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

Mayo de 2017

Avisos

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

Contenido

Resumen

El objetivo de este documento es dar respuesta a preguntas como “¿Cómo ayuda AWS a garantizar que mis datos están protegidos?” En concreto, se describen los procesos de seguridad física y operativa de AWS para infraestructuras de red y de servidor administradas con AWS.

Introducción

Amazon Web Services (AWS) ofrece una plataforma de informática en la nube escalable, con alta disponibilidad y fiabilidad, que proporciona las herramientas que permiten a los clientes ejecutar una gran variedad de aplicaciones. Además de mantener la confianza de nuestros clientes, para AWS es de suma importancia ayudar a proteger la confidencialidad, integridad y disponibilidad de los sistemas y los datos de los clientes.

Modelo de responsabilidad de la seguridad compartida

Antes de adentrarnos en los detalles de cómo AWS protege sus recursos, debemos hablar de cómo la seguridad en la nube es ligeramente diferente de la seguridad en los centros de datos on-premises. Cuando mueve sus sistemas informáticos y datos a la nube, las responsabilidades de seguridad se comparten entre usted y su proveedor de servicios en la nube. En este caso, AWS es responsable de proteger la infraestructura subyacente que respalda la nube, y usted es responsable de todo lo que ponga en la nube o conecte con ella. Este modelo de responsabilidad de la seguridad compartida puede reducir la carga operativa en muchos sentidos, y en algunos casos puede incluso mejorar su enfoque predeterminado hacia la seguridad sin ninguna acción adicional por su parte.

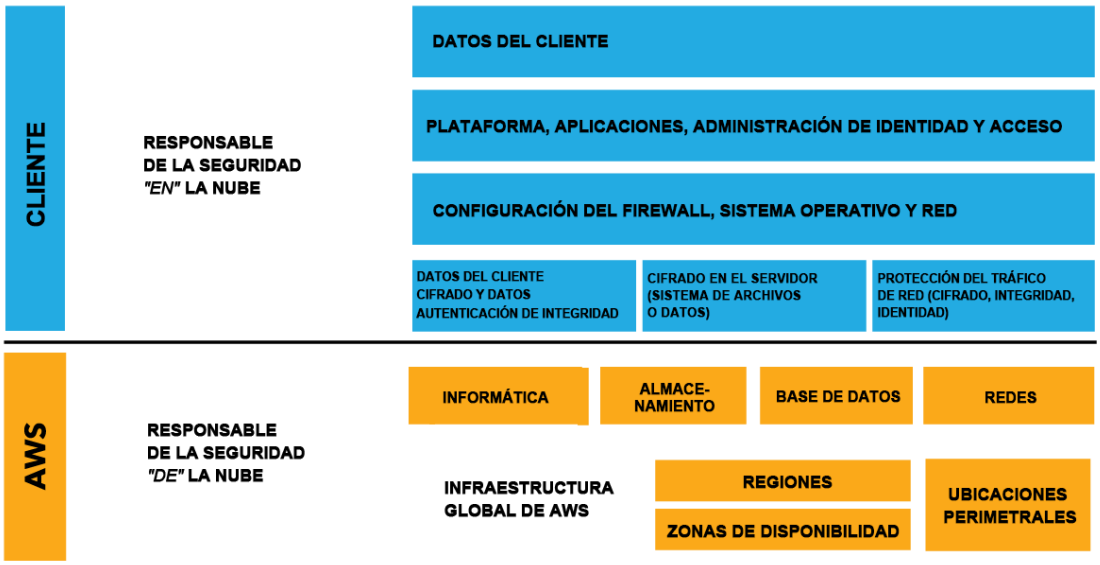


Figura 1: Modelo de responsabilidad de seguridad compartida de AWS

La cantidad de tareas de configuración de seguridad que debe realizar varía en función de los servicios que seleccione y del grado de confidencialidad de sus datos. No obstante, hay varias características de seguridad (como cuentas de usuarios y credenciales individuales, SSL/TLS para transmisiones de datos y registros de actividad de los usuarios) que sí necesitará configurar independientemente de los servicios de AWS que utilice. Para obtener más información sobre estas características de seguridad, consulte la sección "Características de seguridad de las cuentas de AWS" a continuación.

Responsabilidades de seguridad de AWS

Amazon Web Services es responsable de proteger la infraestructura global en la que se ejecutan todos los servicios ofrecidos en la nube de AWS. Esta infraestructura está compuesta por hardware, software, redes e instalaciones que ejecutan servicios de AWS. Proteger esta infraestructura es la mayor prioridad de AWS, y aunque no puede visitar nuestros centros de datos u oficinas para ver estas medidas de protección de primera mano, proporcionamos varios informes de auditores externos que han verificado que esta cumple una gran variedad de normas y regulaciones de seguridad informática (para obtener más información, visite aws.amazon.com/compliance).

Tenga en cuenta que además de proteger su infraestructura global, AWS es responsable de la configuración de seguridad de sus productos que se consideran servicios administrados. Ejemplos de estos tipos de servicios son Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce y Amazon WorkSpaces, entre otros. Estos servicios proporcionan la escalabilidad y flexibilidad de los recursos basados en la nube con la ventaja añadida de que están administrados. Para estos servicios, AWS se ocupará de tareas de seguridad básicas como la aplicación de parches al sistema operativo (SO) invitado y a las bases de datos, la configuración del firewall y la recuperación de desastres. Para 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 sus cuentas. Algunos de ellos pueden requerir tareas adicionales, como configurar cuentas de usuario de base de datos, pero el servicio se encarga de la mayoría de las tareas de configuración de la seguridad.

Responsabilidades de 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 usar herramientas de análisis y flujo de trabajo basadas en la nube para procesar sus datos cuando lo necesite, y almacenar estos datos en sus propios centros de datos o en la nube. Los servicios de AWS que utilice determinarán la cantidad de trabajo de configuración que tendrá que realizar como parte de sus responsabilidades de seguridad.

Los productos de AWS correspondientes a la categoría ampliamente conocida como Infraestructura como servicio (IaaS) —como es el caso de Amazon EC2, Amazon VPC y Amazon S3— están completamente bajo su control y tendrá que realizar todas las tareas de configuración y administración de seguridad necesarias. Por ejemplo, para las instancias EC2, usted es responsable de administrar el sistema operativo invitado (incluidas las actualizaciones y parches de seguridad), todo el software de aplicación o utilidades que instale en las instancias y la configuración del firewall proporcionado por AWS (conocido como grupo de seguridad) en cada instancia. Estas son básicamente las mismas tareas de seguridad que suele realizar con independencia de dónde se encuentren los servidores.

Los servicios de AWS administrados como Amazon RDS o Amazon Redshift proporcionan todos los recursos necesarios para realizar una tarea específica, pero sin el trabajo de configuración que esta conlleva. Con los servicios administrados, no tiene que preocuparse de lanzar o mantener instancias, de aplicar parches al sistema operativo invitado o a la base de datos ni de replicar las bases de datos: AWS se ocupa de todo ello por usted. Pero al igual que con todos los servicios, debe proteger las credenciales de sus cuentas de AWS y configurar cuentas de usuario individuales con Amazon Identity and Access Management (IAM) para que cada usuario tenga sus propias credenciales y usted pueda implementar la división de tareas. También le recomendamos que use la autenticación multifactor (MFA) con cada cuenta, lo que requiere el uso de SSL/TLS para comunicarse con sus recursos de AWS, y que configure el registro de actividades de las API y usuarios con AWS CloudTrail. Para obtener más información sobre las medidas adicionales que puede aplicar, consulte el documento técnico sobre prácticas recomendadas de seguridad de AWS y la lectura recomendada en la página web de recursos de seguridad de AWS.

Seguridad de la infraestructura global de AWS

AWS opera la infraestructura en la nube global que usted usa para aprovisionar diversos recursos informáticos básicos como el procesamiento y el almacenamiento. La infraestructura global de AWS incluye las instalaciones, redes, hardware y software operativo (como el sistema operativo host, el software de virtualización, etc.) que permiten el aprovisionamiento y uso de estos recursos. La infraestructura global de AWS está diseñada y administrada de acuerdo con las prácticas recomendadas de seguridad y con arreglo a diversos estándares de conformidad relacionados con la seguridad. Como cliente de AWS, puede tener la certeza de que sus arquitecturas web se asientan sobre una de las infraestructuras informáticas más seguras del mundo.

Programa de conformidad de AWS

La conformidad de Amazon Web Services permite a los clientes conocer los potentes controles de AWS para mantener la seguridad y la protección de datos en la nube. A medida que se van creando sistemas en la infraestructura de nube de AWS, se deberán compartir las responsabilidades relativas a la conformidad. Mediante la combinación de características de servicio centradas en el control y la auditoría con los estándares aplicables de conformidad o auditoría, los habilitadores de conformidad de AWS crean programas tradicionales que ayudan a los clientes a establecerse y trabajar en un entorno de control de seguridad de AWS. La infraestructura de TI que AWS ofrece a sus clientes está diseñada y se administra de acuerdo con las prácticas recomendadas de seguridad y diversos estándares de seguridad de TI, incluidos los siguientes:

- SOC 1/SSAE 16/ISAE 3402 (anteriormente SAS70)
- SOC 2
- SOC 3
- FISMA, DIACAP y FedRAMP
- DOD CSM niveles 1-5
- PCI DSS Nivel 1
- ISO 9001 / ISO 27001

- ITAR
- FIPS 140-2
- MTCS nivel 3

Asimismo, la flexibilidad y el control que ofrece la plataforma AWS permiten a los clientes implementar soluciones que cumplen los estándares específicos de diferentes sectores:

- CJIS (Criminal Justice Information Services)
- Cloud Security Alliance (CSA)
- Ley de derechos educativos de la familia y privacidad (Family Educational Rights and Privacy Act, FERPA)
- Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA)
- Motion Picture Association of America (MPAA)

AWS ofrece a los clientes una gran variedad de información con respecto al entorno de control de TI a través de documentos técnicos, informes, certificaciones y otras acreditaciones independientes. Puede obtener más información en el documento técnico Riesgo y conformidad disponible en el sitio web: http://aws.amazon.com/compliance/.

Seguridad física y del entorno

Los centros de datos de AWS son de última generación, debido a que utilizan enfoques innovadores en materia de arquitectura e ingeniería. Amazon tiene muchos años de experiencia en el diseño, la construcción y el funcionamiento de centros de datos a gran escala. Esta experiencia se ha aplicado a la plataforma y a la infraestructura de AWS. Los centros de datos de AWS se alojan en instalaciones sin identificación externa. El acceso físico está estrictamente controlado en el perímetro y en los puntos de acceso del edificio por personal de seguridad profesional mediante videovigilancia, sistemas de detección de intrusiones y otros recursos electrónicos. El personal autorizado debe confirmar una autenticación de dos factores, como mínimo dos veces, para acceder a los pisos del centro de datos. Todos los visitantes y contratistas deben presentar su identificación, firmar el registro de entrada e ir acompañados en todo momento de personal autorizado.

AWS solo ofrece acceso al centro de datos y solo facilita información a los empleados y contratistas que tengan una necesidad empresarial legítima de tales privilegios. Cuando un empleado deja de tener una necesidad empresarial de tales privilegios, su acceso se revoca inmediatamente, incluso aunque continúe siendo empleado de Amazon o de Amazon Web Services. El acceso físico a los centros de datos por parte de los empleados de AWS está sujeto a registros y auditorías rutinarios.

Detección y extinción de incendios

Se ha instalado un equipo automático 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 del centro de datos, en los espacios mecánicos y eléctricos de la infraestructura, en las salas del refrigerador y en las salas del equipo del generador. Estas zonas están protegidas por sistemas de acción preventiva de tubos húmedos interconectados o por sistemas de rocío de gases.

Energía

Los sistemas de alimentación eléctrica del centro de datos están diseñados para que puedan redundarse y mantenerse por completo sin que ello repercuta en las operaciones, con un ciclo de 24 horas al día durante los 7 días de la semana. Los sistemas de alimentación ininterrumpida (SAI) ofrecen alimentación de reserva en casos de cortes eléctricos para cubrir las cargas más importantes y esenciales de la instalación. Los centros de datos utilizan generadores para ofrecer energía de reserva para toda la instalación.

Condiciones climáticas y temperatura

Se precisa de control climático para mantener una temperatura de funcionamiento constante para los servidores y otro hardware y, así, impedir el sobrecalentamiento y reducir la posibilidad de que se produzcan interrupciones del servicio. Los centros de datos se acondicionan para mantener las condiciones atmosféricas en niveles óptimos. El personal y los sistemas monitorizan y controlan la temperatura y la humedad a fin de mantenerlas en niveles adecuados.

Administración

AWS supervisa los equipos y sistemas eléctricos, mecánicos y de soporte vital con el fin de poder identificar de inmediato todos los problemas que puedan surgir. Se llevan a cabo tareas de mantenimiento preventivo a fin de que el equipo pueda funcionar sin interrupciones.

Retirada de dispositivos de almacenamiento

Cuando un dispositivo de almacenamiento alcanza el final de su vida útil, los procedimientos de AWS incluyen un proceso de retirada diseñado para prevenir que los datos de los clientes queden expuestos al acceso de personas no autorizadas. AWS utiliza las técnicas detalladas en NIST 800-88 (“Directrices para el saneamiento de soportes”) como parte del proceso de retirada.

Administración de la continuidad empresarial

La infraestructura de Amazon presenta un alto nivel de disponibilidad y ofrece a los clientes las prestaciones necesarias para implementar una arquitectura resistente de TI. AWS ha diseñado sus sistemas para que toleren errores del sistema o del hardware con un impacto mínimo en los clientes. La administración de la continuidad empresarial del centro de datos de AWS es competencia de la dirección del grupo de infraestructuras de Amazon.

Disponibilidad

Los centros de datos están agrupados en varias regiones del mundo. Todos los centros de datos se encuentran online y a disposición de los clientes, por lo que ninguno está “inactivo”. En caso de error, los procesos automatizados desvían el tráfico de datos del cliente de la zona afectada. Las aplicaciones principales 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 para permitir equilibrar la carga del tráfico entre los demás sitios.

AWS le proporciona la flexibilidad necesaria para colocar las 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 de error independiente. Esto significa que las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana habitual y se encuentran en llanuras poco propensas a inundaciones (las categorías específicas de zonas propensas a inundaciones varían según la

región). Además de mediante los sistemas de alimentación ininterrumpida (SAI) discretos y las instalaciones de generación de energía de reserva in situ, las zonas de disponibilidad se alimentan a través de diferentes redes a partir de utilidades independientes para reducir aún más cada uno de los puntos de error. Todas las zonas de disponibilidad están conectadas de forma redundante a varios proveedores de tránsito de nivel 1.

Deberá planificar el uso que haga de AWS para poder utilizar varias regiones y zonas de disponibilidad. La distribución de aplicaciones entre varias zonas de disponibilidad ofrece la posibilidad de mantener la resistencia ante la mayoría de los modos de error, incluidos los desastres naturales o los errores del sistema.

Respuesta frente a incidencias

El equipo de administración de incidentes de Amazon utiliza procedimientos de diagnóstico estándar del sector para administrar las soluciones durante los eventos que repercuten en el negocio. El personal ofrece un servicio de 24 horas al día durante los 365 días de año para poder detectar incidentes y administrar el impacto y su resolución.

Revisión ejecutiva de toda la empresa

El grupo de auditoría interno de Amazon ha revisado recientemente los planes de resistencia de los servicios de AWS, que también revisan periódicamente los miembros del equipo sénior de administración ejecutiva y el Comité de auditoría de la Junta directiva.

Comunicación

AWS ha implementado varios métodos de comunicación interna a escala mundial para ayudar a que los empleados conozcan las funciones y las responsabilidades individuales y para comunicar eventos importantes de manera puntual. Estos métodos incluyen programas de orientación y capacitación para empleados recién contratados, reuniones periódicas de administración con motivo de las actualizaciones en materia de desempeño empresarial y de otras cuestiones 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 varios métodos de comunicación externa para prestar soporte a su cartera de clientes y a la comunidad. El equipo de atención al cliente dispone de mecanismos para recibir notificaciones sobre problemas operativos que afecten a la experiencia de los clientes. El equipo de atención al cliente realiza el mantenimiento del Panel de estado del servicio a fin de advertir al cliente de cualquier problema que pueda tener un gran impacto. Puede encontrar información sobre la seguridad y conformidad de AWS en el Centro de seguridad de AWS. También puede suscribirse al servicio AWS Support que incluye comunicación directa con el equipo de atención al cliente y la recepción de alertas proactivas relacionadas con todos los problemas que afecten a los clientes.

Seguridad de la red

La red de AWS se ha diseñado para permitirle seleccionar el nivel de seguridad y capacidad de recuperación adecuado para su carga de trabajo. Para que pueda desarrollar arquitecturas web geográficamente dispersas y tolerantes a errores con recursos de la nube, AWS ha implementado una infraestructura de red de talla mundial que se supervisa y se gestiona minuciosamente.

Protección de la arquitectura de red

Los dispositivos de red, incluido el firewall y otros dispositivos perimetrales, supervisan y controlan las comunicaciones en el límite externo de la red y en los principales límites internos. Estos dispositivos perimetrales emplean conjuntos de reglas, listas de control de acceso (ACL) y configuraciones para llevar el flujo de información a servicios específicos del sistema de información.

En cada interfaz administrada se establecen ACL o políticas de flujo de tráfico, que administran y dirigen el flujo de tráfico. Las políticas de ACL cuentan con la aprobación de Amazon Information Security. Estas políticas se insertan automáticamente mediante la herramienta ACL-Manage de AWS para ayudar a garantizar que estas interfaces administradas aplican las ACL más actuales.

Protección de los puntos de acceso

AWS ha limitado estratégicamente el número de puntos de acceso a la nube para permitir una monitorización más detallada de las comunicaciones entrantes y salientes y del tráfico de red. Estos puntos de acceso del cliente se denominan puntos de enlace de API y permiten el acceso HTTP seguro (HTTPS), a fin de que pueda establecer una sesión de comunicación segura con sus instancias de almacenamiento o informática en AWS. Para ayudar a los clientes con los requisitos criptográficos de FIPS, los balanceadores de carga con terminación SSL en AWS GovCloud (US) cumplen con la norma FIPS 140-2.

Asimismo, AWS ha implementado dispositivos de red dedicados para administrar las comunicaciones que interactúan con los proveedores de Internet (ISP). AWS emplea una conexión redundante con varios servicios de comunicación en cada extremo conectado a Internet de la red de AWS. Estas conexiones tienen dispositivos de red dedicados.

Protección de las transmisiones

Puede conectarse a un punto de acceso de AWS a través de HTTP o HTTPS mediante Capa de conexión segura (SSL), un protocolo criptográfico diseñado para la protección frente al acceso no autorizado, manipulaciones y falsificación de mensajes.

Para aquellos clientes que necesiten 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 posibilidad de utilizar un dispositivo de red privada virtual (VPN) IPsec que ofrece un túnel cifrado entre Amazon VPC y su centro de datos. Si desea obtener información adicional acerca de las opciones de configuración de VPC, consulte la sección Seguridad de Amazon Virtual Private Cloud (Amazon VPC) a continuación.

Segregación corporativa de Amazon

Como cabría esperar, la red de producción de AWS está separada de la red corporativa de Amazon mediante un complejo conjunto de dispositivos de seguridad y segregación de red. Los desarrolladores y administradores de AWS de la red corporativa que necesitan obtener acceso a componentes de la nube de AWS para mantenerlos tienen que solicitar el acceso explícitamente a través del sistema de tratamiento de incidencias de AWS. El propietario del servicio pertinente debe examinar y aprobar todas las solicitudes.

El personal de AWS autorizado se conecta a la red de AWS a través de un host de protección que restringe el acceso a los dispositivos de la red y otros componentes de la nube, y registra toda la actividad para su posterior examen. Para obtener acceso a los hosts de protección se requiere autenticación de clave pública SSH para todas las cuentas de usuario del host. Para 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 presenta un alto nivel de disponibilidad y le ofrece las prestaciones necesarias para implementar una arquitectura resistente de TI. AWS ha diseñado sus sistemas para que toleren errores del sistema o del hardware con un impacto mínimo en los clientes.

Los centros de datos están agrupados en varias regiones del mundo. Todos los centros de datos se encuentran online y a disposición de los clientes, por lo que ninguno está “inactivo”. En caso de error, los procesos automatizados desvían el tráfico de datos del cliente de la zona afectada. Las aplicaciones principales 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 para permitir equilibrar la carga del tráfico entre los demás sitios.

AWS le proporciona la flexibilidad necesaria para colocar las 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 de error independiente. Esto significa que las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana habitual y se encuentran en llanuras poco propensas a inundaciones (las categorías específicas de zonas propensas a inundaciones varían según la región). Además de utilizar sistemas de alimentación ininterrumpida (SAI) discretos y generadores de backups in situ, estos sistemas reciben la energía de diferentes redes de servicios eléctricos independientes para reducir aún más los puntos únicos de error. Todas las zonas de disponibilidad están conectadas de forma redundante a varios proveedores de tránsito de nivel 1.

Deberá planificar el uso que haga de AWS para poder utilizar varias regiones y zonas de disponibilidad. La distribución de aplicaciones entre varias zonas de disponibilidad ofrece la posibilidad de oponer resistencia ante la mayoría de los tipos de error, incluidos los desastres naturales o las averías del sistema. Sin

embargo, deberá tener en cuenta los requisitos de privacidad y conformidad específicos de cada región, como la Directiva europea relativa a la privacidad de datos. Los datos no se replican entre las regiones a menos que el cliente lo haga por adelantado, lo que permite a los clientes con estos tipos de requisitos de colocación de datos y de privacidad tener la posibilidad de definir entornos compatibles con las normativas. 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 están agrupados en varias regiones del mundo, incluidas: EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (US) (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 una lista completa de las regiones, consulte la página Infraestructura global de AWS.

AWS GovCloud (US) es una región AWS aislada diseñada para permitir que las agencias gubernamentales de EE. UU. y sus clientes trasladen cargas de trabajo a la nube con el fin de respaldar sus requisitos normativos y de conformidad específicos. La plataforma AWS GovCloud (US) permite a las agencias gubernamentales de Estados Unidos y a sus contratistas cumplir las regulaciones sobre el tráfico internacional de armas (ITAR) de EE. UU, así como los requisitos del programa federal de gestión de riesgos y autorizaciones (FedRAMP). AWS GovCloud (US) ha recibido la autorización de agencia operativa (ATO por sus siglas en inglés) del Departamento de Sanidad y Asuntos Sociales (HHS) de EE. UU., que trabaja con una organización de evaluación independiente (3PAO) acreditada por FedRAMP para varios servicios de AWS.

La región AWS GovCloud (US) proporciona el mismo diseño tolerante a errores que otras regiones, con dos zonas de disponibilidad. Asimismo, la región AWS GovCloud (US) 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 Amazon EC2 que tengan direcciones privadas (RFC 1918). Encontrará más información acerca de GovCloud en el sitio web de AWS: http://aws.amazon.com/govcloud-us/.

Monitorización y protección de la red

AWS utiliza sistemas automáticos de monitorización muy diversos para ofrecer un elevado nivel de desempeño y disponibilidad de los servicios. Las herramientas de monitorización 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 monitorizan el uso de los servidores y de la red, las actividades de escaneo de puertos, el uso de las aplicaciones y los intentos de intrusión no autorizados. Las herramientas disponen de la capacidad de definir umbrales de métricas de desempeño personalizados para la actividad inusual.

Los sistemas de AWS disponen de una gran variedad de recursos para poder monitorizar las principales métricas operativas. Las alarmas se configuran para notificar automáticamente al personal de operaciones y de administración cuando las métricas operativas clave superan los umbrales de preaviso. Se utiliza un horario de guardia para que este personal esté siempre disponible para solucionar los problemas de funcionamiento. Incluye además un sistema de localización de personas para que las alarmas se comuniquen al personal de operaciones de forma rápida y fiable.

La documentación también se mantiene actualizada para ayudar e informar al personal de operaciones en el tratamiento de incidentes o problemas. En caso de que se precise de colaboración para solucionar algún problema, se utiliza un sistema de videoconferencia que incorpora funcionalidades de comunicación y registro. Los coordinadores de la llamada cualificados facilitan la comunicación y el progreso durante la gestión de los problemas operativos que precisan de colaboración. Se solicita un análisis final después de cualquier problema operativo importante, independientemente del impacto externo y, además, se elaboran documentos de la causa del error (COE) a fin de detectar la causa principal y de adoptar medidas preventivas en el futuro. Se organizan reuniones operativas semanales para realizar un seguimiento de la aplicación de medidas preventivas.

Acceso de AWS

La red de producción de AWS está separada de la red corporativa de Amazon y se requiere un conjunto de credenciales diferente para el acceso lógico a la misma. La red corporativa de Amazon emplea identificadores de usuario, contraseñas y Kerberos, y la red de producción de AWS requiere la autenticación de claves públicas SSH a través de un host de protección.

Los desarrolladores y administradores de AWS de la red corporativa de Amazon que necesitan tener acceso a componentes de la nube de AWS tienen que solicitarlo explícitamente a través del sistema de administración de accesos de AWS. El propietario o el director pertinente deben examinar y aprobar todas las solicitudes.

Revisión de cuentas y auditoría

Las cuentas se revisan cada 90 días; después de la revisión se precisará de una nueva aprobación explícita o, de lo contrario, se revocará el acceso al recurso automáticamente. El acceso se revoca también automáticamente cuando se cancela el historial de un empleado en el sistema de recursos humanos de Amazon. Se deshabilitan las cuentas de Windows y UNIX, y 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 las herramientas de administración de permisos de Amazon. Cuando se produce un cambio en la función de un empleado, ha de aprobarse de forma explícita el acceso continuado al recurso o, 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 comprueba los antecedentes penales de conformidad con la legislación aplicable, como parte de las prácticas de preselección de empleados con el fin de que estos se adecuen al cargo y al nivel de acceso del empleado a las instalaciones de AWS. Las políticas también identifican responsabilidades funcionales para la administración de la seguridad y del acceso lógico.

Política de credenciales

AWS Security ha establecido una política de credenciales con las configuraciones y los intervalos de caducidad necesarios. Las contraseñas tienen que ser complejas y se tienen que cambiar al menos cada 90 días.

Principios sobre el diseño seguro

El proceso de desarrollo de AWS aplica las prácticas recomendadas de desarrollo de software seguro, que incluyen las revisiones formales de diseño de AWS Security Team, el modelado de amenazas y la realización de una 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 de la industria seleccionados de forma minuciosa. Las revisiones de la evaluación de riesgos de seguridad que realizamos empiezan en la fase de diseño y el compromiso se extiende desde el lanzamiento hasta las operaciones en curso.

Administración de cambios

Los cambios de emergencia, no rutinarios y de configuración en la infraestructura existente de AWS están sujetos a autorización, registros, pruebas, aprobaciones y documentación de conformidad con las normas del sector establecidas para sistemas similares. Se realizan actualizaciones en la infraestructura de AWS para minimizar cualquier impacto en el cliente y en el uso que este hace de los servicios. AWS se comunicará con los clientes, ya sea por correo electrónico o a través del Panel de estado del servicio de AWS (http://status.aws.amazon.com/) cuando quepa la posibilidad de que el servicio pueda verse afectado negativamente.

Software

AWS aplica un enfoque sistemático para administrar los cambios, a fin de revisar minuciosamente, probar, aprobar y comunicar según proceda los cambios introducidos en los servicios que repercutan en los clientes. El proceso de administración de cambios de AWS pretende evitar interrupciones no intencionadas del servicio y ofrecer al cliente la integridad del servicio. Los cambios introducidos en los entornos de producción:

- **Se revisan** – Se requieren revisiones de homólogos de los aspectos técnicos de algún cambio.
- **Se prueban** – Los cambios aplicados se prueban para asegurarse de que se comportarán según lo previsto sin afectar negativamente al desempeño.
- **Se aprueban** – Se deben autorizar todos los cambios para ofrecer previsiones e información adecuadas sobre el impacto empresarial.

Los cambios suelen introducirse en la fase de producción con una implementación gradual, empezando por áreas de impacto mínimo. Las implementaciones se prueban en un único sistema y se monitorizan minuciosamente a fin de poder evaluar el impacto. Los propietarios del servicio cuentan con métricas configurables que permiten medir el estado de las dependencias ascendentes del servicio. Estas métricas se controlan de forma minuciosa mediante umbrales y alarmas. Los procedimientos de restauración se documentan en un ticket de administración de cambios (CM).

Cuando es posible, los cambios se programan durante periodos de tiempo regulares. Los cambios de emergencia en los sistemas de producción que requieren desviaciones de los procedimientos estándar de administración de cambios se asocian con un incidente y se registran y aprueban según proceda.

De forma periódica, AWS realiza auditorías automáticas de los cambios introducidos en los servicios principales para controlar la calidad, mantener altos estándares y facilitar la mejora constante del proceso de administración de cambios. Todas las excepciones se analizan para determinar la causa raíz y se aplican las acciones adecuadas para realizar los cambios oportunos en materia de conformidad o para revertir el cambio en caso de que proceda. A continuación, se adoptan las medidas oportunas para solucionar y remediar el proceso o el problema del usuario.

Infraestructura

El equipo de aplicaciones corporativas de Amazon desarrolla y administra el software para 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 configuración de UNIX/Linux para gestionar la escalabilidad, disponibilidad, auditoría y administración de seguridad del hardware. Gracias a una administración

centralizada de los hosts mediante la utilización de procesos automatizados que administran los cambios, Amazon puede conseguir sus objetivos en términos de alta disponibilidad, repetibilidad, escalabilidad, alta seguridad y recuperación de desastres. Los ingenieros de sistemas y redes controlan el estado de estas herramientas automatizadas periódicamente, además de revisar informes para responder a los hosts que dejan de funcionar a fin de obtener o actualizar su configuración y el software.

Cuando se incorpora nuevo hardware, se instala un software de administración de configuración que se ha desarrollado internamente. Estas herramientas se ejecutan en todos los hosts de UNIX para comprobar que están configurados y que el software está instalado de conformidad con los estándares determinados por la función asignada 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 de administración de la configuración central.

Características de seguridad de la cuenta de AWS

AWS proporciona diversas herramientas y características que puede usar para mantener su cuenta de AWS y recursos a salvo del uso no autorizado. Entre estas se incluyen credenciales para el control de acceso, 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 controlar la seguridad y comprobaciones de seguridad de Trusted Advisor. Puede usar todas estas herramientas de seguridad con independencia de los servicios de AWS que seleccione.

Credenciales de AWS

Para ayudarle a garantizar que solo los usuarios y procesos autorizados tienen acceso a su cuenta y recursos de AWS, AWS usa varios tipos de credenciales para la autenticación. Entre ellos se incluyen contraseñas, claves criptográficas, firmas digitales y certificados. También proporcionamos la opción de exigir la autenticación multifactor (MFA) para iniciar sesión en su cuenta de AWS o en las cuentas de usuario de IAM. En la tabla siguiente se indican las distintas credenciales de AWS y sus usos.

Tipo de credenciales	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 usada para iniciar sesión en su cuenta de AWS o en su cuenta de IAM. Las contraseñas de AWS deben tener un mínimo de 6 caracteres y un máximo de 128.
Autenticación multifactor (MFA)	Inicio de sesión con la cuenta raíz de AWS o la cuenta de usuario de IAM en la consola de administración de AWS	Se requiere un código de un solo uso de seis dígitos, además de la contraseña, para iniciar sesión en la cuenta de AWS o en la cuenta de usuario de IAM.
Claves de acceso	Solicitudes firmadas digitales a las API de AWS (mediante el SDK de AWS, CLI o API REST/Query)	Incluye un ID de clave de acceso y una clave de acceso secreta. Las claves de acceso se usan para firmar digitalmente las soluciones mediante programación que realiza a AWS.
Pares de claves	Inicio de sesión SSH a instancias EC2 URL firmadas por CloudFront	Se requiere un par de claves para conectarse a una instancia EC2 iniciada desde una AMI pública. Las claves que usa Amazon EC2 son claves RSA SSH-2 de 1024 bits. Puede generar un par de claves automáticamente cuando inicie la instancia o puede cargar su propio par.
Certificados X.509	Solicitudes SOAP firmadas digitalmente a las API de AWS Certificados de servidor SSL para HTTPS	Los certificados X.509 solo se usan para firmar solicitudes SOAP (que actualmente solo se utilizan con Amazon S3). Puede pedir a AWS que cree un certificado X.509 y una clave privada que puede 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 esta página. En este informe se indican todos los usuarios de su cuenta y el estado de sus credenciales: si usan 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 han activado la autenticación multifactor.

Por motivos de seguridad, si pierde u olvida sus credenciales, no puede recuperarlas ni volver a descargarlas. Sin embargo, puede crear nuevas credenciales y después deshabilitar 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 simultáneos. Esta funcionalidad permite rotar con regularidad las claves y los certificados, sin que la aplicación sufra periodos de inactividad. Esto ayuda a reducir los riesgos derivados de situaciones en que los certificados o las claves de acceso se han perdido o comprometido. 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, a las distintas cuentas de usuario de IAM, a los foros de debate de AWS y al centro AWS Support. La contraseña se especifica la primera vez que se crea la cuenta, y puede cambiarla en cualquier momento en la página de credenciales de seguridad. Las contraseñas de AWS pueden tener un tamaño de 128 caracteres y 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 usen 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, vaya a Administrar contraseñas en Uso de IAM.

AWS Multi-Factor Authentication (AWS MFA)

AWS Multi-Factor Authentication (AWS MFA) es una capa de seguridad adicional para obtener acceso a los servicios de AWS. Cuando active esta característica opcional, tendrá que facilitar un código de uso exclusivo compuesto de seis dígitos, 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 recursos de AWS. Este código de un solo uso se obtiene en un dispositivo de autenticación que está físicamente en poder del cliente. Se denomina autenticación multifactor porque para poder obtener acceso a la cuenta se comprueban dos factores: una contraseña (algo que conoce) y el código exacto de su dispositivo de autenticación (algo que tiene). Puede habilitar dispositivos MFA para su cuenta de AWS, así como para los usuarios que haya creado con AWS IAM para dicha cuenta de AWS. Asimismo, cuando quiera permitir a un usuario que haya creado en una cuenta de AWS que use un rol de IAM para obtener acceso a los recursos que se encuentran en otra cuenta de AWS, tendrá que añadir protección de MFA para tener acceso a todas las cuentas de AWS. Puede exigir que el usuario utilice MFA antes de adoptar el rol como una capa de seguridad adicional.

AWS MFA es compatible con el uso de tokens de hardware y dispositivos MFA virtuales. Los dispositivos MFA virtuales usan los mismos protocolos que los dispositivos MFA físicos, pero se pueden ejecutar en cualquier dispositivo de hardware móvil, como un smartphone. Un dispositivo MFA virtual usa una aplicación de software que genera códigos de autenticación de seis dígitos compatibles con el estándar para contraseñas de un solo uso basadas en el tiempo (TOTP, por sus siglas en inglés), tal como se describe en RFC 6238. La mayoría de las aplicaciones MFA virtuales permiten alojar varios dispositivos MFA virtuales, por lo que resultan más eficaces que los dispositivos MFA físicos. No obstante, debe tener en cuenta que como una aplicación MFA virtual se puede ejecutar en un dispositivo menos seguro como un smartphone, podría no proporcionar el mismo nivel de seguridad que un dispositivo MFA físico.

También puede forzar la autenticación MFA para las API de servicios de AWS si desea proporcionar una capa adicional de protección a acciones más comprometidas o con privilegios, como terminar instancias Amazon EC2 o leer datos confidenciales almacenados en Amazon S3. Para ello, añada 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 MFA virtuales de una tienda de aplicaciones, y configurarlos para utilizarlos a través del sitio web de AWS. Puede encontrar información adicional acerca de AWS MFA en el sitio web de AWS: http://aws.amazon.com/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 a la función hash, en este caso, incluye el texto de la solicitud y la clave de acceso secreta. Si usa alguno de los SDK de AWS para generar solicitudes, el cálculo de la firma digital se realiza automáticamente; en caso contrario, puede hacer que su aplicación la calcule e incluirla en las solicitudes REST o Query siguiendo las instrucciones de nuestra documentación.

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

La versión más reciente del proceso de cálculo de firmas digitales es Signature Version 4, que calcula la firma usando 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 usar la propia clave de acceso secreta. Asimismo, la clave de firma se obtiene en función del ámbito de credenciales, que proporciona aislamiento criptográfico de la clave de firma.

Como se puede hacer un uso indebido de las claves de acceso si estas van a parar a 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 grupos de instancias EC2 de escalado elástico, el uso de roles de IAM puede ser una forma más segura y cómoda de administrar la distribución de claves de acceso. Los roles de IAM proporcionan credenciales temporales, que no solo se cargan automáticamente en la instancia de destino, sino que también cambian automáticamente varias veces a lo largo del día.

Pares de claves

Las instancias Amazon EC2 creadas a partir de una AMI pública usan un par de claves pública y privada 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 usa 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 nuevas instancias.

Puede generar un par de claves automáticamente cuando inicie la instancia o puede cargar su propio par. Guarde la clave privada en un lugar seguro del sistema y anote el lugar donde la ha guardado.

En el caso de Amazon CloudFront, usará pares de clave para 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 en la página de credenciales de seguridad. Solo se pueden crear mediante la cuenta raíz y no los pueden crear los usuarios de IAM.

Certificados X.509

Los certificados X.509 se usan para firmar solicitudes SOAP. Contienen una clave pública y metadatos adicionales (como una fecha de vencimiento que AWS verifica cuando se 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 se incluye esa firma en la solicitud junto con el certificado. AWS verifica que usted es el remitente descifrando la firma con la clave pública que figura en su certificado. AWS verifica también que el certificado enviado coincide 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 (el certificado de firma) utilizando 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 IAM.

Además de para las solicitudes SOAP, los certificados X.509 se usan como certificados de servidor SSL/TLS para los clientes que desean usar HTTPS para cifrar sus transmisiones. Para usarlas para HTTPS, puede emplear una herramienta de código abierto como OpenSSL para crear una clave privada única. Necesitará la clave privada para crear la solicitud de firma del certificado (CSR) que envía a una entidad de certificación (CA) para obtener el certificado de servidor. A continuación, usará 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 puede 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 los 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 exclusivo dentro de la cuenta de AWS y un conjunto único de credenciales de seguridad no compartidas con otros usuarios. Con AWS IAM no es necesario compartir contraseñas o claves, y puede reducir al mínimo el uso de las credenciales de su cuenta de AWS.

Con IAM, define políticas que controlan a qué servicios de AWS pueden obtener acceso los usuarios y qué pueden hacer con ellos. Puede conceder a los usuarios solo los permisos mínimos que necesitan para realizar su trabajo. Consulte la sección AWS Identity and Access Management (AWS IAM) a continuación para obtener más información.

Protección de los puntos de acceso HTTPS

Para disfrutar de mayor seguridad de comunicación cuando se obtiene acceso a los recursos de AWS, debe usar HTTPS en lugar de HTTP para las transmisiones de datos. HTTPS usa el protocolo SSL/TLS, que utiliza la criptografía de clave pública para evitar el acceso no autorizado, las manipulaciones y la falsificación. Todos los servicios de AWS proporcionan puntos de acceso de cliente seguros (llamados también puntos de enlace de API) que le permiten establecer sesiones de comunicación HTTPS seguras.

Varios servicios ofrecen ahora también funciones de cifrado más avanzadas que usan el protocolo Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). El protocolo ECDHE permite que los clientes SSL/TLS ofrezcan Perfect Forward Secrecy, donde se utilizan claves de sesión que son efímeras y no se almacenan en ningún lugar. Con este método se impide la descodificación de los datos capturados por parte de terceros no autorizados, aunque la clave secreta de larga duración resulte expuesta a riesgos.

Logs de seguridad

Del mismo modo que las credenciales y puntos de enlace cifrados son importantes para evitar problemas de seguridad, los archivos log son igualmente esenciales para conocer los eventos una vez que se produce un problema. Para que sea tan eficaz como una herramienta de seguridad, un archivo log no solo debe incluir un listado de lo que ha sucedido y cuándo ha sucedido, sino que también debe identificar el origen. Para ayudarle con las investigaciones tras los hechos y con la detección de intrusiones prácticamente en tiempo real, AWS CloudTrail proporciona un archivo log de los eventos de su cuenta. Para cada evento, puede ver a qué servicio se obtuvo acceso, qué acción se realizó y quién hizo la solicitud.

CloudTrail captura las llamadas a la API, además de otros eventos como el inicio de sesión en la consola.

Una vez activado CloudTrail, los logs de eventos se envían cada cinco minutos. Puede configurar CloudTrail para que agrupe los archivos log de varias regiones o cuentas en un solo bucket de Amazon S3. De forma predeterminada, se creará un único registro de seguimiento y se enviarán eventos de todas las regiones actuales y futuras. Además de a S3, puede enviar eventos a CloudWatch Logs, para métricas y alarmas personalizadas, o puede cargar los archivos log en las

soluciones de administración y análisis de archivos log que desee para realizar un análisis de seguridad y detectar los patrones de comportamiento de los usuarios. Si desea una respuesta rápida, puede crear reglas de eventos de CloudWatch para emprender las acciones adecuadas ante determinados eventos. De forma predeterminada, los archivos log se almacenan de modo seguro en Amazon S3, pero también puede archivarlos en Amazon Glacier para ayudar a satisfacer los requisitos de auditoría y conformidad.

Además de los logs de actividad del usuario de CloudTrail, puede usar la característica de archivos log de Amazon CloudWatch para recopilar y monitorizar archivos log personalizados, del sistema y de las aplicaciones de sus instancias EC2 y de otros recursos prácticamente en tiempo real. Por ejemplo, puede monitorizar los archivos log del servidor web para identificar los mensajes de usuario no válidos y detectar intentos de inicio de sesión no autorizados en el sistema operativo invitado.

Comprobaciones de seguridad de AWS Trusted Advisor

El servicio de atención al cliente AWS Trusted Advisor no solo monitoriza el desempeño y la resistencia de la nube, sino también la seguridad de la nube. Trusted Advisor inspecciona el entorno de AWS y realiza recomendaciones cuando surge la oportunidad de ahorrar dinero, mejorar el desempeño del sistema o solucionar deficiencias de seguridad. Ofrece alertas sobre varias de las configuraciones erróneas de seguridad más frecuentes que pueden existir, incluido el hecho de dejar abiertos determinados puertos que pueden hacerle vulnerable a piratería y accesos no autorizados, olvidarse de crear cuentas de IAM para sus usuarios internos, permitir el acceso público a los buckets de Amazon S3, no activar el registro de actividad de los usuarios (AWS CloudTrail) o no utilizar MFA en su cuenta raíz de AWS. También tiene la opción de que una persona que trabaje en seguridad en su organización reciba todas las semanas un correo electrónico con el estado actualizado de las comprobaciones de seguridad de Trusted Advisor.

El servicio AWS Trusted Advisor proporciona cuatro comprobaciones sin cargo adicional para todos los usuarios, incluidas tres comprobaciones de seguridad importantes: puertos específicos no restringidos, uso de IAM y MFA en la cuenta raíz. Y si se suscribe al servicio AWS Support de nivel Business o Enterprise, recibirá acceso completo a todas las comprobaciones de Trusted Advisor.

Comprobaciones de seguridad de AWS Config

AWS Config es un servicio de monitorización y evaluación continuas que registra los cambios en la configuración de sus recursos de AWS. Puede consultar las configuraciones actuales e históricas de un recurso, y usar esta información para solucionar problemas de interrupción del servicio o realizar análisis de ataques de seguridad, entre otras operaciones. Puede consultar la configuración en cualquier punto del tiempo, y usar esa información para volver a configurar sus recursos y estabilizarlos durante una interrupción.

Mediante las reglas de configuración, puede realizar comprobaciones de evaluación continuas en sus recursos para verificar que cumplen sus políticas de seguridad, las prácticas recomendadas del sector y los esquemas de conformidad como PCI/HIPAA. Por ejemplo, AWS Config proporciona reglas de configuración administradas que garantizan que el cifrado esté activado para todos los volúmenes EBS de su cuenta. También puede crear una regla de configuración personalizada que básicamente "codifique" sus propias políticas de seguridad corporativas. AWS Config le avisa en tiempo en real cuando un recurso no está configurado correctamente o cuando infringe una determinada política de seguridad.

Seguridad específica del servicio de AWS

La seguridad no solo se integra en cada capa de la infraestructura de AWS, sino también en cada uno de los servicios disponibles en esa infraestructura. Todos los servicios de AWS están creados para que funcionen de forma eficaz y segura con todas las redes y plataformas de AWS. Cada servicio dispone de características de seguridad exhaustivas que le permiten proteger aplicaciones y datos confidenciales.

Servicios de computación

Amazon Web Services proporciona diversos servicios de informática basados en la nube que incluyen una amplia selección de instancias de computación que se pueden aumentar y reducir automáticamente para satisfacer las necesidades de su aplicación o de la empresa.

Seguridad de Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Compute Cloud (EC2) es un componente clave en la infraestructura como servicio (IaaS) de Amazon, que proporciona capacidad informática redimensionable mediante el uso de instancias de servidor en los centros de datos de AWS. Amazon EC2 se ha diseñado para simplificar la informática a escala web al permitirle obtener y configurar la capacidad fácilmente. Puede crear y lanzar instancias, que son conjuntos de hardware y software de la plataforma.

Varios niveles de seguridad

La seguridad dentro de Amazon EC2 se ofrece en diferentes niveles: el sistema operativo (SO) de la plataforma host, el sistema operativo de la instancia virtual o el sistema operativo invitado, un firewall y las llamadas firmadas a las API. Cada uno de estos elementos se basa en las capacidades de los otros. El objetivo consiste en ofrecer protección frente al acceso de sistemas o usuarios no autorizados a los datos almacenados en Amazon EC2, así como ofrecer a las instancias Amazon EC2 la máxima protección posible sin que ello repercuta en la flexibilidad de la configuración que los clientes demandan.

El hipervisor

Amazon EC2 utiliza actualmente una versión muy personalizada del hipervisor Xen para aprovechar la paravirtualización (en el caso de los invitados de Linux). Habida cuenta de que los invitados paravirtualizados dependen del hipervisor para ofrecer soporte para las operaciones que normalmente requieren acceso privilegiado, el SO invitado no tiene acceso elevado a la CPU. La CPU ofrece cuatro modos de privilegios diferentes: 0-3, denominados anillos. El anillo 0 se corresponde con el nivel de máximos privilegios y el 3 con el de menos. El SO host se ejecuta en el anillo 0. Sin embargo, en lugar de ejecutarse en el anillo 0, como lo hacen la mayoría de los sistemas operativos, el SO invitado se ejecuta en el anillo 1, que tiene menos privilegios, y las aplicaciones en el anillo 3, es decir, en el que menos privilegios ofrece. Esta virtualización explícita de los recursos físicos se traduce en una separación clara entre el invitado y el hipervisor, lo que se traduce en una separación de seguridad adicional entre ambos.

Aislamiento de instancias

Las diferentes instancias ejecutadas en el mismo equipo físico se separan entre sí a través del hipervisor Xen. Amazon está activo en la comunidad Xen, que ofrece sensibilización sobre los últimos desarrollos. Además, el firewall de AWS se hospeda en la capa del hipervisor, entre la interfaz de la red física y la interfaz

virtual de la instancia. Todos los paquetes deben pasar por esta capa, por lo que los vecinos de una instancia tienen tanto acceso a dicha instancia como cualquier otro host de Internet y se pueden tratar como si estuvieran en host físicos independientes. La RAM física se separa usando mecanismos similares.

Las instancias de los clientes no tienen acceso a los dispositivos del disco sin procesar, sino que, en su lugar, se presentan con discos virtualizados. La capa de virtualización del disco propietario de AWS restablece automáticamente cada bloque de almacenamiento utilizado por el cliente, de forma que los datos de un cliente no se vean expuestos de forma no intencionada a otros usuarios. Asimismo, el hipervisor restablece (pone a cero) la memoria asignada a los invitados, cuando esta deja de estar asignada a un invitado. La memoria no vuelve al grupo de memoria libre disponible para nuevas asignaciones hasta que se completa el restablecimiento de memoria.

AWS recomienda que los clientes adopten medidas adicionales para proteger sus datos mediante los recursos apropiados. Una solución común consiste en ejecutar un sistema de archivos cifrados sobre el dispositivo del disco virtualizado.

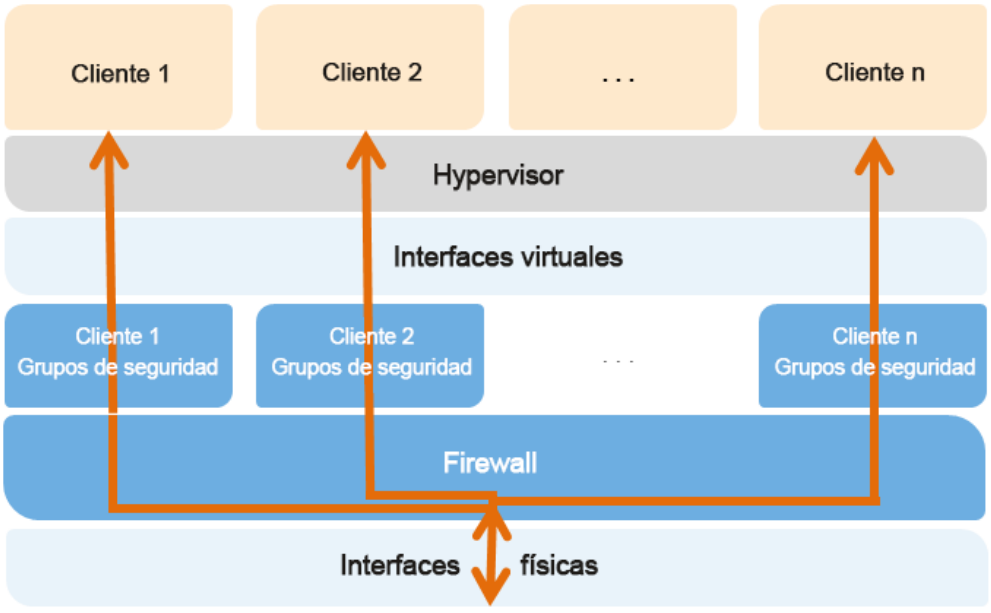


Figura 3: Varias capas de seguridad de Amazon EC2

Sistema operativo host: los administradores que tengan necesidades empresariales de obtener acceso a los planes de administración han de utilizar la autenticación multifactor para poder tener acceso a hosts de administración en función del propósito. Estos hosts de administración son sistemas específicamente diseñados, compilados, configurados y con seguridad extra para proteger el plano de administración de la nube. Todo este acceso está sujeto a registros y auditorías. Cuando algún empleado deja de tener la necesidad empresarial de obtener acceso al ámbito de administración, se revocan los privilegios y el acceso en relación con estos hosts y con los sistemas pertinentes.

Sistema operativo invitado: usted, el cliente, controla completamente las instancias virtuales. Tiene acceso total a la raíz o control administrativo sobre las cuentas, los servicios y las aplicaciones. AWS no tiene ningún derecho de acceso sobre sus instancias o sobre el sistema operativo invitado. AWS recomienda usar un conjunto básico de prácticas recomendadas que incluyan la desactivación del acceso solo mediante contraseña a sus invitados y el uso de alguna forma de autenticación multifactor para obtener acceso a sus instancias (o un acceso mínimo a la versión 2 de SSH mediante certificado). Además, debe utilizar un mecanismo de escalado mediante privilegios basado en un registro por cada usuario. Por ejemplo, si el sistema operativo invitado es Linux, después de proteger su instancia, debe utilizar la versión 2 de SSH basada en certificados para acceder a la instancia virtual, desactivar el acceso remoto a la raíz, utilizar el registro de línea de comandos y usar "sudo" para la ampliación de privilegios. Debe generar sus propios pares de claves a fin de garantizar que sean exclusivas y que no coincidan con las de otros clientes ni con las de AWS.

AWS admite también el uso del protocolo de red Secure Shell (SSH) para que pueda conectarse de forma segura a sus instancias EC2 UNIX o Linux. La autenticación de SSH usada con AWS se realiza a través de un par de claves pública y privada para reducir el riesgo del acceso no autorizado a sus instancias. También puede conectarse de forma remota a sus instancias Windows mediante el protocolo de escritorio remoto (RDP) utilizando un certificado RDP generado para su instancia.

Usted también controla la actualización y revisión de su sistema operativo invitado, incluidas las actualizaciones de seguridad. Las AMI basadas en Windows y Linux proporcionadas por Amazon se actualizan periódicamente con los últimos parches, para que en el caso de que no necesite conservar los datos o las personalizaciones en sus instancias de AMI de Amazon en funcionamiento,

pueda sencillamente volver a lanzar nuevas instancias con la última versión actualizada de la AMI. Asimismo, las actualizaciones de la AMI Linux de Amazon se suministran a través de los repositorios yum Linux de Amazon.

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

El firewall puede configurarse por grupos que permitan que las diferentes clases de instancias tengan diferentes reglas. Pensemos, por ejemplo, en el caso de una aplicación web tradicional de tres niveles. El grupo de servidores web tendría el puerto 80 (HTTP) o el puerto 443 (HTTPS) abierto para Internet. El grupo de servidores de aplicaciones tendría el puerto 8000 (específico de la aplicación) abierto solo para el grupo de servidores web. El grupo de servidores de bases de datos tendría el puerto 3306 (MySQL) abierto solo para el grupo de servidores de aplicaciones. Los tres grupos permitirían el acceso administrativo a través del puerto 22 (SSH), pero solo desde la red corporativa del cliente. Las aplicaciones con un alto nivel de seguridad pueden implementarse utilizando este mecanismo expresivo. Véase la Figura 4 a continuación:

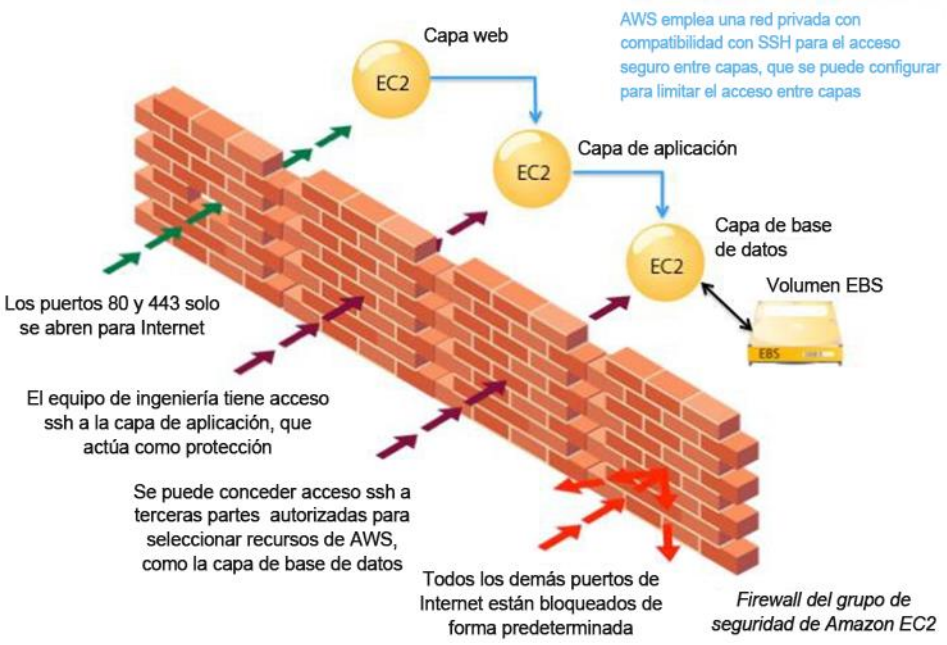


Figura 4: Firewall del grupo de seguridad de Amazon EC2

El firewall no se controla a través del SO invitado, sino que requiere el certificado y la clave X.509 para autorizar cambios, lo que añade una capa adicional de seguridad. AWS admite la posibilidad de conceder acceso pormenorizado a las diferentes funciones administrativas sobre las instancias y el firewall, permitiéndole así implementar una medida de seguridad adicional mediante la separación de obligaciones. El nivel de seguridad que ofrece el firewall depende de los puertos que abra, así como de su duración y finalidad. El estado predeterminado consiste en denegar todo el tráfico entrante, y deberá planificar cuidadosamente lo que estará abierto al crear y proteger sus aplicaciones. Aún se precisa de un diseño de seguridad y una administración del tráfico bien informada por cada instancia. AWS le aconseja también que aplique filtros adicionales para cada instancia con firewalls basados en host como IPtables o el firewall de Windows y las VPN. De esta forma, podrá restringir el tráfico entrante y saliente.

Acceso a la API: todas las llamadas a la API para lanzar y terminar instancias, cambiar los parámetros del firewall y realizar otras funciones están firmadas por la clave de acceso secreta de Amazon del cliente de AWS, que puede ser la clave de acceso secreta de la cuenta de AWS o la clave de acceso secreta de un usuario creado con AWS IAM. Sin el acceso a su clave de acceso secreta, no se pueden realizar llamadas a la API de Amazon EC2 en su nombre. Además, las llamadas a la API pueden cifrarse con SSL para mantener la confidencialidad. Amazon recomienda utilizar siempre puntos de enlace de las API protegidos con el protocolo SSL.

Permisos: AWS IAM también le permite controlar aún más para qué API tiene permiso de llamada un usuario.

Seguridad de Elastic Block Storage (Amazon EBS)

Amazon Elastic Block Storage (EBS) le permite crear volúmenes de almacenamiento de entre 1 GB y 16 TB que las instancias Amazon EC2 pueden montar como dispositivos. Los volúmenes de almacenamiento actúan como dispositivos de bloqueo sin formato, con nombres de dispositivo suministrados por el usuario y una interfaz de dispositivo de bloqueo. Puede utilizar los volúmenes de Amazon EBS para crear un sistema de archivos sobre ellos o usarlos como cualquier otro dispositivo de bloques (como una unidad de disco duro). El acceso al volumen de Amazon EBS está restringido a la cuenta de AWS que ha creado el volumen, así como a los usuarios creados para la cuenta de AWS con AWS IAM en caso de que al usuario se le haya concedido el acceso a las operaciones de EBS, de forma que se deniega el permiso a todas las demás cuentas y usuarios de AWS de visualizar el volumen u obtener acceso a él.

Los datos almacenados en volúmenes EBS de Amazon se almacenan de forma redundante en varias ubicaciones físicas como parte del funcionamiento normal de dichos servicios y sin cargo adicional. No obstante, la replicación de Amazon EBS se almacena en la misma zona de disponibilidad, no en varias zonas y, por tanto, es muy recomendable que los clientes realicen snapshots periódicas de Amazon S3 para disfrutar de una durabilidad de los datos a largo plazo. Si se trata de clientes que han creado bases de datos transaccionales complejas con EBS, se recomienda que los backups de Amazon S3 se realicen a través de un sistema de administración de bases de datos, a fin de que se puedan determinar las transacciones distribuidas y los logs. AWS no realiza backups de los datos que se almacenan en discos virtuales conectados a instancias en ejecución en Amazon EC2.

Puede hacer públicas las snapshots de los volúmenes de Amazon EBS para otras cuentas de AWS, a fin de que se utilicen como base para crear sus propios volúmenes. El hecho de compartir las snapshots del volumen de Amazon EBS no concede el permiso a las demás cuentas de AWS para que puedan alterar o eliminar la snapshot original, ya que dicho privilegio está reservado de forma explícita para la cuenta de AWS que creó el volumen. Una snapshot de EBS se corresponde con una vista de nivel de bloque de un volumen completo de EBS. Tenga en cuenta que los datos que no se puedan visualizar a través del sistema de archivos del volumen, como los archivos que se han eliminado, pueden encontrarse en la snapshot de EBS. Si desea crear snapshots compartidas, debe hacerlo con precaución. Se debe crear un nuevo volumen de EBS en caso de que un volumen haya contenido datos sensibles o si se han eliminado archivos del mismo. Los datos que vaya a contener la snapshot compartida deben copiarse en un nuevo volumen, y la snapshot ha de crearse a partir del nuevo volumen.

Los volúmenes de Amazon EBS se presentan como dispositivos de bloques sin formato y sin procesar que se borran antes de que puedan utilizarse. El borrado se realiza inmediatamente antes de su reutilización, de modo que pueda asegurarse de que el proceso de borrado se complete con éxito. Si usted tiene procedimientos que requieren que todos los datos se borren con un método específico, como los que se detallan en NIST 800-88 (“Directrices para el saneamiento de soportes"), cuenta con la opción de hacerlo en Amazon EBS. Debe realizar un procedimiento de borrado especializado antes de eliminar el volumen, con el fin de cumplir con los requisitos que estableció.

El cifrado de datos confidenciales, por lo general, es una buena práctica de seguridad, y AWS proporciona la capacidad de cifrar volúmenes EBS y sus snapshots con AES-256. El cifrado se realiza en los servidores que alojan las instancias EC2, por lo que los datos se cifran a medida que estos circulan entre las instancias EC2 y el almacenamiento de EBS. Para poder hacer esto eficazmente y con baja latencia, la característica de cifrado de EBS solo está disponible en los tipos de instancias más potentes de EC2 (como M3, C3, R3, G2).

Seguridad de Auto Scaling

La funcionalidad de Auto Scaling le permite aumentar o disminuir su capacidad de Amazon EC2 en función de las condiciones que defina, de forma que el número de instancias Amazon EC2 que utiliza aumenten sin ningún problema durante los picos de demanda para mantener el desempeño y se reduzcan automáticamente durante los estancamientos de la demanda a fin de minimizar los costos.

Al igual que todos los servicios de AWS, Auto Scaling requiere que cada solicitud realizada a su API de control se autentique para que solo los usuarios autenticados puedan obtener acceso a Auto Scaling y administrar este servicio. Las solicitudes se firman con una firma HMAC-SHA1 calculada a partir de una solicitud y la clave privada del usuario. Sin embargo, en el caso de grandes grupos de instancias con escalado elástico, puede resultar complicado asignar credenciales a las nuevas instancias EC2 lanzadas con Auto-Scaling. Para simplificar este proceso, puede usar roles dentro de IAM, de forma que se proporcionen automáticamente credenciales a todas las instancias nuevas lanzadas con un rol. Cuando lanza una instancia EC2 con un rol de IAM, las credenciales de seguridad temporales de AWS con permisos especificados por el rol se aprovisionan de forma segura en la instancia y están disponibles en su aplicación a través del servicio de metadatos de instancias de Amazon EC2. El servicio de metadatos creará nuevas credenciales de seguridad temporales antes de que venzan las credenciales actualmente activas para que la instancia siempre disponga de credenciales válidas. Además, las credenciales de seguridad temporales rotan automáticamente varias veces al día, para mayor seguridad. Puede controlar aún más el acceso a Auto Scaling mediante la creación de usuarios en su cuenta de AWS usando AWS IAM y controlando a qué API de Auto Scaling pueden llamar estos usuarios. Encontrará más información sobre el uso de roles y el lanzamiento de instancias en la guía del usuario de Amazon EC2, disponible en el sitio web de AWS.

Servicios de redes

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

Seguridad de Amazon Elastic Load Balancing

Amazon Elastic Load Balancing se usa para administrar el tráfico en un grupo de instancias Amazon EC2, distribuyendo el tráfico entre las instancias en todas las zonas de disponibilidad de una región. Elastic Load Balancing ofrece todas las ventajas de un balanceador de carga local, así como varios beneficios relativos a la seguridad:

- Se ocupa del trabajo de cifrado y descifrado de las instancias Amazon EC2 y lo administra centralmente en el balanceador de carga.
- Ofrece a los clientes un único punto de contacto y actúa también como la primera línea de defensa frente a los ataques a la red.
- Cuando se utiliza en una VPC de Amazon, permite crear y administrar grupos de seguridad asociados a Elastic Load Balancing para proporcionar opciones de seguridad y de red adicionales.
- Admite el cifrado integral del tráfico mediante TLS (anteriormente SSL) en aquellas redes que usan conexiones HTTP seguras (HTTPS). Cuando se utiliza TLS, el certificado de servidor TLS usado para terminar las conexiones del cliente se puede administrar centralmente en el balanceador de carga, en lugar de en cada instancia individual.

HTTPS/TLS usa una clave secreta de larga duración para generar una clave de sesión de corta duración que se utiliza entre el servidor y el navegador para crear el mensaje cifrado. Amazon Elastic Load Balancing configura su balanceador de carga con un conjunto de códigos cifrados predefinido que se usa para la negociación de TLS cuando se establece una conexión entre un cliente y el balanceador de carga. El conjunto de códigos cifrados predefinido proporciona compatibilidad con una amplia variedad de clientes y usa algoritmos criptográficos seguros. Sin embargo, algunos clientes pueden tener requisitos que solo permitan determinados códigos cifrados y protocolos (como PCI, SOX, etc.) de los clientes para garantizar que se cumplen las normas. En

tales casos, Amazon Elastic Load Balancing proporciona opciones para seleccionar diferentes configuraciones para protocolos y conjuntos de códigos cifrados de TLS. Puede elegir entre activar o desactivar los códigos cifrados en función de sus requisitos específicos.

Para ayudarle a garantizar que se usan los códigos cifrados más recientes y seguros cuando se establece una conexión segura, puede configurar el balanceador de carga de modo que tenga la última palabra sobre la selección de los códigos cifrados durante la negociación entre el cliente y el servidor. Cuando se selecciona la opción de preferencia del orden del servidor, el balanceador de carga selecciona un conjunto de códigos cifrados en función de la prioridad asignada por el servidor y no por el cliente. Esto le ofrece mayor control sobre la capa de seguridad que usan los clientes para conectarse a su balanceador de carga.

Para disfrutar de una privacidad mayor en las comunicaciones, el servicio Elastic Load Balancer de Amazon permite el uso de Perfect Forward Secrecy, que emplea claves de sesión efímeras que no se almacenan en ningún lugar. Con este método se impide la descodificación de los datos capturados, aunque la clave secreta de larga duración resulte atacada.

Amazon Elastic Load Balancing le permite identificar la dirección IP de origen de un cliente cuando se conecta a los servidores, tanto si utiliza HTTPS como el balanceo de carga TCP. Normalmente, la información de conexión del cliente, como la dirección IP y el puerto, se pierde cuando las solicitudes pasan por un balanceador de carga. Esto es así porque el balanceador de carga envía solicitudes al servidor en nombre del cliente, dándole la apariencia del cliente que realiza la solicitud. Disponer de la dirección IP del cliente de origen es útil si necesita más información sobre los visitantes de su aplicación para reunir estadísticas de conexión, analizar logs de tráfico o administrar listas de direcciones IP permitidas.

Los logs de acceso de Amazon Elastic Load Balancing contienen información sobre cada solicitud HTTP y TCP procesada por el balanceador de carga. Entre esta se incluye la dirección IP y el puerto del cliente que hace la solicitud, la dirección IP del backend de la instancia que ha procesado 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). Se registran todas las solicitudes enviadas al balanceador de carga, incluidas las que nunca se hicieron en instancias del backend.

Seguridad de Amazon Virtual Private Cloud (Amazon VPC)

Normalmente, a cada instancia Amazon EC2 que se lanza se le asigna una dirección IP pública de forma aleatoria en el espacio de direcciones de Amazon EC2. Amazon VPC le permite crear una parte aislada de la nube de AWS y lanzar instancias Amazon EC2 que tengan direcciones privadas (RFC 1918) en el intervalo que elija (p. ej., 10.0.0.0/16). Puede definir subredes dentro de su VPC, agrupando tipos similares de instancias en función de su intervalo de direcciones IP, y configurar el enrutamiento y la seguridad para controlar el flujo de entrada y salida de las instancias y las subredes.

AWS ofrece diversas plantillas de arquitectura de VPC con configuraciones que proporcionan distintos niveles de acceso público:

- VPC con una única subred pública. Sus instancias se ejecutan en una sección privada y aislada de la nube de AWS con acceso directo a Internet. Se pueden usar listas de control de acceso (ACL) de red y grupos de seguridad para proporcionar un control estricto sobre el tráfico de red que entra y sale de las instancias.
- VPC con subredes públicas y privadas. Además de incluir una subred pública, esta configuración añade una subred privada cuyas instancias no están disponibles desde Internet. Las instancias de la subred privada pueden establecer conexiones de salida a Internet a través de la subred pública mediante NAT (Traducción de direcciones de red).
- VPC con subredes públicas y privadas y acceso a VPN por hardware. Esta configuración añade una conexión de VPN IPsec entre la VPC de Amazon y el centro de datos, ampliando así eficazmente su centro de datos en la nube y proporcionando acceso directo a Internet a las instancias de la subred pública de su VPC de Amazon. En esta configuración, los clientes añaden un dispositivo VPN en su centro de datos corporativo.
- VPC con una única subred privada y acceso VPN por hardware. Sus instancias se ejecutan en una sección privada y aislada de la nube de AWS con una subred privada cuyas instancias no están disponibles desde Internet. Puede conectar esta subred privada a su centro de datos corporativo a través de un túnel de VPN IPsec.

También puede conectar dos VPC mediante una dirección IP privada que permita a las instancias de las dos VPC conectarse entre sí como si estuvieran en 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 de Amazon VPC incluyen grupos de seguridad, ACL de red, tablas de enrutamiento y puertas de enlace externas. Cada uno de estos elementos es complementario para ofrecer una red aislada y segura que pueda ampliarse a través de una habilitación selectiva del acceso directo a Internet o de la conexión privada a otra red. Las instancias Amazon EC2 que se ejecutan en una VPC de Amazon heredan todas las ventajas descritas a continuación en relación con el sistema operativo invitado y la protección frente al análisis de paquetes.

Tenga en cuenta, sin embargo, que debe crear grupos de seguridad de VPC específicamente para su VPC de Amazon; los grupos de seguridad de Amazon EC2 que haya creado no funcionarán en su VPC de Amazon. Además, los grupos de seguridad de Amazon VPC tienen funciones adicionales inexistentes en los grupos de seguridad de Amazon EC2, como la capacidad de cambiar el grupo de seguridad tras lanzar la instancia y la posibilidad de especificar cualquier protocolo con un número de protocolo estándar (y no solo TCP, UDP o ICMP).

Cada VPC de Amazon es una red distinta y aislada dentro de la nube; el tráfico de red en cada VPC de Amazon está aislado de las demás VPC de Amazon. En el momento de la creación, seleccionará un intervalo de direcciones IP para cada VPC de Amazon. Puede crear y conectar un puerto de enlace a Internet, una gateway privada virtual o ambas para establecer la conexión externa, de conformidad con los siguientes controles.

Acceso a la API: llamadas para crear y eliminar VPC de Amazon, cambiar el enrutamiento, el grupo de seguridad y los parámetros de ACL de la red y para realizar otras funciones firmadas por su clave de acceso secreta de Amazon, que puede ser la clave de acceso secreta de la cuenta de AWS o la clave de acceso secreta de un usuario creado con AWS IAM. Sin el acceso a su clave de acceso secreta, no se pueden realizar llamadas a la API de Amazon VPC en su nombre. Además, las llamadas a la API pueden cifrarse con SSL para mantener la confidencialidad. Amazon recomienda utilizar siempre puntos de enlace de las API protegidos con el protocolo SSL. AWS IAM también permite que un cliente pueda controlar aún más para qué API tiene permiso de llamada un usuario recién creado.

Subredes y tablas de ruteo: puede crear una o varias subredes dentro de cada VPC de Amazon; cada instancia iniciada en la VPC de Amazon está conectada a una subred. Se bloquean los ataques de seguridad de la capa 2 tradicionales, incluida la suplantación de MAC y ARP.

Cada subred de una VPC de Amazon está asociada con una tabla de enrutamiento, y todo el tráfico de red que parte de una subred se procesa mediante la tabla de enrutamiento para determinar el destino.

Firewall (grupos de seguridad): al igual que Amazon EC2, Amazon VPC admite una solución completa de firewall que permite filtrar el tráfico de entrada y salida de una instancia. El grupo predeterminado permite la comunicación de entrada de otros miembros del mismo grupo y la comunicación de salida a cualquier destino. El tráfico puede restringirse mediante cualquier protocolo IP, por puerto de servicio o por dirección IP de origen/destino (IP individual o por bloque de enrutamiento entre dominios sin clases [CIDR]).

El firewall no se controla a través del sistema operativo invitado; solo puede modificarse a través de la invocación de las API de Amazon VPC. AWS admite la posibilidad de conceder acceso pormenorizado a las diferentes funciones administrativas sobre las instancias y el firewall, permitiéndole así implementar una medida de seguridad adicional mediante la separación de obligaciones. El nivel de seguridad que ofrece el firewall depende de los puertos que abra, así como de su duración y finalidad. Aún se precisa de un diseño de seguridad y una administración del tráfico bien informada por cada instancia. AWS le aconseja también que aplique filtros adicionales para cada instancia con firewalls basados en host como IPtables o el firewall de Windows.

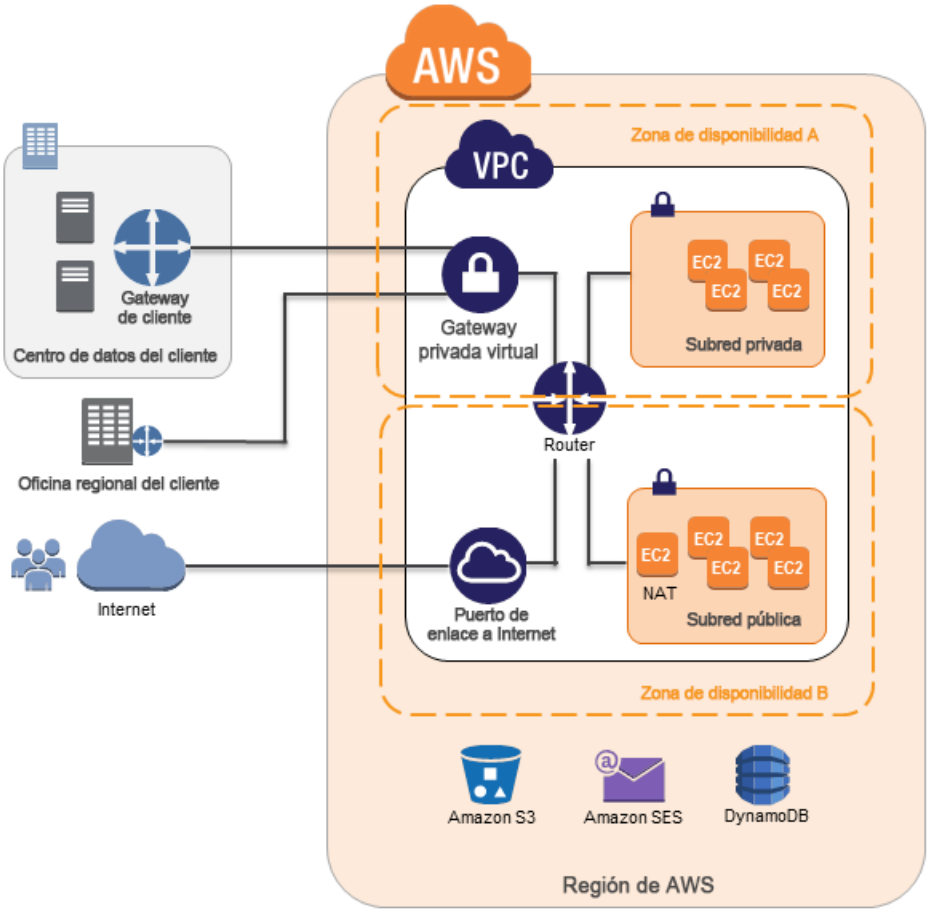


Figura 5: Arquitectura de red de Amazon VPC

Listas de control de acceso a la red: para añadir una capa adicional de seguridad en Amazon VPC, puede configurar listas de control de acceso a la red (ACL). Estas listas son filtros de tráfico sin estado que se aplican a todo el tráfico entrante y saliente procedente de una subred dentro de Amazon VPC. Estas ACL pueden contener reglas ordenadas para permitir o denegar el tráfico basado en el protocolo IP, por el puerto de servicio o la dirección IP de origen/destino.

Como en el caso de los grupos de seguridad, las ACL de red se administran a través de las API de Amazon VPC, con lo que se añade una capa adicional de protección y se activa un nivel adicional de seguridad a través de la separación de obligaciones. En el diagrama siguiente se muestra cómo se interrelacionan los controles de seguridad para habilitar las topologías de redes flexibles al mismo tiempo que ofrecen un control total de los flujos del tráfico de red.

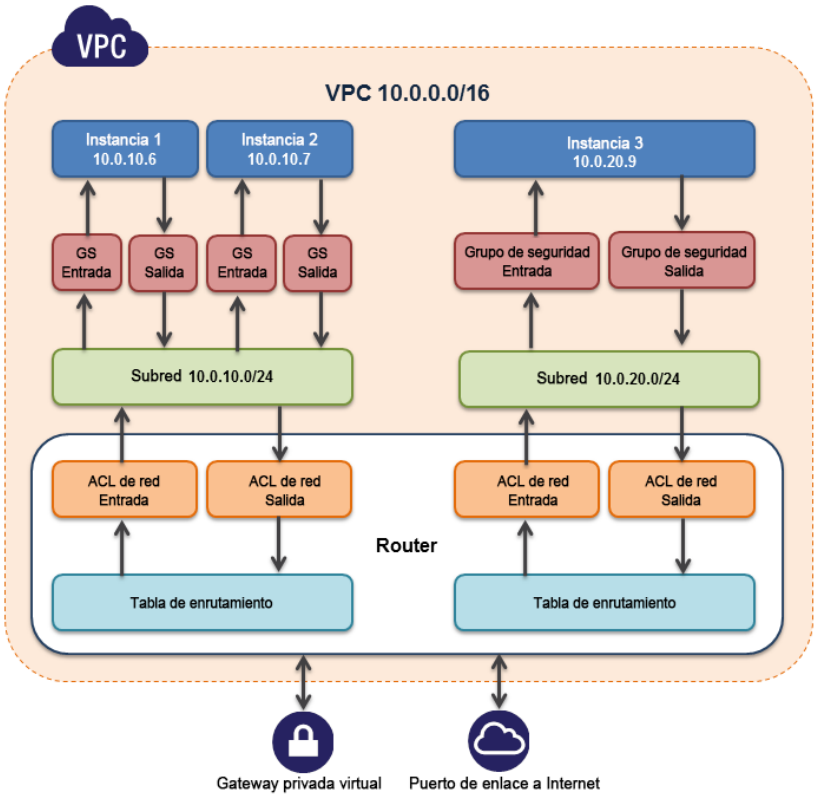


Figura 6: Topologías de red flexibles

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

Puerto de enlace a Internet: un puerto de enlace a Internet puede enlazarse a una VPC de Amazon para permitir la conectividad directa a Amazon S3, a otros servicios de AWS y a Internet. Cada instancia que precise de este acceso debe tener una IP elástica asignada o dirigir el tráfico a través de una instancia NAT. Además, los enrutamientos de red se configuran (véase la información anterior) para dirigir el tráfico hacia el puerto de enlace a Internet. AWS ofrece AMI de NAT de referencia que puede ampliar para realizar registros de red, inspecciones exhaustivas de paquetes, filtros de capas de aplicaciones u otros controles de seguridad.

Este acceso solo puede modificarse a través de la invocación de las API de Amazon VPC. AWS admite la posibilidad de conceder acceso pormenorizado a las diferentes funciones administrativas sobre las instancias y el puerto de enlace a Internet, permitiéndole así implementar medidas de seguridad adicionales mediante la separación de obligaciones.

Instancias dedicadas: dentro de una VPC, puede lanzar instancias Amazon EC2 que estén físicamente aisladas en el nivel de hardware del host (es decir, se ejecutarán en hardware dedicado a un solo inquilino). Una VPC de Amazon se puede crear con una tenencia "dedicada" para que todas las instancias lanzadas en la VPC de Amazon utilicen esta característica. También se puede crear una VPC de Amazon con una tenencia "predeterminada" y especificar la tenencia "dedicada" para instancias concretas lanzadas dentro de la VPC.

Interfaces de redes elásticas: cada instancia Amazon EC2 tiene una interfaz de red predeterminada a la que se asigna una dirección IP privada en la red de Amazon VPC. Puede crear y asociar una interfaz de red adicional, denominada "interfaz de red elástica" (ENI), a cualquier instancia Amazon EC2 de su VPC de Amazon hasta un total de dos interfaces de red por instancia. Asociar varias interfaces de red a una instancia es útil cuando se quiere crear una red de administración, usar dispositivos de red y seguridad en la VPC de Amazon o crear instancias de doble alojamiento con cargas de trabajo o roles en subredes distintas. Los atributos de una ENI, incluida la dirección IP privada, las direcciones IP elásticas y la dirección MAC, siguen estando en la ENI cuando esta se asocia o desasocia de una instancia y se vuelve a asociar a otra instancia. Encontrará más información sobre Amazon VPC en el sitio web de AWS: http://aws.amazon.com/vpc/

Control de acceso de red adicional con EC2-VPC

Si lanza instancias en una región en la que no tenía instancias antes de que AWS lanzara la nueva característica EC2-VPC (denominada también "VPC predeterminada"), todas las instancias se aprovisionan automáticamente en una VPC predeterminada lista para usar. Puede elegir entre crear VPC adicionales o crear VPC para instancias en regiones en las que ya tenía instancias antes de que se lanzara EC2-VPC.

Si crea una VPC más adelante, utilizando una VPC normal, tendrá que especificar un bloque de CIDR, crear las subredes, especificar el enrutamiento y la seguridad de esas subredes y aprovisionar un puerto de enlace a Internet o una instancia NAT, si desea que se pueda obtener acceso a una de las subredes desde Internet. Cuando lanza instancias EC2 en una EC2-VPC, la mayor parte del trabajo se realiza automáticamente.

Cuando lanza una instancia en una VPC predeterminada usando EC2-VPC, realizamos las siguientes tareas para configurarla:

- Crear una subred predeterminada en cada zona de disponibilidad
- Crear un puerto de enlace a Internet y conectarlo con su VPC predeterminada
- Crear una tabla de ruteo principal para su VPC predeterminada con una regla que envía todo el tráfico dirigido a Internet al puerto de enlace a Internet
- Crear un grupo de seguridad predeterminado y asociarlo a su VPC predeterminada
- Crear una lista de control de acceso (ACL) de red predeterminada y asociarla a su VPC predeterminada
- Asociar las opciones de DHCP predeterminadas configuradas para su cuenta de AWS con su VPC predeterminada

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

En la tabla siguiente se indican las diferencias entre las instancias lanzadas en EC2-Classic, las instancias lanzadas en una VPC predeterminada y las instancias lanzadas en una VPC que no es la predeterminada.

Característica	EC2-Classic	EC2-VPC (VPC predeterminada)	VPC normal
		La instancia no recibe una dirección IP pública de forma predeterminada.	A no ser que especifique lo contrario durante el lanzamiento.
Dirección IP privada	La instancia recibe una dirección IP privada del intervalo de EC2-Classic cada vez que se inicia.	La instancia recibe una dirección IP privada estática del intervalo de direcciones de su VPC predeterminada.	La instancia recibe una dirección IP privada estática del intervalo de direcciones de su VPC.
Varias direcciones IP privadas	Seleccionamos una sola dirección IP para su instancia. No se permite tener varias direcciones IP privadas.	Puede asignar varias direcciones IP privadas a su instancia.	Puede asignar varias direcciones IP privadas a su instancia.
Dirección IP elástica	Una EIP se desasocia de su instancia cuando se detiene.	Una EIP sigue asociada a su instancia cuando se detiene.	Una EIP sigue asociada a su instancia cuando se detiene.
Nombre de host DNS	Los nombres de host DNS están habilitados de forma predeterminada.	Los nombres de host DNS están habilitados de forma predeterminada.	Los nombres de host DNS están deshabilitados de forma predeterminada.
Grupo de seguridad	Un grupo de seguridad puede hacer referencia a grupos de seguridad que pertenezcan a otras cuentas de AWS.	Un grupo de seguridad puede hacer referencia únicamente a grupos de seguridad de su VPC.	Un grupo de seguridad puede hacer referencia únicamente 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 la instancia en ejecución.	Puede cambiar el grupo de seguridad de la instancia en ejecución.
Reglas del grupo de seguridad	Puede añadir reglas solo para el tráfico entrante.	Puede añadir reglas para el tráfico de entrada y salida.	Puede añadir reglas para el tráfico de entrada y salida.
Tenencia	La instancia se ejecuta en hardware compartido; no puede ejecutar una instancia en hardware de un solo propietario.	Puede ejecutar la instancia en hardware compartido o en hardware de un solo propietario.	Puede ejecutar la instancia en hardware compartido o en hardware de un solo propietario.

Nota: los grupos de seguridad de las instancias EC2-Classic son ligeramente diferentes de los grupos de seguridad de las instancias EC2-VPC. Por ejemplo, puede añadir reglas de tráfico entrante para EC2-Classic, pero no puede añadir reglas de tráfico entrante y saliente a EC2-VPC. En EC2-Classic, no puede cambiar los grupos de seguridad asignados a una instancia una vez iniciada, pero sí en EC2-VPC. Tampoco puede usar los grupos de seguridad que ha creado para usarlos con EC2-Classic con instancias en su VPC. Debe crear grupos de seguridad específicamente para usarlos con instancias de su VPC. Las reglas que cree para usarlas con un grupo de seguridad de una VPC no pueden hacer referencia a un grupo 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) altamente disponible y escalable que responde a las consultas DNS traduciendo los nombres de dominio en direcciones IP para que los equipos puedan comunicarse entre sí. Route 53 se puede usar para conectar las solicitudes de los usuarios a la infraestructura que se ejecuta en AWS, como una instancia Amazon EC2 o un bucket de Amazon S3, o a infraestructura fuera de AWS.

Amazon Route 53 le permite administrar las direcciones IP (registros) de sus nombres de dominio y responde a las respuestas (consultas) para convertir nombres de dominio específicos en sus direcciones IP correspondientes. Las consultas de su dominio se enrutan automáticamente al servidor DNS más próximo mediante difusión para proporcionar la menor latencia posible. Route 53

permite administrar el tráfico de manera global a través de varios tipos de direccionamiento, incluido 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 para ayudar a crear varias arquitecturas de baja latencia y tolerantes a errores. Los algoritmos de conmutación por error implementados por Amazon Route 53 se han diseñado no solo para dirigir el tráfico a puntos de enlace en buen estado, sino también para ayudar a mitigar los desastres provocados por comprobaciones de estado y aplicaciones configuradas incorrectamente, sobrecargas de los puntos de enlace y errores de partición.

Route 53 también ofrece el registro de nombres de dominio: puede adquirir y administrar nombres de dominio como ejemplo.com y Route 53 establecerá automáticamente la configuración DNS predeterminada para sus dominios. Puede comprar, administrar y transferir (en ambos sentidos) dominios de una amplia selección de dominios de nivel superior (TLD) genéricos y específicos del país. Durante el proceso de registro, tiene la opción de habilitar la protección de privacidad de su dominio. Esta opción ocultará la mayor parte de su información personal de la base de datos Whois pública para ayudarle a frustrar los intentos de rastreo y envío de spam.

Route 53 se ha diseñado mediante la infraestructura de confianza y de alta disponibilidad de AWS. La naturaleza distribuida de los servidores DNS de AWS permite garantizar una capacidad constante de direccionamiento de los usuarios finales a su aplicación. Route 53 también ayuda a garantizar la disponibilidad de su sitio web proporcionando comprobaciones de estado y funciones de conmutación por error a nivel de DNS. Puede configurar fácilmente Route 53 para que compruebe el estado de su sitio web periódicamente (incluso en el caso de sitios web que solo estén disponibles a través de SSL) y para cambiar a un sitio de backup si el principal deja de responder.

Al igual que todos los servicios de AWS, Amazon Route 53 requiere que cada solicitud realizada a su API de control se autentique para que solo los usuarios autenticados puedan obtener acceso a Route 53 y administrar este servicio. Las solicitudes API se firman con una firma MAC-SHA1 o HMAC-SHA256 calculada a partir de una solicitud y de la clave de acceso secreta de AWS del usuario. Además, a la API de control de Amazon Route 53 solo se puede tener acceso a través de los puntos de enlace cifrados por SSL. Admite el enrutamiento IPv4 e IPv6.

Puede controlar el acceso a las funciones de administración de DNS de Amazon Route 53 creando usuarios en su cuenta de AWS mediante AWS IAM y controlando qué operaciones de Route 53 pueden realizar estos usuarios.

Seguridad de Amazon CloudFront

Amazon CloudFront proporciona a los clientes una forma sencilla de distribuir contenido a los usuarios finales con baja latencia y una alta velocidad de transferencia de datos. Ofrece contenido dinámico, estático y por transmisión mediante una red global de ubicaciones de borde. Las solicitudes de objetos de los clientes se enrutan de forma automática hasta la ubicación de borde más

cercana, para que el contenido se entregue con el máximo desempeño posible. Amazon CloudFront es una solución optimizada para funcionar en combinación con otros servicios de AWS, como Amazon S3, Amazon EC2, Amazon Elastic Load Balancing y Amazon Route 53. Funciona perfectamente con cualquier otro servidor de origen que no sea de AWS en el que se almacenen las versiones originales definitivas de sus archivos.

Amazon CloudFront requiere que todas las solicitudes realizadas a su API de control se autentiquen para que solo los usuarios autenticados puedan crear, modificar o eliminar sus propias distribuciones de Amazon CloudFront. Las solicitudes se firman con una firma HMAC-SHA1 calculada a partir de una solicitud y la clave privada del usuario. Además, a la API de control de Amazon CloudFront solo se puede obtener acceso a través de los puntos de enlace habilitados por SSL.

No se garantiza la durabilidad de los datos almacenados en las ubicaciones de borde de Amazon CloudFront. En algunas ocasiones, el servicio puede eliminar los objetos de las ubicaciones de borde si dichos objetos no se solicitan con frecuencia. La durabilidad la ofrece Amazon S3, que funciona como el servidor de origen de Amazon CloudFront que hospeda las copias originales y definitivas de los objetos que ofrece Amazon CloudFront.

Si quiere tener el control de quién puede descargar el contenido de Amazon CloudFront, puede activar la función de contenido privado del servicio. Esta característica tiene dos componentes: el primero controla la forma en que las ubicaciones de borde de Amazon CloudFront ofrecen el contenido a los visitantes de Internet. El segundo controla el modo en que las ubicaciones de borde de Amazon CloudFront obtienen acceso a los objetos de Amazon S3. CloudFront admite también la restricción geográfica, que restringe el acceso a su contenido en función de la ubicación geográfica de los visitantes.

Para controlar el acceso a las copias originales de los objetos de Amazon S3, Amazon CloudFront le permite crear una o varias “Origin Access Identities” y asociarlas con las distribuciones. Cuando se asocia una identidad de acceso de origen con una distribución de Amazon CloudFront, la distribución utiliza dicha identidad para recuperar los objetos de Amazon S3. Por tanto, puede utilizar la característica de ACL de Amazon S3, que limita el acceso a dicha identidad de acceso de origen a fin de que la copia original del objeto no pueda leerse de forma pública.

Para controlar quién puede descargar objetos desde las ubicaciones de borde de Amazon CloudFront, el servicio utiliza un sistema de verificación firmado mediante URL. Para utilizar este sistema, primero debe crear un par de claves pública y privada, y cargar la clave pública en la cuenta a través de la consola de administración de AWS. En segundo lugar, debe configurar la distribución de Amazon CloudFront para indicar qué cuentas autorizaría para firmar solicitudes (puede indicar hasta cinco cuentas de AWS en las que confíe para firmar las solicitudes). En tercer lugar, a medida que reciba solicitudes, podrá crear documentos sobre políticas en los que se indiquen bajo qué condiciones quiere que Amazon CloudFront muestre el contenido. Estos documentos sobre políticas pueden especificar el nombre del objeto solicitado, la fecha y la hora de la solicitud y la IP de origen (o el rango de CIDR) del cliente que realiza la solicitud. A continuación, calcula el valor hash SHA1 del documento de la política y lo firma con la clave privada. Finalmente, puede incluir el documento de política codificado y la firma como parámetros de cadena de consulta cuando haga referencia a sus objetos. Cuando Amazon CloudFront recibe una solicitud, descodificará la firma con la clave pública. Amazon CloudFront solo atenderá las solicitudes que tengan un documento de política válido y firmas coincidentes.

> **Nota:** el contenido privado es una característica opcional que debe estar habilitada cuando configure la distribución de CloudFront. El contenido entregado sin esta característica activada podrá leerlo cualquier persona.

Amazon CloudFront proporciona la opción de transferir contenido a través de una conexión cifrada (HTTPS). De forma predeterminada, CloudFront aceptará las solicitudes enviadas a través de los protocolos HTTP y HTTPS. Sin embargo, también puede configurar CloudFront para que requiera HTTPS para todas las solicitudes o para que redirija las solicitudes HTTP a HTTPS. Puede incluso configurar las distribuciones de CloudFront para que permitan HTTP para algunos objetos pero requieran HTTPS para otros.

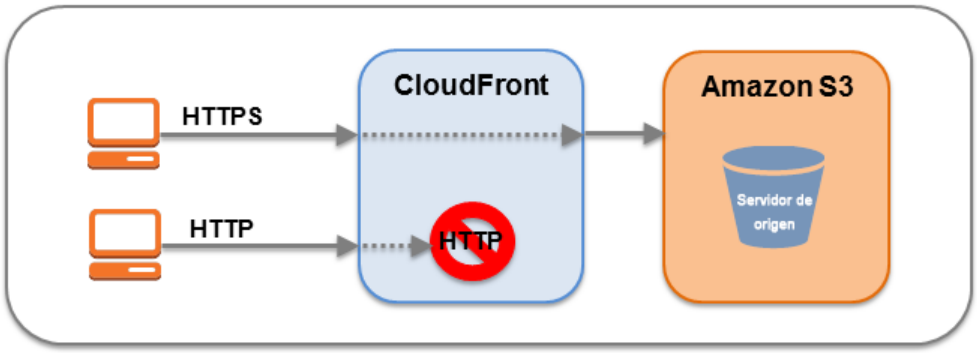


Figura 7: Transmisión cifrada de Amazon CloudFront

Puede configurar uno o varios orígenes de CloudFront de forma que requieran que CloudFront recupere los objetos del origen mediante el protocolo que el visitante ha usado para solicitar los objetos. Por ejemplo, cuando usa esta configuración de CloudFront y el visitante usa HTTPS para solicitar un objeto de CloudFront, CloudFront también usa HTTPS para reenviar la solicitud al origen.

Amazon CloudFront usa los protocolos SSLv3 o TLSv1 y un grupo de códigos cifrados que incluyen el protocolo Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) en las conexiones con los visitantes y el origen. El protocolo ECDHE permite que los clientes SSL/TLS ofrezcan Perfect Forward Secrecy, donde se utilizan claves de sesión que son efímeras y no se almacenan en ningún lugar. Con este método se impide la descodificación de los datos capturados por parte de terceros no autorizados, aunque la clave secreta de larga duración resulte expuesta a riesgos.

> **Nota:** si usa su propio servidor como origen y quiere usar HTTPS entre los visitantes y CloudFront y entre CloudFront y el origen, debe instalar un certificado SSL válido en el servidor HTTP que esté firmado por una entidad de certificación externa, como VeriSign o DigiCert.

De forma predeterminada, puede entregar el contenido a los usuarios a través de HTTPS mediante el uso del nombre de dominio de distribución de CloudFront en las URL, por ejemplo, https://dxxxxx.cloudfront.net/image.jpg. Si desea entregar el contenido a través de HTTPS a través de su propio nombre de dominio y su propio certificado SSL, puede usar SSL personalizado de SNI o SSL personalizado con direcciones IP dedicadas. Con SSL personalizado de

identificación de nombres de servidor (SNI), CloudFront utiliza la extensión de SNI del protocolo de TLS, compatible con la mayoría de los navegadores web modernos. Sin embargo, es posible que algunos usuarios no puedan obtener acceso al contenido, ya que algunos navegadores más antiguos no admiten SNI. (Para ver una lista de los navegadores compatibles, visite http://aws.amazon.com/cloudfront/faqs/). Con SSL personalizado con direcciones IP dedicadas, CloudFront asigna direcciones IP dedicadas a su certificado SSL en cada ubicación de borde de CloudFront para que CloudFront pueda asociar las solicitudes entrantes al certificado SSL adecuado.

Los logs de acceso de Amazon CloudFront contienen un conjunto completo de información acerca de las solicitudes de contenido, incluido el objeto solicitado, la fecha y la hora de la solicitud, la ubicación de borde que aloja la solicitud, la dirección IP del cliente, el referente y el agente del usuario. Para habilitar los logs de acceso, solo debe especificar el nombre del bucket de Amazon S3 para almacenar los logs cuando configure la distribución de Amazon CloudFront.

Seguridad de AWS Direct Connect

Con AWS Direct Connect, puede aprovisionar un enlace directo entre su red interna y una región de AWS mediante una conexión dedicada de alta velocidad. Esto puede ayudar a reducir los costos de red, a mejorar el desempeño o a proporcionar una experiencia en la red más coherente. Con esta conexión dedicada, puede crear interfaces virtuales directamente con la nube de AWS (por ejemplo, con Amazon EC2 y Amazon S3) y con Amazon VPC.

Con Direct Connect, elude los proveedores de Internet en su ruta de acceso de red. Puede obtener espacio de bastidor en la instalación que aloja la ubicación de AWS Direct Connect e implementar el equipo al lado. Una vez implementado, puede conectar el equipo a AWS Direct Connect mediante una conexión cruzada. Cada ubicación de AWS Direct Connect permite la conectividad con la región de AWS más próxima geográficamente, así como el acceso a otras regiones de EE. UU. Por ejemplo, puede aprovisionar una sola conexión a cualquier ubicación de AWS Direct Connect en EE. UU. y usarla para obtener acceso a los servicios públicos de AWS en todas las regiones de AWS y en AWS GovCloud (US).

Mediante el uso de conexiones VLAN 802.1q estándares del sector, la conexión dedicada se puede particionar en varias interfaces virtuales. Esto le permite utilizar la misma conexión para obtener acceso a recursos públicos como, por ejemplo, objetos almacenados en Amazon S3 utilizando un espacio de direcciones IP públicas y a recursos privados como, por ejemplo, instancias de Amazon EC2 que se ejecuten dentro de una VPC de Amazon utilizando un espacio de IP privado al tiempo que se mantiene la separación de red entre los entornos públicos y privados.

Amazon Direct Connect requiere el uso del protocolo de puerta de enlace fronteriza (BGP) con un número de sistema autónomo (ASN). Para crear una interfaz virtual, se usa una clave criptográfica MD5 para la autorización de los mensajes. MD5 crea un algoritmo hash con clave usando su clave secreta. Puede hacer que AWS genere automáticamente una clave MD5 de BGP o puede proporcionar la suya propia.

Servicios de almacenamiento

Amazon Web Services ofrece un almacenamiento de datos de bajo costo con alta durabilidad y disponibilidad. AWS ofrece opciones de almacenamiento para backup, archivado, recuperación de desastres, además de almacenamiento en bloque y de objetos.

Seguridad de Amazon Simple Storage Service (Amazon S3)

Amazon Simple Storage Service (S3) le permite cargar y recuperar cualquier cantidad de datos en cualquier momento determinado, desde cualquier parte de la web. Amazon S3 almacena datos como objetos dentro de buckets. Un objeto puede ser cualquier tipo de archivo: un archivo de texto, una foto, un vídeo, etc. Cuando añade un archivo a Amazon S3, tiene la opción de incluir los metadatos con el archivo y de configurar los permisos para controlar el acceso al archivo. Para cada bucket, puede controlar el acceso al bucket (quién puede crear, eliminar y mostrar los objetos del bucket), consultar logs de acceso del bucket y sus objetos, y elegir la región geográfica en la que Amazon S3 almacenará el bucket y su contenido.

Acceso a los datos

El acceso a los datos almacenados en Amazon S3 está restringido de forma predeterminada; solo los propietarios de los buckets y de los objetos tienen acceso a los recursos de Amazon S3 que crean (tenga en cuenta que un propietario de un bucket u objeto es el propietario de la cuenta de AWS y no el usuario que ha creado el bucket u objeto). Hay varias formas de controlar el acceso a los buckets y objetos:

- **Políticas de Identity and Access Management (IAM).** AWS IAM permite a las organizaciones con muchos empleados crear y administrar varios usuarios bajo una única cuenta de AWS. Las políticas de IAM se asocian a los usuarios, lo que permite el control centralizado de los permisos de los usuarios de su cuenta de AWS para obtener acceso a los buckets u objetos. Con las políticas de IAM, solo puede conceder permiso a los usuarios de su propia cuenta de AWS para obtener acceso a sus recursos de Amazon S3.
- **Listas de control de acceso (ACL).** En Amazon S3, puede usar listas de control de acceso para conceder acceso de lectura o escritura en los buckets u objetos a grupos de usuarios. Con las listas de control de acceso, solo puede conceder acceso a otras cuentas de AWS (no a usuarios específicos) a sus recursos de Amazon S3.
- **Políticas de buckets.** Las políticas de buckets de Amazon S3 se pueden utilizar para añadir o denegar permisos respecto a algunos o todos los objetos de un bucket. Las políticas se pueden asociar a usuarios, grupos o buckets de Amazon S3, lo que permite la administración centralizada de los permisos. Con las políticas de buckets, puede conceder a los usuarios de su cuenta de AWS u otras cuentas de AWS acceso a sus recursos de Amazon S3.

Tipo de control de acceso	¿Control de nivel de cuenta de AWS?	¿Control de nivel de usuario?
Políticas de IAM	No	Sí
ACL	Sí	No
Políticas de buckets	Sí	Sí

Puede restringir aún más el acceso a recursos específicos en función de determinadas condiciones. Por ejemplo, puede restringir el acceso en función de la hora de solicitud (condición de fecha), de si la solicitud se envió mediante SSL (condiciones booleanas), de la dirección IP del solicitante (condición de dirección IP) o de la aplicación cliente del solicitante (condiciones de cadena). Para identificar estas condiciones, se usan claves de política. Para obtener más información sobre las claves de política específicas de acciones disponibles en Amazon S3, consulte la guía para desarrolladores de Amazon Simple Storage Service.

Amazon S3 ofrece también a los desarrolladores la opción de usar la autenticación por query string, que les permite compartir objetos de Amazon S3 a través de direcciones URL válidas durante un período de tiempo predefinido. La autenticación por query string (cadena de consulta) es útil para ofrecer acceso HTTP o al navegador a los recursos que requerirían normalmente autenticación. La firma de la cadena de consulta protege la solicitud.

Transferencia de datos

Para disfrutar de la máxima seguridad, puede cargar y descargar de forma segura los datos de Amazon S3 a través de puntos de enlace cifrados mediante el protocolo SSL. Los puntos de enlace cifrados son accesibles desde Internet o desde Amazon EC2 para poder transferir los datos de manera segura dentro de AWS, así como desde y hacia todos los orígenes de fuera de AWS.

Almacenamiento de datos

Amazon S3 ofrece varias opciones para el cifrado de datos en reposo. Los clientes que prefieran administrar sus propias claves de cifrado pueden utilizar una biblioteca de cifrado del cliente como Amazon S3 Encryption Client para cifrar los datos antes de cargarlos en Amazon S3. También puede utilizar Amazon Server Side Encryption (SSE) de Amazon S3 si quiere que Amazon S3 se encargue del proceso de cifrado por usted. Los datos se cifran con una clave generada por AWS o con una clave que usted suministre, en función de sus requisitos. Gracias a SSE de Amazon S3, puede cifrar los datos al cargarlos. Solo tiene que añadir un encabezado de solicitud opcional al escribir el objeto. El descifrado se realiza automáticamente cuando se recuperan los datos.

> **Nota:** los metadatos que puede incluir con el objeto no se cifran. Por tanto, AWS recomienda a los clientes que no coloquen información confidencial en los metadatos de Amazon S3.

Amazon S3 SSE utiliza uno de los cifrados de bloques más seguros disponibles: Advanced Encryption Standard de 256 bits (AES-256). Con Amazon S3 SSE, cada objeto protegido está cifrado con una clave exclusiva. La propia clave del objeto está cifrada con una clave maestra que cambia periódicamente. Amazon S3 SSE proporciona seguridad adicional almacenando los datos cifrados y las claves de cifrado en hosts diferentes. Amazon S3 SSE también permite forzar requisitos de cifrado. Por ejemplo, puede crear y aplicar políticas de buckets que exijan que solo los datos cifrados puedan cargarse en los buckets.

Para el almacenamiento a largo plazo, puede archivar automáticamente el contenido de los buckets de Amazon S3 en el servicio de archivado de AWS llamado Glacier. Puede hacer que los datos se transfieran a intervalos específicos a Glacier creando reglas de ciclo de vida en Amazon S3 qué describan qué objetos deben archivarse en Glacier y cuándo. Como parte de su estrategia de administración de datos, también puede especificar cuánto tiempo debe esperar Amazon S3 una vez que los objetos se colocan en Amazon S3 para eliminarlos.

Cuando se elimina un objeto de Amazon S3, se inicia de inmediato la eliminación del mapeo del nombre público al objeto, tarea que suele procesarse en todo el sistema distribuido en cuestión de segundos. Una vez eliminado el mapeo, no se puede obtener acceso remoto al objeto eliminado. Posteriormente, el sistema reclama el área de almacenamiento subyacente para su uso.

Durabilidad y fiabilidad de los datos

Amazon S3 está diseñado para ofrecer una durabilidad del 99,999999999% y una disponibilidad de los objetos del 99,99% durante un año concreto. Los objetos se almacenan de forma redundante en varios dispositivos de diversas instalaciones dentro de una región de Amazon S3. Para contribuir a ofrecer durabilidad, las operaciones PUT y COPY de Amazon S3 almacenan de forma sincrónica los datos de los clientes en varias instalaciones antes de devolver SUCCESS. Una vez almacenados, Amazon S3 ayuda a mantener la durabilidad de los objetos detectando y reparando rápidamente cualquier pérdida de redundancia. Del mismo modo, Amazon S3 comprueba de forma regular la integridad de los datos almacenados mediante sumas de comprobación. Si se

detecta algún tipo de daño en los objetos, se reparan utilizando los datos redundantes. Además, Amazon S3 calcula las sumas de comprobación de todo el tráfico de la red para detectar paquetes de datos con daños durante el almacenamiento o la recuperación de los datos.

Amazon S3 proporciona protección adicional a través del control de versiones. Puede utilizar el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en un bucket de Amazon S3. Gracias al control de versiones, puede recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación. De forma predeterminada, las solicitudes recuperarán la versión escrita más recientemente. Las versiones más antiguas de un objeto podrán recuperarse especificando una versión en la solicitud. Puede proteger aún más las versiones mediante la característica MFA Delete del control de versiones de Amazon S3. Una vez activada para un bucket de Amazon S3, cada solicitud de eliminación de versiones debe incluir un código de seis dígitos y un número de serie del dispositivo de autenticación multifactor.

Logs de acceso

Se puede configurar un bucket de Amazon S3 para registrar el acceso al bucket y a los objetos incluidos en él. El log de acceso contiene los detalles sobre cada solicitud de acceso, entre otros, el tipo de solicitud, el recurso solicitado, la IP del solicitante y la hora y la fecha de la solicitud. Cuando el registro está activado para un bucket, los registros logs se añaden de forma periódica a los archivos logs y se entregan al bucket específico de Amazon S3.

Cross-Origin Resource Sharing (CORS, Uso compartido de recursos entre orígenes)

Los clientes de AWS que usen Amazon S3 para alojar páginas web estáticas o almacenar objetos usados por otras páginas web pueden cargar contenido de forma segura configurando un bucket de Amazon S3 para habilitar explícitamente los recursos entre orígenes. Los navegadores modernos usan la política Mismo origen para impedir que JavaScript o HTML5 realicen solicitudes para cargar contenido desde otro sitio o domino como un medio de garantizar que el contenido malintencionado no se cargue desde un origen con peor reputación (por ejemplo, durante los ataques de scripting entre sitios). Cuando la política Cross-Origin Resource Sharing (CORS) está habilitada, las páginas web, hojas de estilo y aplicaciones HTML5 externas pueden hacer referencia de manera segura a elementos como fuentes e imágenes web almacenados en un bucket de Amazon S3.

Seguridad de AWS Glacier

Al igual que Amazon S3, el servicio Amazon Glacier proporciona almacenamiento seguro y duradero de bajo costo. Pero mientras que Amazon S3 está diseñado para una recuperación rápida, Glacier debe usarse como un servicio de archivado de datos a los que no se obtenga acceso a menudo y para los que sean apropiados tiempos de recuperación de varias horas.

Amazon Glacier almacena los archivos como archivos de almacenamiento dentro de almacenes. Los archivos de almacenamiento pueden ser datos como una foto, vídeo o documento, o pueden contener uno o varios archivos. Puede almacenar un número ilimitado de archivos de almacenamiento en un solo almacén y puede crear hasta 1 000 almacenes por región. Cada archivo de almacenamiento puede contener hasta 40 TB de datos.

Carga de datos

Para transferir datos en almacenes en Amazon Glacier, puede cargar un archivo de almacenamiento en una sola operación de carga o en operaciones multiparte. Si utiliza una sola operación de carga, puede cargar archivos de almacenamiento de hasta 4 GB. Sin embargo, los clientes consiguen mejores resultados utilizando la API de carga multiparte para cargar archivos de almacenamiento de más de 100 MB. Esta API permite cargar archivos de almacenamiento grandes, de hasta aproximadamente 40 000 GB. La llamada a la API de carga multiparte tiene como objetivo mejorar la experiencia de carga para archivos de almacenamiento grandes; permite que las partes se carguen por separado, en cualquier orden y en paralelo. Si una carga multiparte da un error, solo necesita cargar de nuevo la parte que ha dado el error y no todo el archivo de almacenamiento.

Cuando cargue datos en Glacier, deberá calcular y suministrar un algoritmo hash en árbol. Glacier comprueba el algoritmo hash con los datos para ayudar a garantizar que no se haya alterado mientras se encontraba en tránsito. Para generar un algoritmo hash en árbol, se calcula un valor hash para cada segmento de datos de varios megabytes, y después se combinan los distintos valores hash para representar los segmentos adyacentes de datos cada vez mayores.

Como alternativa al uso de la característica de carga multiparte, los clientes que necesiten realizar cargas muy grandes en Amazon Glacier pueden considerar la posibilidad de usar el servicio AWS Import/Export en su lugar para transferir los datos. AWS Import/Export facilita el movimiento de grandes volúmenes de

datos en AWS utilizando dispositivos de almacenamiento portátiles para el transporte. AWS transfiere los datos directamente de los dispositivos de almacenamiento utilizando la red interna de alta velocidad de Amazon, sin tener que pasar por Internet.

También puede configurar Amazon S3 para que transfiera los datos a Glacier a intervalos específicos. Puede crear reglas de ciclo de vida en Amazon S3 qué describan qué objetos deben archivarse en Glacier y cuándo. También puede especificar cuánto tiempo debe esperar Amazon S3 una vez que los objetos se colocan en Amazon S3 para eliminarlos.

Para disponer de mayor seguridad, puede cargar y descargar de forma segura los datos en Amazon Glacier a través de puntos de enlace cifrados mediante el protocolo SSL. Los puntos de enlace cifrados son accesibles desde Internet o desde Amazon EC2 para poder transferir los datos de manera segura dentro de AWS, así como desde y hacia todos los orígenes de fuera de AWS.

Recuperación de datos

Para recuperar datos de Amazon Glacier, es necesario iniciar un trabajo de recuperación, que suele tardar en completarse entre tres y cinco horas. A continuación, puede obtener acceso a los datos a través de solicitudes GET HTTP. Los datos estarán disponibles durante 24 horas.

Puede recuperar un archivo de almacenamiento completo o varios archivos incluidos en un archivo de almacenamiento. Si solo quiere recuperar parte de un archivo de almacenamiento, puede usar una solicitud de recuperación para especificar el intervalo del archivo de almacenamiento que contiene los archivos que le interesan, o puede iniciar varias solicitudes de recuperación, cada una con un intervalo de uno o varios archivos. También puede limitar el número de elementos del inventario del almacén recuperados filtrando por un intervalo de fechas de creación del archivo de almacenamiento o definiendo un límite máximo de elementos. Independientemente del método que elija, cuando recupere parte del archivo de almacenamiento, puede usar la suma de comprobación proporcionada para ayudar a garantizar la integridad de los archivos, siempre y cuando el intervalo que se va recuperar coincida con el algoritmo hash en árbol de todo el archivo de almacenamiento.

Almacenamiento de datos

Amazon Glacier cifra automáticamente los datos con AES-256 y los almacena a largo plazo en un formato inmutable. Amazon Glacier está diseñado para ofrecer una durabilidad anual media de archivos del 99,999999999%. Almacena cada archivo de almacenamiento en varias instalaciones y varios dispositivos. A diferencia de los sistemas tradicionales, que requieren laboriosas verificaciones de datos y reparaciones manuales, Glacier realiza comprobaciones sistemáticas de la integridad de los datos y está diseñado para recuperarse automáticamente.

Acceso a los datos

A los datos de Amazon Glacier solo puede obtener acceso su cuenta. Para controlar el acceso a los datos en Amazon Glacier, puede usar AWS IAM para especificar qué usuarios de su cuenta tienen permisos para realizar operaciones en un almacén determinado.

Seguridad de AWS Storage Gateway

El servicio AWS Storage Gateway conecta un dispositivo de software presente en sus instalaciones con almacenamiento basado en la nube para ofrecer una integración completa y segura entre su entorno de TI y la infraestructura de almacenamiento de AWS. El servicio le permite cargar de manera segura datos en el servicio de almacenamiento escalable, fiable y seguro de Amazon S3 de AWS, que le ofrece una solución económica de backup y recuperación de desastres.

AWS Storage Gateway realiza de forma transparente backups externos de los datos en Amazon S3 en forma de snapshots de Amazon EBS. Amazon S3 almacena estas snapshots de forma redundante en múltiples dispositivos en diversas instalaciones, detectando y reparando cualquier pérdida de redundancia. La snapshot de Amazon EBS proporciona un backup de un momento en el tiempo que puede restaurarse en sus instalaciones o emplearse para crear instancias de nuevos volúmenes de Amazon EBS. Los datos se almacenan en una única región que usted especifica.

AWS Storage Gateway ofrece tres opciones:

- **Volúmenes almacenados en la gateway (donde la nube es el almacenamiento de respaldo).** Con esta opción, los datos de los volúmenes se almacenan localmente y después se insertan en Amazon

S3, donde se almacenan de forma redundante y cifrada, y están disponibles en forma de snapshots de Elastic Block Storage (EBS). Cuando se usa este modelo, el almacenamiento local es el principal, lo que proporciona acceso de baja latencia a todo el conjunto de datos, y el almacenamiento en la nube es el almacenamiento de respaldo.

- **Volúmenes almacenados en caché en la gateway (donde la nube es el almacenamiento principal).** Con esta opción, los datos de los volúmenes se almacenan cifrados en Amazon S3 y están visibles en la red de la empresa a través de una interfaz iSCSI. Los datos a los que se ha obtenido acceso recientemente se almacenan en la memoria caché local para un acceso local de baja latencia. Cuando se usa este modelo, el almacenamiento en la nube es el principal, pero obtiene acceso de baja latencia a su grupo de trabajo activo en volúmenes almacenados en la caché local.
- **Biblioteca de cintas virtuales de gateway (Gateway-VTL).** Con esta opción, puede configurar una VTL de gateway con hasta 10 unidades de cinta virtuales por gateway, 1 cargador de medios y hasta 1 500 cartuchos de cinta virtuales. Cada unidad de cinta virtual responde al conjunto de comandos de SCSI, por lo que sus aplicaciones de backup locales (de disco a cinta o de disco a disco y a cinta) funcionarán sin modificaciones.

Cualquiera que sea la opción que elija, los datos se transfieren de forma asíncrona desde el hardware de almacenamiento local a AWS a través de SSL. Los datos se almacenan cifrados en Amazon S3 mediante el estándar de cifrado avanzado (AES) 256, un estándar de cifrado de clave simétrica que utiliza claves de cifrado de 256 bits. AWS Storage Gateway solo carga los datos que se hayan modificado para minimizar la cantidad de datos enviados por Internet.

AWS Storage Gateway se ejecuta como una máquina virtual (VM) que se implementa en un host en su centro de datos que ejecuta VMware ESXi Hypervisor v 4.1 o v 5 o Microsoft Hyper-V (el software de VMware se descarga durante el proceso de instalación). También puede ejecutarlo desde dentro de EC2 mediante una AMI de gateway. Durante el proceso de instalación y configuración, puede crear hasta 12 volúmenes almacenados, 20 volúmenes en caché o 1 500 cartuchos de cinta virtuales por gateway. Una vez instalada, cada gateway descargará, instalará e implementará automáticamente actualizaciones y parches. Esta actividad tiene lugar durante un período de mantenimiento que puede definir para cada gateway.

El protocolo iSCSI admite la autenticación entre los destinos y los iniciadores a través de CHAP (Challenge-Handshake Authentication Protocol, Protocolo de autenticación por desafío mutuo). El protocolo CHAP ofrece protección contra ataques de tipo man-in-the-middle y de reproducción; para ello, verifica periódicamente la identidad de un iniciador iSCSI tal y como se ha autenticado para obtener acceso a un destino de volumen de almacenamiento. CHAP debe configurarse tanto en la consola de AWS Storage Gateway como en el software del iniciador iSCSI que usa para conectarse al destino.

Tras implementar la máquina virtual de AWS Storage Gateway, debe activar la gateway desde la consola de AWS Storage Gateway. El proceso de activación asocia la gateway con su cuenta de AWS. En cuanto se establece esta conexión, puede administrar casi todos los aspectos de la gateway desde la consola. En el proceso de activación, especifica la dirección IP de la gateway, asigna un nombre a su gateway, identifica la región de AWS en la que desea que se almacenen los backups de las snapshots y especifica la zona horaria de la gateway.

Seguridad de AWS Import/Export

AWS Import/Export es un método sencillo y seguro de transferir físicamente grandes cantidades de datos a Amazon S3, EBS o al almacenamiento de Glacier. Este servicio lo suelen usar los clientes que tienen más de 100 GB de datos o velocidades de conexión demasiado lentas para transferir los datos por Internet. Con AWS Import/Export, prepara un dispositivo de almacenamiento portátil que envía a una instalación segura de AWS. AWS transfiere los datos directamente del dispositivo de almacenamiento utilizando la red interna de alta velocidad de Amazon, sin tener que pasar por Internet. De igual forma, los datos también se pueden exportar de AWS a un dispositivo de almacenamiento portátil.

Al igual que los demás servicios de AWS, el servicio AWS Import/Export requiere que identifique y autentique de forma segura el dispositivo de almacenamiento. En este caso, enviará una solicitud de trabajo a AWS que incluya su bucket de Amazon S3, la región de Amazon EBS, el ID de clave de acceso de AWS y la dirección de envío de devolución. A continuación, recibirá un identificador exclusivo del trabajo, una firma digital para autenticar su dispositivo y una dirección de AWS a la que enviar su dispositivo de almacenamiento. Para Amazon S3, tendrá que colocar el archivo de firma en el directorio raíz del dispositivo. Para Amazon EBS, tendrá que pegar con cinta adhesiva el código de barras de la firma en el exterior del dispositivo. El archivo de firma solo se usa para la autenticación y no se carga en Amazon S3 ni en EBS.

Para las transferencias a Amazon S3, especificará los buckets específicos en los que deben cargarse los datos y se asegurará de que la cuenta desde la que realiza la carga tenga permiso de escritura en los buckets. Deberá especificar también la lista de control de acceso que debe aplicarse a cada objeto cargado en Amazon S3.

Para las transferencias a EBS, especificará la región de destino de la operación de importación de EBS. Si la capacidad del dispositivo de almacenamiento es menor o igual al tamaño de volumen máximo de 1 TB, su contenido se cargará directamente en una snapshot de Amazon EBS. Si la capacidad del dispositivo de almacenamiento es mayor de 1 TB, se guardará una imagen del dispositivo en el bucket de registro de S3 que especifique. A continuación, podrá crear un RAID de volúmenes Amazon EBS utilizando software como Logical Volume Manager y copiar la imagen de S3 en este nuevo volumen.

Para disfrutar de mayor protección, puede cifrar los datos del dispositivo antes de enviarlo a AWS. Para los datos de Amazon S3, puede usar un dispositivo de código PIN con cifrado por hardware o software TrueCrypt para cifrar los datos antes de enviarlos a AWS. Para los datos de EBS y Glacier, puede usar el método de cifrado que prefiera, incluido un dispositivo de código PIN. AWS descifrará los datos de Amazon S3 antes de importarlos usando el código PIN o la contraseña de TrueCrypt que proporciona en el manifiesto de importación. AWS usa su PIN para obtener acceso al dispositivo de código PIN, pero no descifra los datos cifrados por software para la importación a Amazon EBS o Amazon Glacier. En la tabla siguiente se indican las opciones de cifrado de cada tipo de trabajo de importación/exportación.

Importar a Amazon S3		
Origen	Destino	Resultado
• Archivos en el sistema de archivos de un dispositivo • Cifrar los datos mediante un dispositivo de código PIN o TrueCrypt antes de enviar el dispositivo	• Objetos en un bucket de Amazon S3 existente • AWS descifra los datos antes de permitir la importación	• Un objeto para cada archivo • AWS borra el dispositivo después de cada trabajo de importación antes de su envío

Exportar desde Amazon S3		
Origen	Destino	Resultado
• Objetos en uno o varios buckets de Amazon S3 • Proporcionar un código PIN o 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 cifrado en su dispositivo	• Un archivo para cada objeto • AWS cifra los datos antes del envío • Usar un dispositivo de código PIN o TrueCrypt para descifrar los archivos
Importar a Amazon Glacier		
Origen	Destino	Resultado
• Todo el dispositivo • Cifrar los datos mediante el método de cifrado que elija antes del envío	• Un archivo de almacenamiento en un almacén de Amazon Glacier existente • AWS no cifra el dispositivo	• Imagen del dispositivo almacenada como un solo archivo de almacenamiento • AWS borra el dispositivo después de cada trabajo de importación antes de su envío
Importar a Amazon EBS (capacidad del dispositivo < 1 TB)		
Origen	Destino	Resultado
• Todo el dispositivo • Cifrar los datos mediante el método de cifrado que elija antes del envío	• Una snapshot de Amazon EBS • AWS no cifra el dispositivo	• La imagen del dispositivo se almacena como una sola snapshot • Si el dispositivo estaba cifrado, la imagen se cifra • AWS borra el dispositivo después de cada trabajo de importación antes de su envío
Importar a Amazon EBS (capacidad del dispositivo > 1 TB)		
Origen	Destino	Resultado
• Todo el dispositivo • Cifrar los datos mediante el método de cifrado que elija antes del envío	• Varios objetos en un bucket de Amazon S3 existente • AWS no cifra el dispositivo	• La imagen del dispositivo se fragmenta en series de snapshots de 1 TB almacenadas como objetos en el bucket de Amazon S3 especificado en el archivo de manifiesto • Si el dispositivo estaba cifrado, la imagen se cifra • AWS borra el dispositivo después de cada trabajo de importación antes de su envío

Una vez completada la importación, AWS Import/Export borrará el contenido del dispositivo de almacenamiento para proteger los datos durante su devolución. AWS sobrescribe todos los bloques grabables del dispositivo de almacenamiento con ceros. Tendrá que crear nuevas particiones y formatear el dispositivo tras el borrado. Si AWS no puede borrar los datos del dispositivo, se programará su destrucción, y nuestro equipo de soporte técnico se pondrá en contacto con usted utilizando la dirección de correo electrónico especificada en el archivo de manifiesto que envió con el dispositivo.

Cuando se realiza un envío internacional del dispositivo, deben incluirse las opciones de pago de aranceles y alguna otra información necesaria en el archivo de manifiesto enviado a AWS. AWS Import/Export utiliza estos valores para validar el envío entrante y preparar la documentación para los aranceles de salida. Dos de estas opciones son si los datos del dispositivo están o no están cifrados y la clasificación del software de cifrado. Cuando se envían datos cifrados a o desde Estados Unidos, el software de cifrado debe tener la clasificación 5D992 de acuerdo con la Normativa de la administración estadounidense en materia de exportación.

Seguridad de Amazon Elastic File System

Amazon Elastic File System (Amazon EFS) proporciona un almacenamiento de archivos sencillo y escalable para su uso con instancias de Amazon EC2 en la nube de AWS. Con Amazon EFS, la capacidad de almacenamiento es elástica: aumenta y disminuye automáticamente a medida que se añaden o eliminan archivos. Los sistemas de archivos de Amazon EFS se distribuyen por un número sin restricción de servidores de almacenamiento, por lo que pueden crecer de forma elástica hasta la escala de petabytes, además de permitir un acceso en paralelo masivo a sus datos desde instancias de Amazon EC2.

Acceso a los datos

Con Amazon EFS, puede crear un sistema de archivos, montar el sistema de archivos en una instancia Amazon EC2 y después leer y escribir datos en su sistema de archivos. Puede montar un sistema de archivos de Amazon EFS en instancias EC2 de su VPC, a través del protocolo Network File System, versiones 4.0 y 4.1 (NFSv4).

Para obtener acceso al sistema de archivos de Amazon EFS de una VPC, crea uno o varios destinos de montaje en la VPC. Un destino de montaje proporciona una dirección IP para un punto de enlace NFSv4. A continuación, puede montar un sistema de archivos de Amazon EFS en este punto de enlace usando su nombre DNS, que se resolverá en 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 de su VPC, debe crear un destino de montaje en una de las subredes; todas las instancias EC2 de esa zona de disponibilidad compartirán ese destino de montaje. También puede montar un sistema de archivos de EFS en un host de un centro de datos local usando AWS Direct Connect.

Cuando use Amazon EFS, especificará los grupos de seguridad de Amazon EC2 para sus instancias EC2 y los grupos de seguridad de los destinos de montaje de EFS asociados al sistema de archivos. Los grupos de seguridad actúan como firewalls y las reglas que usted añade definen el flujo de tráfico. Puede autorizar el acceso entrante y saliente a su sistema de archivos de EFS añadiendo reglas que permitan a la instancia EC2 conectarse al sistema de archivos de Amazon EFS a través del destino de montaje mediante el puerto NFS.

Después de montar el sistema de archivos a través del destino de montaje, lo podrá usar como cualquier otro sistema de archivos compatible con POSIX. Los archivos y directorios del sistema de archivos de EFS admiten los permisos de lectura, escritura y ejecución estándar de tipo Unix basados en el ID de usuario y de grupo certificado al montar el cliente de NFSv4.1. Para obtener información sobre los permisos de nivel de NFS y otras consideraciones, consulte Network File System (NFS)–Level Users, Groups and Permissions en la documentación del usuario.

Todos los sistemas de archivos de Amazon EFS son propiedad de una cuenta de AWS. Puede usar políticas de IAM para conceder permisos a otros usuarios para que puedan realizar operaciones administrativas en sus sistemas de archivos, incluida la eliminación de un sistema de archivos o la modificación de los grupos de seguridad de un destino de montaje. Para obtener más información sobre los permisos de EFS, consulte Overview of Managing Access Permissions to Your Amazon EFS Resources.

Durabilidad y fiabilidad de los datos

Amazon EFS está diseñado para ofrecer alta disponibilidad y larga duración. Todos los datos y metadatos se almacenan en varias zonas de disponibilidad, y todos los componentes del servicio se han diseñado para proporcionar una alta disponibilidad. EFS ofrece un gran nivel de coherencia al replicar sincrónicamente los datos de las zonas de disponibilidad con semántica de lectura tras escritura para la mayoría de las operaciones con los archivos. Amazon EFS incorpora sumas de comprobación para todos los metadatos y datos en todo el servicio. Mediante un proceso de comprobación del sistema de archivos (FSCK), EFS valida continuamente la integridad de los metadatos y los datos del sistema de archivos.

Saneamiento de los datos

Amazon EFS se ha diseñado para que cuando elimine datos de un sistema de archivos, esos datos no se vuelvan a servir nunca de nuevo. Si sus procedimientos requieren que todos los datos se borren con un método específico, como los que se detallan en DoD 5220.22-M ("Manual de operaciones del programa de seguridad industrial nacional ") o NIST 800-88 ("Directrices para el saneamiento de soportes"), le recomendamos que realice un procedimiento de borrado especializado antes de eliminar el sistema de archivos.

Servicios de bases de datos

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

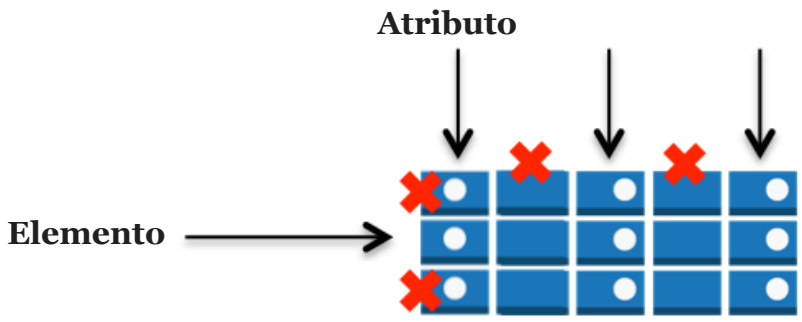
Seguridad de Amazon DynamoDB

Amazon DynamoDB es un servicio de base de datos NoSQL administrado que ofrece un desempeño rápido y previsible, así como una perfecta escalabilidad. Amazon DynamoDB le permite trasladar a AWS las cargas administrativas que supone tener que utilizar y escalar bases de datos distribuidas, para que no tenga que preocuparse del aprovisionamiento, la instalación y la configuración del hardware, ni tampoco de las tareas de replicación, revisión del software o escalado de clústeres.

Puede crear una tabla de base de datos capaz de almacenar y recuperar cualquier cantidad de datos, así como de atender cualquier nivel de tráfico de solicitudes. DynamoDB distribuye automáticamente los datos y el tráfico de la tabla entre un número de servidores adecuado para administrar la capacidad de solicitudes que usted especifique y la cantidad de datos almacenados, manteniendo al mismo tiempo un desempeño uniforme y rápido. Todos los elementos de datos se almacenan en unidades de estado sólido (SSD) y se replican automáticamente en varias zonas de disponibilidad de una región a fin de ofrecer las prestaciones integradas de alta disponibilidad y durabilidad de los datos.

Puede configurar backups automáticos mediante una plantilla especial de AWS Data Pipeline creada simplemente para copiar tablas de DynamoDB. Puede elegir entre backups totales o incrementales en una tabla en la misma región o en una diferente. Puede usar la copia para la recuperación de desastres (DR) en caso de que un error en el código dañe la tabla original, o para federar los datos de DynamoDB entre regiones con el fin de admitir una aplicación en varias regiones.

Para controlar quién puede usar los recursos de DynamoDB y la API, configura permisos en AWS IAM. Además de controlar el acceso en el nivel de recursos con IAM, también puede controlar el acceso en el nivel de base de datos: puede crear permisos de nivel de base de datos que permitan o denieguen el acceso a elementos (filas) y atributos (columnas) en función de las necesidades de su aplicación. Estos permisos de nivel de base de datos se denominan "controles precisos de acceso" y se crean mediante una política de IAM que especifica en qué circunstancias un usuario o aplicación puede tener acceso a una tabla de DynamoDB. La política de IAM puede restringir el acceso a elementos individuales de una tabla, a los atributos de estos elementos o a ambas cosas al mismo tiempo.



Si lo desea, puede usar la federación de identidad web para controlar el acceso de los usuarios de la aplicación que están autenticados mediante el inicio de sesión en Amazon, Facebook o Google. La federación de identidad web evita tener que crear usuarios de IAM individuales; en su lugar, los usuarios pueden iniciar sesión en un proveedor de identidad y obtener credenciales de seguridad temporales de AWS Security Token Service (AWS STS). AWS STS devuelve las credenciales temporales de AWS a la aplicación y permite a la aplicación obtener acceso a la tabla específica de DynamoDB.

Además de exigir permisos de base de datos y usuario, todas las solicitudes que se realizan al servicio DynamoDB deben contener una firma HMAC-SHA256 válida o, de lo contrario, se rechaza la solicitud. Los SDK de AWS firman automáticamente las solicitudes, pero, si desea escribir sus propias solicitudes HTTP POST, debe facilitar 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. Use las credenciales de seguridad temporales para firmar las solicitudes a Amazon DynamoDB.

Amazon DynamoDB está disponible a través de puntos de enlace cifrados por TSL/SSL.

Seguridad de Amazon Relational Database Service (Amazon RDS)

Amazon RDS le permite crear rápidamente una instancia de base de datos relacional y escalar de forma flexible los recursos informáticos asociados y la capacidad de almacenamiento para satisfacer la demanda de la aplicación. Amazon RDS administra la instancia de base de datos en su nombre mediante la realización de backups, la administración de conmutaciones por error y el mantenimiento del software de base de datos. Actualmente, Amazon RDS está disponible para los motores de base de datos de MySQL, Oracle, Microsoft SQL Server y PostgreSQL.

Amazon RDS cuenta con diversas características que mejoran la fiabilidad de las bases de datos de producción de vital importancia, entre las que se incluyen grupos de seguridad de base de datos, permisos, conexiones SSL, backups automatizados, snapshots de base de datos e implementaciones en zonas de disponibilidad múltiples (Multi-AZ). También se pueden implementar instancias de base de datos en una VPC de Amazon para lograr un aislamiento de red adicional.

Control de acceso

Cuando cree por primera vez una instancia de base de datos en Amazon RDS, creará una cuenta de usuario maestra, que se utiliza únicamente dentro del 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 puede utilizar para conectarse a su instancia de base de datos con todos los privilegios de la base de datos. Al crear cada instancia de base de datos, puede especificar el nombre de usuario maestro y la contraseña que desea asociarles. Cuando haya creado su instancia de base de datos, podrá conectarse a la base de datos utilizando las credenciales de usuario maestro. Posteriormente, puede crear cuentas de usuario adicionales para restringir quién puede obtener acceso a su instancia de base de datos.

Puede controlar la instancia de base de datos de Amazon RDS a través de grupos de seguridad de base de datos, que son similares a los grupos de seguridad de Amazon EC2, pero no son intercambiables. Un grupo de seguridad de base de datos realiza las mismas funciones que un firewall que controla el acceso de red a su instancia de base de datos. El valor predeterminado de los grupos de seguridad de base de datos es un modo de acceso “denegar todo”, por lo que los clientes deben autorizar específicamente el acceso a la red. Hay dos formas de hacerlo: autorizar un intervalo de direcciones IP de red o autorizar un grupo de seguridad existente de Amazon EC2. Los grupos de seguridad de base de datos solo permiten obtener acceso al puerto del servidor de la base de datos (todos los demás están bloqueados) y se pueden actualizar sin reiniciar la instancia de base de datos de Amazon RDS, lo que permite al cliente ejercer un control directo del acceso a la base de datos.

Con AWS IAM, puede controlar aún más el acceso a sus instancias de base de datos de RDS. AWS IAM le permite controlar qué operaciones de RDS puede llamar cada uno de los usuarios de AWS IAM con permisos para ello.

Aislamiento de red

Si desea mayor control del acceso de red, puede ejecutar las instancias de base de datos en una VPC de Amazon. Amazon VPC le permite aislar sus instancias de base de datos especificando el intervalo de direcciones IP que desea utilizar y conectarse a la infraestructura de TI existente a través de una VPN IPsec cifrada estándar del sector. De esta forma, podrá tener una instancia de base de datos en una subred privada. También puede configurar una gateway privada virtual que amplíe su red corporativa en la VPC y que permita obtener acceso a la

instancia de base de datos de RDS en dicha VPC. Consulte la guía Amazon VPC User Guide para obtener más detalles.

Para las implementaciones Multi-AZ, definir una subred para todas las zonas de disponibilidad en una región permitirá a Amazon RDS crear una nueva instancia en espera en otra zona de disponibilidad en caso de que surja la necesidad. Puede crear grupos de subredes de base de datos, que son colecciones de subredes que puede designar para las instancias de base de datos de RDS en una VPC. Cada grupo de subredes de base de datos debe tener al menos una subred para cada zona de disponibilidad en una región determinada. En este caso, cuando cree una instancia de base de datos en una VPC, seleccionará un grupo de subredes de base de datos; Amazon RDS utiliza dicho grupo de subredes de base de datos y su zona de disponibilidad preferida para seleccionar una subred y una dirección IP dentro de dicha subred. Amazon RDS crea y asocia una interfaz de red elástica a su instancia de base de datos con dicha dirección IP.

Es posible obtener acceso a las instancias de base de datos implementadas en una VPC de Amazon desde Internet o desde las instancias Amazon EC2 fuera de la VPC a través de VPN o de hosts de protección que puede iniciar en una subred pública. Para utilizar un host de protección, tiene que configurar una subred pública con una instancia EC2 que actúa como protección SSH. Esta subred pública debe tener un puerto de enlace a Internet y reglas de enrutamiento que permitan que el tráfico se redirija a través del host SSH, que posteriormente debe reenviar las solicitudes a la dirección IP privada de su instancia de base de datos de Amazon RDS.

Se pueden usar grupos de seguridad de base de datos para ayudar a proteger las instancias de base de datos dentro de una VPC de Amazon. Además, el tráfico de red que entra y sale de cada subred puede autorizarse o denegarse por medio de listas de control de acceso (ACL) de la red. Todo el tráfico de red que entre o salga de la VPC de Amazon a través de la conexión de VPN IPsec puede inspeccionarse por medio de la infraestructura que tenga en sus instalaciones, como firewalls de red y sistemas de detección de intrusos.

Cifrado

Puede cifrar las conexiones que se realizan entre su aplicación y su instancia de base de datos mediante SSL. Para MySQL y SQL Server, RDS crea un certificado SSL y lo instala en la instancia de base de datos cuando se aprovisiona la instancia. Para MySQL, tendrá que iniciar el cliente de mysql usando el parámetro --ssl_ca para hacer referencia a la clave pública con el fin de cifrar las conexiones. Para SQL Server, descargará la clave pública e importará el certificado en su sistema operativo Windows. Oracle RDS usa el cifrado de red nativo de Oracle con una instancia de base de datos. Simplemente tendrá que añadir la opción de cifrado de red nativo a un grupo de opciones y asociar dicho grupo a la instancia de base de datos. En cuanto se establece una conexión cifrada, los datos transferidos entre la instancia de base de datos y su aplicación se cifrarán durante el proceso de transferencia. También puede exigir que su instancia de base de datos solo acepte conexiones cifradas.

Amazon RDS admite Transparent Data Encryption (TDE) para SQL Server (SQL Server Enterprise Edition) y Oracle (parte de la opción Oracle Advanced Security disponible en Oracle Enterprise Edition). La característica TDE cifra automáticamente los datos antes de que se graben en el sistema de almacenamiento y los descifra también automáticamente cuando se leen.

> **Nota:** debe tener en cuenta asimismo que la compatibilidad con SSL de Amazon RDS se ciñe al cifrado de la conexión entre la aplicación y la instancia de base de datos; no debe confiarse en ella para la autenticación de la instancia de base de datos.

Aunque SSL ofrece ventajas relativas a la seguridad, tenga en cuenta que el cifrado SSL es una operación que hace un uso intensivo de los recursos informáticos y que aumentará la latencia de la conexión de la base de datos. Para obtener más información sobre cómo SSL funciona con MySQL, puede consultar directamente la documentación sobre MySQL que encontrará aquí. Para saber cómo SSL funciona con SQL Server, puede obtener más información en la guía de usuario de RDS.

Backups automatizados y snapshots de base de datos

Amazon RDS ofrece dos métodos diferentes para la realización de backups y restauración de instancias de base de datos: backups automatizados y snapshots de base de datos.

Activada de forma predeterminada, la función de backup automatizada de Amazon RDS permite la recuperación a un punto del tiempo de su instancia de BBDD. Amazon RDS realizará un backup de su base de datos y sus registros de transacciones y los almacenará durante un periodo de retención especificado por el usuario. Estos métodos le permitirán restaurar la instancia de base de datos a cualquier segundo dentro de su período de retención, hasta los últimos cinco minutos. El período de retención de backup automático se puede configurar hasta un máximo de 35 días.

Durante el período de backup podría suspenderse la entrada y salida (E/S) de almacenamiento mientras se realiza el backup de los datos. Esta suspensión de E/S suele durar unos minutos. La suspensión de E/S se evita mediante implementaciones en zonas de disponibilidad múltiples (Multi-AZ), ya que el backup se realiza de la instancia que se encuentra en espera.

Las instantáneas de base de datos son backups iniciados por el usuario de su instancia de base de datos. Amazon RDS almacenará estos backups completos de la base de datos hasta que los elimine expresamente. Puede copiar snapshots de base de datos de cualquier tamaño y moverlas entre cualquier región pública de AWS, o copiar la misma snapshot en varias regiones a la vez. A continuación, puede crear una nueva instancia de base de datos a partir de una snapshot de base de datos donde desee.

Replicación de instancias de base de datos

Los recursos de informática en la nube de Amazon están alojados en instancias de centros de datos con alta disponibilidad en diferentes regiones del mundo, y cada región contiene varias ubicaciones distintas llamadas "zonas de disponibilidad". Cada zona de disponibilidad está diseñada para estar aislada de los errores que se produzcan en otras zonas de disponibilidad y para proporcionar conectividad de red de baja latencia económica con otras zonas de disponibilidad de la misma región.

Para diseñar sus bases de datos de Oracle, PostgreSQL o MySQL de manera que dispongan de alta disponibilidad, puede ejecutar su instancia de base de datos de RDS en varias zonas de disponibilidad, lo que recibe el nombre de implementación Multi-AZ. Cuando selecciona esta opción, Amazon aprovisiona y mantiene automáticamente una réplica de reserva sincrónica de la instancia de base de datos en una zona de disponibilidad diferente. La instancia de base de datos principal se replica sincrónicamente en las zonas de disponibilidad en

la réplica en espera. En caso de que la instancia de base de datos o la zona de disponibilidad produzcan un error, Amazon RDS conmutará automáticamente a la instancia de reserva, para que las operaciones de la base de datos puedan reanudarse rápidamente sin intervención administrativa.

Para los clientes que deseen usar MySQL y tengan requisitos de escalabilidad que superen las restricciones de capacidad de una sola instancia de base de datos para cargas de trabajo de base de datos con un uso intensivo de operaciones de lectura, Amazon RDS proporciona una opción de réplica de lectura. Una vez creada una réplica de lectura, las actualizaciones de base de datos que se realicen en la instancia de base de datos de origen se replicarán en la réplica de lectura mediante la replicación asincrónica nativa de MySQL. Podrá crear varias réplicas de lectura para una instancia de base de datos de origen determinada y distribuir entre ellas el tráfico de lectura de su aplicación. Las réplicas de lectura se pueden crear con implementaciones Multi-AZ para obtener ventajas de escalado de lectura además de los niveles de disponibilidad de escritura en la base de datos y de durabilidad de los datos que proporcionan las implementaciones Multi-AZ.

Parches de software automáticos

Amazon RDS garantizará que el software de base de datos relacional de sus implementaciones permanezca actualizado con los últimos parches. Cuando sea necesario, se aplicarán parches durante el período de mantenimiento del que usted posee el control. Puede contemplar el período de mantenimiento de Amazon RDS como una oportunidad de controlar cuándo se producen modificaciones en las instancias de base de datos (como el escalado de la clase de instancia de base de datos) y se aplican parches de software, en caso de que se solicite o sea necesario. Si hay un evento de "mantenimiento" programado para una determinada semana, se iniciará y completará en un punto determinado dentro del período de mantenimiento de 30 minutos que usted identifique.

Los únicos eventos de mantenimiento que necesitan que Amazon RDS desconecte su instancia de base de datos son las operaciones de ampliación de la capacidad de cómputo (que generalmente se realizan en cuestión de minutos) o la aplicación de parches de software necesarias. Los parches requeridos que tienen que ver con seguridad o durabilidad son los únicos que se programan automáticamente. La aplicación de estos parches tiene lugar con poca frecuencia (normalmente, una vez cada varios meses) y raramente necesitará

más de una fracción del plazo de mantenimiento. Si no especifica un período de mantenimiento semanal preferido al crear la instancia de base de datos, se asignará un valor predeterminado de 30 minutos. Si desea modificar el momento en el que tiene lugar el mantenimiento, puede hacerlo modificando su instancia de base de datos en la consola de administración de AWS o mediante la API ModifyDBInstance. Puede configurar ventanas de mantenimiento diferentes para cada una de sus instancias de base de datos.

La ejecución de la instancia de base de datos como un despliegue Multi-AZ puede reducir aún más el impacto que tiene un evento de mantenimiento, ya que Amazon RDS realizará el mantenimiento mediante los pasos siguientes: 1) Realizar el mantenimiento en la instancia de reserva 2) Elevar la instancia de reserva a instancia principal 3) Realizar el mantenimiento en la antigua instancia principal, que pasa a ser la nueva instancia de reserva.

Cuando se ejecuta una API de eliminación de instancias de base de datos de Amazon RDS (DeleteDBInstance), la instancia de base de datos se marca para su eliminación. La instancia se habrá eliminado totalmente cuando su estado ya no indique "eliminándose". En este punto, la instancia deja de estar accesible y, a menos que se haya solicitado una copia de la snapshot final, no podrá restablecerse y no se mostrará para ninguna de las herramientas ni para las API.

Notificación de eventos

Puede recibir notificaciones de varios eventos importantes que pueden tener lugar en su instancia de RDS, como si se ha cerrado la instancia, si se ha iniciado un backup, si se ha producido una conmutación por error, si el grupo de seguridad ha cambiado o si el espacio de almacenamiento es insuficiente. El servicio Amazon RDS agrupa los eventos en categorías a las que puede suscribirse para recibir una notificación cuando se produzca un evento de esa categoría. Puede suscribirse a una categoría de eventos para una instancia de base de datos, una snapshot de base de datos, un grupo de seguridad de base de datos o un grupo de parámetros de base de datos. Los eventos de RDS se publican a través de AWS SNS y se envían por correo electrónico o como un mensaje de texto. Para obtener más información sobre las categorías de eventos de notificación de RDS, consulte la guía del usuario de RDS.

Seguridad de Amazon Redshift

Amazon Redshift es un servicio de almacenamiento de datos SQL a escala de petabytes, que se ejecuta en recursos de informática y almacenamiento de AWS altamente optimizados y administrados. El servicio se ha diseñado no solo para la rápida ampliación y reducción de recursos, sino para mejorar ostensiblemente la velocidad de consulta incluso en conjuntos de datos extremadamente grandes. Para aumentar el desempeño, Redshift utiliza técnicas como el almacenamiento en columnas, la compresión de datos y las asignaciones de zona para reducir la cantidad de operaciones de E/S necesarias para realizar consultas. También dispone de una arquitectura de procesamiento en paralelo de forma masiva (MPP), que paraleliza y distribuye operaciones SQL para que pueda beneficiarse de todos los recursos disponibles.

Cuando crea un almacén de datos de Redshift, aprovisiona un clúster de uno o varios nodos especificando el tipo y el número de nodos que componen el clúster. El tipo de nodo determina el tamaño de almacenamiento, la memoria y la CPU de cada nodo. Cada clúster de varios nodos incluye un nodo principal y dos o más nodos de computación. El nodo principal se encarga de las conexiones, analiza las consultas, crea planes de ejecución y administra la ejecución de consultas en los nodos de proceso. Los nodos de computación almacenan datos, realizan cálculos y ejecutan consultas, siguiendo instrucciones del nodo principal. El nodo principal de cada clúster está accesible a través de puntos de enlace de ODBC y JDBC, que utilizan controladores PostgreSQL estándar. Los nodos de computación se ejecutan en una red aislada independiente y nunca se obtiene acceso a ellos directamente.

Después de aprovisionar un clúster, puede cargar su conjunto de datos y realizar consultas de análisis de datos mediante herramientas basadas en SQL y aplicaciones de inteligencia empresarial comunes.

Acceso a los clústeres

De forma predeterminada, los clústeres que crea están cerrados a los demás usuarios. Amazon Redshift le permite configurar las reglas del firewall (grupos de seguridad) para controlar el acceso de red al clúster de almacén de datos. También puede ejecutar Redshift en una VPC de Amazon para aislar el clúster de almacén de datos en su propia red virtual y conectarlo a la infraestructura de TI existente mediante la utilización de las conexiones IPsec VPN cifradas estándar del sector.

La cuenta de AWS que crea el clúster tiene acceso total al mismo. En su cuenta de AWS, puede usar AWS IAM para crear cuentas de usuario y administrar los permisos de esas cuentas. Mediante IAM, puede conceder diferentes permisos a los usuarios para que estos realicen solo las operaciones del clúster necesarias para su trabajo.

Al igual que con todas las bases de datos, debe conceder permiso en Redshift en el nivel de base de datos además de en el nivel de recurso. Los usuarios de base de datos son cuentas de usuario designadas que pueden conectarse a una base de datos y que se autentican cuando inician sesión en Amazon Redshift. En Redshift, los permisos de usuario de base de datos se conceden para cada clúster en lugar de para cada tabla. Sin embargo, un usuario solo puede ver los datos de las filas de tabla generadas por sus propias actividades; no podrá ver las filas generadas por otros usuarios.

El usuario que crea el objeto de base de datos es el propietario. De forma predeterminada, solo un superusuario o el propietario de un objeto pueden consultar, modificar o conceder permisos en el objeto. Para los usuarios que utilizan un objeto, debe conceder los permisos necesarios al usuario o grupo que contiene al usuario. Y solo el propietario de un objeto puede modificarlo o eliminarlo.

Backups de datos

Amazon Redshift distribuye sus datos entre todos los nodos de computación de un clúster. Cuando ejecuta un clúster con al menos dos nodos de computación, los datos de cada nodo siempre se reflejan en discos en el otro nodo, lo que reduce el riesgo de pérdida de datos. Además, se realiza un backup constante de todos los datos escritos en un nodo del clúster en Amazon S3 mediante snapshots. Redshift almacena las snapshots durante periodos definidos por el usuario, que pueden ser de 1 a 35 días. También puede crear sus propias snapshots cuando lo desee, para lo que se utilizan las snapshots existentes en el sistema y, además, se conservan hasta que se eliminan explícitamente.

Amazon Redshift monitoriza constantemente el estado del clúster, vuelve a replicar automáticamente los datos desde unidades defectuosas y reemplaza los nodos según proceda. Todo esto ocurre sin ninguna intervención por su parte, aunque tal vez observe cierta degradación del desempeño durante el proceso continuo de replicación.

Puede utilizar cualquier snapshot del sistema o del usuario para restablecer el clúster con la consola de administración de AWS o con las API de Amazon Redshift. El clúster se encuentra disponible en cuanto se restablecen los metadatos del sistema y puede comenzar a ejecutar consultas mientras los datos de usuario se ponen en cola en segundo plano.

Cifrado de datos

Cuando cree un clúster, tendrá la opción de cifrarlo para proporcionar protección adicional a sus datos en reposo. Cuando se habilita el cifrado del clúster, Amazon Redshift almacena todos los datos en las tablas creadas por el usuario en un formato cifrado mediante claves de cifrado en bloque de AES-256 con aceleración por hardware. Esto incluye todos los datos escritos en disco y todos los backups.

Amazon Redshift usa una arquitectura de cuatro niveles basada en claves para el cifrado. Estas claves constan 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* cifran los bloques de datos del clúster. A cada bloque de datos se le asigna una clave AES-256 generada aleatoriamente. Estas claves se cifran mediante la clave de base de datos del clúster.
- La *clave de base de datos* cifra las claves de cifrado de datos del clúster. La clave de base de datos es una clave AES-256 generada aleatoriamente. Se almacena en disco en una red independiente del clúster de Amazon Redshift y se cifra mediante una clave maestra. Amazon Redshift pasa la clave de base de datos a través de un canal seguro y la conserva en memoria en el clúster.
- La *clave del clúster* cifra la clave de base de datos del clúster de Amazon Redshift. Puede usar AWS o un módulo de seguridad por hardware (HSM) para almacenar la clave del clúster. Los HSM proporcionan control directo de la generación y administración de claves, y separan la administración de claves de la de la aplicación y la base de datos.
- La *clave maestra* cifra la clave del clúster si esta se almacena en AWS. La clave maestra cifra la base de datos cifrada con la clave del clúster si esta última se almacena en un HSM.

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

> **Nota:** si habilita el cifrado en el clúster, el desempeño resultará afectado, aunque disponga de aceleración por hardware. El cifrado se aplica también a los backups. Cuando se restauran desde una snapshot cifrada, el nuevo clúster también se cifra.

Para cifrar los archivos de datos de carga de la tabla al cargarlos en Amazon S3, puede usar el cifrado de lado servidor de Amazon S3. Cuando cargue los datos desde Amazon S3, el comando COPY descifrará los datos conforme se carga la tabla.

Registro de auditoría de base de datos

Amazon Redshift registra todas las operaciones SQL, entre otras, los intentos de conexión, las consultas y los cambios realizados en la base de datos. Puede obtener acceso a estos logs realizando consultas SQL en las tablas del sistema u optar por descargarlos en un bucket seguro de Amazon S3. A continuación, puede usar estos logs de auditoría para supervisar la seguridad y los problemas que puedan surgir en el clúster.

Parches de software automáticos

Amazon Redshift se encarga de todo el trabajo necesario para configurar, utilizar y escalar el almacén de datos, incluido el aprovisionamiento de capacidad, la monitorización del clúster y la aplicación de parches y actualizaciones al motor de Amazon Redshift. Los parches solo se aplican durante los períodos de mantenimiento especificados.

Conexiones SSL

Para proteger los datos en tránsito en la nube de AWS, Amazon Redshift usa SSL con aceleración por hardware para comunicarse con Amazon S3 o Amazon DynamoDB para las operaciones de COPY, UNLOAD, backup y restauración. Puede cifrar la conexión entre el cliente y el clúster especificando SSL en el grupo de parámetros asociado al clúster. Para que los clientes autentiquen el servidor de Redshift, puede instalar la clave pública (archivo .pem) del certificado SSL en su cliente y usar la clave para conectarse a sus clústeres.

Amazon Redshift ofrece las funciones de cifrado más nuevas y seguras, que usan el protocolo Elliptic Curve Diffie-Hellman Ephemeral. ECDHE permite a los clientes de SSL proporcionar Perfect Forward Secrecy entre el cliente y el clúster de Redshift. Perfect Forward Secrecy usa claves de sesión que son efímeras y no se almacenan en ningún sitio, lo que impide la descodificación de los datos capturados por parte de terceros no autorizados, incluso en el caso de que se divulgue la propia clave secreta de larga duración. No necesita configurar nada en Amazon Redshift para habilitar ECDHE; si se conecta desde una herramienta cliente SQL que usa ECDHE para cifrar la comunicación entre el cliente y el servidor, Amazon Redshift usará la lista de códigos de cifrado proporcionada para establecer la conexión correspondiente.

Seguridad de Amazon ElastiCache

Amazon ElastiCache es un servicio web que facilita la configuración, la administración y el escalado de entornos de caché en memoria en la nube. El servicio mejora el desempeño de las aplicaciones web, lo que le permite recuperar información de un sistema de almacenamiento de caché en memoria rápido y administrado en lugar de depender totalmente de bases de datos basadas en disco más lentas. Se puede usar para mejorar considerablemente la latencia y el desempeño de muchas cargas de trabajo de aplicaciones con un uso intensivo de operaciones de lectura (como, por ejemplo, redes sociales, juegos, intercambio de contenido multimedia y portales de preguntas y respuestas) o de cargas de trabajo con muchos procesos informáticos (como un motor de recomendaciones). El almacenamiento en caché mejora el desempeño de las aplicaciones almacenando los datos críticos en memoria para un acceso de baja latencia. La información en caché puede incluir los resultados de las consultas de base de datos con mucha E/S o los resultados de cálculos que utilicen muchos recursos informáticos.

El servicio Amazon ElastiCache automatiza las laboriosas tareas de administración en entornos de caché en memoria, como la administración de parches, la detección de errores y la recuperación. Funciona conjuntamente con otros Amazon Web Services (como Amazon EC2, Amazon CloudWatch y Amazon SNS) para proporcionar una caché en memoria administrada, segura y de alto desempeño. Por ejemplo, una aplicación que se ejecuta en Amazon EC2 puede obtener acceso de manera segura a un clúster de Amazon ElastiCache de la misma región con baja latencia.

Con el servicio Amazon ElastiCache, crea un clúster de caché, que es una colección de uno o varios nodos de caché, cada uno de los cuales ejecuta una instancia del servicio Memcached. Un nodo de caché es un fragmento de tamaño fijo de RAM segura conectada a la red. Cada nodo de caché ejecuta una instancia del servicio Memcached y tiene su propio puerto y nombre DNS. Se admiten varios tipos de nodos de caché, cada uno de los cuales tiene una cantidad diferente de memoria asociada. Se puede configurar un clúster de caché con un número específico de nodos de caché y un grupo de parámetros de caché que controle las propiedades de cada nodo de caché. Todos los nodos de caché de un clúster de caché están diseñados para ser del mismo tipo y tener los mismos valores de configuración de parámetros y grupo de seguridad.

Amazon ElastiCache permite controlar el acceso a sus clústeres de caché a través de grupos de seguridad de caché. Un grupo de seguridad de caché actúa como un firewall, ya que controla el acceso de red a su clúster de caché. De forma predeterminada, el acceso de red a sus clústeres de caché está desactivado. Si desea que sus aplicaciones obtengan acceso al clúster de caché, debe habilitar de forma explícita el acceso de los hosts de grupos de seguridad de EC2 específicos. Cuando se configuran las reglas de entrada, se aplican las mismas reglas a todos los clústeres de caché asociados a ese 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 Authorize Cache Security Group Ingress o el comando de la CLI para autorizar el grupo de seguridad deseado de EC2 (que a su vez especifica las instancias EC2 permitidas). El control de acceso basado en un intervalo de direcciones IP no está habilitado actualmente para los clústeres de caché. Todos los clientes de un clúster de caché deben estar dentro de la red de EC2 y recibir la autorización a través de grupos de seguridad de caché.

ElastiCache para Redis proporciona funciones de backup y restauración, con las que puede crear una snapshot de todo el clúster de Redis tal como existe en un punto determinado en el tiempo. Puede programar snapshots periódicas diarias automáticas o puede crear una snapshot manual en cualquier momento. Para las snapshots automáticas, tendrá que especificar un período de retención; las snapshots manuales se conservan hasta que se eliminan. Las snapshots se almacenan en Amazon S3 con una alta durabilidad, y se pueden usar para arranques en caliente, backups y archivado.

Servicios de aplicaciones

Amazon Web Services ofrece una serie de servicios administrados para utilizarlos con las aplicaciones, entre los que se incluyen servicios que ofrecen streaming de aplicaciones, colocación en colas, notificaciones push, entrega de correo electrónico, búsqueda y transcodificación.

Seguridad de Amazon CloudSearch

Amazon CloudSearch es un servicio totalmente administrado en la nube que facilita la configuración, la administración y el escalado de una solución de búsqueda para su sitio web. Amazon CloudSearch le permite buscar grandes conjuntos de datos, como páginas web, archivos de documentos, publicaciones en foros o información de productos. Le permite añadir rápidamente funciones de búsqueda a su sitio web sin necesidad de convertirse en un experto en búsquedas o preocuparse por el abastecimiento, la configuración y el mantenimiento de hardware. Si el volumen de datos y tráfico fluctúa, Amazon CloudSearch escala el servicio automáticamente para satisfacer sus necesidades.

Un dominio de Amazon CloudSearch encapsula una colección de datos que admiten búsquedas, las instancias de búsqueda que procesan las peticiones de búsqueda y una configuración que controla el modo en que se indexan y buscan los datos. Puede crear un dominio de búsqueda independiente para cada colección de datos que desee que se pueda buscar. Para cada dominio, configurará opciones de indexación que describan los campos que desea incluir en el índice y el modo en que desee usarlos; opciones de texto que definan palabras excluidas, palabras derivadas y sinónimos; expresiones de clasificación que puede usar para personalizar el modo en que se ordenan los resultados de búsqueda; y políticas de acceso que controlen el acceso a los puntos de enlace de búsqueda y documentos del dominio.

Todas las solicitudes de configuración de Amazon CloudSearch deben autenticarse mediante la autenticación de AWS estándar.

Amazon CloudSearch proporciona puntos de enlace distintos para obtener acceso a los servicios de configuración, búsqueda y documentos:

- Al servicio de configuración se tiene acceso a través de un punto de enlace general: cloudsearch.us-east-1.amazonaws.com

- El punto de conexión al servicio de documentos se usa para enviar documentos al dominio para su indexación y se obtiene acceso 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 usa para enviar peticiones de búsqueda al dominio y se obtiene acceso a él a través de un punto de enlace específico del dominio: http://search-domainname-domainid.us-east-1.cloudsearch.amazonaws.com

Al igual que todos los servicios de AWS, Amazon CloudSearch requiere que cada solicitud realizada a su API de control se autentique para que solo los usuarios autenticados puedan obtener acceso al dominio de CloudSearch. Las solicitudes API se firman con una firma MAC-SHA1 o HMAC-SHA256 calculada a partir de una solicitud y de la clave de acceso secreta de AWS del usuario. Además, a la API de control de Amazon CloudSearch solo se puede tener acceso a través de los puntos de enlace cifrados por SSL. Puede controlar el acceso a las funciones de administración de Amazon CloudSearch creando usuarios en su cuenta de AWS mediante AWS IAM y controlando qué operaciones de CloudSearch pueden realizar estos usuarios.

Seguridad de Amazon Simple Queue Service (Amazon SQS)

Amazon SQS es un servicio de cola de mensajes escalable y de alta confianza que permite la comunicación asíncrona de los mensajes entre los componentes distribuidos de una aplicación. Los componentes pueden ser equipos o instancias de Amazon EC2 o una combinación de ambos. Con Amazon SQS, puede enviar una serie de mensajes a una cola de Amazon SQS en cualquier momento desde cualquier componente. Los mensajes pueden recuperarse desde el mismo componente o desde otro distinto de forma inmediata o en un momento posterior (en un periodo de 4 días). Los mensajes son muy duraderos; cada mensaje se almacena de forma permanente en colas de alta disponibilidad y confianza. En una cola de Amazon SQS se pueden leer o grabar varios procesos al mismo tiempo sin que interfieran entre sí.

El acceso a Amazon SQS se concede a través de una cuenta de AWS o un usuario creado con AWS IAM. Tras la autenticación, una cuenta de AWS tiene acceso total a todas las operaciones de los usuarios. No obstante, un usuario de AWS IAM solo tiene acceso a las operaciones y colas para las que se le haya concedido acceso a través de una política. De forma predeterminada, el acceso a cada una de las colas se restringe a la cuenta de AWS que la haya creado. Sin embargo,

puede permitir otro acceso a una cola, usando una política generada por SQS o una política que usted cree.

Se puede obtener acceso a Amazon SQS a través de los puntos de enlace cifrados con SSL. Es posible obtener acceso a los puntos de enlace cifrados tanto desde Internet como desde Amazon EC2. AWS no cifra los datos almacenados en Amazon SQS, pero el usuario puede cifrar los datos antes de cargarlos en Amazon SQS, siempre que la aplicación que utiliza la cola tenga recursos para descifrar el mensaje cuando se recupera. El cifrado de los mensajes antes de enviarlos a Amazon SQS ayuda a ofrecer protección frente al acceso no autorizado a datos sensibles del cliente, incluso por parte de AWS.

Seguridad de Amazon Simple Notification Service (Amazon SNS)

Amazon Simple Notification Service (Amazon SNS) es un servicio web que facilita las tareas de configuración, utilización y envío de notificaciones desde la nube. Ofrece a los desarrolladores una funcionalidad muy escalable, flexible y rentable para publicar mensajes desde una aplicación y entregarlos inmediatamente a suscriptores o a otras aplicaciones.

Amazon SNS ofrece una sencilla interfaz de servicios web que puede utilizarse para crear temas de los que los clientes desean informar a las aplicaciones (o a personas), para suscribir a clientes a estos temas, para publicar mensajes y para que estos mensajes se entreguen a través del protocolo de su elección (como, por ejemplo, HTTP/HTTPS, correo electrónico, etc.). Amazon SNS envía las notificaciones a través de un mecanismo “push” que elimina la necesidad de comprobar o "sondear" periódicamente si hay nueva información o actualizaciones. Amazon SNS se puede usar para crear flujos de trabajo y aplicaciones de mensajería controlados por eventos altamente fiables sin necesidad de middleware complejo ni de administrar las aplicaciones. Entre los posibles usos de Amazon SNS se incluye la monitorización de aplicaciones, sistemas de flujo de trabajo, actualizaciones de información en las que el factor tiempo es importante, aplicaciones móviles y muchos otros. Amazon SNS proporciona mecanismos de control de acceso diseñados para garantizar que los temas y los mensajes están protegidos frente a acceso no autorizado. Los propietarios de temas pueden definir políticas para un tema que restrinjan quién puede publicar un tema o suscribirse a él. Además, los propietarios de los temas podrán cifrar la transmisión especificando que el mecanismo de entrega debe ser HTTPS.

El acceso a Amazon SNS se concede a través de una cuenta de AWS o de un usuario creado con AWS IAM. Tras la autenticación, una cuenta de AWS tiene acceso total a todas las operaciones de los usuarios. No obstante, un usuario de AWS IAM solo tiene acceso a las operaciones y temas para los que se le haya concedido acceso a través de una política. De forma predeterminada, el acceso a cada uno de los temas se restringe a la cuenta de AWS que lo haya creado. Sin embargo, puede permitir otro acceso a SNS, usando una política generada por SNS o una política que usted cree.

Seguridad de Amazon Simple Workflow Service (Amazon SWF)

Amazon Simple Workflow Service (SWF) facilita la creación de aplicaciones que coordinen el trabajo entre componentes distribuidos. Mediante Amazon SWF, puede estructurar los diversos pasos de procesamiento de una aplicación en "tareas" que dirigen el trabajo en aplicaciones distribuidas; Amazon SWF se encargará de coordinar estas tareas de forma fiable y escalable. Amazon SWF administra las dependencias de la ejecución de las tareas, la programación y la simultaneidad en función de la lógica de la aplicación del desarrollador. El servicio almacena tareas, las envía a componentes de aplicaciones, realiza un seguimiento de su progreso y mantiene su estado más reciente.

Amazon SWF proporciona llamadas sencillas a la API que se pueden ejecutar a partir de un código escrito en cualquier lenguaje y ejecutarse en sus instancias de EC2, o desde cualquiera de sus máquinas ubicadas en cualquier lugar del mundo desde el que tengan acceso a Internet. Amazon SWF actúa como núcleo de coordinación con el que interactúan sus hosts de aplicaciones. Usted crea los flujos de trabajo que desee con sus tareas asociadas y la lógica condicional que quiera aplicar y los almacena en Amazon SWF.

El acceso a Amazon SWF se concede a través de una cuenta de AWS o un usuario creado con AWS IAM. Todos los agentes que participan en la ejecución de un flujo de trabajo (responsables de la toma de decisiones, empleados de actividades y administradores del flujo de trabajo) deben ser usuarios de IAM bajo la cuenta de AWS que posee los recursos de Amazon SWF. No puede conceder acceso a usuarios asociados a otras cuentas de AWS a sus flujos de trabajo de Amazon SWF. No obstante, un usuario de AWS IAM solo tiene acceso a los flujos de trabajo y recursos para los que se le haya concedido acceso a través de una política.

Seguridad de Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (SES) es un servicio de correo electrónico, basado en la infraestructura fiable y escalable de Amazon, capaz de enviar y recibir correo en nombre del dominio. Amazon SES le ayuda a mejorar la capacidad de entrega de correo electrónico y a conocer el estado de entrega de su correo electrónico. Amazon SES se integra con otros servicios de AWS, lo que facilita el envío de correo electrónico desde aplicaciones alojadas en servicios como Amazon EC2.

Desgraciadamente, con otros sistemas de correo electrónico, un spammer podría falsificar un encabezado de correo electrónico y suplantar la dirección de correo electrónico de origen para aparentar que el correo electrónico procede de una fuente diferente. Para reducir estos problemas, Amazon SES requiere que los usuarios verifiquen su dirección de correo electrónico o dominio para que confirmen que son suyos e impedir que otras personas los utilicen. Para verificar un dominio, Amazon SES requiere que el remitente publique un registro DNS que Amazon SES suministra como prueba de control del dominio. Amazon SES revisa periódicamente el estado de verificación del dominio y revoca la verificación cuando esta deja de ser válida.

Amazon SES toma medidas preventivas para impedir el envío de contenidos dudosos, de tal modo que los ISP reciben siempre correo electrónico de alta calidad y, consecuentemente, confían en Amazon SES como origen de correo electrónico de confianza. A continuación se muestran algunas de las características que optimizan la capacidad de entrega y la fiabilidad para todos nuestros remitentes:

- Amazon SES utiliza tecnologías de filtrado de contenido que ayudan a detectar y bloquear los mensajes que contienen virus o malware antes de que se envíen.
- Amazon SES mantiene bucles de retroalimentación de reclamaciones de los principales ISP. Los bucles de retroalimentación de reclamaciones indican qué correos ha marcado como spam un destinatario. Amazon SES le ofrece acceso a estas métricas de entregas con objeto de ayudarle a orientar su estrategia de envío de correo electrónico.
- Amazon SES usa diversas técnicas para medir la calidad de lo que envía cada usuario. Estos mecanismos ayudan a identificar y a bloquear los intentos de usar Amazon SES para enviar correo no solicitado, y

permiten detectar otros patrones de envío que podrían dañar la reputación de Amazon SES con los ISP, los proveedores de bandeja de correo y los servicios antispam.

- Amazon SES admite mecanismos de autenticación, como Sender Policy Framework (SPF) y el correo identificado con claves de dominio (DKIM). Cuando autentica un correo electrónico, proporciona pruebas a los ISP de que usted es el propietario del dominio. Amazon SES le facilita el trabajo de autenticación del correo electrónico. Si configura su cuenta para utilizar Easy DKIM, Amazon SES marcará sus mensajes de correo electrónico con la firma de DKIM en su nombre, de modo que usted pueda centrarse en otros aspectos de su estrategia de envío. Para garantizar una capacidad de entrega óptima, le recomendamos que autentique su correo electrónico.

Al igual que con otros servicios de AWS, usa credenciales de seguridad para verificar quién es usted y si tiene permiso para interactuar con Amazon SES. Para obtener información sobre las credenciales que debe usar, consulte Usar credenciales con Amazon SES. Amazon SES se integra con AWS IAM, lo que le permite especificar qué acciones de la API de Amazon SES puede llevar a cabo un usuario concreto.

Si elige comunicarse con Amazon SES a través de su interfaz SMTP, tendrá que cifrar su conexión mediante TLS. Amazon SES admite dos mecanismos para establecer la conexión cifrada por TLS: STARTTLS y TLS Wrapper. Si elige comunicarse con Amazon SES a través de HTTP, toda la comunicación se protegerá mediante TLS a través del punto de enlace HTTPS de Amazon SES. Cuando envía correo electrónico a su destino final, Amazon SES cifra el contenido del correo electrónico con TLS oportunista, si lo admite el receptor.

Seguridad del servicio Amazon Elastic Transcoder

El servicio Amazon Elastic Transcoder simplifica y automatiza el proceso, normalmente complejo, de convertir archivos multimedia de un formato, tamaño o calidad a otro. El servicio Elastic Transcoder convierte archivos de vídeo de definición estándar (SD) o alta definición (HD), además de 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 usar el mismo bucket para la entrada y la salida, y los buckets pueden estar en cualquier región de AWS. Elastic Transcoder acepta archivos de entrada en una gran variedad de formatos web, comerciales y profesionales. Los tipos de archivo de salida son

MP3, MP4, OGG, TS, WebM, HLS mediante MPEG-2 TS y Smooth Streaming mediante tipos de contenedores fmp4, vídeo H.264 o VP8 de almacenamiento y audio AAC, MP3 o Vorbis.

Empezará con uno o varios archivos de entrada y creará tareas de transcodificación en un tipo de flujo de trabajo denominado línea de transcodificación para cada archivo. Cuando cree la línea de transcodificación, especificará los buckets de entrada y salida, además de un rol de IAM. Cada tarea debe hacer referencia a una plantilla de conversión de contenido multimedia, llamada modelo predeterminado de transcodificación, que generará uno o varios archivos de salida. Un modelo predeterminado indica a Elastic Transcoder qué configuración debe usar cuando procesa un archivo de entrada en concreto. Puede especificar muchos valores cuando crea un modelo predeterminado, incluida la velocidad de muestreo, la tasa de bits (ancho y alto de la salida), el número de referencias y fotogramas clave, una tasa de bits de vídeo, opciones de creación de miniaturas, etc.

Se hace todo lo posible para que las tareas se inicien en el orden en que se emiten, pero esto no se puede garantizar en todos los casos, y las tareas finalizan normalmente de forma desordenada ya que se procesan en paralelo y varían en cuanto a su complejidad. Puede detener y reanudar cualquiera de sus líneas de transcodificación, si surge la necesidad.

Elastic Transcoder admite el uso de notificaciones de SNS cuando inicia y finaliza cada tarea, y cuando necesita informarle de que ha detectado una condición de error o advertencia. Los parámetros de las notificaciones de SNS están asociados a cada línea de transcodificación. El servicio también puede usar la función Mostrar tareas por estado para buscar todas las tareas con un determinado estado (como "Completada"), o la función Leer tarea para recuperar información detallada de una tarea determinada.

Al igual que otros servicios de AWS, Elastic Transcoder se integra 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 requiere, incluidos los buckets de Amazon S3 y los temas de Amazon SNS. De forma predeterminada, los usuarios de IAM no tienen acceso a Elastic Transcoder ni a los recursos que este utiliza. Si desea que los usuarios de IAM puedan trabajar con Elastic Transcoder, debe concederles permisos explícitamente.

Amazon Elastic Transcoder requiere que todas las solicitudes realizadas a su API de control se autentiquen para que solo los procesos o usuarios autenticados puedan crear, modificar o eliminar sus propias líneas y modelos predeterminados de Amazon Transcoder. Las solicitudes se firman con una firma HMAC-SHA256 calculada a partir de una solicitud y de una clave derivada de la clave secreta del usuario. Además, a la API de Amazon Elastic Transcoder solo se puede obtener acceso a través de los puntos de enlace cifrados por SSL.

Amazon S3 proporciona durabilidad, ya que los archivos multimedia se almacenan de forma redundante en varios dispositivos de diversas instalaciones dentro de una región de Amazon S3. Para disfrutar de mayor protección frente a la posibilidad de que los usuarios eliminen por error archivos multimedia, puede usar la característica de control de versiones de Amazon S3 para conservar, recuperar y restaurar todas las versiones de cada objeto almacenado en un bucket de Amazon S3. Puede proteger aún más las versiones mediante la característica MFA Delete del control de versiones de Amazon S3. Una vez activada para un bucket de Amazon S3, cada solicitud de eliminación de versiones debe incluir un código de seis dígitos y un número de serie del dispositivo de autenticación multifactor.

Seguridad de Amazon AppStream

El servicio Amazon AppStream proporciona un marco de trabajo para ejecutar aplicaciones de streaming, en concreto, aplicaciones que requieren clientes ligeros ejecutándose en dispositivos móviles. Este servicio le permite almacenar y ejecutar su aplicación en potentes GPU de procesamiento en paralelo en la nube, y después transmitir la entrada y la salida en cualquier dispositivo cliente. Puede tratarse de una aplicación existente que modifique para que funcione con Amazon AppStream o de una nueva aplicación que diseñe específicamente para que opere con el servicio.

El SDK de Amazon AppStream simplifica el desarrollo de aplicaciones de streaming y aplicaciones cliente interactivas. El SDK proporciona API que conectan los dispositivos de los clientes directamente a la aplicación, capturan y codifican audio y vídeo, transmiten contenido por Internet en tiempo casi real, descodifican contenido en los dispositivos cliente y devuelven las acciones del usuario a la aplicación. Como el procesamiento de la aplicación tiene lugar en la nube, se puede ampliar para atender cargas de trabajo computacionales extremadamente grandes.

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

En la mayoría de los casos, querrá asegurarse de que el usuario que ejecuta el cliente está autorizado para usar su aplicación antes de permitirle que obtenga un ID de sesión. Le recomendamos que use algún tipo de servicio de concesión de derechos, es decir, un servicio que autentique a los clientes y autorice su conexión a la aplicación. En este caso, el servicio de concesión de derechos llamará también a la API REST de Amazon AppStream para crear una nueva sesión de streaming para el cliente. Cuando el servicio de concesión de derechos crea una nueva sesión, devuelve el identificador de sesión al cliente autorizado como una URL de derechos de un solo uso. El cliente utiliza entonces la URL de derechos para conectarse a la aplicación. El servicio de concesión de derechos puede estar alojado en una instancia Amazon EC2 o en AWS Elastic Beanstalk.

Amazon AppStream utiliza una plantilla de AWS CloudFormation que automatiza el proceso de implementación de una instancia EC2 de GPU que tiene instaladas las bibliotecas del SDK de aplicaciones y clientes Windows de AppStream; se configura para el acceso SSH, RDC o VPN, y tiene una dirección IP elástica asignada. Si usa esta plantilla para implementar su servidor de streaming independiente, todo lo que tendrá que hacer es cargar la aplicación en el servidor y ejecutar el comando para iniciarla. A continuación, puede usar la herramienta de simulación de servicio de Amazon AppStream para probar la aplicación en modo independiente antes de implementarla en producción.

Amazon AppStream utiliza también el protocolo STX para administrar la transmisión de su aplicación desde AWS a los dispositivos locales. El protocolo STX de Amazon AppStream es un protocolo propietario para transmitir vídeo de aplicaciones de alta calidad a través de distintas condiciones de red; monitoriza las condiciones de red y adapta automáticamente la transmisión de vídeo para proporcionar una experiencia de baja latencia y alta resolución a los clientes. Minimiza la latencia durante la sincronización del audio y el vídeo, además de capturar las acciones de los clientes para enviarlas a la aplicación que se ejecuta en AWS.

Servicios de análisis

Amazon Web Services ofrece servicios de análisis basados en la nube para ayudarle a procesar y analizar cualquier volumen de datos, ya sea para clústeres Hadoop administrados, streaming de datos en tiempo real, almacenamiento de datos de varios petabytes u orquestación.

Seguridad de Amazon Elastic MapReduce (Amazon EMR)

Amazon Elastic MapReduce (Amazon EMR) es un servicio web administrado que puede usar para ejecutar clústeres Hadoop que procesen grandes cantidades de datos distribuyendo el trabajo entre varios servidores. Utiliza una versión mejorada del marco de trabajo de Amazon Hadoop que se ejecuta en la infraestructura web de Amazon EC2 y Amazon S3. Solo tiene que cargar los datos de entrada y una aplicación de procesamiento de datos en Amazon S3. Amazon EMR lanzará el número de instancias Amazon EC2 que usted especifique. El servicio comienza a ejecutar el flujo de trabajo al tiempo que extrae los datos de entrada de Amazon S3 en las instancias Amazon EC2 que se hayan lanzado. Una vez finalizado el flujo de trabajo, Amazon EMR transfiere los datos de salida a Amazon S3, donde puede recuperarlos o utilizarlos como entrada para otro flujo de trabajo.

Cuando se lanzan flujos de trabajo en su nombre, Amazon EMR configura dos grupos de seguridad de Amazon EC2: uno para los nodos principales y otro para los esclavos. El grupo de seguridad principal tiene un puerto abierto para comunicarse con el servicio. También tiene abierto el puerto SSH para que pueda utilizar SSH en las instancias por medio de la clave especificada al iniciar sesión. Los esclavos se inician en otro grupo de seguridad aparte que solamente permite la interacción con la instancia principal. La opción predeterminada es configurar estos dos grupos de seguridad para no permitir el acceso de fuentes externas, incluidas instancias Amazon EC2 pertenecientes a otros clientes. Dado que se trata de grupos de seguridad incluidos en su cuenta, podrá cambiar su configuración utilizando el panel o las herramientas estándar de EC2. Para proteger los conjuntos de datos de entrada y salida de los clientes, Amazon EMR transfiere datos a y desde Amazon S3 usando SSL.

Amazon EMR proporciona varias formar de controlar el acceso a los recursos del clúster. Puede usar AWS IAM para crear cuentas y roles de usuario, y configurar permisos para controlar a qué características de AWS tienen acceso esos usuarios y roles. Cuando inicia un clúster, puede asociar un par de claves de Amazon EC2 al clúster, que podrá usar cuando se conecte al clúster mediante SSH. También puede definir permisos que permitan a los usuarios distintos del usuario predeterminado de Hadoop enviar tareas al clúster.

De forma predeterminada, si un usuario de IAM inicia un clúster, ese clúster está oculto para otros usuarios de IAM en la cuenta de AWS. Este filtrado se produce en todas las interfaces de Amazon EMR (la consola, la CLI, la API y los SDK), y ayuda a impedir que los usuarios de IAM obtenga acceso a los clústeres creados por otros usuarios de IAM y los cambien sin querer. Esto es útil para los clústeres diseñados como de solo lectura para un solo usuario de IAM y para la cuenta de AWS principal. También tiene la opción de hacer que el clúster esté visible y accesible a todos los usuarios de IAM de la misma cuenta de AWS.

Para disponer de una capa de protección adicional, puede lanzar las instancias EC2 de su clúster de EMR en una VPC de Amazon, que es lo mismo que lanzarlas en una subred privada. Esto permite controlar el acceso a toda la subred. También puede iniciar el clúster en una VPC y permitir que el clúster obtenga acceso a los recursos de su red interna mediante una conexión de VPN. Puede cifrar los datos de entrada antes de cargarlos en Amazon S3 mediante cualquier herramienta común de cifrado de datos. Si cifra los datos antes de cargarlos, necesitará añadir un paso de descifrado al principio del flujo de trabajo cuando Amazon Elastic MapReduce obtenga los datos de Amazon S3.

Seguridad de Amazon Kinesis

Amazon Kinesis es un servicio administrado diseñado para administrar la transmisión en tiempo real de Big Data. Puede aceptar cualquier cantidad de datos, de cualquier número de fuentes, ampliando y reduciendo los recursos según sea necesario. Puede usar Kinesis en situaciones que requieran la incorporación y procesamiento de datos en tiempo real a gran escala, como logs de servidor, orígenes de datos de redes sociales o del mercado y datos de secuencias de clics en sitios web.

Las aplicaciones leen y escriben los registros de datos en Amazon Kinesis en secuencias. Puede crear cualquier número de secuencias de Kinesis para capturar, almacenar y transportar los datos. Amazon Kinesis administra automáticamente la infraestructura, el almacenamiento, las redes y la configuración para recopilar y procesar los datos con el nivel de desempeño que la aplicación necesita. No debe preocuparse por el aprovisionamiento, la implementación y el mantenimiento continuo del hardware, el software ni otros servicios para poder capturar y almacenar datos en tiempo real a gran escala. Además, Amazon Kinesis replica los datos de forma sincrónica en tres centros de una misma región de AWS, lo que proporciona un alto nivel de disponibilidad y de 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 inmutable y no interpretada de bytes. El servicio de Amazon Kinesis no inspecciona, interpreta ni cambia los datos del blob de ninguna forma. Los registros de datos solo están accesibles durante 24 horas desde el momento en que se añaden a una secuencia de Amazon Kinesis, y se descartan automáticamente.

Su aplicación es un consumidor de una secuencia de Amazon Kinesis, que normalmente se ejecuta en un grupo de instancias Amazon EC2. Una aplicación Kinesis utiliza la biblioteca cliente de Amazon Kinesis para leer la secuencia de Amazon Kinesis. La biblioteca cliente de Kinesis se ocupa de distintos aspectos por usted, incluida la conmutación por error, la recuperación y el balanceo de carga, lo que permite a su aplicación centrarse en el procesamiento de los datos cuando estos están disponibles. Después de procesar el registro, su código de consumidor puede transferirse junto con otra secuencia de Kinesis, escribirse en un bucket de Amazon S3, un almacén de datos de Redshift o una tabla de DynamoDB, o simplemente descartarse. Dispone de una biblioteca de conectores para poder integrar Kinesis con otros servicios de AWS (como DynamoDB, Redshift y Amazon S3) y productos de terceros como Apache Storm.

Puede controlar el acceso lógico a los recursos y funciones de administración de Kinesis creando usuarios en su cuenta de AWS mediante AWS IAM y controlando qué operaciones de Kinesis pueden realizar estos usuarios. Para facilitar la ejecución de aplicaciones de consumo o producción en una instancia Amazon EC2, puede configurar esa instancia con un rol de IAM. De ese modo, las credenciales de AWS que reflejan los permisos asociados al rol de IAM estarán disponibles para las aplicaciones en la instancia, lo que significa que no

tiene que usar sus credenciales de seguridad de AWS de larga duración. Los roles tienen la ventaja añadida de proporcionar credenciales temporales que vencen en un corto período de tiempo, lo que añade una medida adicional de protección. Consulte la guía de uso de IAM para obtener más información sobre los roles de IAM.

La API de Amazon Kinesis solo está accesible a través de un punto de enlace cifrado por SSL (kinesis.us-east-1.amazonaws.com) para ayudarle a garantizar una transmisión segura de sus datos a AWS. Debe conectarse a ese punto de enlace para obtener acceso a Kinesis, pero puede usar después la API para indicarle a AWS Kinesis que cree una secuencia en cualquier región de AWS.

Seguridad de AWS Data Pipeline

El servicio AWS Data Pipeline le ayuda a procesar y transferir datos entre diferentes orígenes de datos a intervalos especificados mediante flujos de trabajo orientados a los datos y la función integrada de comprobación de dependencias. Cuando crea una canalización, define los orígenes de datos, las condiciones previas, los destinos, los pasos de procesamiento y un calendario de operaciones. Una vez definida y activada una canalización, esta se ejecuta automáticamente de acuerdo con el calendario especificado.

Con AWS Data Pipeline, no tiene que preocuparse de comprobar la disponibilidad de los recursos, administrar las dependencias entre tareas, reintentar errores transitorios o tiempos de espera en tareas individuales, o crear un sistema de notificación de errores. AWS Data Pipeline se ocupa de lanzar los servicios y recursos de AWS que su canalización necesita para procesar los datos (por ejemplo, Amazon EC2 o EMR) y de transferir los resultados al sistema de almacenamiento (por ejemplo, Amazon S3, RDS, DynamoDB o EMR).

Cuando usa la consola, AWS Data Pipeline crea los roles y las políticas de IAM necesarios, incluida una lista de entidades de confianza. Los roles de IAM determinan a lo que la canalización puede obtener acceso y las acciones que puede realizar. Asimismo, cuando la canalización crea un recurso, como una instancia EC2, los roles de IAM determinan los recursos y acciones permitidos por la instancia EC2. Cuando crea una canalización, especifica un rol de IAM que rige la canalización y otro rol de IAM que rige los recursos de la canalización (denominado "rol de recursos"), que puede ser el mismo para ambos. Como parte de la práctica recomendada de seguridad de privilegios mínimos, le

recomendamos que considere la posibilidad de usar los permisos mínimos necesarios para que la canalización realice el trabajo y defina los roles de IAM en consecuencia.

Al igual que muchos servicios de AWS, AWS Data Pipeline también proporciona la opción de puntos de enlace seguros (HTTPS) para el acceso a través de SSL.

Servicios de implementación y administración

Amazon Web Services proporciona una serie de herramientas que le ayudan a implementar y administrar sus aplicaciones. Entre estas se incluyen servicios que le permiten crear cuentas de usuario individuales con credenciales para obtener acceso a los servicios de AWS. También se incluyen servicios para crear y actualizar pilas de recursos de AWS, implementar aplicaciones en estos recursos y monitorizar el estado de estos recursos de AWS. Otras herramientas le ayudan a administrar claves criptográficas mediante módulos de seguridad por hardware (HSM) y registrar la actividad de la API de AWS para fines de seguridad y cumplimiento.

AWS Identity and Access Management (AWS IAM)

AWS IAM permite crear varios usuarios y administrar los permisos para cada uno de ellos dentro de su cuenta de AWS. Un usuario es una identidad (dentro de una cuenta de AWS) con credenciales de seguridad únicas que pueden usarse para obtener acceso a los servicios de AWS. Con AWS IAM no tiene que compartir contraseñas ni claves de acceso, y es muy sencillo habilitar o deshabilitar el acceso de un usuario, según proceda.

AWS IAM permite a los clientes implementar prácticas recomendadas de seguridad, como los privilegios mínimos, mediante la concesión de credenciales exclusivas a cada usuario dentro de su cuenta de AWS y concediendo permisos exclusivos para obtener acceso a los servicios y recursos de AWS necesarios para que los usuarios puedan hacer su trabajo. AWS IAM es un servicio seguro de forma predeterminada; los usuarios nuevos no tendrán acceso a AWS hasta que se concedan de forma explícita los permisos.

AWS IAM también se integra con AWS Marketplace para que pueda controlar qué personas de su organización pueden suscribirse al software y los servicios ofrecidos en Marketplace. Como al suscribirse a un determinado programa en Marketplace se inicia una instancia EC2 para ejecutar el software, esta no es una característica importante de control de acceso. Cuando se usa AWS IAM para controlar el acceso a AWS Marketplace, los propietarios de una cuenta de AWS pueden controlar de manera detallada los costos de uso y del software.

AWS IAM le permite minimizar el uso de las credenciales de su cuenta de AWS. Una vez creadas las cuentas de usuario de AWS IAM, todas las interacciones con los servicios y los recursos de AWS deben realizarse con las credenciales de seguridad del usuario de AWS IAM. Encontrará más información acerca de AWS IAM en el sitio web de AWS: http://aws.amazon.com/iam/

Roles

Un rol de IAM usa credenciales de seguridad temporales para que pueda delegar el acceso a usuarios o servicios que normalmente no tienen acceso a los recursos de AWS. Un rol es un conjunto de permisos para obtener acceso a recursos específicos de AWS, pero estos permisos no están asociados a ningún usuario o grupo de IAM específico. Una entidad autorizada (como un usuario móvil o una instancia EC2) asume un rol y recibe credenciales de seguridad temporales para autenticarse en los recursos definidos en el rol. Las credenciales de seguridad temporales proporcionan mayor seguridad debido a su breve vigencia (el período de vencimiento predeterminado es de 12 horas) y al hecho de que no se pueden reutilizar cuando vencen. Esto puede ser especialmente útil al proporcionar acceso controlado limitado en determinadas situaciones:

- **Acceso a usuarios federados (fuera de AWS).** Los usuarios federados son usuarios (o aplicaciones) que no tienen cuentas de AWS. Con los roles, puede otorgarles acceso a sus recursos de AWS durante un período de tiempo limitado. Esto es útil si tiene usuarios que no utilizan AWS que puede autenticar con un servicio externo, como Microsoft Active Directory, LDAP o Kerberos. Las credenciales de seguridad temporales de AWS usadas con los roles proporcionan federación de identidades entre los usuarios de AWS y los que no utilizan AWS en su sistema de identidad y autorización corporativo.

Si su organización admite SAML 2.0 (Security Assertion Markup Language 2.0), puede crear una relación de confianza entre su organización como proveedor de identidad (IdP) y otras organizaciones como proveedores de servicios. En AWS, puede configurar AWS como el proveedor de servicios y usar SAML para proporcionar a los usuarios el inicio de sesión único (SSO) federado a la consola de administración de AWS o para obtener acceso federado a las llamadas API de AWS.

Los roles también son útiles si crea una aplicación móvil o web que tiene acceso a los recursos de AWS. Los recursos de AWS requieren credenciales de seguridad para solicitudes realizadas mediante programación; sin embargo, no puede incluir credenciales de seguridad de larga duración en su aplicación porque estarían accesibles a los usuarios de la aplicación y serían difíciles de rotar. En lugar de ello, puede permitir que los usuarios inicien sesión en su aplicación mediante Login con Amazon, Facebook o Google, y usar la información de autenticación para asumir un rol y obtener credenciales de seguridad temporales.

- **Acceso entre cuentas.** Para las organizaciones que usan varias cuentas de AWS para administrar los recursos, se pueden definir roles para proporcionar a los usuarios que tienen permisos en una cuenta acceso a los recursos bajo otra cuenta. Para las organizaciones que tienen empleados que solo en contadas ocasiones necesitan obtener acceso a los recursos bajo otra cuenta, el uso de roles ayuda a garantizar que las credenciales se proporcionen temporalmente solo cuando sea necesario.
- **Aplicaciones que se ejecutan en instancias EC2 que necesitan obtener acceso a recursos de AWS.** Si una aplicación se ejecuta en una instancia Amazon EC2 y necesita realizar solicitudes de recursos de AWS como buckets de Amazon S3 o una tabla de DynamoDB, necesita tener credenciales de seguridad. El uso de roles en lugar de crear cuentas de IAM individuales para cada aplicación en cada instancia puede ahorrar mucho tiempo a los clientes que administran una gran cantidad de instancias o un grupo de instancias de escalado elástico mediante la función Auto Scaling de AWS.

Las credenciales temporales incluyen un token de seguridad, un ID de clave de acceso y una clave de acceso secreta. Para proporcionar a un usuario acceso a determinados recursos, distribuye las credenciales de seguridad temporales al usuario al que desea conceder acceso temporal. Cuando el usuario realiza llamadas a los recursos, pasa 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. El modo en que el usuario pasa el token depende de la API y de la versión del producto de AWS al que llama el usuario. Encontrará más información acerca de las credenciales de seguridad temporales en el sitio web de AWS: http://docs.amazonwebservices.com/STS

El uso de credenciales temporales implica un nivel de protección adicional porque no tiene que administrar ni distribuir credenciales de larga duración a usuarios temporales. Además, las credenciales temporales se cargan automáticamente en la instancia de destino, por lo que no tiene que incluirlas en ningún lugar poco seguro como su código. Las credenciales temporales rotan o cambian automáticamente varias veces al día, sin ninguna acción por su parte, y se almacenan de forma segura de manera predeterminada.

Encontrará más información sobre el uso de roles de IAM para aprovisionar automáticamente claves en instancias EC2 en la guía de uso de IAM, en el sitio web de AWS: http://docs.amazonwebservices.com/IAM

Seguridad de Amazon CloudWatch

Amazon CloudWatch es un servicio web que permite la monitorización de recursos en la nube de AWS, empezando por Amazon EC2. Ofrece a los clientes visibilidad sobre el uso de los recursos, el desempeño de las operaciones y patrones generales de demanda como, por ejemplo, métricas de uso de CPU, operaciones de lectura y escritura en disco y tráfico de red. Puede configurar alarmas de CloudWatch que le avisen si se superan determinados umbrales o para realizar otras acciones automatizadas como añadir o eliminar instancias EC2 si Auto-Scaling está habilitado.

CloudWatch captura y agrupa métricas de uso de forma nativa para los recursos de AWS, pero puede enviar también otros logs a CloudWatch para su monitorización. Puede enviar archivos log personalizados, del SO invitado y de las aplicaciones para el software instalado en sus instancias EC2 a CloudWatch, donde se almacenan todo el tiempo que desee. Puede configurar CloudWatch para que monitorice las entradas log entrantes para cualquier símbolo o mensaje que desee y mostrar los resultados como métricas de CloudWatch. Podría, por ejemplo, monitorizar los archivos log del servidor web para los errores 404 para detectar enlaces de entrada erróneos o mensajes de usuario no válidos, con el fin de detectar intentos de inicio de sesión no autorizados en el sistema operativo invitado.

Amazon CloudWatch requiere, como todos los servicios de AWS, que cada solicitud realizada a su API de control se autentique para que solo los usuarios autenticados puedan obtener acceso a CloudWatch y administrar este servicio. Las solicitudes se firman con una firma HMAC-SHA1 calculada a partir de una solicitud y la clave privada del usuario. Además, a la API de control de Amazon CloudWatch solo se puede tener acceso a través de los puntos de enlace cifrados por SSL.

Puede controlar aún más el acceso a Amazon CloudWatch mediante la creación de usuarios en su cuenta de AWS usando AWS IAM, y controlando a qué operaciones de CloudWatch pueden llamar esos usuarios.

Seguridad de AWS CloudHSM

El servicio AWS CloudHSM ofrece a los clientes acceso dedicado a un módulo de seguridad por hardware (HSM), que está diseñado para proporcionar almacenamiento seguro de claves de cifrado y operaciones dentro de un dispositivo resistente a intrusiones y antimanipulación. Puede crear, almacenar y administrar de manera segura las claves utilizadas para el cifrado de datos de modo que solo sean accesibles para usted. Los dispositivos AWS CloudHSM se han diseñado para almacenar y procesar de forma segura las claves de cifrado para distintos usos, como el cifrado de bases de datos, la administración de derechos digitales (DRM), la infraestructura de clave pública (PKI), la autenticación y autorización, la firma de documentos y el procesamiento de transacciones. Admiten algunos de los algoritmos criptográficos más seguros disponibles, como AES, RSA y ECC, entre otros muchos.

El servicio AWS CloudHSM se ha diseñado para su uso con Amazon EC2 y VPC, y dispone de su propia dirección IP privada dentro de una subred privada. Puede conectarse a dispositivos CloudHSM desde sus servidores EC2 a través de SSL/TLS, que usa la autenticación bidireccional de certificados digitales y el cifrado SSL de 256 bits para proporcionar un canal de comunicación seguro.

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

Antes de empezar a usar un HSM, debe configurar al menos una partición en el dispositivo. Una partición criptográfica es un límite de seguridad lógico y físico que restringe el acceso a sus claves, por lo que solo usted controla sus claves y las operaciones que realiza el HSM. AWS dispone de credenciales administrativas para el dispositivo, pero dichas credenciales solo se pueden utilizar para realizar tareas de administración en este, no en las particiones del HSM. AWS utiliza estas credenciales para realizar tareas de mantenimiento y monitorizar el estado y la disponibilidad del dispositivo. AWS no puede extraer sus claves ni ordenar al dispositivo que realice operaciones criptográficas con ellas.

El dispositivo HSM dispone de detección de intrusiones físicas y lógicas, y un mecanismo de respuesta que borra las claves de cifrado y crea registros de eventos si se detectan intrusiones. El HSM se ha diseñado para detectar intrusiones si se traspasa la barrera física del dispositivo. Además, tras tres intentos fallidos para obtener acceso a una partición del HSM con credenciales de administración del HSM, el dispositivo borra sus particiones.

Cuando termine su suscripción a CloudHSM y una vez que haya confirmado que ya no necesita el contenido del HSM, debe borrar todas las particiones y su contenido, así como todos los logs. Como parte del proceso de retirada, AWS restablece el dispositivo, borrando permanentemente todo el material de claves.

Seguridad de AWS CloudTrail

AWS CloudTrail proporciona un registro de todas las acciones realizadas por los usuarios y el sistema que afectan a los recursos de AWS en su cuenta. Para cada evento registrado, puede ver a qué servicio se obtuvo acceso, qué acción se realizó, los parámetros de la acción y quién hizo la solicitud. Para las acciones de mutación, puede ver los resultados de la acción. No solo puede saber qué usuario o servicio ha realizado una acción en un servicio de AWS, sino también si fue un usuario de la cuenta raíz de AWS o un usuario de IAM, o si se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado quien realizó la acción.

CloudTrail captura básicamente la información de cada llamada API a un recurso de AWS, tanto si la llamada se hizo desde la consola de administración de AWS o CLI como desde un SDK. Si la solicitud de la API devuelve un error, CloudTrail proporciona la descripción del error, incluidos los mensajes de los errores de autorización. Incluso captura los eventos de inicio de sesión en la consola de administración de AWS, creando un log cada vez que un propietario

de una cuenta de AWS, un usuario federado o un usuario de IAM inicia sesión en la consola.

Una vez activado CloudTrail, los logs de eventos se envían cada cinco minutos al bucket de Amazon S3 que elija. Los archivos log están organizados por ID de cuenta de AWS, región, nombre del servicio, fecha y hora. Puede configurar CloudTrail para que agrupe los archivos log de varias regiones o cuentas en un solo bucket de Amazon S3. De forma predeterminada, se creará un único registro de seguimiento y se enviarán eventos de todas las regiones actuales y futuras. Además de a S3, puede enviar eventos a CloudWatch Logs, para métricas y alarmas personalizadas, o puede cargar los archivos log en las soluciones de administración y análisis de archivos log que desee para realizar un análisis de seguridad y detectar los patrones de comportamiento de los usuarios. Si desea una respuesta rápida, puede crear reglas de eventos de CloudWatch para actuar inmediatamente ante determinados eventos.

De forma predeterminada, los archivos log se almacenan indefinidamente. Los archivos log se cifran automáticamente mediante el servicio S3's Server Side Encryption de Amazon y permanecerán en el bucket hasta que decida eliminarlos o archivarlos. Para disfrutar de mayor seguridad, puede usar KMS para cifrar los archivos log mediante una clave que usted posea. Puede usar las reglas de configuración del ciclo de vida de Amazon S3 para eliminar automáticamente los archivos log antiguos o archivarlos en Amazon Glacier para conservarlos durante más tiempo.

Si habilita la validación de archivos log opcional, podrá cerciorarse de que no se hayan añadido archivos log o de que no se hayan eliminado o manipulado.

Al igual que con cualquier otro servicio de AWS, puede limitar el acceso a CloudTrail solo a determinados usuarios. Puede usar IAM para controlar qué usuarios de AWS pueden crear, configurar o eliminar registros de AWS CloudTrail, así como qué usuarios pueden iniciar y detener el registro. Puede controlar el acceso a los archivos log aplicando políticas de IAM o de bucket de Amazon S3. Puede añadir una capa de seguridad adicional habilitando la opción MFA Delete en su bucket de Amazon S3.

Servicios para móviles

Los servicios móviles de AWS le permiten crear, distribuir, ejecutar, monitorizar, optimizar y escalar fácilmente sus aplicaciones basadas en la nube para dispositivos móviles. Estos servicios le ayudan también a autenticar a los usuarios en su aplicación móvil, sincronizar los datos y recopilar y analizar el uso de la aplicación.

Amazon Cognito

Amazon Cognito proporciona servicios de identidad y sincronización para aplicaciones móviles y web. Simplifica la tarea de autenticar a los usuarios y de almacenar, administrar y sincronizar sus datos entre varios dispositivos, plataformas y aplicaciones. Proporciona credenciales temporales con privilegios limitados a los usuarios autenticados y no autenticados sin tener que administrar ninguna infraestructura interna.

Cognito funciona con proveedores de identidad populares 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 proporcionadas por estos servicios, en lugar de tener que crear y mantener las suyas propias. Su aplicación se autentica con uno de estos proveedores de identidad mediante el SDK del proveedor. Una vez que el usuario final está autenticado con el proveedor, la aplicación transfiere el token de OAuth u OpenID Connect obtenido del proveedor a Cognito, que proporciona un nuevo ID de Cognito para el usuario y un conjunto de credenciales de AWS temporales con privilegios limitados.

Para empezar a usar Amazon Cognito, se crea un grupo de identidades a través de la consola de Amazon Cognito. El grupo de identidades es un almacén de identidades de usuarios específico de su cuenta de AWS. Durante la creación del grupo de identidades, se le pedirá que cree un nuevo rol de IAM o que seleccione uno existente para sus usuarios finales. Un rol de IAM es un conjunto de permisos para obtener acceso a recursos específicos de AWS, pero estos permisos no están asociados a ningún usuario o grupo de IAM específico. Una entidad autorizada (como un usuario móvil o una instancia EC2) asume un rol y recibe credenciales de seguridad temporales para autenticarse en los recursos de AWS definidos en el rol. Las credenciales de seguridad temporales proporcionan mayor seguridad debido a su breve vigencia (el período de vencimiento predeterminado es de 12 horas) y al hecho de que no se pueden

reutilizar cuando vencen. El rol seleccionado afecta a los servicios de AWS a los que pueden tener acceso los usuarios finales 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 Cognito Sync y a Amazon Mobile Analytics. Si su aplicación necesita obtener acceso a otros recursos de AWS como Amazon S3 o DynamoDB, puede modificar sus roles directamente desde la consola de administración de IAM.

Con Amazon Cognito, no es necesario crear cuentas de AWS individuales ni siquiera cuentas de IAM para cada uno de los usuarios finales de sus aplicaciones móviles o web que necesiten tener acceso a los recursos de AWS. Junto con los roles de IAM, los usuarios móviles pueden obtener acceso de forma segura a los recursos de AWS y a las características de la aplicación, e incluso guardar los datos en la nube de AWS sin tener que crear una cuenta o iniciar sesión. Sin embargo, si decide hacer esto más tarde, Cognito combinará los datos y la información de identificación.

Como Amazon Cognito almacena los datos localmente y en el servicio, sus usuarios finales pueden continuar interactuando con los datos aunque trabajen sin conexión. Puede que sus datos sean obsoletos, pero todo aquello que coloquen en el conjunto de datos podrán recuperarlo inmediatamente tanto si están conectados como si no. El SDK del cliente administra una tienda de SQLite local para que la aplicación pueda funcionar aunque no esté conectada. La tienda de SQLite funciona como memoria caché y es el destino 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 extrae o inserta las versiones diferenciales según sea necesario. Tenga en cuenta que para sincronizar los datos entre los dispositivos, su grupo de identidades debe admitir identidades autenticadas. Las identidades sin autenticar están asociadas al dispositivo, así que al menos que el usuario final se autentique no se podrán sincronizar los datos entre varios dispositivos.

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

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

Amazon Mobile Analytics

Amazon Mobile Analytics es un servicio para recopilar, visualizar y comprender los datos de uso de las aplicaciones móviles. Le permite realizar un seguimiento del comportamiento de los clientes, agrupar métricas e identificar patrones relevantes en sus aplicaciones móviles. Amazon Mobile Analytics calcula y actualiza automáticamente las métricas de uso cuando se reciben datos de los dispositivos cliente que ejecutan su aplicación, y muestra los datos en la consola.

Puede integrar Amazon Mobile Analytics con su aplicación sin requerir que los usuarios de la aplicación se autentiquen con un proveedor de identidad (como Google, Facebook o Amazon). Para estos usuarios sin autenticar, Mobile Analytics trabaja con Amazon Cognito para proporcionar credenciales temporales con privilegios limitados. Para ello, primero deberá crear un grupo de identidades en Cognito. El grupo de identidades usará roles de IAM, que son un conjunto de permisos que no están asociados a un usuario o grupo de IAM específico, pero que permiten que una entidad tenga acceso a recursos específicos de AWS. La entidad asume un rol y recibe credenciales de seguridad temporales para autenticarse en 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 Cognito Sync y a Amazon Mobile Analytics. Si su aplicación necesita obtener acceso a otros recursos de AWS como Amazon S3 o DynamoDB, puede modificar sus roles directamente desde la consola de administración de IAM.

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

Aplicaciones

Las aplicaciones de AWS son servicios administrados que le permiten proporcionar a los usuarios almacenamiento centralizado seguro y áreas de trabajo 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. Solo tiene que elegir un grupo de escritorios de Windows 7 que satisfaga las necesidades de los usuarios y el número de escritorios de WorkSpaces que desee iniciar. Cuando los escritorios de WorkSpaces estén listos, los usuarios recibirán un correo electrónico para informarles de dónde descargar el cliente correspondiente para conectarse a su escritorio. Pueden obtener acceso a sus escritorios basados en la nube desde diversos dispositivos de punto de enlace, incluidos PCs, portátiles y dispositivos móviles. Sin embargo, los datos de la organización no se envían ni se almacenan nunca en el dispositivo del usuario final, porque Amazon WorkSpaces usa PC-over-IP (PCoIP), que proporciona una secuencia de vídeo interactiva 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 obtener acceso a su escritorio de WorkSpaces, los usuarios deben iniciar sesión con un conjunto de credenciales exclusivas o con sus credenciales de Active Directory habituales. Cuando integra Amazon WorkSpaces con su directorio corporativo de Active Directory, cada escritorio de WorkSpaces se une al dominio de Active Directory y se puede administrar como los demás escritorios de la organización. Esto significa que puede usar las políticas de grupo de Active Directory para administrar los escritorios de WorkSpaces de los usuarios con el fin de especificar las opciones de configuración que controlan el escritorio. Si decide no usar Active Directory ni otro tipo de directorio local para administrar los escritorios de WorkSpaces de los usuarios, puede crear un directorio en la nube privada dentro de Amazon WorkSpaces, que puede usar para la administración.

Para proporcionar una capa de seguridad adicional, también puede exigir el uso de la autenticación multifactor tras el inicio de sesión en forma de un token de hardware o software. Amazon WorkSpaces permite realizar la autenticación multifactor mediante un servidor Remote Authentication Dial In User Service (RADIUS) local o cualquier proveedor de seguridad que admita la autenticación RADIUS. Actualmente admite los protocolos PAP, CHAP, MS-CHAP1 y MS-CHAP2, junto con proxies RADIUS.

Cada escritorio de WorkSpaces reside en su propia instancia EC2 dentro de una VPC. Puede crear escritorios de WorkSpaces en una VPC que ya tenga o pedir al servicio WorkSpaces que cree uno automáticamente mediante la opción Quick Start (Inicio rápido) de WorkSpaces. Cuando usa la opción Quick Start, WorkSpaces no solo crea la VPC, sino que realiza otras tareas de aprovisionamiento y configuración, como crear un puerto de enlace a Internet para la VPC, configurar un directorio dentro de la VPC que se usa para almacenar la información de los usuarios y los escritorios de WorkSpaces, crear una cuenta de administrador del directorio, crear las cuentas de usuarios especificadas y añadirlas al directorio y crear las instancias de WorkSpaces. Asimismo, la VPC se puede conectar a una red local mediante una conexión de VPN segura para permitir el acceso a un servicio de Active Directory local existente y a otros recursos de la intranet. Puede añadir un grupo de seguridad que haya creado en la VPC de Amazon a todos los escritorios de WorkSpaces que pertenecen a su directorio. De esta forma, puede controlar el acceso de red desde Amazon WorkSpaces en su VPC a otros recursos de la VPC de Amazon y de la red local.

Amazon EBS proporciona almacenamiento persistente para WorkSpaces y se realizan backups automáticos dos veces al día en Amazon S3. Si WorkSpaces Sync está habilitado en un escritorio de WorkSpaces, se realizará un backup constante de la carpeta que el usuario elija y este se almacenará en Amazon S3. También puede usar WorkSpaces Sync en un Mac o un PC para sincronizar documentos desde o hacia su escritorio de WorkSpaces y, de este modo, tener siempre acceso a los datos con independencia del equipo de escritorio que utilice.

Como es un servicio administrado, AWS se ocupa de varias tareas de seguridad y mantenimiento, como backups diarios y aplicación de parches. Las actualizaciones se entregan automáticamente en los escritorios de WorkSpaces durante el período de mantenimiento. Puede controlar cómo se configura la aplicación de parches para un escritorio de WorkSpaces del usuario. Windows Update está activado de forma predeterminada, pero puede personalizar la

configuración o, si lo desea, utilizar un enfoque de administración de parches alternativo. En el caso del sistema operativo subyacente, Windows Update está habilitado de forma predeterminada en WorkSpaces y, además, está configurado para instalar actualizaciones semanalmente. Puede optar por utilizar un enfoque de aplicación de parches alternativo o por configurar Windows Update para que instale las actualizaciones a la hora que elija.

Puede usar IAM para controlar qué miembros de su equipo pueden realizar funciones administrativas, como crear o eliminar escritorios de WorkSpaces o configurar directorios de usuario. También puede configurar un escritorio de WorkSpaces para la administración del directorio, instalar sus herramientas de administración de Active Directory favoritas y crear unidades organizativas y políticas de grupo para aplicar más fácilmente los cambios de Active Directory a todos los usuarios de WorkSpaces.

Amazon WorkDocs

Amazon WorkDocs es un servicio empresarial de almacenamiento y uso compartido administrado con funciones de comentarios para la colaboración de los usuarios. Los usuarios pueden almacenar cualquier tipo de archivo en una carpeta de WorkDocs y permitir que otros usuarios vean o descarguen los archivos. Las funciones de comentarios y anotaciones funcionan en determinados tipos de archivos como MS Word, sin que sea necesario disponer de la aplicación que se usó originalmente para crear el archivo. WorkDocs notifica a los colaboradores las actividades de revisión y los plazos a través del correo electrónico, y controla las versiones de los archivos que ha sincronizado mediante la aplicación WorkDocs Sync.

La información del usuario se almacena en un directorio de red compatible con Active Directory. Puede crear un nuevo directorio en la nube o conectar Amazon WorkDocs a su directorio local. Cuando crea un directorio en la nube mediante la configuración de inicio rápido de WorkDocs, también se crea una cuenta de administrador del directorio con la dirección de correo electrónico del administrador como nombre de usuario. Se envía un correo electrónico al administrador con instrucciones para completar el registro. El administrador usa entonces esta cuenta para administrar el directorio.

Cuando crea un directorio en la nube mediante la configuración de inicio rápido de WorkDocs, también se crea y se configura una VPC para el directorio. Si necesita más control sobre la configuración del directorio, puede elegir la configuración estándar, que le permite especificar su propio nombre de dominio del directorio, además de una de sus VPC existentes para usarla con el directorio. Si desea usar una de sus VPC existentes, la VPC debe tener un puerto de enlace a Internet y al menos dos subredes. Cada una de las subredes debe estar en una zona de disponibilidad diferente.

Mediante la Amazon WorkDocs Management Console, los administradores pueden ver los logs de auditoría para realizar un seguimiento de la actividad de los archivos y usuarios por hora, dirección IP y dispositivo, así como permitir a los usuarios compartir archivos con personas externas a su organización.

Los usuarios pueden controlar quién tiene acceso a los distintos archivos y desactivar la posibilidad de descargar los archivos que comparten.

Todos los datos se transmiten en formato cifrado usando el estándar SSL. Las aplicaciones móviles y web de WorkDocs, así como los clientes de sincronización de escritorio, transmiten los datos directamente a Amazon WorkDocs usando SSL. Los usuarios de WorkDocs pueden utilizar también la autenticación multifactor o MFA, si la organización ha implementado un servidor Radius. MFA usa los siguientes factores: nombre de usuario, contraseña y los métodos admitidos por el servidor Radius. Los protocolos admitidos son PAP, CHAP, MS-CHAPv1 y MS-CHAPv2.

Puede seleccionar la región de AWS donde se almacenan los archivos de cada uno de los sitios de WorkDocs. Amazon WorkDocs está disponible actualmente en las regiones de AWS EE.UU Este (Virginia), EE.UU Oeste (Oregón) y UE (Irlanda). Todos los archivos, comentarios y anotaciones almacenados en WorkDocs se cifran automáticamente con el método de cifrado AES-256.

Revisiones del documento

Fecha	Descripción
Mayo de 2017	Sección añadida sobre las comprobaciones de seguridad de AWS Config.
Abril de 2017	Sección añadida sobre Amazon Elastic File System.
Marzo de 2017	Se ha migrado a un nuevo formato.
Enero de 2017	Regiones actualizadas.