede usar la característica de ACL de Amazon S3, la cual restringe el acceso a esa identidad de acceso de origen a fin de que el público general no pueda leer la copia original del objeto.

Para controlar quién puede descargar objetos de las ubicaciones de borde de Amazon CloudFront, el servicio usa un sistema de verificación con direcciones URL firmadas. Para usar el sistema, en primer lugar, debe crear un par de claves pública-privada y cargar la clave pública en su cuenta mediante la consola de administración de AWS.

En segundo lugar, debe configurar la distribución de Amazon CloudFront para indicar las cuentas que autorizaría para la firma de solicitudes; puede indicar hasta cinco cuentas de AWS para esta tarea. En tercer lugar, al tiempo que reciba solicitudes, debe crear documentos de políticas en que se consignen las condiciones conforme a las cuales quiere que Amazon CloudFront atienda su contenido. En estos documentos de políticas, se puede especificar el nombre del objeto que se solicita, la fecha y la hora de la solicitud, y la IP de origen (o el intervalo de CIDR) del cliente que realiza la solicitud. Después puede determinar el algoritmo hash seguro SHA1 de su documento de políticas y firmarlo con la clave privada. Por último, debe incorporar el documento de políticas codificado y la firma como parámetros de cadena de consulta cuando haga referencia a los objetos. Si Amazon CloudFront recibe una solicitud, decodificará la firma con la clave pública. Amazon CloudFront solo atiende solicitudes que vengan acompañadas de un documento de políticas válido y de la firma complementaria.

> **Nota:** El contenido privado es una característica opcional que debe habilitar cuando configure su distribución de CloudFront. El público general podrá leer el contenido que se entregue sin previa habilitación de esta característica.

Amazon CloudFront ofrece la opción de transferir contenido a través de una conexión cifrada (HTTPS). De forma predeterminada, CloudFront acepta las solicitudes que se hagan mediante los protocolos HTTP y HTTPS. No obstante, también puede configurar CloudFront para que solo acepte el protocolo HTTPS o para que redirija las solicitudes que se hagan mediante el protocolo HTTP al protocolo HTTPS. Incluso puede configurar las distribuciones de CloudFront para que algunos objetos puedan usar HTTP y otros tengan que usar HTTPS.

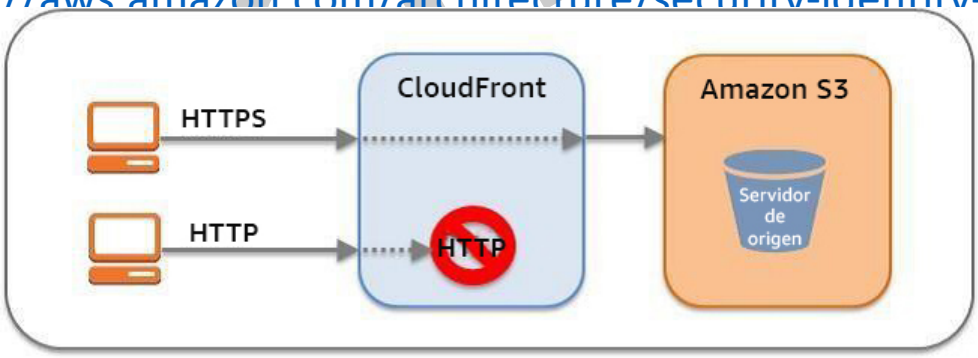


Imagen 6: Transmisión cifrada de Amazon CloudFront

Puede configurar uno o más orígenes de CloudFront para que dicho servicio recupere objetos del origen usando el protocolo que el lector haya empleado para solicitar los

objetos. Por ejemplo, si usa este ajuste de CloudFront y el lector recurre a HTTPS para solicitar un objeto de CloudFront, dicho servicio también usará HTTPS para enviar la solicitud al origen.

Amazon CloudFront usa los protocolos SSLv3 o TLSv1, además de una selección de paquetes de cifrados, incluido el protocolo Elliptic Curve Diffie-Hellman Ephemeral (ECDHE), en las conexiones establecidas con los lectores y el origen. El protocolo ECDHE permite a los clientes SSL/TLS proporcionar confidencialidad directa total, la cual usa claves de sesión efímeras que no se almacenan en ningún lugar. Eso contribuye a impedir que terceros sin autorización decodifiquen los datos recopilados, incluso si la propia clave secreta configurada para el largo plazo se haya visto comprometida.

> **Nota:** Si usa su propio servidor como origen y quiere utilizar HTTPS entre los lectores y CloudFront, y entre CloudFront y el origen, debe instalar un certificado SSL válido en el servidor HTTP que lleve la firma de una entidad de certificación externa, por ejemplo, VeriSign o DigiCert.

De forma predeterminada, puede entregar contenido a los lectores a través de HTTPS con el nombre de dominio de su distribución de CloudFront en las direcciones URL, por ejemplo, https://dxxxxx.cloudfront.net/image.jpg. Si quiere entregar su contenido a través de HTTPS usando su propio nombre de dominio y certificado SSL, puede usar uno de capa de conexión segura (SSL) personalizado con indicación de nombre de servidor (SNI) o de SSL personalizado con una IP exclusiva. Respecto del SSL personalizado con SNI, CloudFront depende de la extensión de la SNI del protocolo TLS, compatible con la mayor parte de los navegadores de hoy en día. No obstante, es posible que algunos usuarios no puedan acceder a su contenido, pues algunos navegadores antiguos no son compatibles con la SNI. (Para ver una lista de los navegadores compatibles, consulte Preguntas frecuentes sobre CloudFront). Respecto del SSL personalizado con una IP exclusiva, CloudFront asigna direcciones IP exclusivas a su certificado SSL en cada una de las ubicaciones de borde de CloudFront para que este servicio pueda asociar las solicitudes entrantes al certificado SSL que corresponda.

En los registros de acceso de Amazon CloudFront, se consigna información exhaustiva acerca de las solicitudes de contenido, incluidos el objeto que se solicitó, la fecha y la hora de la solicitud, la ubicación de borde que atendió la solicitud, la dirección IP del cliente, el que hace la derivación y el agente de usuario. Para

habilitar los registros de acceso, solo debe indicar el nombre del bucket de Amazon S3 en el cual se almacenarán los registros cuando configure la distribución de Amazon CloudFront.

Seguridad de AWS Direct Connect

Con AWS Direct Connect, puede establecer un enlace directo entre la red interna y una región de AWS mediante una conexión exclusiva de alto rendimiento.

Hacer eso puede contribuir a reducir los costos relativos a la red, aumentar el rendimiento u ofrecer una experiencia más estable en materia de redes. Sirviéndose de esa conexión exclusiva, después puede crear interfaces virtuales vinculadas de forma directa en la nube de AWS (por ejemplo, Amazon EC2 y Amazon S3) y Amazon VPC.

Gracias a Direct Connect, no necesita proveedores de Internet en su ruta de red. Puede conseguir espacio en los bastidores de las instalaciones donde esté AWS Direct Connect e implementar su equipo en las cercanías. Una vez que se haya implementado el equipo, puede conectarlo a AWS Direct Connect mediante una conexión cruzada. En cada una de las ubicaciones de AWS Direct Connect, está habilitada la conexión a la región de AWS geográficamente más cercana, además del acceso a otras regiones de EE. UU. Por ejemplo, puede establecer una conexión individual con cualquier ubicación de AWS Direct Connect en Estados Unidos y usarla para acceder a los servicios públicos de AWS en todas las regiones de EE. UU. y en AWS GovCloud (EE. UU.).

Sirviéndose de las estándares del área local virtuales (VLAN) 802.1Q estándar de la industria, la conexión exclusiva puede dividirse en varias interfaces virtuales. Ello le permite usar la misma conexión para acceder a recursos públicos, como objetos almacenados en Amazon S3, usando espacio de una dirección IP pública, así como a recursos privados, como instancias de Amazon EC2 que se ejecutan en una Amazon VPC, usando espacio de una dirección IP privada, sin dejar de mantener la separación de redes entre los entornos públicos y privados.

Amazon Direct Connect requiere el uso del protocolo de gateway de frontera (BGP), junto con un número de sistema autónomo (ASN). Crear una interfaz virtual requiere que use una clave criptográfica MD5 para autorizar mensajes. MD5 crea una función hash con clave mediante su clave secreta. Puede hacer que AWS genere de forma automática una clave MD5 con BGP o puede facilitar una propia.

Servicios de almacenamiento

Amazon Web Services brinda un servicio de almacenamiento de datos de bajo costo con mucha durabilidad y disponibilidad. AWS ofrece opciones de almacenamiento para copias de seguridad, archivo y recuperación de desastres, así como opciones de almacenamiento de bloques y objetos.

Seguridad de Amazon Simple Storage Service (Amazon S3)

Amazon Simple Storage Service (Amazon S3) le permite cargar y recuperar datos en cualquier momento y desde cualquier lugar en la Web. Amazon S3 almacena datos como objetos en los buckets. Los objetos pueden ser cualquier tipo de archivo: un archivo de texto, una foto, un video, etc.

Cuando agrega un archivo a Amazon S3, tiene la opción de incorporar metadatos en el archivo y establecer permisos para controlar el acceso al archivo. Para cada bucket, puede controlar el acceso al bucket (quién puede crear, eliminar y enumerar objetos en el bucket), consultar los registros de acceso correspondiente al bucket y sus objetos, y escoger la región geográfica en la que Amazon S3 almacenará el bucket y el contenido.

Acceso a los datos

De forma predeterminada, el acceso a los datos que se almacenen en Amazon S3 estará restringido; los propietarios de buckets y objetos serán los únicos que tendrán acceso a los recursos que hayan creado y que estén almacenados en Amazon S3 (cabe recordar que el propietario de un bucket u objeto es el propietario de la cuenta de AWS y no el usuario que creó dicho recurso). Hay muchas maneras de controlar el acceso a los buckets y los objetos.

- **Políticas de Identity and Access Management (IAM).** AWS IAM permite que las organizaciones con muchos empleados creen y gestionen varios usuarios con una única cuenta de AWS. Las políticas de IAM están asociadas a los usuarios, lo que habilita el control centralizado de los permisos para los usuarios de su cuenta de AWS respecto del acceso a los buckets o los objetos. Con las políticas de IAM, solo puede permitir el acceso a sus recursos de Amazon S3 a los usuarios de su propia cuenta de AWS.
- **Listas de control de acceso (ACL).** En Amazon S3, puede usar las ACL para otorgar a grupos de usuarios permisos de lectura o escritura en torno a los buckets o los objetos. Con las ACL, solo puede permitir el acceso a sus recursos de Amazon S3 a otras cuentas de AWS (y no a usuarios particulares).

- **Políticas de buckets.** Las políticas de buckets en Amazon S3 se pueden emplear para otorgar o denegar permisos respecto de todos o algunos de los objetos en un solo bucket. Las políticas se pueden asociar a usuarios, grupos o buckets de Amazon S3, lo que habilita la administración centralizada de los permisos. Con las políticas de buckets, puede permitir el acceso a sus recursos de Amazon S3 a los usuarios de su cuenta de AWS o de otras cuentas de AWS.

Tabla 3: Tipos de control de acceso

Tipo de control de acceso	Control a nivel de la cuenta de AWS	Control a nivel del usuario
Políticas de IAM	No	Sí
ACL	Sí	No
Políticas de buckets	Sí	Sí

Puede extender las restricciones al acceso a recursos determinados en función de ciertas condiciones. Por ejemplo, puede restringir el acceso en función de la hora de la solicitud (condición de fecha), de si la solicitud se envió con SSL (condiciones booleanas), de la dirección IP del solicitante (condición de dirección IP) o de la aplicación cliente del solicitante (condiciones de cadena). Para determinar esas condiciones, se usan claves de políticas. Para obtener más información acerca de las claves de políticas que dependen de la acción disponibles en Amazon S3, consulte la Guía para desarrolladores de Amazon Simple Storage Service

Además, Amazon S3 admite la autenticación por cadena de consulta, la cual permite compartir objetos de Amazon S3 mediante direcciones URL que son válidas durante un periodo preestablecido. La autenticación por cadena de consulta es útil para otorgar acceso por protocolo HTTP o por navegador a recursos que, en condiciones normales, exigirían autenticación. La firma que acompaña la cadena de consulta protege la solicitud.

Transferencia de datos

Para lograr la mayor seguridad posible, puede cargar o descargar datos de manera segura en Amazon S3 sirviéndose de los puntos de enlace cifrados de SSL. Se puede acceder a los puntos de enlace cifrados a través de Internet y desde Amazon EC2, de manera que los datos se transfieran de forma segura tanto dentro de AWS como hacia y desde las fuentes externas a AWS.

Almacenamiento de datos

Amazon S3 ofrece múltiples opciones para la protección de los datos en reposo. Los clientes que prefieran gestionar su propio cifrado pueden usar una biblioteca de cifrado para clientes, como Amazon S3 Encryption Client, a fin de cifrar los datos antes de cargarlos en Amazon S3.

Asimismo, puede usar el cifrado del lado del servidor (SSE) de Amazon S3 si prefiere que Amazon S3 se encargue de gestionar el proceso de cifrado por usted. Según sus requisitos, los datos se cifran mediante una clave que genera AWS o mediante una clave que usted suministra. Con el SSE de Amazon S3, puede cifrar datos a la hora de cargarlos agregando simplemente un encabezado de solicitud adicional al escribir el objeto. El descifrado ocurre de manera automática al recuperarse los datos.

> **Nota:** Los metadatos que puede incorporar en su objeto no están cifrados. Por lo tanto, AWS recomienda a los clientes que no incluyan información confidencial en los metadatos de Amazon S3.

El SSE de Amazon S3 usa uno de los sistemas de cifrado de bloque más seguros: Advanced Encryption Standard de 256 bits (AES-256). Con el SSE de Amazon S3, cada uno de los objetos protegidos está cifrado con su propia clave de cifrado. La clave del objeto a su vez se cifra con una clave maestra que se cambia periódicamente. El SSE de Amazon S3 ofrece seguridad adicional, ya que se almacenan los datos cifrados y las claves de cifrado en hosts diferentes. Además, el SSE de Amazon S3 le permite establecer requisitos de cifrado. Por ejemplo, puede crear y aplicar políticas de buckets por las que se determine que solo datos cifrados se pueden cargar en sus buckets.

En cuanto al almacenamiento a largo plazo, puede archivar de forma automática el contenido de sus buckets de Amazon S3 en el servicio de archivo de AWS llamado Amazon S3 Glacier. Puede indicar que los datos se transfieran según intervalos específicos a Amazon S3 Glacier creando reglas de ciclo de vida en Amazon S3 por las que se determine qué objetos quiere que se archiven en Amazon S3 Glacier y cuándo. En el marco de su estrategia de administración de datos, también puede especificar cuánto debe esperar Amazon S3 para eliminar los objetos después de colocarlos en Amazon S3.

Cuando se elimina un objeto de Amazon S3, la eliminación del mapeo del nombre público hacia el objeto comienza inmediatamente y, por lo general, se procesa en todo el sistema distribuido al cabo de varios segundos. Una vez que se elimina el

mapeo, no se podrá acceder de manera remota al objeto eliminado. Luego, el sistema recupera el área de almacenamiento subyacente para su uso.

Durabilidad y fiabilidad de los datos

Amazon S3 está diseñado para que los objetos tengan un grado de durabilidad del 99.999999999 % y un grado de disponibilidad del 99.99 % durante un periodo de un año. Los objetos se almacenan de forma redundante en múltiples dispositivos e instalaciones en una región de Amazon S3. Para contribuir a la durabilidad, las operaciones PUT y COPY de Amazon S3 almacenan de forma sincronizada los datos de los clientes en varias instalaciones antes de comunicar el estado SUCCESS. Después del almacenamiento, Amazon S3 ayuda a mantener la durabilidad de los objetos mediante la detección y la corrección rápidas de la pérdida de redundancia. Además, Amazon S3 corrobora periódicamente la integridad de los datos almacenados con sumas de comprobación. En el caso de que se detecte corrupción, se corrige con los datos almacenados de forma redundante. Asimismo, Amazon S3 usa sumas de comprobación en todo el tráfico de red para detectar corrupción en conjuntos de datos al almacenar o recuperar datos.

Amazon S3 ofrece más formas de protección a través del control de versiones. Puede usar el control de versiones para conservar, recuperar y restablecer todas las versiones de cada uno de los objetos que se haya almacenado en un bucket de Amazon S3. Con el control de versiones, no tendrá inconvenientes en la recuperación tras acciones involuntarias de usuarios o errores de la aplicación. De forma predeterminada, las solicitudes recuperarán la última versión escrita. Se pueden recuperar versiones anteriores de un objeto determinando la versión en la solicitud. Puede proteger más las versiones usando la característica de eliminación de MFA del control de versiones de Amazon S3. Una vez que esta característica se habilite para un bucket de Amazon S3, cada solicitud de eliminación de una versión debe incluir el número de serie y el código de seis dígitos de su dispositivo de autenticación multifactor.

Registros de acceso

Es posible configurar un bucket de Amazon S3 para que se registre el acceso al bucket y a los objetos dentro de él. En el registro de acceso, se consigna información sobre todas las solicitudes de acceso, incluidos el tipo de solicitud, el recurso que se solicitó, la dirección IP del solicitante y la hora y la fecha de la solicitud. Si se ha habilitado el registro para un bucket, los registros se agrupan periódicamente en archivos de registro y se entregan al bucket de Amazon S3 especificado.

Intercambio de recursos de origen cruzado (CORS)

Los clientes de AWS que usen Amazon S3 para alojar páginas web estáticas o almacenar objetos que se usen en otras páginas web pueden cargar contenido de forma segura mediante la configuración de un bucket de Amazon S3 para que habilite de forma explícita las solicitudes de recursos de origen cruzado. Los navegadores de hoy en día usan la política del mismo origen para que ni JavaScript ni HTML5 permitan solicitudes de carga de contenido de otro sitio o dominio. Esto se hace con el objetivo de velar que no se cargue contenido malicioso de una fuente menos fiable (por ejemplo, durante los ataques de comandos en sitios cruzados). Si se habilita la política CORS, los recursos, como las fuentes web y las imágenes, que se almacenen en un bucket de Amazon S3 podrán mencionarse sin peligro en páginas web, hojas de estilo y aplicaciones en HTML5 externas.

Seguridad de Amazon S3 Glacier

Al igual que Amazon S3, el servicio Amazon S3 Glacier ofrece almacenamiento seguro y duradero de bajo costo. No obstante, mientras que Amazon S3 está diseñado para ofrecer una recuperación rápida, Amazon S3 Glacier se creó como un servicio de archivo de datos a los que se accede con poca frecuencia y para el cual es aceptable un periodo de recuperación de varias horas.

Amazon S3 Glacier almacena ficheros en almacenes como archivos. Los archivos pueden contener uno o más objetos, y cualquier tipo de información, por ejemplo, fotos, videos o documentos. En cada almacén, entra un número ilimitado de archivos y puede crear hasta 1,000 almacenes por región. Cada archivo puede contener hasta 40 TB de información.

Carga de datos

Para transferir datos a los almacenes de Amazon S3 Glacier, puede cargar un archivo en una sola operación de carga o en varias operaciones. En una operación de carga total, puede cargar archivos de hasta 4 GB. No obstante, los clientes pueden tener mejores resultados si usan la API de carga multiparte para cargar archivos de más de 100 MB. Con la API de carga multiparte, puede cargar archivos grandes de hasta unos 40,000 GB. La llamada a la API de carga multiparte está concebida para mejorar la experiencia de carga de archivos grandes y posibilita que las partes se carguen por separado, en cualquier orden y al mismo tiempo. Si la carga por partes deja de funcionar, solo tiene que volver a cargar la parte que presentó error sin tener que trabajar con todo el archivo otra vez.

Cuando cargue datos en Amazon S3 Glacier, debe computar y aportar un hash en árbol. Amazon S3 Glacier compara el árbol con los datos como forma de corroborar que no haya sufrido cambios en el camino. Un hash en árbol se genera calculando un hash por cada segmento de datos con tamaño de megabyte y, luego, combinando los hashes en forma de árbol para representar segmentos adyacentes de datos cada vez más grandes.

Como alternativa al uso de la característica de carga multiparte, los clientes que tienen cargas muy grandes en Amazon S3 Glacier pueden considerar el uso del servicio AWS Snowball en su lugar para transferir datos. AWS Snowball facilita la migración de grandes cantidades de datos a AWS a través de dispositivos de almacenamiento portátiles para la transferencia. AWS transfiere los datos directamente fuera de los dispositivos de almacenamiento mediante la red interna de alta velocidad de Amazon sin tener que usar Internet.

También puede configurar Amazon S3 para transferir datos en intervalos específicos a Amazon S3 Glacier. Puede crear reglas de ciclo de vida en Amazon S3 que describan qué objetos quiere archivar en Amazon S3 Glacier y en qué momento. Además, puede especificar cuánto debe esperar Amazon S3 para eliminar los objetos después de que se colocan en Amazon S3.

Para lograr mayor seguridad, puede cargar o descargar datos de manera segura en Amazon S3 Glacier a través de los puntos de enlace cifrados de acuerdo con el protocolo SSL. Se puede acceder a los puntos de enlace cifrados a través de Internet y desde Amazon EC2, de manera que los datos se transfieran de forma segura tanto dentro de AWS como hacia y desde las fuentes externas a AWS.

Recuperación de datos

Para recuperar archivos de Amazon S3 Glacier, se debe iniciar un trabajo de recuperación, que generalmente se completa en un periodo de 3 a 5 horas. Luego, podrá acceder a los datos a través de las solicitudes HTTP GET. Los datos estarán disponibles durante 24 horas.

Puede recuperar un archivo completo o varios ficheros de un archivo. Si desea recuperar solamente un subconjunto de un archivo, puede usar una solicitud de recuperación para especificar el rango del archivo que contiene los ficheros que le interesan, o puede iniciar varias solicitudes de recuperación y que en cada una se especifique un rango para uno o más ficheros. También puede limitar la cantidad de

elementos del inventario de almacenes que se recuperó filtrando el rango de la fecha de creación de un archivo o configurando un límite máximo de elementos. Independientemente del método que elija, cuando recupere partes de su archivo, puede usar la suma de comprobación provista para ayudar a garantizar la integridad de los ficheros siempre que el rango que se recupere esté alineado con el hash en árbol del archivo general.

Almacenamiento de datos

Amazon S3 Glacier cifra automáticamente los datos usando AES-256 y los almacena de manera duradera sin modificaciones. Amazon S3 Glacier está diseñado para proporcionar una durabilidad anual promedio del 99.999999999 % para un archivo. Almacena cada archivo en varios dispositivos e instalaciones. A diferencia de los sistemas tradicionales que pueden requerir verificación laboriosa de los datos y reparación manual, Amazon S3 Glacier realiza comprobaciones de integridad de datos sistemáticos de manera regular y está creado para recuperarse automáticamente.

Cuando se elimina un objeto de Amazon S3 Glacier, la eliminación del mapeo del nombre público en el objeto comienza inmediatamente y, por lo general, se procesa en todo el sistema distribuido durante varios segundos. Una vez que se elimina el mapeo, no se podrá acceder de manera remota al objeto eliminado. Luego, el sistema recupera el área de almacenamiento subyacente para su uso.

Acceso a los datos

Solo su cuenta puede acceder a los datos en Amazon S3 Glacier. Para controlar el acceso a sus datos en Amazon S3 Glacier, puede usar AWS IAM y especificar qué usuarios dentro de su cuenta tienen derecho a operaciones en un almacén determinado.

Seguridad de AWS Storage Gateway

El servicio AWS Storage Gateway conecta su dispositivo de software en las instalaciones con el almacenamiento basado en la nube a fin de proporcionar una integración segura y sin inconvenientes entre el entorno de TI y la infraestructura de almacenamiento de AWS. El servicio permite que cargue datos de manera segura en el servicio de almacenamiento Amazon S3 seguro, confiable y escalable de AWS para realizar copias de seguridad rentables y recuperaciones rápidas de desastres.

AWS Storage Gateway realiza de manera transparente una copia de seguridad de los datos fuera de las instalaciones en Amazon S3 en la forma de instantáneas de Amazon EBS. Amazon S3 almacena de manera redundante estas instantáneas de

diversos dispositivos en varias instalaciones, y detecta y repara cualquier pérdida de redundancia. La instantánea de Amazon EBS proporciona una copia de seguridad en un momento dado que puede volver a almacenarse en las instalaciones o usarse para crear una instancia de nuevos volúmenes de Amazon EBS.

Los datos se almacenan dentro de una única región que usted especifica. AWS Storage Gateway ofrece tres opciones:

- **Volúmenes almacenados de la gateway (la nube es una copia de seguridad).** En esta opción, sus datos por volumen se almacenan localmente y, luego, se envían a Amazon S3, donde se almacenan de manera redundante y cifrada, y se ponen a disposición en forma de instantáneas de Amazon Elastic Block Storage (Amazon EBS). Cuando usa este modelo, el almacenamiento en las instalaciones es el principal, por lo que ofrece acceso de baja latencia a todo su conjunto de datos, y el almacenamiento en la nube es la copia de seguridad.
- **Volúmenes almacenados en memoria caché de la gateway (la nube es el almacenamiento principal).** En esta opción, sus datos por volumen se almacenan cifrados en Amazon S3, visibles dentro de la red de su empresa a través de una interfaz iSCSI. Los últimos datos a los que se ha accedido están almacenados en memoria caché en las instalaciones para recibir un acceso local de baja latencia. Cuando usa este modelo, el almacenamiento en la nube es el principal, pero recibe acceso de baja latencia a su conjunto de trabajo activo en los volúmenes almacenados en memoria caché en las instalaciones.
- **Biblioteca de cintas virtuales (VTL) de la gateway.** En esta opción, puede configurar una VTL de la gateway con hasta 10 unidades de cintas virtuales por gateway, 1 cambiador de medios y hasta 1500 cartuchos de cintas virtuales. Cada unidad de cinta virtual responde al conjunto de comandos de SCSI, por lo que sus aplicaciones de copia de seguridad existentes en las instalaciones (ya sea disco a cinta o disco a disco a cinta) funcionarán sin modificaciones.

Independientemente de la opción que elija, los datos se transfieren de manera asíncrona desde el hardware de almacenamiento en las instalaciones hacia AWS a través de SSL. Los datos se almacenan cifrados en Amazon S3 mediante Advanced Encryption Standard (AES) 256, un estándar de cifrado de clave simétrica usando claves de cifrado de 256 bits. AWS Storage Gateway solo carga datos que han cambiado, lo que minimiza la cantidad de datos que se envía a través de Internet.

AWS Storage Gateway ejecuta una máquina virtual (VM) que usted implementa en un host en su centro de datos mediante VMware ESXi Hypervisor v. 4.1 o v. 5 o Microsoft Hyper-V (descarga el software de VMware durante el proceso de configuración). También puede ejecutarla dentro de EC2 usando una AMI de la gateway. Durante el procedimiento de instalación y configuración, puede crear hasta 12 volúmenes almacenados, 20 volúmenes almacenados en memoria caché o 1500 cartuchos de cintas virtuales por gateway. Una vez instalada, cada gateway descargará, instalará e implementará automáticamente cargas y parches. Esta actividad se lleva a cabo durante un periodo de mantenimiento que puede configurar en función de la gateway.

El protocolo iSCSI admite la autenticación entre destinos e iniciadores a través del protocolo CHAP (protocolo de autenticación por desafío mutuo). El protocolo CHAP ofrece protección contra ataques del tipo “man-in-the-middle” y “playback” mediante la verificación periódica de la identidad de un iniciador iSCSI respecto de la autenticación para acceder al destino de los volúmenes de almacenamiento. Para configurar CHAP, debe configurarlo en la consola de AWS Storage Gateway y en el software del iniciador iSCSI que usa para conectarse al destino.

Después de implementar la máquina virtual de AWS Storage Gateway, debe activar la gateway mediante la consola de AWS Storage Gateway. El proceso de activación asocia la gateway con su cuenta de AWS. Después de establecer esta conexión, puede administrar casi todos los aspectos de la gateway desde la consola. En el proceso de activación, debe especificar la dirección IP de su gateway, nombrar la gateway, identificar la región de AWS en la que desea almacenar las copias de seguridad de las instantáneas y especificar la zona horaria de la gateway.

Seguridad de AWS Snowball

AWS Snowball es un método simple y seguro para transferir físicamente grandes cantidades de datos al almacenamiento de Amazon S3, EBS o Amazon S3 Glacier. Por lo general, los clientes que usan este servicio son los que tienen más de 100 GB de datos o velocidades lentas de conexión que resultarían en velocidades de transferencia muy lentas a través de Internet. Con AWS Snowball, debe preparar un dispositivo de almacenamiento portátil que luego envía a una instalación de AWS segura. AWS transfiere los datos directamente fuera de los dispositivos de almacenamiento mediante la red interna de alta velocidad de Amazon y, por lo tanto, no utiliza Internet. Por otro lado, los datos también pueden exportarse desde AWS hacia un dispositivo de almacenamiento portátil.

Al igual que todos los otros servicios de AWS, el servicio AWS Snowball requiere que identifique y autentique de manera segura su dispositivo de almacenamiento. En este caso, enviará una solicitud de trabajo a AWS que incluya el bucket de Amazon S3, la región de Amazon EBS, el ID de clave de acceso de AWS y la dirección de envío de devolución. Luego, recibirá un identificador único para el trabajo, una firma digital para autenticar su dispositivo y una dirección de AWS a la cual enviar el dispositivo de almacenamiento. Para Amazon S3, debe colocar el archivo de la firma en el directorio raíz del dispositivo. Para Amazon EBS, debe pegar el código de barras de la firma en el exterior del dispositivo. El archivo de la firma se usa solo para la autenticación y no se carga en Amazon S3 ni EBS.

Para transferencias a Amazon S3, debe especificar los buckets específicos en los que deben cargarse los datos y asegurarse de que la cuenta que realiza la carga tenga permiso escrito para los buckets. También debe especificar la lista de control de acceso que debe aplicarse a cada objeto cargado en Amazon S3.

Para transferencias a EBS, debe especificar la región de destino para la operación de importación de EBS. Si el dispositivo de almacenamiento es menor o igual que el tamaño máximo de volumen de 1 TB, su contenido se carga directamente en una instantánea de Amazon EBS. Si la capacidad del dispositivo de almacenamiento supera 1 TB, se almacena una imagen del dispositivo dentro de un bucket de registro especificado de S3. Luego, puede crear una matriz RAID de volúmenes de Amazon EBS usando software como Logical Volume Manager y copiar la imagen desde S3 hacia este nuevo volumen.

Para una mayor protección, puede cifrar los datos en el dispositivo antes de enviarlos a AWS. Para los datos de Amazon S3, puede usar un dispositivo que tenga código PIN con cifrado de hardware o software TrueCrypt para cifrar sus datos antes de enviarlos a AWS. Para los datos de EBS y Amazon S3 Glacier, puede usar cualquier método de cifrado que elija, incluido un dispositivo con código PIN. AWS cifrará los datos de Amazon S3 antes de la importación usando el código PIN o la contraseña de TrueCrypt que proporciona en el manifiesto de importación. AWS usa el PIN para acceder al dispositivo con código PIN, pero no descifra los datos cifrados mediante software para importarlos a Amazon EBS o Amazon S3 Glacier. La siguiente tabla resume las opciones de cifrado para cada tipo de trabajo de importación y exportación.

Tabla 4: Opciones de cifrado para los trabajos de importación y exportación

Importación a Amazon S3		
Origen	**Destino**	**Resultado**
• Archivos en un sistema de archivos de dispositivo • Cifre datos usando un dispositivo con código PIN o TrueCrypt antes de enviar el dispositivo	• Objetos en un bucket de Amazon S3 existente • AWS cifra los datos antes de realizar la importación	• Un objeto por cada archivo • AWS elimina su dispositivo después de cada trabajo de importación previo al envío
Exportación desde Amazon S3		
Origen	**Destino**	**Resultado**
• Objetos en uno o más buckets de Amazon S3 • Proporcione un código PIN o una contraseña que AWS usará para cifrar los datos	• Archivos en el dispositivo de almacenamiento • AWS formatea el dispositivo • AWS copia los datos en un contenedor de archivos cifrados en el dispositivo	• Un archivo por cada objeto • AWS cifra los datos antes de enviarlos • Use un dispositivo con código PIN o TrueCrypt para descifrar los archivos
Importación a Amazon S3 Glacier		
Origen	**Destino**	**Resultado**
• Todo el dispositivo • Cifre los datos usando el método de cifrado que elija antes de enviarlos	• Un archivo en un almacén de Amazon S3 Glacier existente • AWS no descifra el dispositivo	• Imagen del dispositivo almacenada como un solo archivo • AWS elimina su dispositivo después de cada trabajo de importación previo al envío

Importación a Amazon EBS (capacidad del dispositivo < 1 TB)		
Origen	**Destino**	**Resultado**
• Todo el dispositivo • Cifre los datos usando el método de cifrado que elija antes de enviarlos	• Una instantánea de Amazon EBS • AWS no descifra el dispositivo	• La imagen del dispositivo se almacena como un solo archivo • Si se cifró el dispositivo, se cifra la imagen • AWS elimina su dispositivo después de cada trabajo de importación previo al envío
Importación a Amazon EBS (capacidad del dispositivo > 1 TB)		
Origen	**Destino**	**Resultado**
• Todo el dispositivo • Cifre los datos usando el método de cifrado que elija antes de enviarlos	• Múltiples objetos en un bucket de Amazon S3 existente • AWS no descifra el dispositivo	• Imagen del objeto fragmentada en series de instantáneas de 1 TB almacenadas como objetos en un bucket de Amazon S3 especificado en un archivo de manifiesto • Si se cifró el dispositivo, se cifra la imagen • AWS elimina su dispositivo después de cada trabajo de importación previo al envío

Después de que se complete la importación, AWS Snowball eliminará el contenido del dispositivo de almacenamiento para proteger los datos durante el envío de devolución. AWS sobrescribe todos los bloques de escritura en el dispositivo de almacenamiento con ceros. Deberá volver a particionar y formatear el dispositivo después del borrado. Si AWS no puede eliminar los datos del dispositivo, se programará para su destrucción y nuestro equipo de soporte se comunicará con usted a la dirección de email especificada en el archivo de manifiesto que envíe con el dispositivo.

Cuando envía un dispositivo a otro país, se requiere la opción de aduanas y ciertos subcampos obligatorios en el archivo de manifiesto que se envía a AWS. AWS Snowball usa estos valores para validar el envío entrante y preparar los documentos salientes de aduanas. Dos de estas opciones son si los datos del dispositivo están cifrados o no y la clasificación del software de cifrado. Cuando envíe datos cifrados hacia o desde Estados Unidos, el software de cifrado debe estar clasificado como 5D992 según las normativas de administración de las exportaciones de Estados Unidos.

Seguridad de Amazon Elastic File System

Amazon Elastic File System (Amazon EFS) proporciona almacenamiento de archivos escalable y sencillo para usar con las instancias de Amazon EC2 en la nube de AWS. Con Amazon EFS, la capacidad de almacenamiento es elástica, por lo que aumenta y disminuye automáticamente a medida que agrega o elimina archivos. Los sistemas de archivos de Amazon EFS se distribuyen en una cantidad ilimitada de servidores de almacenamiento, lo que permite que los sistemas de archivos aumenten elásticamente a una escala de petabytes y permite un acceso paralelo masivo desde las instancias de Amazon EC2 hacia sus datos.

Acceso a los datos

Con Amazon EFS, puede crear un sistema de archivos, montarlo en una instancia de Amazon EC2 y, luego, leer y escribir los datos hacia el sistema de archivos y desde este. Puede montar un sistema de archivos de Amazon EFS en instancias EC2 en su VPC a través del protocolo de las versiones 4.0 y 4.1 del sistema de archivos de red (NFSv4).

Para acceder al sistema de archivos de Amazon EFS en una VPC, puede crear uno o más destinos de montaje en la VPC. Un destino de montaje proporciona una dirección IP para un punto de enlace de NFSv4. Luego, puede montar el sistema de archivos de Amazon EFS en este punto de enlace usando el nombre de DNS, lo que resolverá la dirección IP del destino de montaje de EFS en la misma zona de disponibilidad que su instancia EC2.

Puede crear un destino de montaje en cada zona de disponibilidad de una región. Si hay varias subredes en una zona de disponibilidad en su VPC, puede crear un destino de montaje en una de las subredes, y todas las instancias EC2 en esa zona de disponibilidad compartirán ese destino de montaje. También puede montar un sistema de archivos de EFS de un host en un centro de datos en las instalaciones usando AWS Direct Connect.

Cuando usa Amazon EFS, debe especificar los grupos de seguridad de Amazon EC2 para sus instancias EC2 y los grupos de seguridad para los destinos de montaje de EFS asociados al sistema de archivos. Los grupos de seguridad actúan como un firewall y las reglas que agrega definen el flujo de tráfico. Puede autorizar el acceso de entrada y salida a su sistema de archivos de EFS agregando reglas que permitan que su instancia EC2 se conecte a su sistema de archivos de Amazon EFS a través del destino de montaje que usa el puerto NFS.

Después de montar el sistema de archivos a través del destino de montaje, lo usa como cualquier otro sistema de archivos que cumpla con POSIX. Los archivos y los directorios en un sistema de archivos de EFS admiten los permisos estándar de lectura, escritura y ejecución de estilo Unix según el usuario y el ID del grupo confirmado por el cliente que monta NFSv4.1. Para obtener información acerca de los permisos de nivel NFS y las consideraciones relacionadas, consulte Trabajar con usuarios, grupos y permisos en el nivel de Network File System (NFS).

Todos los sistemas de archivos de Amazon EFS son propiedad de una cuenta de AWS. Puede usar las políticas de IAM a fin de otorgar permisos a otros usuarios para que puedan realizar operaciones administrativas en sus sistemas de archivos, lo que incluye eliminar un sistema de archivos o modificar los grupos de seguridad de un destino de montaje. Para obtener más información acerca de los permisos de EFS, consulte Información general sobre la administración de los permisos de acceso a los recursos de Amazon EFS.

Durabilidad y fiabilidad de los datos

Amazon EFS está diseñado para tener alta durabilidad y disponibilidad. Todos los datos y metadatos se almacenan en varias zonas de disponibilidad, y todos los componentes del servicio están diseñados para tener una alta disponibilidad. EFS proporciona consistencia sólida mediante la replicación de datos de forma sincrónica en todas las zonas de disponibilidad, con semántica de lectura tras escritura para la mayoría de las operaciones de archivos. Amazon EFS incorpora sumas de comprobación para todos los metadatos y los datos en todo el servicio. Con un proceso de comprobación del sistema de archivos (FSCK), EFS valida continuamente la integridad de los metadatos y los datos de un sistema de archivos.

Saneamiento de los datos

Amazon EFS está diseñado para que cuando elimine datos de un sistema de archivos, esos datos no vuelvan a usarse nunca más. Si sus procedimientos requieren que todos los datos sean borrados con un método específico, como los que se indican en

DoD 5220.22-M (“Manual de operaciones del programa de seguridad industrial nacional”) o NIST 800-88 (“Directrices para el saneamiento de soportes”), recomendamos que realice un procedimiento de borrado especializado antes de eliminar el sistema de archivos.

Servicios de bases de datos

Amazon Web Services ofrece una serie de soluciones de bases de datos para desarrolladores y empresas: desde servicios administrados de bases de datos relacionales y NoSQL hasta almacenamiento de caché en memoria como servicio y un servicio de almacén de datos a escala de petabytes.

Seguridad de Amazon DynamoDB Security

Amazon DynamoDB es un servicio de base de datos NoSQL completamente administrado que ofrece un rendimiento rápido y previsible, así como una escalabilidad óptima. Amazon DynamoDB le permite descargar las cargas administrativas de operar y escalar bases de datos distribuidas en AWS, por lo que no debe preocuparse por el aprovisionamiento, la instalación y la configuración de hardware, ni tampoco las tareas de replicación, aplicación de parches de software o escalado en clúster.

Puede crear una tabla de bases de datos que pueda almacenar y recuperar cualquier cantidad de datos, y abarcar cualquier nivel de tráfico de solicitudes. DynamoDB distribuye automáticamente los datos y el tráfico de la tabla en una cantidad apropiada de servidores con el fin de controlar la capacidad de solicitudes que usted especifique y la cantidad de datos almacenados, al mismo tiempo que mantiene la consistencia y un rendimiento rápido. Todos los elementos de los datos se almacenan en discos de estado sólido (SSD) y se replican automáticamente en múltiples zonas de disponibilidad de una región para brindar durabilidad de los datos y alta disponibilidad incorporadas.

Puede configurar copias de seguridad automáticas mediante una plantilla especial en AWS Data Pipeline, que se creó simplemente para copiar las tablas de DynamoDB. Puede elegir copias de seguridad totales o graduales para una tabla en la misma región o en una región diferente. Puede usar la copia de recuperación de desastres (DR) en caso de que un error en el código dañe la tabla original o para federar los datos de DynamoDB en todas las regiones con el fin de admitir una aplicación de varias regiones.

Para controlar quién puede usar los recursos y la API de DynamoDB, debe configurar permisos en AWS IAM. Además de controlar el acceso a nivel de recursos con IAM, también puede controlar el acceso a nivel de base de datos. Es decir, puede crear permisos a nivel de base de datos para permitir o denegar el acceso a elementos (filas) y atributos (columnas) en función de las necesidades de su aplicación. Estos permisos a nivel de base de datos se denominan controles de acceso precisos. Puede crearlos usando la política de IAM que especifica bajo qué circunstancias un usuario o una aplicación pueden acceder a una tabla de DynamoDB. La política de IAM puede restringir el acceso a elementos individuales en una tabla, el acceso a los atributos en esos elementos o ambos al mismo tiempo.

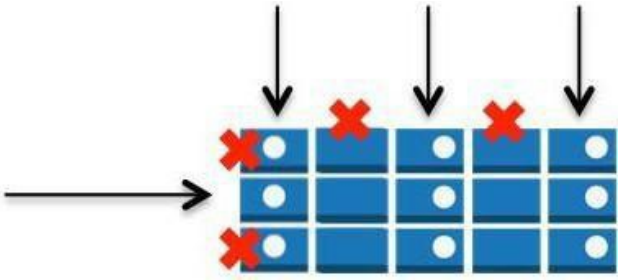


Imagen 7: Permisos a nivel de base de datos

De manera opcional, puede usar la federación de identidad web para controlar el acceso según los usuarios de la aplicación que son autenticados por Login with Amazon, Facebook o Google. La federación de identidad web elimina la necesidad de crear usuarios de IAM individuales. En su lugar, los usuarios pueden iniciar sesión en un proveedor de identidad y, luego, obtener credenciales de seguridad temporales de AWS Security Token Service (AWS STS). AWS STS devuelve a la aplicación las credenciales temporales de AWS y le permite acceder a la tabla específica de DynamoDB.

Además de necesitar permisos de usuario y base de datos, cada solicitud que se efectúa al servicio de DynamoDB debe contener una firma HMAC-SHA256 válida. De lo contrario, se rechazará la solicitud. Los SDK de AWS automáticamente firman las solicitudes. Sin embargo, si desea escribir sus propias solicitudes HTTP POST, debe proporcionar la firma en el encabezado de la solicitud a Amazon DynamoDB. Para calcular la firma, debe solicitar credenciales de seguridad temporales a AWS Security Token Service. Utilice las credenciales de seguridad temporales para firmar las solicitudes en Amazon DynamoDB. Puede acceder a Amazon DynamoDB a través de los puntos de enlace cifrados de acuerdo con los protocolos TSL/SSL.

Seguridad de Amazon Relational Database Service (Amazon RDS)

Amazon RDS le permite crear rápidamente una instancia de base de datos (DB) relacional y escalar de forma flexible los recursos informáticos asociados y la capacidad de almacenamiento para satisfacer las demandas de la aplicación. Además, Amazon RDS realiza las copias de seguridad, gestiona las conmutaciones por error y mantiene el software de la base de datos a fin de administrar la instancia de base de datos por usted. Actualmente, Amazon RDS se encuentra disponible para los motores de bases de datos de MySQL, Oracle, Microsoft SQL Server y PostgreSQL.

Amazon RDS presenta numerosas características para mejorar la fiabilidad en las bases de datos de producción esenciales. Entre estas características, se incluyen los grupos de seguridad de bases de datos, los permisos, las conexiones SSL, las copias de seguridad automatizadas, las instantáneas de base de datos y las implementaciones Multi-AZ. Las instancias de base de datos también pueden implementarse en la VPC de Amazon para ofrecer un aislamiento de redes adicional.

Control de acceso

Cuando crea por primera vez una instancia de base de datos dentro de Amazon RDS, debe crear una cuenta de usuario maestra que utilizará únicamente en el contexto de Amazon RDS para controlar el acceso a sus instancias de base de datos. La cuenta de usuario maestra es una cuenta de usuario de base de datos nativa que le permite ingresar a su instancia de base de datos con todos los privilegios que esto implica. Cuando cree la instancia de base de datos, puede especificar el nombre y la contraseña de usuario maestros que desee asociar con cada instancia. Una vez que haya creado la instancia de base de datos, puede conectarse a la base de datos a través de las credenciales de usuario maestras. Posteriormente, puede crear cuentas de usuario adicionales para restringir el acceso a su instancia de base de datos.

A través de los grupos de seguridad de base de datos, puede controlar el acceso a la instancia de base de datos de Amazon RDS. Estos grupos se asemejan a los grupos de seguridad de Amazon EC2, pero con la diferencia de que no son intercambiables. Los grupos de seguridad de base de datos actúan como un firewall que se encarga de controlar el acceso de red a su instancia de base de datos. Estos grupos de seguridad establecen el modo de acceso “Denegar todos” como valor predeterminado, por lo que los clientes deben autorizar específicamente la entrada de la red. Existen dos formas de hacerlo: puede autorizar un rango de IP de red o

puede autorizar un grupo de seguridad de Amazon EC2 existente. Los grupos de seguridad de base de datos solo permiten el acceso al puerto del servidor de la base de datos (los demás puertos están bloqueados). Además, pueden actualizarse sin necesidad de reiniciar la instancia de base de datos de Amazon RDS, lo que permite que el cliente controle fácilmente el acceso a su base de datos.

Mediante AWS IAM, puede controlar en mayor medida el acceso a sus instancias de base de datos de Amazon RDS. AWS IAM le permite controlar las operaciones de RDS que cada usuario de AWS IAM en particular tiene permitido ejecutar.

Aislamiento de redes

Para obtener un control de acceso de red adicional, puede ejecutar sus instancias de base de datos en una VPC de Amazon. Amazon VPC le permite aislar sus instancias de base de datos a través de la especificación del rango de IP que desee utilizar. Además, le permite conectarse a su infraestructura de TI existente a través de la VPN IPsec cifrada estándar de la industria. Ejecutar Amazon RDS en una VPC le permite contar con una instancia de base de datos dentro de una subred privada. Puede también configurar una gateway privada virtual que amplíe su red empresarial a su VPC y que permita el acceso a la instancia de base de datos de RDS en dicha VPC. Para obtener más información, consulte la Guía del usuario de Amazon VPC.

En el caso de las implementaciones Multi-AZ, definir una subred para todas las zonas de disponibilidad de una región permite a Amazon RDS crear una nueva instancia de reserva en otra zona de disponibilidad que pueda necesitarla. Puede crear grupos de subred de base de datos que sigan las normativas de cumplimiento para sus instancias de base de datos de RDS en una VPC. Cada grupo de subred de base de datos debe contar con al menos una subred para cada zona de disponibilidad en una región determinada. En este caso, cuando crea una instancia de base de datos en una VPC, selecciona un grupo de subred de base de datos. A continuación, Amazon RDS utiliza ese mismo grupo de subred y su zona de disponibilidad preferida para seleccionar una subred y una dirección IP dentro de esa subred. Amazon RDS crea una interfaz de red elástica y la asocia a su instancia de base de datos con esa dirección IP.

Se puede acceder a las instancias de base de datos implementadas dentro de una VPC de Amazon desde Internet o desde las instancias de Amazon EC2 que se encuentran fuera de la VPC a través de una VPN o de hosts bastiones que puede lanzar en la subred pública. Para utilizar un host bastión, deberá configurar una subred pública con una instancia EC2 que actúe como un bastión SSH. Esta subred pública debe contar con una gateway de Internet y reglas de direccionamiento que permitan dirigir

el tráfico a través del host SSH, el cual debe enviar posteriormente las solicitudes a la dirección IP privada de su instancia de base de datos de Amazon RDS.

Los grupos de seguridad de base de datos pueden utilizarse para proteger las instancias de base de datos que se encuentran dentro de una VPC de Amazon. Además, el tráfico de red entrante y saliente de cada subred puede ser aceptado o denegado a través de las listas de control de acceso (ACL) de redes. Todo el tráfico de red que ingrese a su VPC de Amazon o salga de ella a través de su conexión de VPN IPsec puede inspeccionarse por medio de su infraestructura de seguridad en las instalaciones, incluidos los firewalls de redes y los sistemas de detección de intrusiones.

Cifrado

Puede cifrar las conexiones entre su aplicación y su instancia de base de datos a través de SSL. Para MySQL y SQL Server, RDS crea un certificado SSL e instala el certificado en la instancia de base de datos cuando se aprovisiona la instancia. En el caso de MySQL, puede lanzar el cliente mysql a través del parámetro --ssl_ca para hacer referencia a la clave pública a fin de cifrar las conexiones. Por otro lado, en el caso de SQL Server, puede descargar la clave pública e importar el certificado en su sistema operativo de Windows.

Amazon RDS for Oracle utiliza el cifrado de red nativo de Oracle con una instancia de base de datos. Simplemente, debe agregar la opción de cifrado de red nativo en un grupo de opciones y asociar ese grupo con la instancia de base de datos. Una vez que se establezca una conexión cifrada, los datos transferidos entre la instancia de base de datos y su aplicación se cifrarán durante la transferencia. También puede solicitar que su instancia de base de datos solo acepte las conexiones cifradas.

Amazon RDS admite el cifrado de datos transparente (TDE) para SQL Server (SQL Server Enterprise Edition) y Oracle (parte de la opción Oracle Advanced Security disponible en Oracle Enterprise Edition). Esta característica cifra automáticamente los datos antes de que se escriban para su posterior almacenamiento y descifra los datos cuando se leen desde el almacenamiento.

> **Nota:** La compatibilidad de SSL dentro de Amazon RDS permite cifrar la conexión entre su aplicación y su instancia de base de datos. No debe depender de ella para llevar a cabo la autenticación de la instancia de base de datos.

Si bien SSL ofrece beneficios de seguridad, tenga en cuenta que el cifrado SSL representa una operación informática de uso intensivo que aumentará la latencia de su conexión de

base de datos. Para obtener más información acerca de cómo funciona SSL con SQL Server, consulte la Guía del usuario de Amazon Relational Database Service.

Copias de seguridad automatizadas e instantáneas de base de datos

Amazon RDS ofrece dos métodos diferentes para realizar copias de seguridad y restaurar sus instancias de base de datos: las copias de seguridad automatizadas y las instantáneas de base de datos.

Por defecto, la característica de copias de seguridad automatizadas de Amazon RDS permite que su instancia de base de datos se someta a una recuperación en un momento dado. Amazon RDS realizará una copia de seguridad de su base de datos y de los registros de transacciones, y los almacenará durante un periodo de retención especificado por el usuario. Esto le permite restaurar su instancia de base de datos a cualquier momento durante el periodo de retención, hasta los últimos 5 minutos. El periodo de retención de las copias de seguridad automatizadas puede configurarse por un máximo de 35 días.

Durante el periodo de copia de seguridad, es posible que la E/S de almacenamiento se suspenda mientras se realiza la copia de seguridad de sus datos. En general, la suspensión de la E/S dura unos pocos minutos. Esta suspensión se puede evitar con las implementaciones Multi-AZ de base de datos, ya que las copias de seguridad se toman de la instancia de reserva.

Las instantáneas de base de datos son copias de seguridad de su instancia de base de datos iniciadas por el usuario. Amazon RDS almacena la totalidad de las copias de seguridad de base de datos hasta que usted las elimina de forma explícita. Puede copiar las instantáneas de base de datos de cualquier tamaño y trasladarlas entre las regiones públicas de AWS o puede copiar la misma instantánea en varias regiones de forma simultánea. Cuando lo desee, puede crear una nueva instancia de base de datos a partir de una instantánea de base de datos.

Replicación de la instancia de base de datos

Los recursos informáticos de la nube de Amazon se alojan en las instalaciones de centros de datos que cuentan con una alta disponibilidad en diferentes regiones del mundo. Cada región comprende varias ubicaciones denominadas “zonas de disponibilidad”. Cada zona de disponibilidad se diseña de forma que se encuentre aislada de los errores que se producen en otras zonas de disponibilidad, y que proporcione una conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

Para diseñar bases de datos de Oracle, PostgreSQL o MySQL que dispongan de alta disponibilidad, puede ejecutar su instancia de base de datos de RDS en varias zonas de disponibilidad, una opción denominada “implementación Multi-AZ”. Cuando selecciona esta opción, Amazon automáticamente aprovisiona y mantiene una réplica sincrónica de reserva de su instancia de base de datos en una zona de disponibilidad diferente. La instancia de base de datos principal se replica de forma sincrónica entre las zonas de disponibilidad en la réplica de reserva. Si se produjera algún error en la instancia de base de datos o en una zona de disponibilidad, Amazon RDS automáticamente ejecuta una conmutación por error a la réplica de reserva, de forma que las operaciones que lleva a cabo la base de datos puedan reanudarse rápidamente sin necesidad de una intervención administrativa.

Amazon RDS ofrece la opción de réplica de lectura para aquellos clientes que utilizan MySQL y necesitan escalar más allá de los límites de la capacidad de una única instancia de base de datos para las cargas de trabajo de lectura pesada. Una vez que haya creado una réplica de lectura, las actualizaciones de la base de datos en la instancia de base de datos de origen se replican en la réplica de lectura a través de la replicación nativa y asincrónica de MySQL. Puede crear varias réplicas de lectura para una instancia de base de datos de origen determinada y distribuir el tráfico de lectura de su aplicación entre ellas. Las réplicas de lectura pueden crearse con las implementaciones Multi-AZ para obtener beneficios de escalado de lectura, además de la disponibilidad de escritura de la base de datos y la durabilidad de los datos mejoradas y proporcionadas por dichas implementaciones.

Aplicación automatizada de parches del software

Amazon RDS se asegurará de que el software de la base de datos relacional que impulsa su implementación se mantenga actualizado con los últimos parches. Cuando sea necesario, se aplicarán los parches durante un periodo de mantenimiento que puede controlar. Puede considerar al periodo de mantenimiento de Amazon RDS como una oportunidad para controlar las modificaciones de instancias de base de datos (como el escalado de una clase de instancia de base de datos) y la aplicación de parches de software cuando algunas de estas opciones se soliciten o sean necesarias. Si se programa un evento de “mantenimiento” en una semana determinada, este evento se iniciará y completará en algún momento durante el periodo de mantenimiento de 30 minutos que identifique.

Los únicos eventos de mantenimiento que Amazon RDS necesita para desactivar su instancia de base de datos son las de operaciones informáticas de escala (las cuales

tardan generalmente unos pocos minutos entre el inicio y la finalización) o la aplicación de parches requerida. La aplicación de parches necesaria se programa de forma automática únicamente en el caso de los parches relacionados con la seguridad y la durabilidad. Además, la aplicación de parches se ejecuta con poca frecuencia (generalmente, una vez cada varios meses) y, en pocas ocasiones, requiere más de una fracción de su periodo de mantenimiento. Si no especifica un periodo de mantenimiento semanal preferido cuando cree la instancia de base de datos, se asignará el valor predeterminado de 30 minutos. Si desea efectuar alguna modificación mientras se ejecuta el mantenimiento por usted, puede hacerlo si modifica su instancia de base de datos en la consola de administración de AWS o mediante la API ModifyDBInstance. Cada una de las instancias de base de datos puede contar con diferentes periodos de mantenimiento preferidos, si así lo decide.

Ejecutar su instancia de base de datos como una implementación Multi-AZ puede reducir en mayor medida el impacto del evento de mantenimiento, ya que Amazon RDS realizará el mantenimiento mediante los siguientes pasos: 1) ejecutar el mantenimiento en espera; 2) convertir la instancia de reserva a instancia principal; 3) ejecutar el mantenimiento en la instancia principal anterior, la cual ahora es la nueva instancia de reserva.

Cuando se ejecuta una API de eliminación de instancia de base de datos de Amazon RDS (DeleteDBInstance), se selecciona la instancia de base de datos para su eliminación. Cuando la instancia aparece en la consola de RDS, significa que ha sido eliminada. En este momento, ya no es posible acceder a la instancia y, a menos que se solicite una copia final de la instancia, no se puede restaurar ninguna herramienta o API la mencionará.

Notificaciones de eventos

Puede recibir notificaciones de una amplia variedad de eventos importantes que tienen lugar en su instancia de RDS como por ejemplo si la instancia finalizó, si comenzó una copia de seguridad, si se realizó una conmutación por error, si el grupo de seguridad sufrió un cambio o si hay poco espacio de almacenamiento. El servicio de Amazon RDS agrupa los eventos en diferentes categorías a las cuales puede suscribirse para recibir notificaciones cuando se produzca algún evento. Puede suscribirse a la categoría de un evento para una instancia, una instantánea, un grupo de seguridad o un grupo de parámetro de base de datos. Los eventos de RDS se publican a través de AWS SNS y se le envían por email o mensaje de texto. Para obtener más información acerca de las categorías de eventos de RDS sobre las cuales

puede recibir notificaciones, consulte la Guía del usuario de Amazon Relational Database Service.

Seguridad de Amazon Redshift

Amazon Redshift es un servicio de almacenamiento de datos SQL a escala de petabytes que ejecuta recursos informáticos y de almacenamiento de AWS administrados y sumamente optimizados. El servicio se diseñó de manera que no solo aumente o reduzca la escala rápidamente, sino que también mejore considerablemente la velocidad de consulta, incluso en el caso de conjuntos de datos masivos. Para aumentar el rendimiento, Redshift utiliza técnicas como el almacenamiento en columnas, la compresión de datos y los mapas de zonas para reducir la cantidad necesaria de entradas y salidas a fin de ejecutar consultas. Además, cuenta con una arquitectura masiva de procesamiento paralelo (MPP) que iguala y distribuye las operaciones SQL para aprovechar todos los recursos disponibles.

Cuando crea un almacén de datos de Redshift, debe aprovisionar un clúster de nodos múltiples o de un único nodo y especificar el tipo y la cantidad de nodos que conformarán el clúster. El tipo de nodo determina el tamaño de almacenamiento, la memoria y la CPU de cada nodo. Cada clúster de nodos múltiples incluye un nodo principal y dos o más nodos de computación. El nodo principal administra las conexiones, analiza las consultas, crea planes de ejecución y administra la ejecución de las consultas en los nodos de computación. Los nodos de computación almacenan datos, realizan los cálculos y ejecutan las consultas tal como lo indica el nodo principal. Se puede acceder al nodo principal de cada clúster a través de los puntos de enlace ODBC y JDBC, mediante los controladores estándar PostgreSQL. Los nodos de computación se ejecutan en una red diferente y aislada, y nunca puede accederse a ellos de forma directa.

Después de que aprovisione un clúster, puede cargar su conjunto de datos y ejecutar las consultas de análisis de datos a través de las aplicaciones de inteligencia empresarial y las herramientas basadas en SQL.

Acceso al clúster

De forma predeterminada, nadie tiene acceso a los clústeres. Amazon Redshift le permite configurar reglas de firewall (grupos de seguridad) para controlar el acceso de red a su clúster de almacenamiento de datos. Además, puede ejecutar Redshift dentro de una VPC de Amazon para aislar su clúster de almacenamiento de datos en

su propia red virtual y conectarlo a su infraestructura de TI existente a través de la VPN IPsec cifrada y estándar de la industria.

La cuenta de AWS que crea el clúster tiene acceso total al clúster. Dentro de su cuenta de AWS, puede utilizar AWS IAM para crear cuentas de usuario y administrar los permisos para dichas cuentas. A través de IAM, puede otorgar a diferentes usuarios el permiso para ejecutar únicamente operaciones relacionadas con el clúster que sean necesarias para su funcionamiento.

Al igual que todas las bases de datos, debe otorgar un permiso en Redshift a nivel de base de datos, además de otorgar acceso a nivel de recurso. Los usuarios de bases de datos son cuentas de usuario con nombres que pueden conectarse a una base de datos y se autentican cuando inician sesión en Amazon Redshift. En Redshift, puede otorgar permisos de usuario de base de datos por clúster en lugar otorgarlos por tabla. Sin embargo, un usuario puede observar los datos que figuran únicamente en las filas de la tabla que se generaron a partir de sus propias actividades. No puede observar las filas generadas por otros usuarios.

El usuario que crea un objeto de la base de datos se convierte en su propietario. De forma predeterminada, solo un superusuario o el propietario de un objeto puede consultar, modificar u otorgar permisos con respecto al objeto. Para que los usuarios puedan utilizar un objeto, debe otorgar los permisos necesarios al usuario o al grupo que comprende al usuario. Solo el propietario del objeto puede modificar o eliminar el objeto.

Copias de seguridad de los datos

Amazon Redshift distribuye sus datos en todos los nodos de computación de un clúster. Cuando ejecute un clúster con al menos dos nodos de computación, los datos de cada nodo siempre se reflejarán en los discos de otro nodo, lo que reducirá el riesgo de la pérdida de datos. Además, se realizan continuamente copias de seguridad en Amazon S3 de todos los datos escritos en un nodo de su clúster mediante las instantáneas. Redshift almacena sus instantáneas por un periodo especificado por el usuario, que puede abarcar de 1 a 35 días. Puede también tomar sus propias instantáneas en cualquier momento. Estas instantáneas aprovechan, a su vez, todas las instantáneas existentes del sistema y se retienen hasta que las elimine de forma explícita.

Amazon Redshift monitorea continuamente el estado del clúster, vuelve a replicar de forma automática los datos de las unidades que presenten errores y reemplaza los nodos según sea necesario. Aunque es posible que note un ligero deterioro del

rendimiento durante la repetición del proceso de replicación, ninguna de estas tareas requiere su participación.

A través de la consola de administración de AWS o las API de Amazon Redshift, puede utilizar cualquier instantánea de sistema o usuario para restaurar su clúster. El clúster se encontrará disponible tan pronto como los metadatos del sistema se restauren y pueda comenzar a ejecutar las consultas mientras los datos del usuario se envían en segundo plano.

Cifrado de datos

Cuando crea un clúster, puede optar por cifrarlo para brindar protección adicional a sus datos en reposo. Cuando habilita el cifrado en el clúster, Amazon Redshift almacena todos los datos en las tablas creadas por el usuario en un formato cifrado mediante las claves de cifrado del bloque AES-256 acelerado por hardware. Esto incluye a todos los datos escritos en un disco, así como todas las copias de seguridad.

Amazon Redshift utiliza una arquitectura basada en claves de cuatro niveles para el cifrado. Estas claves se componen de claves de cifrado de datos, una clave de base de datos, una clave de clúster y una clave maestra:

- Las ***claves de cifrado de datos*** se encargan de cifrar los bloques de datos en el clúster. Se asigna a cada bloque de datos una clave AES-256 que se genera de forma aleatoria. Estas claves se cifran a través de la clave de base de datos del clúster.
- La ***clave de base de datos*** se encarga de cifrar las claves de cifrado de datos en el clúster. La clave de base de datos es una clave AES-256 generada de forma aleatoria. Se almacena en un disco en una red diferente del clúster de Amazon Redshift y se envía al clúster a través de un canal seguro.
- La ***clave del clúster*** se encarga de cifrar la clave de base de datos para el clúster de Amazon Redshift. Puede utilizar AWS o un módulo de seguridad de hardware (HSM) para almacenar la clave del clúster. HSM ofrece un control directo de la generación y la administración de claves, y separa esta última de la aplicación y la base de datos.
- La ***clave maestra*** se encarga de cifrar la clave del clúster si se almacena en AWS. Si la clave del clúster se almacena en un HSM, la clave maestra cifra la clave de base de datos, la cual está cifrada, a su vez, por la clave del clúster.

Puede solicitar que Redshift rote las claves de cifrado para sus clústeres cifrados en cualquier momento. Como parte del proceso de rotación, las claves también se actualizan para todas las instantáneas manuales y automáticas del clúster.

> **Nota:** Habilitar el cifrado en su clúster afectará el rendimiento, aunque se trate de cifrado acelerado por hardware. El cifrado se implementa también en las copias de seguridad. Cuando restaure una instantánea cifrada, el nuevo clúster también se cifrará.

Para cifrar sus archivos de datos de la carga de tablas cuando los carga a Amazon S3, puede utilizar el cifrado del lado del servidor de Amazon S3. Cuando cargue los datos de Amazon S3, el comando COPY descifrará los datos a medida que se cargue la tabla.

Registros de auditorías de la base de datos

Amazon Redshift registra todas las operaciones SQL, incluidos los intentos de conexión, las consultas y los cambios que se efectúen en su base de datos. Puede acceder a estos registros a través de las consultas SQL en las tablas del sistema o puede descargarlos en un bucket de Amazon S3 seguro. Luego, puede utilizar estos registros de auditoría para monitorear su clúster y, de esta forma, ocuparse de la seguridad y la resolución de los problemas.

Aplicación automatizada de parches de software

Amazon Redshift administra todo el trabajo que conlleva la configuración, el funcionamiento y el escalado del almacenamiento de datos, que incluye el aprovisionamiento de la capacidad, el monitoreo del clúster y la aplicación de parches y actualizaciones en el motor de Amazon Redshift. Los parches se aplican únicamente durante periodos de mantenimiento específicos.

Conexiones SSL

Para proteger sus datos en tránsito dentro de la nube de AWS, Amazon Redshift utiliza conexiones SSL aceleradas por hardware a fin de comunicarse con Amazon S3 o Amazon DynamoDB y, de esta forma, llevar a cabo tanto las operaciones COPY y UNLOAD como las operaciones de restauración y de copia de seguridad. Especifique la conexión SSL en el grupo de parámetros asociado con el clúster para poder cifrar la conexión entre su cliente y el clúster. Además, puede instalar la clave pública (archivo .pem) para el certificado SSL de su cliente y puede utilizar la clave para

conectarse con sus clústeres. De esta forma, logrará que sus clientes también autentiquen el servidor de Redshift.

Amazon Redshift ofrece los conjuntos de cifrado más recientes y fiables que emplean el protocolo Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Este protocolo permite a los clientes de SSL proporcionar una confidencialidad directa total entre el cliente y el clúster de Redshift. La confidencialidad directa total recurre a las claves de la sesión, las cuales son efímeras y no se almacenan en ningún lado. De esta forma, se evita que terceros no autorizados decodifiquen los datos capturados, incluso si la clave secreta de largo plazo se ve comprometida. No necesita establecer ninguna configuración en Amazon Redshift para habilitar el protocolo. Si se conecta desde la herramienta de un cliente de SQL que utiliza el protocolo ECDHE para cifrar la comunicación entre el cliente y el servidor, Amazon Redshift utilizará la lista de cifrado que se haya proporcionado para establecer la conexión adecuada.

Seguridad de Amazon ElastiCache

Amazon ElastiCache es un servicio web que facilita la configuración, la administración y el escalado de los entornos de caché en memoria distribuida en la nube. El servicio mejora el rendimiento de las aplicaciones web, ya que le permite recuperar la información de un sistema de almacenamiento de caché en memoria rápido y administrado, en lugar de depender totalmente de bases de datos basadas en discos más lentos. Además, puede utilizarse para mejorar considerablemente la latencia y el rendimiento de varias cargas de trabajo de las aplicaciones con uso intensivo de lectura (como redes sociales, videojuegos, uso compartido de contenido multimedia y portales de preguntas y respuestas) o las cargas de trabajo de recursos informáticos de uso intensivo (como un motor de recomendación). El almacenamiento de datos esenciales en la memoria para un acceso de baja latencia permite que el almacenamiento en caché mejore el rendimiento de la aplicación. La información almacenada en caché puede incluir los resultados de las consultas de las bases de datos con respecto a las E/S de uso intensivo o los resultados de los cálculos de los recursos informáticos de uso intensivo.

El servicio de Amazon ElastiCache automatiza las tareas de administración que requieren mucho tiempo en los entornos de caché en memoria, como la administración de parches, la detección de errores y la recuperación. Funciona junto con otros servicios de Amazon Web Services (como Amazon EC2, Amazon CloudWatch, and Amazon SNS) para proporcionar un almacenamiento de caché en

memoria administrado, seguro y de alto rendimiento. Por ejemplo, una aplicación que se ejecuta en Amazon EC2 puede acceder de forma segura al clúster de Amazon ElastiCache que se ubica en la misma región y que presenta una latencia muy baja.

A través del servicio de Amazon ElastiCache, puede crear un clúster de caché. Se trata de una recopilación de uno o más nodos de caché, en la que cada uno de ellos ejecuta una instancia del servicio de Memcached. Un nodo de caché es un fragmento de tamaño fijo de RAM segura y asociada a la red. Cada nodo de caché ejecuta una instancia del servicio de Memcached y cuenta con su propio nombre y puerto DNS. Se admiten varios tipos de nodos de caché, cada uno de ellos presentan diferentes cantidades de memoria asociada. Un clúster de caché puede configurarse con una cantidad específica de nodos de caché y un grupo de parámetros de caché que controla las propiedades de cada uno de los nodos. Todos los nodos de caché que se encuentran dentro del clúster de caché se diseñan para que sean del mismo tipo de nodo y tengan las mismas configuraciones de parámetros y grupos de seguridad.

Amazon ElastiCache le permite controlar el acceso a sus clústeres de caché a través de los grupos de seguridad de caché. Un grupo de seguridad de caché actúa como un firewall, ya que se encarga de controlar el acceso de red a su clúster de caché. De forma predeterminada, el acceso de red de los clústeres de caché se encuentra desactivado. Si desea que las aplicaciones tengan acceso a su clúster de caché, debe habilitar el acceso de forma explícita desde los hosts en los grupos de seguridad de EC2 específicos. Una vez que se hayan configurado las reglas de entrada para autorizar las mismas reglas en los clústeres de caché asociados con el grupo de seguridad de caché.

Para permitir el acceso de red a su clúster de caché, cree un grupo de seguridad de caché y utilice la API de autorización de entrada del grupo de seguridad de caché o el comando de la CLI para autorizar el grupo de seguridad de EC2 deseado (que, a su vez, especifica las instancias EC2 permitidas). Actualmente, el control de acceso basado en un rango de IP no está habilitado para los clústeres de caché. Todos los clientes que dispongan de un clúster de caché deben ubicarse dentro de la red de EC2 y estar autorizados por medio de los grupos de seguridad de caché.

ElastiCache for Redis ofrece las funcionalidades de copia de seguridad y restauración, con las cuales podrá crear una instantánea de todo su clúster de Redis tal como existe en un momento específico. Puede programar instantáneas diarias, automatizadas y recurrentes, o puede crear una instantánea manual en cualquier momento. En el caso de las instantáneas automatizadas, debe especificar un periodo de retención. En cambio, las instantáneas manuales se retienen hasta que usted las

elimine. Las instantáneas se almacenan en Amazon S3 con una alta durabilidad y pueden utilizarse en los inicios en caliente, las copias de seguridad y el archivado.

Servicios de aplicaciones

Amazon Web Services ofrece una serie de servicios administrados para que los utilice con sus aplicaciones. Se incluyen servicios que brindan streaming de aplicaciones, colas, notificaciones push, entrega de emails, búsquedas y transcodificación.

Seguridad de Amazon CloudSearch

Amazon CloudSearch es un servicio administrado en la nube que facilita la configuración, la administración y el escalado de una solución de búsqueda para su sitio web. Además, este servicio le permite realizar búsquedas de grandes recopilaciones de datos, como páginas web, archivos de documentos, publicaciones en foros o información de productos. Le permite también agregar rápidamente capacidades de búsqueda a su sitio web sin necesidad de ser un experto en el tema o de preocuparse por el aprovisionamiento, la configuración y el mantenimiento del hardware. Debido a la fluctuación del volumen de sus datos y su tráfico, Amazon CloudSearch escala automáticamente para satisfacer sus necesidades.

Un dominio de Amazon CloudSearch abarca la recopilación de datos que usted desee buscar, las instancias de búsqueda que procesan sus solicitudes de búsqueda y una configuración que controla la forma en que sus datos se indexan y se buscan. Debe crear un dominio de búsqueda diferente por cada recopilación de datos en las que desee realizar una búsqueda. En cada dominio, debe configurar las opciones de indexación que describen los campos que desea incluir en su índice y la forma en que desea utilizarlos, las opciones de texto que definan las palabras excluidas específicas de un dominio, las raíces y los sinónimos, las expresiones de clasificación que puede utilizar para personalizar la forma en que se clasifican los resultados de las búsquedas y las políticas de acceso que controlan el acceso a los puntos de enlace de la búsqueda y el documento del dominio.

Todas las solicitudes de configuración de Amazon CloudSearch deben autenticarse por medio de la autenticación estándar de AWS. Amazon CloudSearch proporciona puntos de enlace diferentes para acceder a los servicios de configuración, búsqueda y documentos:

- Se puede acceder al servicio de configuración a través de un punto de enlace general: cloudsearch.us-east-1.amazonaws.com

- El punto de enlace del servicio de documentos se utiliza a fin de enviar los documentos al dominio para su indexación y se accede a él a través de un punto de enlace específico del dominio: http://doc-domainname-domainid.us-east-1.cloudsearch.amazonaws.com/
- El punto de enlace de búsqueda se utiliza para enviar las solicitudes de búsqueda al dominio. Se puede acceder a él a través de un punto de enlace específico del dominio: http://search-domainname-domainid.us-east-1.cloudsearch.amazonaws.com

Como todos los servicios de AWS, Amazon CloudSearch requiere que cada solicitud que se haya efectuado a su API de control se autentique, de forma que solo los usuarios autenticados puedan acceder y administrar su dominio de CloudSearch. Las solicitudes de API llevan una firma HMAC-SHA1 o HMAC-SHA256, las cuales se calculan a partir de la solicitud y la clave de acceso secreta de AWS del usuario. Además, se puede acceder a la API de control de Amazon CloudSearch a través de los puntos de enlace cifrados con SSL. Para controlar el acceso a las funciones de administración de Amazon CloudSearch, cree usuarios en su cuenta de AWS a través de AWS IAM y controle qué operaciones de CloudSearch estos usuarios tienen permitido realizar.

Seguridad de Amazon Simple Queue Service (Amazon SQS)

Amazon SQS es un servicio de mensajería altamente confiable que permite una comunicación asincrónica basada en mensajes entre los componentes distribuidos de una aplicación. Los componentes pueden estar en instancias de Amazon EC2 o una combinación de ambas opciones. Con Amazon SQS, puede enviar cualquier cantidad de mensajes a la cola de Amazon SQS en cualquier momento y desde cualquier componente. Puede recuperar los mensajes desde el mismo componente o desde uno diferente inmediatamente o más tarde (dentro de un plazo de 4 días). Los mensajes son sumamente duraderos. Cada mensaje se almacena de forma continua en colas de alta confiabilidad y disponibilidad. Varios procesos pueden escribir o leer desde una cola de Amazon SQS o hacia ella al mismo tiempo sin interrumpir a la otra.

El acceso a Amazon SQS se otorga en función de una cuenta de AWS o de un usuario creado con AWS IAM. Una vez que la cuenta de AWS se autentica, esta tiene acceso completo a todas las operaciones del usuario. Sin embargo, los usuarios de AWS IAM solo tienen acceso a las operaciones y las colas para las cuales se les otorgó acceso a través de la política correspondiente. De forma predeterminada, la cuenta de AWS

que creó la cola es la única que tiene acceso a la cola de cada usuario. No obstante, puede permitir otros tipos de acceso a la cola a través de una política generada por SQS o una política que usted mismo escriba.

Se puede acceder a Amazon SQS a través de los puntos de enlace cifrados con SSL. Por otro lado, se puede acceder a los puntos de enlace cifrados desde Internet y desde Amazon EC2.

AWS no cifra los datos almacenados dentro de Amazon SQS. Sin embargo, el usuario puede cifrarlos antes de que se carguen a Amazon SQS, siempre y cuando la aplicación que utiliza la cola disponga de un medio para descifrar el mensaje una vez que se recupera. Cifrar los mensajes antes de enviarlos a Amazon SQS ayuda a protegerlos de aquellas personas no autorizadas, incluido AWS, que acceden a los datos confidenciales de los clientes.

Seguridad de Amazon Simple Notification Service (Amazon SNS)

Amazon Simple Notification Service (Amazon SNS) es un servicio web que facilita la configuración, el funcionamiento y el envío de notificaciones desde la nube. Este servicio ofrece a los desarrolladores una capacidad sumamente flexible, rentable y escalable para publicar mensajes desde una aplicación y entregarlos de forma inmediata a los suscriptores o a otras aplicaciones.

Además, Amazon SNS ofrece una interfaz de servicios web simple que puede utilizarse para crear temas sobre los cuales los clientes deseen notificar a sus aplicaciones (o personas), suscribir a los clientes a estos temas, publicar mensajes, entregar estos mensajes de acuerdo al protocolo que prefiera el cliente (como HTTP/HTTPS, email, etc.).

Amazon SNS también entrega notificaciones a los clientes a través de un mecanismo "push" que elimina la necesidad de verificar o "sondear" regularmente nueva información o actualizaciones. Se puede aprovechar este servicio para crear aplicaciones de mensajería y cargas de trabajo basadas en eventos y sumamente confiables sin necesidad de una administración compleja de aplicaciones y middleware. Entre los posibles usos de Amazon SNS, se incluye el monitoreo de aplicaciones, sistemas de flujos de trabajo, actualizaciones de información urgentes, aplicaciones móviles, entre muchos otros. Amazon SNS ofrece mecanismos para el control de acceso, de forma que los temas y los mensajes estén protegidos contra los accesos no autorizados. Los propietarios de los temas pueden establecer políticas para un tema que restrinjan a las personas que pueden publicar o suscribirse a temas. Además, los propietarios de los temas pueden especificar que el mecanismo de entrega deba ser HTTPS para que logren cifrar la transmisión.

El acceso a Amazon SNS se otorga en función de una cuenta de AWS o de un usuario creado con AWS IAM. Una vez que la cuenta de AWS se autentica, esta tiene acceso completo a todas las operaciones del usuario. Sin embargo, los usuarios de AWS IAM solo tienen acceso a las operaciones y los temas para los cuales se les otorgó acceso a través de la política correspondiente. De forma predeterminada, la cuenta de AWS que creó el tema es la única que tiene acceso al tema de cada persona. No obstante, puede permitir otros tipos de acceso a SNS a través de una política generada por SNS o una política que usted mismo escriba.

Seguridad de Amazon Simple Workflow Service (Amazon SWF)

Amazon Simple Workflow Service (Amazon SWF) es un servicio que facilita la creación de aplicaciones que coordinen el trabajo entre los componentes distribuidos. A través de este servicio, puede estructurar los diferentes pasos de procesamiento en una aplicación como “tareas” que impulsan el trabajo en las aplicaciones distribuidas. Amazon SWF, además, coordina estas tareas de forma confiable y escalable. Amazon SWF administra las dependencias, la programación y la simultaneidad de la ejecución de tareas en función de la lógica de la aplicación del desarrollador. El servicio almacena tareas, las envía a los componentes de la aplicación, realiza un seguimiento de su progreso y mantiene su estado más reciente.

Amazon SWF ofrece llamadas a la API simples que pueden ejecutarse a partir de un código escrito en cualquier lenguaje y en las instancias EC2 o en cualquiera de sus máquinas ubicadas en cualquier parte del mundo donde haya acceso a Internet. Actúa como un núcleo de coordinación con el que interactúan sus hosts de aplicación. Puede crear sus flujos de trabajo deseados con las tareas asociadas y cualquier lógica condicional que desee implementar, y puede almacenarlos en Amazon SWF.

El acceso a Amazon SWF se otorga en función de una cuenta de AWS o de un usuario creado con AWS IAM. Aquellas personas que participan en la ejecución de un flujo de trabajo (responsables de la toma de decisiones, trabajadores de actividades, administradores del flujo de trabajo) deben ser usuarios de IAM desde la cuenta de AWS que posee los recursos de Amazon SWF. No puede otorgar el acceso a los flujos de trabajo de Amazon SWF a los usuarios asociados con otras cuentas de AWS. Sin embargo, los usuarios de AWS IAM solo tienen acceso a los flujos de trabajo y los recursos para los cuales se les otorgó acceso a través de la política correspondiente.

Seguridad de Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (Amazon SES) es un servicio de correo desarrollado en la infraestructura confiable y escalable de Amazon que se encarga de enviar y recibir correos en nombre de su dominio. Este servicio lo ayuda a maximizar su capacidad de entrega de emails y a mantenerse informado respecto del estado de entrega de sus emails. Además, se integra con otros servicios de AWS, de forma que facilita el envío de emails desde aplicaciones que se alojan en servicios como Amazon EC2.

Lamentablemente es posible que, en otros sistemas de email, los spammers falsifiquen el encabezado del email y alteren su dirección de origen para aparentar que proviene de una fuente diferente. Para mitigar estos problemas, Amazon SES necesita que los usuarios verifiquen su dirección o dominio de email a fin de confirmar que ellos son los propietarios y evitar que otras personas los utilicen. A fin de verificar el dominio, Amazon SES necesita que el remitente publique un registro de DNS que Amazon SES debe proporcionar como prueba de control sobre el dominio.

Amazon SES revisa regularmente el estado de verificación del dominio y anula la verificación en los casos en que ya no sea válida.

Además, Amazon SES toma medidas preventivas para impedir que se envíe contenido dudoso, de forma que los proveedores de servicios de Internet reciban constantemente emails de alta calidad desde nuestros dominios y puedan considerar a Amazon SES como un origen de email confiable. A continuación, se mencionan algunas de las características que optimizan la seguridad, la entrega y fiabilidad para todos nuestros remitentes:

- Amazon SES emplea tecnología de filtrado de contenido que ayudan a detectar y bloquear los mensajes que contengan virus o malware antes de que los envíen.
- Amazon SES mantiene los bucles de retroalimentación de quejas con los principales proveedores de servicios de Internet. Los bucles de retroalimentación de quejas indican los emails que el destinatario marcó como spam. Amazon SES le proporciona el acceso a estas métricas de entrega para ayudarlo a orientar su estrategia de envíos.
- Además, Amazon SES utiliza una amplia variedad de técnicas para medir la calidad de los envíos de cada usuario. Estos mecanismos ayudan a identificar y bloquear los intentos de utilizar Amazon SES para enviar correos no solicitados, y a detectar otros patrones de envío que podrían dañar la reputación de Amazon SES con los proveedores de servicio de Internet, los proveedores de cuentas de correo y los servicios antispam.

- Amazon SES admite mecanismos de autenticación, como el marco de directivas de remitente (SPF) y correo identificado con claves de dominio (DKIM). Cuando autentica un email, el proveedor de servicios de Internet recibe evidencia de que usted es el propietario del dominio. Amazon SES facilita la autenticación de sus emails. Si configura su cuenta de forma que pueda utilizar Easy DKIM, Amazon SES firmará sus emails en su nombre por medio de DKIM para que usted pueda enfocarse en otros aspectos de su estrategia de envío de emails. Para asegurar una capacidad entrega óptima, recomendamos que autentique sus emails.

Tal como sucede con otros servicios de AWS, debe utilizar credenciales de seguridad para verificar su identificación y si tiene el permiso necesario para interactuar con Amazon SES. Para obtener más información acerca de las credenciales que debe utilizar, consulte "Uso de credenciales con Amazon SES". Amazon SES también se integra a AWS IAM para que pueda especificar las acciones de la API de Amazon SES que un usuario puede realizar.

Si opta por comunicarse con Amazon SES a través de su interfaz SMTP, debe cifrar su conexión mediante TLS. Amazon SES admite dos mecanismos para establecer una conexión cifrada con TLS: STARTTLS y TLS Wrapper. Si opta por comunicarse con Amazon SES por medio de HTTP, se protegerá toda la comunicación mediante TLS a través del punto de enlace HTTPS de Amazon SES. Cuando entrega emails a su destino final, Amazon SES cifra el contenido del email con TLS oportunista, si lo admite el receptor.

Seguridad del servicio de Amazon Elastic Transcoder

El servicio de Amazon Elastic Transcoder simplifica y automatiza la conversión de archivos digitales desde un formato, tamaño o calidad hacia otro, lo que suele ser un proceso complejo. Además, este servicio convierte los archivos de video de alta definición (HD) o de definición estándar (SD), así como los archivos de audio. Lee la entrada de un bucket de Amazon S3, la transcodifica y escribe el archivo resultante en otro bucket de Amazon S3. Puede utilizar el mismo bucket para las entradas y las salidas, y los buckets pueden ubicarse en cualquier región de AWS. Elastic Transcoder acepta los archivos de entrada en una amplia variedad de formatos web, profesionales y de consumo. Entre los tipos de archivos de salida, se incluyen MP3, MP4, OGG, TS, WebM, HLS por medio de MPEG-2 TS y Smooth Streaming por medio de tipos de contenedor fmp4, que almacenan videos H.264 o VP8 y audios AAC, MP3 o Vorbis.

Comenzará con uno o más archivos de entrada y creará trabajos de transcodificación en un tipo de flujo de trabajo denominado “canalización de transcodificación” para cada archivo. Cuando cree la canalización, debe especificar los buckets de entrada y salida, así como el rol de IAM. Cada trabajo debe hacer referencia a una plantilla de conversión de contenido multimedia denominada “modelo predeterminado de transcodificación”, y como resultado, se generarán uno o más archivos de salida. El modelo predeterminado indica a Elastic Transcoder las configuraciones que debe implementar a la hora de procesar un archivo de entrada en particular. Cuando crea un modelo predeterminado, puede especificar varias configuraciones, incluidas la tasa de muestra, la tasa de bits, la resolución (ancho y altura de la salida), la cantidad de referencias y fotogramas clave, tasa de bits de video, algunas opciones de creación en miniatura, etc.

Se realiza un gran esfuerzo para comenzar los trabajos en el orden en que se enviaron, pero esto no es una garantía. En general, los trabajos se finalizan sin seguir un orden específico, ya que se analizan en paralelo y varían en su complejidad. Si fuera necesario, puede pausar y reanudar cualquiera de sus canalizaciones.

Elastic Transcoder admite el uso de las notificaciones de SNS cuando comienza y finaliza cada trabajo, y cuando necesita informarle que ha detectado errores o advertencias. Los parámetros de notificación de SNS se asocian con cada canalización. Además, puede utilizar la función “List Jobs by Status” para buscar todos los trabajos que presenten un estado determinado (por ejemplo, “Completed”) o la función “Read Job” para recuperar la información detallada sobre un trabajo en particular.

Controle el acceso a AWS Elastic Transcoder con AWS Identity and Access Management (IAM), lo que le permite controlar el acceso al servicio y a otros recursos de AWS que Elastic Transcoder necesita, incluidos los buckets de Amazon S3 y los temas de Amazon SNS. De forma predeterminada, los usuarios de IAM no pueden acceder a Elastic Transcoder o a los recursos que este servicio utiliza. Si desea que los usuarios de IAM trabajen con Elastic Transcoder, debe otorgarles los permisos correspondientes de forma explícita.

Amazon Elastic Transcoder requiere que cada solicitud que se haya efectuado a la API de control se autentique, de manera que solo los procesos o los usuarios autenticados puedan crear, modificar o eliminar sus propios modelos predeterminados y canalizaciones de Amazon Transcoder. Las solicitudes llevan una firma HMAC-SHA256, la cual se calcula a partir de la solicitud y una clave que deriva de la clave secreta del usuario. Además, solo se puede acceder a la API de Amazon Elastic Transcoder a través de los puntos de enlace cifrados con SSL.

Amazon S3 proporciona la durabilidad. Con este servicio, los archivos de contenido multimedia se almacenan de forma redundante en diferentes dispositivos que se encuentran en varias instalaciones en una región de Amazon S3. Para brindar una mayor protección contra los usuarios que eliminan los archivos de contenido multimedia por accidente, puede utilizar la característica de control de versiones de Amazon S3 para preservar, recuperar y restaurar cada una de las versiones de los objetos almacenados en el bucket de Amazon S3. Puede proteger más las versiones usando la característica de eliminación de MFA del control de versiones de Amazon S3. Una vez que esta característica esté habilitada para un bucket de Amazon S3, cada solicitud de eliminación de una versión debe incluir el número de serie y el código de seis dígitos de su dispositivo de autenticación multifactor.

Seguridad de Amazon AppStream 2.0

El servicio de Amazon AppStream 2.0 ofrece un marco para ejecutar las aplicaciones de streaming, especialmente aquellas aplicaciones que requieren clientes ligeros que las ejecuten en dispositivos móviles. Le permite almacenar y ejecutar su aplicación en potentes GPU de procesamiento en paralelo en la nube, y luego transmite la entrada y la salida al dispositivo de cualquier cliente. Esta puede ser una aplicación preexistente que modifica para funcionar con Amazon AppStream o una aplicación nueva que diseña específicamente para que funcione con el servicio.

El SDK de Amazon AppStream 2.0 proporciona [illegible] aplicaciones de streaming interactivas y las aplicaciones de cliente. El SDK ofrece API que conectan los dispositivos de sus usuarios finales con su aplicación, autentican, codifican audio y video, transmiten contenido a través de Internet prácticamente en tiempo real, decodifican contenido en dispositivos cliente y devuelven las entradas del usuario a la aplicación.

Como el procesamiento de la aplicación sucede en la nube, esta puede escalar para manejar cargas informáticas sumamente grandes.

Amazon AppStream 2.0 implementa aplicaciones de streaming en Amazon EC2. Cuando agrega una aplicación de streaming a través de la consola de administración de AWS, el servicio crea la AMI necesaria para alojar su aplicación y hace que su aplicación esté disponible para los clientes de streaming. El servicio escala su aplicación según sea necesario dentro de los límites de capacidad que haya establecido para satisfacer la demanda. Los clientes que utilizan el SDK de Amazon AppStream 2.0 se conectan automáticamente a su aplicación transmitida.

En la mayoría de los casos, es mejor asegurarse de que el usuario que ejecuta el cliente esté autorizado para usar la aplicación antes de permitirle obtener un ID de sesión. Recomendamos que utilice algún tipo de servicio de concesión de derechos, es decir, un servicio que autentique los clientes y los autorice a que se conecten a la aplicación. En este caso, el servicio de concesión de derechos también llamará a la API REST de Amazon AppStream 2.0 para crear una nueva sesión de streaming para el cliente. Una vez que el servicio de concesión de derechos crea una nueva sesión, devuelve el identificador de sesión al cliente autorizado como una URL de derecho de uso único. Luego, el cliente utiliza la URL de concesión de derechos para conectarse a la aplicación. Su servicio de concesión de derechos puede alojarse en una instancia de Amazon EC2 o en AWS Elastic Beanstalk.

Amazon AppStream 2.0 utiliza una plantilla de AWS CloudFormation que automatiza el proceso de implementación de una instancia EC2 de GPU que tiene instaladas las bibliotecas de AppStream 2.0 Windows Application y del SDK de Windows Client; está configurada para acceder mediante SSH, RDC, o VPN y tiene una dirección IP de Elastic asignada a ella. Cuando utiliza esta plantilla para implementar su servidor independiente de streaming, todo lo que debe hacer es cargar su aplicación al servidor y ejecutar el comando para lanzarlo.

Luego, puede utilizar la herramienta Amazon AppStream 2.0 Service Simulator para probar su aplicación en modo independiente antes de implementarla en producción.

Amazon AppStream 2.0 también utiliza el protocolo STX para administrar lo que transmite su aplicación desde AWS hacia dispositivos locales. El protocolo STX de Amazon AppStream 2.0 es un protocolo patentado utilizado para transmitir videos de aplicaciones de alta calidad en diferentes condiciones de red. Monitorea las condiciones de red y adapta automáticamente la transmisión de video para proporcionar a sus clientes una experiencia de baja latencia y alta resolución. Minimiza la latencia al tiempo que sincroniza el audio y video, además de capturar las entradas de sus clientes para enviarlas a la aplicación que se ejecuta en AWS.

Servicios de análisis

Amazon Web Services proporciona servicios de análisis basados en la nube para ayudarlo a procesar y analizar cualquier volumen de datos, ya sea que necesite clústeres de Hadoop administrados, datos de streaming en tiempo real, almacenamiento de datos a nivel de petabyte u organización.

Seguridad de Amazon EMR

Amazon EMR es un servicio web administrado que puede utilizar para ejecutar clústeres de Hadoop que procesan grandes cantidades de datos distribuyendo el trabajo y los datos entre varios servidores. Utiliza una versión mejorada del marco Apache Hadoop que se ejecuta en la infraestructura de nivel web de Amazon EC2 y Amazon S3. Simplemente carga sus datos de entrada y una aplicación de procesamiento de datos en Amazon S3. Luego, Amazon EMR lanza la cantidad de instancias de Amazon EC2 que usted especifique. El servicio comienza la ejecución del flujo de trabajo al tiempo que obtiene los datos de entrada de Amazon S3 para las instancias de Amazon EC2. Una vez que el flujo de trabajo está terminado, Amazon EMR transfiere los datos de salida a Amazon S3, de donde usted puede recuperarlos o usarlos como entrada en otro flujo de trabajo.

Cuando lanza flujos de trabajo para usted, Amazon EMR configura dos grupos de seguridad de Amazon EC2: uno para los nodos maestros y otro para los nodos esclavos. El grupo de seguridad maestro tiene un puerto abierto para comunicarse con el servicio. También tiene abierto el puerto SSH para permitirle el uso de SSH en las instancias mediante la clave especificada en el inicio. Los nodos esclavos comienzan en un grupo de seguridad separado que solo permite la interacción con la instancia maestra. De manera predeterminada, ambos grupos de seguridad se configuran de manera que no permitan el acceso a recursos externos, incluidas las instancias de Amazon EC2 que pertenecen a otros clientes. Debido a que estos son grupos de seguridad de su cuenta, puede reconfigurarlos usando las herramientas o el panel de EC2 estándar. Para proteger los conjuntos de datos de entrada y salida, Amazon EMR transfiere datos hacia y desde Amazon S3 usando SSL.

Amazon EMR brinda varias maneras de controlar el acceso a los recursos de su clúster. Puede utilizar AWS IAM para crear cuentas de usuario y roles, y configurar los permisos que controlan a qué funciones de AWS pueden acceder esos usuarios y roles. Cuando lanza un clúster, puede asociar un par de claves de Amazon EC2 con el clúster, el cual luego puede utilizar cuando se conecte al clúster mediante SSH. También puede establecer permisos que permitan otros usuarios que no sean el usuario predeterminado de Hadoop para enviar trabajos a su clúster.

De manera predeterminada, si un usuario de IAM lanza un clúster, ese clúster estará oculto para otros usuarios de IAM en la cuenta de AWS. El filtrado ocurre en todas las interfaces de Amazon EMR (la consola, la CLI, la API y los SDK) y ayuda a evitar que los usuarios de IAM accedan y cambien involuntariamente los clústeres creados por otros usuarios de IAM.

Esto es útil para los clústeres que se supone que serán vistos por un solo usuario de IAM y la cuenta principal de AWS. También tiene la opción de establecer que todos los usuarios de IAM de una misma cuenta AWS puedan ver el clúster y acceder a él.

Para obtener una capa adicional de protección, puede lanzar las instancias EC2 de su clúster de EMR a una VPC de Amazon, que es similar a lanzarlo a una subred privada. Esto le permite controlar el acceso a toda la subred. También puede lanzar el clúster a una VPC y habilitar el clúster para que acceda a recursos de su red interna mediante una conexión de VPN. Puede cifrar los datos de entrada antes de cargarlos a Amazon S3 utilizando cualquier herramienta común de cifrado de datos. Si hace esto, debe agregar un paso de descifrado al comienzo del flujo de trabajo cuando Amazon Elastic MapReduce recupere los datos de Amazon S3.

Seguridad de Amazon Kinesis

Amazon Kinesis es un servicio administrado diseñado para controlar el streaming en tiempo real de big data. Puede aceptar cualquier cantidad de datos, de cualquier cantidad de orígenes, y aumentar o reducir la escala según sea necesario. Puede utilizar Kinesis en situaciones que requieran la entrada y el procesamiento de datos en tiempo real y a gran escala, como, por ejemplo, registros de servidores, redes sociales o fuentes de datos comerciales, y datos de secuencias de clics web.

Las aplicaciones leen y escriben registros de datos en Amazon Kinesis en secuencias. Puede crear cualquier cantidad de secuencias de Kinesis para capturar, almacenar y transportar datos. Amazon Kinesis administra automáticamente la infraestructura, el almacenamiento, la red y la configuración que se necesita para recolectar y procesar sus datos al nivel de rendimiento que demandan sus aplicaciones de streaming. No necesita preocuparse acerca del aprovisionamiento, la implementación o el mantenimiento continuo del hardware, el software u otros servicios para habilitar la captura y el almacenamiento en tiempo real de datos a gran escala.

Amazon Kinesis también replica datos de manera sincrónica en tres instalaciones de una región de AWS, por lo que ofrece una alta disponibilidad y durabilidad de los datos.

En Amazon Kinesis, los registros de datos contienen un número de secuencia, una clave de partición y un blob de datos, que es una secuencia de bytes inmutable que no fue interpretada. El servicio de Amazon Kinesis no inspecciona, interpreta ni modifica los datos en el blob de ninguna manera. Se puede acceder a los registros de datos durante solo 24 horas desde el momento en que se agregan a una secuencia de Amazon Kinesis y, luego, se descartan automáticamente.

Su aplicación consume una secuencia de Amazon Kinesis, que normalmente se ejecuta en una flota de instancias de Amazon EC2. Una aplicación de Kinesis utiliza la biblioteca de clientes de Amazon Kinesis para leer de la secuencia de Amazon Kinesis. La biblioteca de clientes de Kinesis se ocupa de varios detalles, como la conmutación por error, la recuperación y el equilibrio de carga, lo que permite a su aplicación centrarse en el procesamiento de los datos en cuanto estén disponibles. Después de procesar el registro, su código de consumidor puede pasarlo a otra secuencia de Kinesis, escribirlo en un bucket de Amazon S3, un almacén de datos de Redshift o una tabla DynamoDB, o simplemente puede descartarlo. Cuenta con una biblioteca de conectores disponible para ayudarlo a integrar Kinesis a otros

servicios de AWS (como DynamoDB, Redshift y Amazon S3), además de productos de terceros, como Apache Storm.

Puede controlar el acceso lógico a los recursos y las funciones administrativas de Kinesis creando usuarios en su cuenta de AWS mediante AWS IAM y controlando qué operaciones de Kinesis estos usuarios tiene permitido realizar. Para facilitar la ejecución de sus aplicaciones productoras o consumidoras en una instancia de Amazon EC2, puede configurar esa instancia con un rol de IAM. De esa manera, las credenciales de AWS que reflejan los permisos asociados con el rol de IAM se habilitan para las aplicaciones en la instancia, lo que significa que no es necesario que utilice las credenciales de seguridad de AWS a largo plazo. Los roles tienen el beneficio adicional de ofrecer credenciales temporales que vencen con un corto lapso, lo que agrega una medida adicional de protección. Consulte la Guía del usuario de AWS Identity and Access Management para obtener más información acerca de los roles de IAM.

Solo se puede acceder a la API de Amazon Kinesis a través de un punto de enlace cifrado con SSL (kinesis.us-east-1.amazonaws.com) para garantizar una transmisión segura de sus datos a AWS. Debe conectarse a ese punto de enlace para acceder a Kinesis, pero luego puede utilizar la API para indicarle a AWS Kinesis que cree una secuencia en cualquier región de AWS.

Seguridad de AWS Data Pipeline

El servicio de AWS Data Pipeline lo ayuda a procesar y migrar datos entre diferentes orígenes de datos en intervalos especificados mediante flujos de trabajo basados en datos y comprobaciones de dependencias integradas. Cuando crea una canalización, define los orígenes de datos, las precondiciones, los destinos, los pasos de procesamiento y un programa operativo. Una vez que defina y active una canalización, esta se ejecutará de manera automática de acuerdo con el programa que usted especificó.

Con AWS Data Pipeline, no necesita preocuparse por comprobar la disponibilidad de los recursos, administrar las dependencias entre tareas, volver a probar errores o tiempos de espera en tareas individuales ni crear un sistema de notificación de errores. AWS Data Pipeline se ocupa de lanzar los servicios y los recursos de AWS que su canalización necesita para procesar los datos (p. ej. Amazon EC2 o EMR) y transferir los resultados que se debe almacenar (p. ej. Amazon S3, RDS, DynamoDB o EMR).

Cuando utiliza la consola, AWS Data Pipeline crea los roles y las políticas de IAM necesarios, incluida una lista de entidades confiables. Los roles de IAM determinan a qué puede acceder su canalización y las acciones que puede llevar a cabo. Además, cuando su canalización crea un recurso, como, por ejemplo, una instancia EC2, los roles de IAM determinan los recursos y las acciones que permite la instancia EC2. Cuando crea una canalización, especifica un rol de IAM que gobierna la canalización y otro rol de IAM que gobierna los recursos de la canalización (conocido como “rol de recurso”), que puede ser el mismo para ambos. Como parte de la práctica recomendada de seguridad de mínimo privilegio, le recomendamos que considere cuáles son los permisos mínimos necesarios para que la canalización funcione y defina los roles de IAM en consecuencia.

Como la mayoría de los servicios de AWS, AWS Data Pipeline también ofrece la opción de puntos de enlace seguros (HTTPS) para acceder mediante SSL.

Servicios de implementación y administración

Amazon Web Services ofrece varias herramientas para ayudar con la implementación y la administración de sus aplicaciones. Esto incluye servicios que le permiten crear cuentas individuales de usuario con credenciales para acceder a los servicios de AWS. También incluye servicios para crear y actualizar pilas de recursos de AWS, implementar aplicaciones en dichos recursos y monitorear sus estados. Otras herramientas lo ayudan a administrar claves criptográficas usando módulos de seguridad de hardware (HSM) y registrar la actividad de la API de AWS con fines de seguridad y cumplimiento.

AWS Identity and Access Management (IAM)

IAM le permite crear varios usuarios y administrar los permisos de cada uno de estos usuarios dentro de su cuenta de AWS. Un usuario es una identidad (dentro de la cuenta de AWS) con credenciales de seguridad únicas que se pueden utilizar para acceder a los servicios de AWS. IAM elimina la necesidad de compartir contraseñas o claves, y facilita habilitar o deshabilitar el acceso de un usuario según sea necesario.

IAM le permite implementar prácticas recomendadas de seguridad, como el mínimo privilegio, al otorgar credenciales únicas a cada usuario en su cuenta de AWS y otorgar permisos solamente para acceder a los servicios y recursos de AWS necesarios para que los usuarios lleven a cabo sus trabajos. IAM es seguro de manera predeterminada. Los usuarios nuevos no tienen acceso a AWS hasta que se otorguen permisos explícitos.

IAM también está integrado a AWS Marketplace, de manera que pueda controlar quién en su organización puede suscribirse al software y los servicios que se ofrecen en Marketplace. Se trata de una función importante de control de acceso, ya que suscribirse a determinado software en Marketplace implica el lanzamiento de una instancia EC2 para ejecutar el software. Usar IAM para controlar el acceso a AWS Marketplace también permite a los dueños de cuentas de AWS tener un control detallado del uso y los costos de software.

IAM le permite minimizar el uso de sus credenciales de la cuenta de AWS. Una vez que crea cuentas de usuario de IAM, todas las interacciones con los servicios y los recursos de AWS deben ocurrir con credenciales de seguridad de usuario de IAM.

Roles

Un rol de IAM utiliza credenciales temporales de seguridad para permitirle delegar el acceso a usuarios o servicios que normalmente no tienen acceso a sus recursos de AWS. Un rol es un conjunto de permisos para acceder a recursos de AWS específicos, pero estos permisos no están ligados a un usuario o grupo de IAM específico. Una entidad autorizada (p. ej. usuario móvil, instancia EC2) asume un rol y recibe credenciales de seguridad temporales para autenticar a los recursos definidos en el rol.

Las credenciales de seguridad temporales proporcionan mejoras en la seguridad debido a su corta duración (el vencimiento predeterminado es de 12 horas) y el hecho de que no se pueden reutilizar una vez que se vencen. Esto puede ser particularmente útil para proporcionar acceso limitado y controlado en ciertas situaciones:

- **Acceso de usuario federado (que no pertenecen a AWS).** Los usuarios federados son usuarios (o aplicaciones) que no tienen cuentas de AWS. Con los roles, les puede otorgar acceso a sus recursos de AWS durante un periodo limitado. Esto es útil si usted tiene usuarios que no pertenecen a AWS que puede autenticar con un servicio externo, como Microsoft Active Directory, LDAP o Kerberos. Las credenciales de AWS temporales utilizadas con los roles proporcionan identidad federada entre AWS y los usuarios que no pertenecen a AWS en su sistema de autorización e identidad corporativa.

Si su organización admite SAML 2.0 (Security Assertion Markup Language 2.0), puede crear relaciones de confianza entre su organización, en calidad de proveedora de identidad (IdP), y otras organizaciones, en calidad de proveedoras de servicio. En AWS, puede configurar AWS como el proveedor de servicio y usar SAML para proporcionar a los usuarios un inicio de sesión único (SSO) federado a la consola de administración de AWS o para obtener acceso federado a fin de llamar a las API de AWS.

Los roles también son útiles si crea una aplicación móvil o web que acceda a los recursos de AWS. Los recursos de AWS requieren credenciales de seguridad para las solicitudes mediante programación. Sin embargo, no debe incorporar credenciales de seguridad de largo plazo en su aplicación, ya que los usuarios de la aplicación pueden acceder a ellas y puede ser difícil rotarlas.

En su lugar, deje que los usuarios inicien sesión usando Login with Amazon, Facebook o Google y, luego, usen su información de autenticación para asumir un rol y obtener credenciales de seguridad temporales.

- **Acceso entre cuentas.** En el caso de las organizaciones que usan varias cuentas de AWS para administrar sus recursos, puede configurar roles para permitir que los usuarios que tienen permisos en una cuenta accedan a recursos desde otra cuenta. En el caso de las organizaciones con personal que no suele necesitar acceso a recursos desde otra cuenta, el uso de roles ayuda a garantizar que las credenciales se proporcionen de manera temporal, solo cuando sea necesario.
- **Aplicaciones que se ejecutan en instancias EC2 que necesitan acceder a recursos de AWS.** Si una aplicación se ejecuta en una instancia de Amazon EC2 y necesita hacer solicitudes de recursos de AWS, como buckets de Amazon S3 o una tabla de DynamoDB, debe tener credenciales de seguridad. Usar roles en lugar de crear cuentas individuales de IAM para cada aplicación en cada instancia puede ahorrar bastante tiempo a los clientes que administran una gran cantidad de instancias o una flota de escalado elástico mediante AWS Auto Scaling.

Las credenciales temporales incluyen un token de seguridad, un ID de clave de acceso y una clave de acceso secreta. Para otorgarle a un usuario acceso a ciertos recursos, debe distribuir las credenciales de seguridad temporales al usuario al que le otorga el acceso temporal. Cuando el usuario realiza llamadas a sus recursos, presenta el token y el ID de clave de acceso, y firma la solicitud con la clave de acceso secreta.

El token no funcionará con claves de acceso diferentes. La manera en que el usuario presenta el token depende de la API y la versión del producto de AWS al que realiza las llamadas. Para obtener más información acerca de las credenciales de seguridad temporales, consulte la referencia de la API de servicio del token de seguridad de AWS.

El uso de credenciales temporales implica protección adicional para usted porque no tiene que administrar ni distribuir credenciales de largo plazo a usuarios temporales. Además, las credenciales temporales se cargan automáticamente a la instancia de destino para que no tenga que incorporarlas en algún lugar poco seguro como su código. Las credenciales temporales reciben rotaciones y modificaciones automáticas varias veces al día sin ninguna acción de su parte, y cuentan con almacenamiento seguro de manera predeterminada.

Para obtener más información acerca del uso de roles de IAM para aprovisionar claves de manera automática en instancias EC2, consulte la documentación de AWS Identity and Access Management.

Seguridad Amazon CloudWatch

Amazon CloudWatch es un servicio web que proporciona monitoreo para recursos en la nube de AWS, comenzando con Amazon EC2. Ofrece a los clientes visibilidad de la utilización de recursos, rendimiento operativo y patrones generales de demanda, incluidas las métricas como el uso de CPU, las lecturas y las escrituras de disco y el tráfico de red. Puede configurar alarmas de CloudWatch para que lo notifiquen si se cruzan ciertos límites o para tomar otras medidas automatizadas, como agregar o eliminar instancias EC2 si está activado Auto Scaling.

CloudWatch captura y resume las métricas de uso de manera nativa para los recursos de AWS, pero también puede establecer que se envíen otros registros a CloudWatch para su monitoreo. Puede dirigir archivos de su sistema operativo invitado, aplicación y registro personalizado para el software instalado en sus instancias EC2 a CloudWatch, donde se almacenarán durante el tiempo que desee. Puede configurar CloudWatch para que monitoree las entradas de registro que ingresan para cualquier símbolo o mensaje que desee y para presentar los resultados como métricas de CloudWatch. Por ejemplo, podría monitorear los archivos de registros del servidor web para buscar los mensajes de error 404 y detectar vínculos de entrada incorrectos, o los mensajes de usuario no válido para detectar intentos de inicio de sesión sin autorización en su sistema operativo invitado.

Como todos los servicios de AWS, Amazon CloudWatch requiere la autenticación de todas las solicitudes que se hagan a su API de control a fin de que el acceso y la gestión de CloudWatch se circunscriba a los usuarios autenticados. Las solicitudes llevan una firma HMAC-SHA1 que se calcula a partir de la solicitud y la clave privada que tiene el usuario. Asimismo, la única vía de acceso a la API de control de Amazon CloudWatch son los puntos de enlace cifrados con SSL.

También puede controlar el acceso a Amazon CloudWatch creando los usuarios en su cuenta de AWS mediante AWS IAM y controlando a qué operaciones de CloudWatch estos usuarios tienen permitido llamar.

Seguridad de AWS CloudHSM

El servicio de AWS CloudHSM ofrece a los clientes acceso dedicado a un dispositivo de módulo de seguridad de hardware (HSM) diseñado para proporcionar almacenamiento y operaciones de claves criptográficas de manera segura en un dispositivo resistente a intrusiones y manipulaciones. Puede generar, almacenar, y administrar las claves criptográficas utilizadas para el cifrado de datos de manera que solo usted pueda acceder. Los dispositivos AWS CloudHSM están diseñados para almacenar y procesar material de claves criptográficas de manera segura para una amplia variedad de usos, como el cifrado de base de datos, la administración de derechos digitales (DRM), la infraestructura de claves públicas (PKI), la autenticación y la autorización, la firma de documentos y el procesamiento de transacciones. Admiten algunos de los algoritmos criptográficos más fiables disponibles, incluidos AES, RSA y ECC, entre muchos otros.

El servicio de AWS CloudHSM está diseñado para usarse con Amazon EC2 y VPC, lo que le brinda al dispositivo su propia IP privada dentro de una subred privada. Puede conectarse a dispositivos CloudHSM desde sus servidores EC2 a través de SSL/TLS, que utiliza autenticación bidireccional de certificados digitales y cifrado SSL de 256 bits para proporcionar un canal de comunicación seguro.

Si selecciona el servicio de CloudHSM en la misma región que la instancia EC2, se reduce la latencia de la red, lo que puede mejorar el rendimiento de la aplicación. Puede configurar un cliente en su instancia EC2 que permita que sus aplicaciones utilicen las API proporcionadas por el HSM, incluidos PKCS#11, MS CAPI y Java JCA/JCE (Java Cryptography Architecture/Java Cryptography Extensions).

Antes de comenzar a usar un HSM, debe crear al menos una partición en el dispositivo. Una partición criptográfica es un límite de seguridad lógica y física que

restringe el acceso a sus claves, de manera tal que usted controla sus claves y las operaciones que lleva a cabo el HSM. AWS tiene credenciales administrativas para el dispositivo, pero solo es posible usar estas credenciales para administrar el dispositivo, no las particiones de HSM en el dispositivo. AWS utiliza estas credenciales para monitorear y mantener el estado y la disponibilidad del dispositivo. AWS no puede extraer sus claves ni provocar que el dispositivo realice ninguna operación criptográfica con sus claves.

El dispositivo HSM cuenta con mecanismos de detección de manipulación física y lógica y respuesta, que borran el material de la clave criptográfica y generan registros de eventos si se detecta una manipulación. El HSM está diseñado para detectar la manipulación si se viola la barrera física del dispositivo HSM. Además, luego de tres intentos infructuosos de acceder a una partición de HSM con credenciales de administrador de HSM, el dispositivo HSM elimina sus particiones de HSM.

Cuando finaliza su suscripción de CloudHSM y confirma que los contenidos del HSM ya no son necesarios, debe eliminar cada partición y su contenido, además de todos los registros. Como parte del proceso de retirada, AWS restablece a cero el dispositivo, lo que elimina permanentemente todo el material de claves.

AWS CloudTrail Security

AWS CloudTrail ofrece un registro de acciones de los usuarios y del sistema que afectan los recursos de AWS dentro de su cuenta. Para cada evento registrado, puede ver a qué servicio se accedió, qué acción se llevó a cabo, cuáles fueron los parámetros de dicha acción y quién efectuó la solicitud. Para acciones de mutación, puede ver el resultado de la acción. No solo puede ver cuáles de sus usuarios o servicios llevaron a cabo una acción en un servicio de AWS, sino que también puede ver si fue en calidad de usuario de la cuenta raíz de AWS o de usuario de IAM, o si se realizó con credenciales de seguridad temporales para un rol o un usuario federado.

CloudTrail captura información sobre llamadas a la API a un recurso de AWS, independientemente de si la llamada se realizó desde la consola de administración, la CLI o un SDK de AWS. Si la solicitud de la API devolvió un error, CloudTrail proporciona la descripción del error, incluidos los mensajes para errores de autorización. Incluso captura los eventos de inicio de sesión de la consola de administración de AWS mediante la creación de una entrada de registro cada vez que un propietario de una cuenta de AWS, un usuario federado o un usuario de IAM simplemente inicia sesión en la consola.

Una vez que haya activado CloudTrail, los registros de eventos se entregan, aproximadamente, cada 5 minutos al bucket de Amazon S3 de su elección. Los archivos de registro se organizan según ID de cuenta de AWS, región, nombre de servicio, fecha y hora. Puede configurar CloudTrail para que agrupe los archivos de registros provenientes de varias regiones o cuentas en un único bucket de Amazon S3. De forma predeterminada, un único registro de seguimiento registrará y entregará eventos de todas las regiones actuales y futuras. Además de S3, puede enviar eventos a CloudWatch Logs para establecer métricas y alarmas personalizadas, o puede cargar los registros en sus soluciones de administración y análisis de registros favoritas a fin de llevar a cabo análisis de seguridad y detectar patrones de comportamiento de los usuarios. Para obtener una respuesta rápida, puede crear reglas de CloudWatch Events y tomar medidas inmediatas respecto de eventos específicos.

De forma predeterminada, los archivos de registro se almacenan por tiempo indefinido. Los archivos de registro se cifran automáticamente usando el cifrado del lado del servidor de Amazon S3 y permanecen en el bucket hasta que decida eliminarlos o archivarlos. Si desea mayor seguridad, puede usar KMS para cifrar los archivos de registro utilizando una clave de su propiedad. Puede usar las reglas de configuración del ciclo de vida de Amazon S3 para eliminar de manera automática los archivos de registro antiguos o archivarlos en Amazon S3 Glacier con el fin de obtener una mayor longevidad con ahorros significativos.

Si habilita la validación de archivos de registro opcional, CloudTrail crea un archivo de registro digital que puede utilizar para validar que no se hayan agregado, eliminado ni manipulado registros.

Como todos los demás servicios de AWS, puede limitar el acceso a CloudTrail solo a ciertos usuarios. Puede usar IAM para controlar qué usuarios de AWS pueden crear, configurar o eliminar registros de seguimiento de AWS CloudTrail, además de qué usuarios pueden iniciar o detener la creación de registros. Puede controlar el acceso a los archivos de registro aplicando políticas de bucket de Amazon S3 o IAM. También puede agregar una capa adicional de seguridad habilitando Eliminación de MFA en su bucket de Amazon S3.

Servicios móviles

Los servicios móviles de AWS le facilitan la creación, el envío, la ejecución, el monitoreo, la optimización y el escalado de aplicaciones basadas en la nube para dispositivos móviles. Estos servicios también lo ayudan a autenticar usuarios en su aplicación móvil, sincronizar datos y recopilar y analizar el uso de la aplicación.

Amazon Cognito

Amazon Cognito proporciona servicios de identidad y sincronización para aplicaciones móviles y basadas en la web. Simplifica la tarea de autenticación de usuarios y almacenamiento, administración y sincronización de sus datos entre varios dispositivos, plataformas y aplicaciones. Proporciona credenciales temporales con privilegios limitados tanto para usuarios autenticados como no autenticados sin tener que administrar ningún tipo de infraestructura de backend.

Amazon Cognito trabaja con proveedores de identidad conocidos, como Google, Facebook y Amazon, para autenticar a los usuarios finales de sus aplicaciones móviles y web. Puede aprovechar las características de identificación y autorización que proporcionan estos servicios en lugar de tener que construir y mantener sus propias funciones. Su aplicación usa la autenticación de uno de estos proveedores de identidad mediante el SDK del proveedor. Una vez que se autenticó al usuario final con el proveedor, la aplicación le envía a Cognito un token de OAuth u OpenID Connect que devolvió el proveedor. Cognito, a su vez, devuelve una nueva ID de Amazon Cognito para el usuario y un conjunto de credenciales temporales con privilegios limitados de AWS.

Para comenzar a usar Amazon Cognito, debe crear un grupo de identidades a través de la consola de Amazon Cognito. El grupo de identidades es un almacén de información de identidades de usuarios específica para su cuenta de AWS. Durante la creación del grupo de identidades, se le pedirá que cree un nuevo rol de IAM o que elija uno existente para sus usuarios finales. Un rol de IAM es un conjunto de permisos para acceder a recursos de AWS específicos, pero estos permisos no están ligados a un usuario o un grupo de IAM específico. Una entidad autorizada (p. ej. un usuario móvil o una instancia EC2) asume un rol y recibe credenciales de seguridad temporales para autenticar a los recursos de AWS definidos en el rol. Las credenciales de seguridad temporales proporcionan mejoras en la seguridad debido a su corta duración (el vencimiento predeterminado es de 12 horas) y el hecho de que no se pueden reutilizar una vez que se vencen. El rol que selecciona afecta a los servicios de AWS a los que los usuarios finales podrán acceder con las credenciales temporales. De forma predeterminada, Amazon Cognito crea un nuevo rol con permisos limitados: los usuarios finales solo tienen acceso al servicio de Amazon Cognito Sync y a Amazon Mobile Analytics. Si su aplicación necesita acceder a otros recursos de AWS como Amazon S3 o DynamoDB, puede modificar los roles directamente desde la consola de administración de IAM.

Con Amazon Cognito, no hay necesidad de crear cuentas individuales de AWS ni cuentas de IAM para cada usuario final de la aplicación web o móvil que necesite acceder a los recursos de AWS. Gracias a los roles de IAM, los usuarios móviles pueden acceder de manera segura a los recursos de AWS y las características de la aplicación e, incluso, guardar datos en la nube de AWS sin tener que crear una cuenta o iniciar sesión.

Sin embargo, si deciden hacer esto más tarde, Amazon Cognito combina los datos con la información de identificación. Como Amazon Cognito almacena datos en las instalaciones y en el servicio, los usuarios pueden continuar interactuando con sus datos incluso cuando trabajan sin conexión. Sus datos sin conexión pueden estar obsoletos, pero pueden recuperar de inmediato todo lo que hayan cargado en el conjunto de datos, independientemente de si están en línea o no. El SDK de cliente administra un almacén SQLite, de manera tal que la aplicación pueda funcionar incluso cuando no está conectada. El almacén de SQLite funciona como una caché y es el objetivo de todas las operaciones de lectura y escritura. El servicio de sincronización de Cognito compara la versión local de los datos con la versión en la nube y prioriza o posterga deltas según sea necesario. Tenga en cuenta que el grupo de identidades debe admitir identidades autenticadas para sincronizar datos entre dispositivos. Las identidades no autenticadas están vinculadas con el dispositivo, por lo que a menos que se autentique un usuario final, no podrán sincronizarse datos entre varios dispositivos.

Con Amazon Cognito, su aplicación se comunica directamente con un proveedor de identidad público compatible (Amazon, Facebook o Google) para autenticar usuarios. Amazon Cognito no recibe ni almacena credenciales de usuario, solo el token de OAuth u OpenID Connect recibido del proveedor de identidad. Una vez que Amazon Cognito recibe el token, devuelve un nuevo ID de Amazon Cognito para el usuario y un conjunto de credenciales de AWS temporales con privilegios limitados.

Cada identidad de Amazon Cognito tiene acceso únicamente a sus propios datos en el almacén de sincronización y estos datos se cifran cuando se almacenan. Además, todos los datos de identidad se transmiten mediante HTTPS. El identificador único de Amazon Cognito del dispositivo se almacena en la ubicación segura correspondiente. En iOS, por ejemplo, el identificador de Amazon Cognito se almacena en la cadena de claves de iOS. Los datos de usuario se almacenan en caché en una base de datos local de SQLite dentro del entorno de pruebas de la aplicación. Si requiere más seguridad, puede cifrar estos datos de identidad en la caché local implementando cifrado en su aplicación.

Amazon Mobile Analytics

Amazon Mobile Analytics es un servicio destinado a recopilar, visualizar y comprender datos de uso de aplicaciones móviles. Le permite hacer un seguimiento de los comportamientos de los clientes, agregar métricas e identificar patrones significativos en sus aplicaciones móviles. Amazon Mobile Analytics calcula y actualiza automáticamente las métricas de uso a medida que se reciben los datos desde los dispositivos de los clientes que ejecutan su aplicación y muestra los datos en la consola.

Puede integrar Amazon Mobile Analytics a su aplicación sin requerir que los usuarios de su aplicación se autentiquen con un proveedor de identidades (como Google, Facebook o Amazon). Para estos usuarios no autenticados, Mobile Analytics trabaja con Amazon Cognito a fin de ofrecer credenciales temporales con privilegios limitados. Para hacer esto, primero debe crear un grupo de identidades en Amazon Cognito. El grupo de identidades usará roles de IAM, que son un conjunto de permisos no vinculados con un usuario o grupo de usuarios de IAM, pero que permiten que una entidad acceda a recursos específicos de AWS. La entidad asume un rol y recibe credenciales de seguridad temporales para autenticar a los recursos de AWS definidos en el rol. De forma predeterminada, Amazon Cognito crea un nuevo rol con permisos limitados: los usuarios finales solo tienen acceso al servicio de Amazon Cognito Sync y a Amazon Mobile Analytics. Si su aplicación necesita acceder a otros recursos de AWS como Amazon S3 o DynamoDB, puede modificar los roles directamente desde la consola de administración de IAM.

Puede integrar los SDK para móviles de AWS de Android o iOS a su aplicación, o puede usar la API REST de Amazon Mobile Analytics para enviar eventos desde cualquier dispositivo o servicio conectado y visualizar los datos en los informes. Solo es posible acceder a la API de Amazon Mobile Analytics a través de un punto de enlace cifrado con SSL (https://mobileanalytics.us-east-1.amazonaws.com).

Aplicaciones

Las aplicaciones de AWS son servicios administrados que le permiten proporcionar a los usuarios áreas de trabajo y almacenamiento seguras y centralizadas en la nube.

Amazon WorkSpaces

Amazon WorkSpaces es un servicio de escritorio administrado que le permite

aprovisionar rápidamente escritorios basados en la nube para los usuarios. Simplemente elija el paquete de Windows 7 que mejor satisfaga las necesidades de los usuarios y la cantidad de WorkSpaces que desee lanzar. Una vez que los WorkSpaces estén listos, los usuarios recibirán un email que les informará dónde pueden descargar el cliente pertinente e iniciar sesión en su WorkSpace. Entonces, podrán acceder a sus escritorios basados en la nube desde distintos dispositivos de puntos de enlace, incluidos los equipos de escritorio, los equipos portátiles y los dispositivos móviles.

Sin embargo, los datos de su organización no se envían en ningún momento ni se almacenan en el dispositivo del usuario final, ya que Amazon WorkSpaces usa PC-over-IP (PCoIP), que proporciona una secuencia de video interactivo sin transmitir datos reales. El

protocolo PCoIP comprime, cifra y codifica la experiencia informática de escritorio de los usuarios y transmite "solo píxeles" a través de cualquier red IP estándar a los dispositivos de los usuarios finales.

Para acceder a su WorkSpace, los usuarios deben iniciar sesión usando un conjunto de credenciales únicas o sus credenciales regulares de Active Directory. Cuando integra Amazon WorkSpaces al Active Directory corporativo, cada WorkSpace se une a su dominio de Active Directory y puede administrarse igual que cualquier otro escritorio en su organización. Esto significa que puede usar políticas de grupos de Active Directory para administrar los WorkSpaces de sus usuarios con el fin de especificar opciones de configuración que controlen el escritorio. Si usted elige no usar Active Directory ni otro tipo de directorio en las instalaciones para administrar los WorkSpaces de los usuarios, puede crear un directorio privado en la nube dentro de Amazon WorkSpaces que puede usar con fines de administración.

Para ofrecer una capa de seguridad adicional, también puede requerir el uso de autenticación multifactor en el inicio de sesión en forma de token de hardware o software. Amazon WorkSpaces admite MFA usando un servidor en las instalaciones de Remote Authentication Dial-in User Service (RADIUS) o cualquier proveedor de seguridad que admita autenticación con RADIUS. Actualmente admite los protocolos PAP, CHAP, MS-CHAP1 y MS-CHAP2, junto con los proxies de RADIUS.

Cada WorkSpace reside en su propia instancia EC2 dentro de una VPC. Puede crear WorkSpaces en una VPC que ya sea de su propiedad o hacer que el servicio de WorkSpaces cree una para usted automáticamente usando la opción Quick Start de WorkSpaces. Cuando usa la opción Quick Start, WorkSpaces no solo crea la VPC, sino

que lleva a cabo otra serie de tareas de aprovisionamiento y configuración por usted, como crear una gateway de Internet para la VPC, configurar un directorio dentro de la VPC que se utilice para almacenar información de usuarios y WorkSpace, crear una cuenta de administrador del directorio, crear las cuentas de usuario especificadas y agregarlas al directorio, y crear las instancias de WorkSpace. De forma alternativa, la VPC puede conectarse a una red local usando una conexión de VPN segura para permitir el acceso a un Active Directory en las instalaciones existente y otros recursos de la intranet. Puede agregar un grupo de seguridad que haya creado en la VPC de Amazon a todos los WorkSpaces que pertenecen a su directorio. Esto le permite controlar el acceso a la red desde Amazon WorkSpaces en la VPC a otros recursos en la VPC de Amazon y la red local.

Amazon EBS proporciona el almacenamiento constante para WorkSpaces y la creación automática de copias de seguridad dos veces por día en Amazon S3. Si se habilita WorkSpaces Sync en un WorkSpace, se harán copias de seguridad continuamente de la carpeta que un usuario elija sincronizar y se almacenarán en Amazon S3. También puede usar WorkSpaces Sync en un equipo o Mac para sincronizar documentos desde o hacia el WorkSpace, de manera tal que siempre tenga acceso a sus datos, independientemente de la computadora de escritorio que esté usando.

Como es un servicio administrado, AWS se encarga de distintas tareas de seguridad y mantenimiento como la aplicación de parches y la creación de copias de seguridad diarias. Las actualizaciones se implementan automáticamente en WorkSpaces durante un periodo de mantenimiento semanal. Puede controlar cómo está configurada la aplicación de parches para el WorkSpace de manera predeterminada. De forma predeterminada, Windows Update está activado, pero tiene la capacidad de personalizar estos parámetros o usar un enfoque alternativo de administración de parches si lo desea. Para el sistema operativo subyacente, Windows Update está activado de forma predeterminada en WorkSpaces y está configurado para instalar actualizaciones semanalmente. Puede usar un enfoque alternativo de aplicación de parches o configurar Windows Update para realizar actualizaciones en el momento que usted elija.

Puede usar IAM para controlar qué usuarios de su equipo pueden llevar a cabo funciones administrativas como crear o eliminar WorkSpaces o configurar el directorio de usuarios. También puede crear un WorkSpace para administración del directorio, instalar sus herramientas de administración de Active Directory favoritas y crear unidades organizativas y políticas de grupos con el fin de aplicar cambios en Active Directory a todos los usuarios de WorkSpaces con mayor facilidad.

Amazon WorkDocs

Amazon WorkDocs es un servicio empresarial administrado de almacenamiento y uso compartido con funciones de retroalimentación para la colaboración entre usuarios. Los usuarios pueden almacenar cualquier tipo de archivos en una carpeta de WorkDocs y permitir que otros los vean y descarguen. Las capacidades de comentarios y anotaciones funcionan en ciertos tipos de archivos, como MS Word, sin requerir la aplicación que se usó para crear originalmente el archivo.

WorkDocs notifica a los colaboradores sobre actividades de revisión y fechas límites por email y realiza el control de versiones de archivos que ha sincronizado usando la aplicación de WorkDocs Sync.

La información de los usuarios se almacena en un directorio de red compatible con Active Directory. Puede optar entre crear un nuevo directorio en la nube o conectar Amazon WorkDocs con su directorio local. Cuando crea un directorio en la nube usando la configuración de inicio rápido de WorkDocs, también se crea una cuenta de administrador de directorio con el email del administrador como nombre de usuario. Se envía un email al administrador con las instrucciones para completar el registro. Luego, el administrador utiliza esta cuenta para administrar el directorio.

Cuando crea un directorio en la nube usando la configuración de inicio rápido de WorkDocs, también se crea una VPC en su cuenta de AWS para alojar el directorio. Si necesita más control sobre la configuración del directorio, puede elegir la configuración estándar para especificar el nombre de dominio del directorio, además de una de sus VPC existentes para usar con el directorio. Si desea usar una de las VPC existentes, esta debe contar con una gateway de Internet y, al menos, dos subredes. Cada una de las subredes debe estar en una zona de disponibilidad diferente.

Con la consola de administración de Amazon WorkDocs, los administradores pueden ver los registros de auditoría para realizar un seguimiento de la actividad de archivos y usuarios según la hora, la dirección IP y el dispositivo, y elegir si se permite a los usuarios compartir archivos con otras personas fuera de la organización. Los usuarios pueden controlar quién accede a los archivos individuales y desactivar las descargas de archivos que comparten.

Todos los datos en tránsito se cifran usando el protocolo SSL estándar de la industria. Las aplicaciones web y móvil y los clientes de sincronización de escritorio de

WorkDocs transmiten archivos directamente a Amazon WorkDocs mediante SSL. Los usuarios de WorkDocs también pueden utilizar Multi-Factor Authentication, o MFA, si su organización implementó un servidor de RADIUS. MFA utiliza los siguientes factores: nombre de usuario, contraseña y métodos admitidos por el servidor de RADIUS. Los protocolos admitidos son PAP, CHAP, MS-CHAPv1 y MS-CHAPv2.

Usted elige la región de AWS en la que se almacenan los archivos de cada sitio de WorkDocs. Amazon WorkDocs está disponible actualmente en las regiones de AWS de EE. UU. Este (Virginia), EE. UU. Oeste (Oregón) y UE (Irlanda). Todos los archivos, los comentarios y las anotaciones que se almacenan en WorkDocs se cifran automáticamente con cifrado AES-256.

Revisiones del documento

Fecha	Descripción
Marzo de 2020	Se actualizaron las secciones de certificaciones de cumplimiento, hipervisor y AWS Snowball.
Febrero de 2019	Se agregó información sobre la eliminación de objetos en Amazon S3 Glacier.
Diciembre de 2018	Se realizó una edición en el tema de seguridad de Amazon Redshift.
Mayo de 2017	Se agregó una sección sobre comprobaciones de seguridad de AWS Config.
Abril de 2017	Se agregó una sección sobre Amazon Elastic File System.
Marzo de 2017	Se migró al nuevo formato.
Enero de 2017	Se actualizaron las regiones.