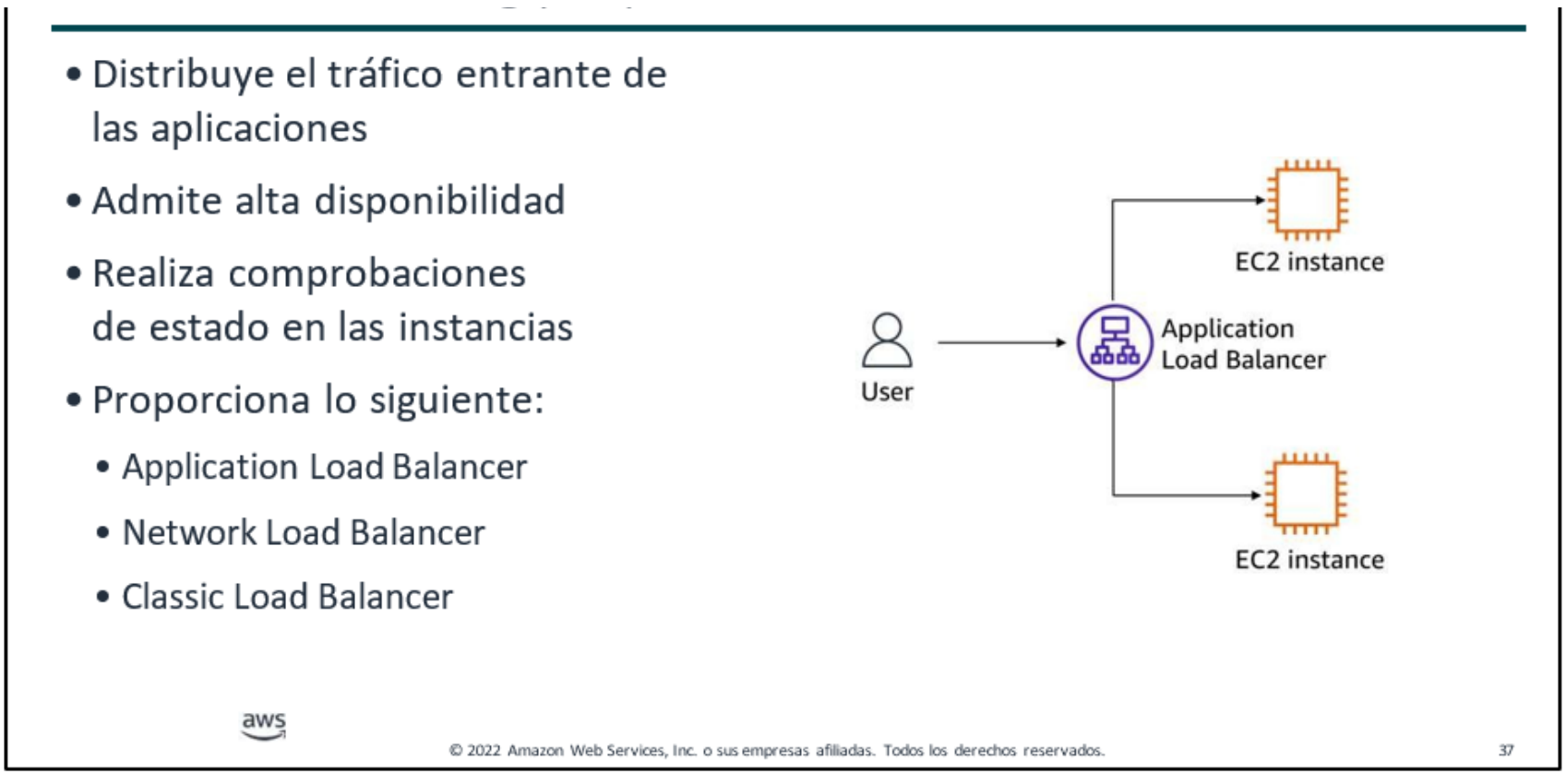
LECCIÓN 5: USO DE EQUILIBRADORES DE CARGA DE AWS, RESUMEN GLOBAL Y PROTECCIÓN DE LOS RECURSOS DE CÓMPUTO

En esta se proporciona información sobre el uso de equilibradores de carga como parte de la seguridad de su infraestructura, resumen global y protección de los recursos de cómputo.

Elastic Load Balancing (ELB)



El diagrama del tráfico de un usuario que se dirige a Application Load Balancer. A continuación, el tráfico se divide entre dos instancias de EC2.

El servicio Elastic Load Balancing (ELB) distribuye automáticamente el tráfico entrante de las aplicaciones entre varios objetivos, como instancias de EC2, contenedores y direcciones IP. Puede configurar el equilibrador de carga para que acepte el tráfico entrante especificando uno o más agentes de escucha. Un agente de escucha es un proceso que verifica las solicitudes de conexión.

ELB escala el balanceador de carga a medida que el tráfico dirigido a la aplicación cambia con el tiempo. Además, es capaz de escalar de forma automática a la mayoría de las cargas de trabajo. Esto aumenta la disponibilidad y la tolerancia a errores de las aplicaciones. Puede agregar y eliminar instancias del balanceador de carga en función de sus necesidades sin interrumpir el flujo general de solicitudes a la aplicación. ELB puede controlar la carga variable del tráfico de su aplicación en una o más zonas de disponibilidad.

También puede configurar comprobaciones de estado, que supervisan el estado de los objetivos registrados. Una vez realizadas las comprobaciones de estado, el dispositivo de equilibrio de carga puede enviar solicitudes solo a los objetivos en buen estado. Cuando el equilibrador de carga detecta un objetivo fuera de estado, detiene el enrutamiento de tráfico al objetivo. El equilibrador de carga reanuda el enrutamiento de tráfico a ese objetivo después de detectar que el objetivo está en buen estado de nuevo.

ELB está integrado con otros servicios populares de AWS, como Amazon EC2 Auto Scaling, Amazon Elastic Container Service (Amazon ECS), AWS CloudFormation y AWS Certificate Manager (ACM).

ELB admite tres tipos de balanceadores de carga: Application, Network y Classic Load Balancers.

Un Application Load Balancer opera a nivel de solicitud y enruta el tráfico a los objetivos (instancias de EC2, contenedores, direcciones IP y funciones de AWS Lambda) en función del contenido de la solicitud. Un Application Load Balancer es ideal para el balanceo de carga avanzado del tráfico HTTP y HTTPS. Este tipo de equilibrador de carga proporciona enrutamiento avanzado de solicitudes orientado a la entrega de arquitecturas de aplicaciones modernas, incluidos microservicios y aplicaciones basadas en contenedores.

Un Application Load Balancer simplifica y mejora la seguridad de su aplicación, garantizando que se utilicen en todo momento los cifrados y protocolos SSL y TLS más recientes.

Un Network Load Balancer opera a nivel de conexión y enruta las conexiones a los objetivos (instancias de EC2, microservicios y contenedores) dentro de una VPC, basándose en los datos del protocolo IP. Un Network Load Balancer es ideal para el balanceo de carga del tráfico TCP y UDP. Este tipo de equilibrador de carga es capaz de administrar millones de peticiones por segundo manteniendo latencias ultrabajas. Un Network Load Balancer está optimizado para administrar patrones de tráfico volátiles y repentinos con una sola dirección IP estática por cada zona de disponibilidad.

El Classic Load Balancer proporciona balanceo de carga básico en varias instancias de EC2 y funciona tanto al nivel de solicitud como al nivel de conexión. Un Classic Load Balancer se destina a las aplicaciones creadas dentro de la red EC2-Classic.
Consulte ¿Qué es Elastic Load Balancing?en la Guía del usuario de ELB en
https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html

Protección de datos en ELB

Primer punto de contacto

Cifrado en reposo

Cifrado en tránsito

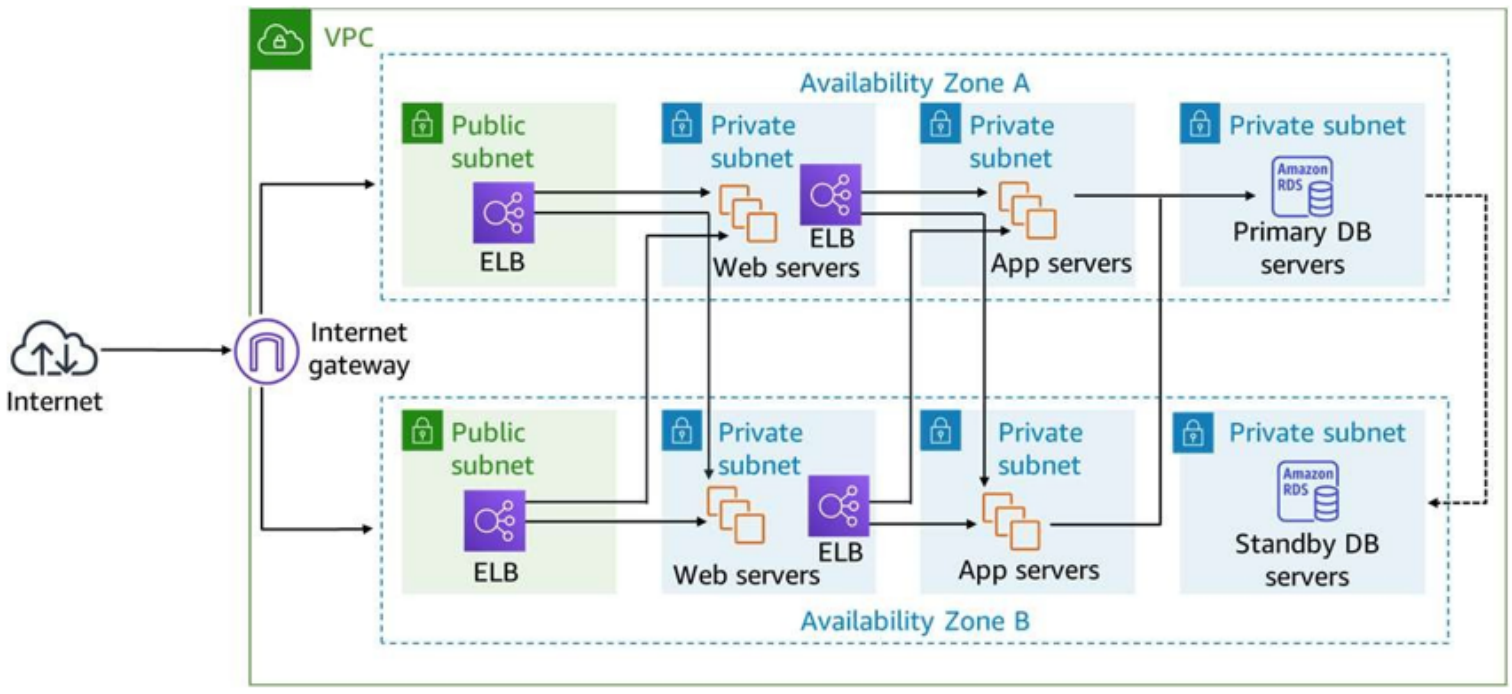
Punto de contacto único: Un equilibrador de carga sirve como único punto de contacto para los clientes. El Load Balancer distribuye el tráfico entrante de las aplicaciones entre varios objetivos, tales como instancias de EC2, en varias zonas de disponibilidad. Esto aumenta la disponibilidad de la aplicación.
Un Application Load Balancer puede mantener una comunicación HTTPS segura y certificados para las comunicaciones con los clientes. Opcionalmente, puede terminar la conexión SSL a nivel del equilibrador de carga para que no necesite manejar certificados en su propia aplicación.

Cifrado en reposo: Si habilita el cifrado del lado del servidor con claves de cifrado administradas de Amazon S3 (SSE-S3) para su bucket de S3 para registros de acceso de ELB, ELB cifra automáticamente cada archivo de registro de acceso antes de almacenarlo en su bucket de S3. ELB también descifra los archivos de registro de acceso cuando se accede a ellos. Cada archivo de registro se cifra con una clave única, que a su vez se cifra con una clave que se rota periódicamente.

Cifrado en tránsito: ELB simplifica el proceso de creación de aplicaciones web seguras mediante la terminación del tráfico HTTPS y TLS de los clientes en el equilibrador de carga. El equilibrador de carga realiza el trabajo de cifrado y descifrado del tráfico, en lugar de requerir que cada instancia de EC2 se encargue del trabajo de terminación de TLS.

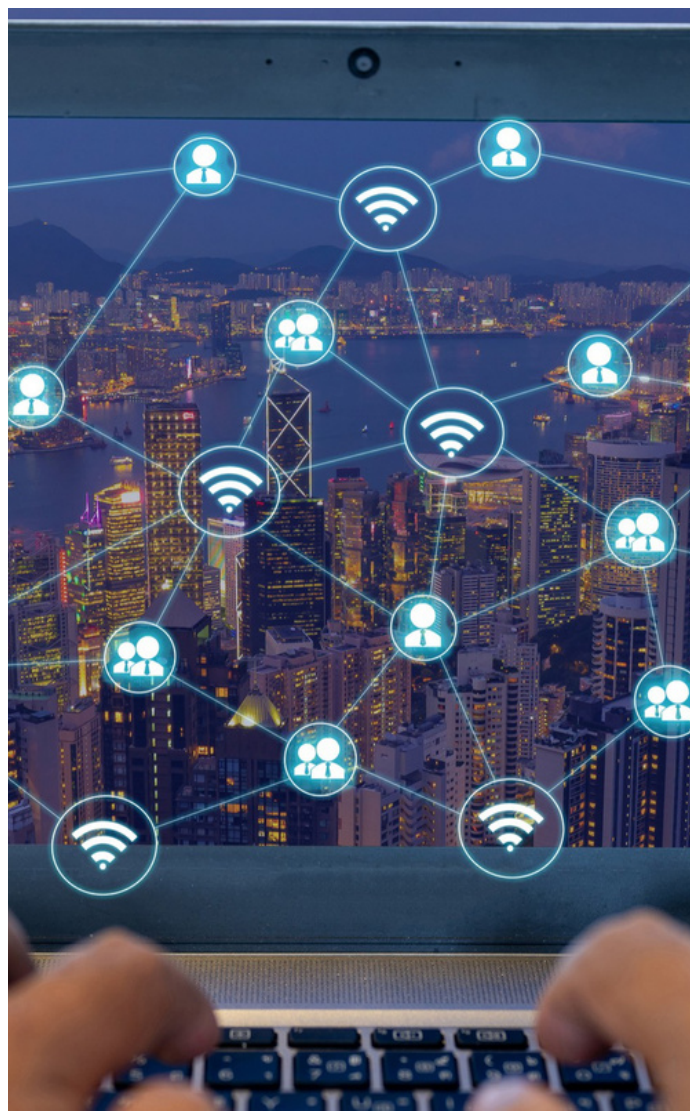
Para más información, consulte Protección de datos en Elastic Load Balancing en la ELB User Guide (Guía del usuario del ELB) en https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/data-protection.html

Equilibradores de carga en acción

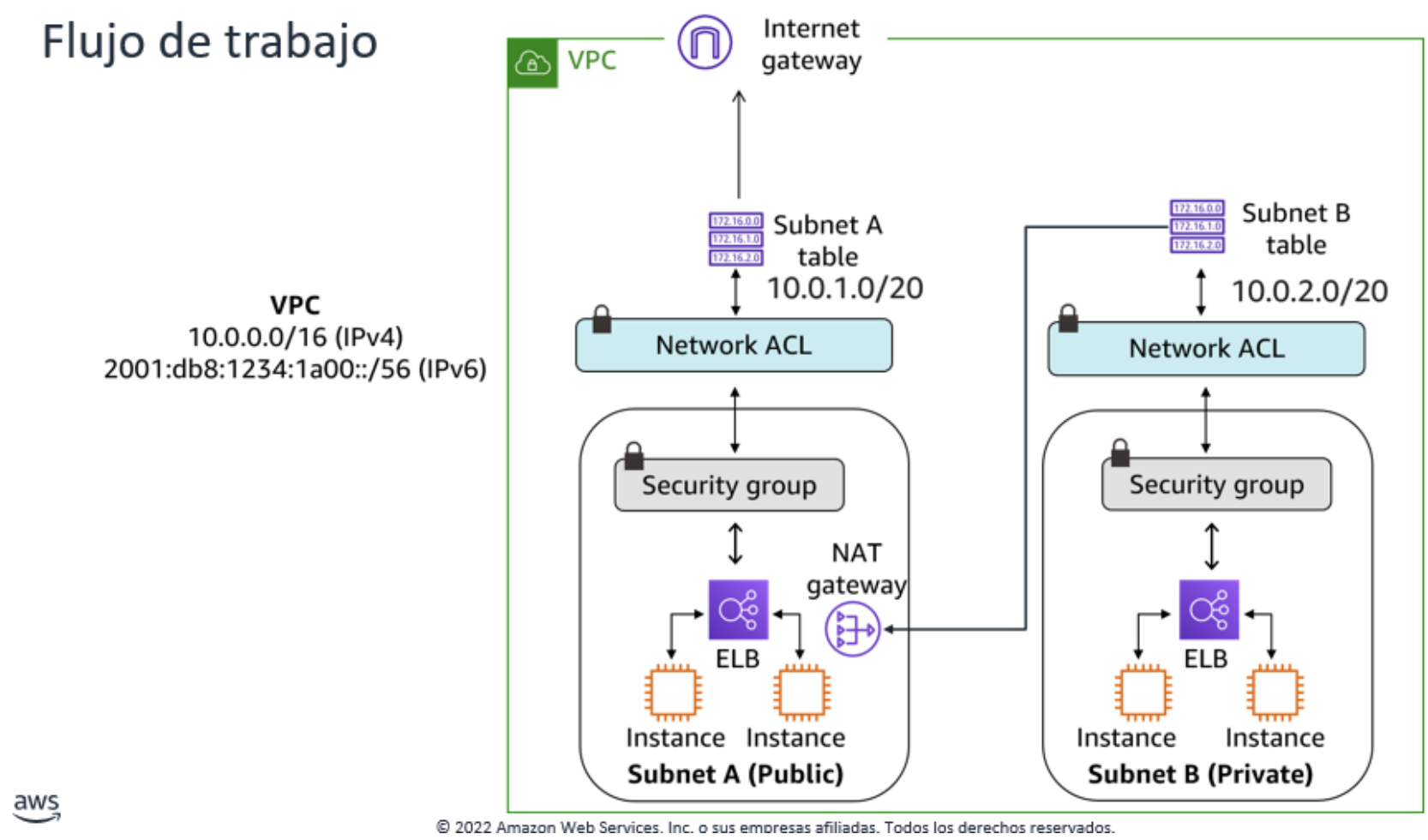


En este diagrama, se muestra cómo funcionan los equilibradores de carga. Esta VPC tiene subredes en dos zonas de disponibilidad. Cada zona de disponibilidad tiene una subred pública y varias subredes privadas.

El tráfico de Internet va de una puerta de enlace de internet a cada zona de disponibilidad. Un equilibrador de carga en cada subred pública dirige el tráfico a los servidores web de una subred privada en cualquiera de las dos zonas de disponibilidad. El tráfico de los servidores web va a un equilibrador de carga, que dirige el tráfico a los servidores de aplicaciones en otra subred privada en cualquiera de las dos zonas de disponibilidad. El tráfico de los servidores de aplicaciones se dirige al servidor de base de datos primaria en otra subred privada de la primera zona de disponibilidad. La base de datos primaria puede comunicarse con un servidor de base de datos en espera en una subred privada de la segunda zona de disponibilidad.



Flujo de trabajo



El diagrama de esta diapositiva muestra cómo funcionan juntos el equilibrio de carga y los componentes de la VPC.

Una VPC tiene dos subredes. La subred A, que es una subred pública, contiene dos instancias de EC2. El tráfico de cada instancia se dirige a través de un equilibrador de carga a un grupo de seguridad y, a continuación, a una red ACL de red. A continuación, el tráfico se encamina a través de una tabla de enrutamiento hacia una puerta de enlace de Internet.

La subred B, que es una subred privada, contiene dos instancias de EC2. El tráfico de cada instancia se dirige a través de un equilibrador de carga a un grupo de seguridad y, a continuación, a una red ACL de red. A continuación, el tráfico se encamina a través de una tabla de enrutamiento a una puerta de enlace NAT en la subred A, la subred pública.

Prácticas recomendadas para proteger su red

- **Controle el tráfico en todas las capas.**
- **Inspeccione y filtre su tráfico a nivel de aplicación.**
- **Automatice la protección de la red.**
- **Limite la exposición**

Una de las prácticas recomendadas para proteger su red es aplicar controles tanto al tráfico entrante como al saliente. Para una VPC, esto incluye el uso de grupos de seguridad, ACL de red y subredes. Utilice subredes en varias zonas de disponibilidad para separar las capas de su aplicación. Configure grupos de seguridad y ACL de red para permitir únicamente el tráfico entrante y saliente necesario.

Otra práctica recomendada consiste en inspeccionar y filtrar el tráfico de red a nivel de aplicación.

Además, utilice la inteligencia sobre amenazas y la detección de anomalías para automatizar los mecanismos de protección y proporcionar una red de autodefensa.

Por último, límite la exposición de la carga de trabajo a internet y a las redes internas. Para ello, permita el acceso requerido mínimo.

Amazon inspector

• Ejecute evaluaciones de seguridad automatizadas en instancias y aplicaciones de EC2

• Detecte problemas de seguridad en las aplicaciones.

• Aplique estándares de y prácticas recomendadas.

• Genere informes de evaluación

Amazon Inspector

Amazon Inspector es un servicio automatizado de seguridad que ayuda a mejorar la seguridad y la conformidad de las aplicaciones implementadas en AWS. El servicio ayuda a identificar las vulnerabilidades de seguridad y las desviaciones de las prácticas recomendadas de seguridad en las aplicaciones, tanto antes de que se implementen como mientras se ejecutan en un entorno de producción. Por ejemplo, el servicio puede ayudarle a comprobar la accesibilidad no intencionada a la red de sus instancias de EC2 y las vulnerabilidades de dichas instancias.

Amazon Inspector le ofrece la oportunidad de definir estándares y prácticas recomendadas para sus aplicaciones y validar el cumplimiento de estos estándares. Esto simplifica el proceso de cumplimiento de los estándares y las prácticas recomendadas de seguridad en su organización y ayuda a administrar los problemas de seguridad de forma proactiva antes de que afecten a la aplicación de producción.

Amazon Inspector realiza una evaluación y genera una lista detallada de los resultados vinculados con la seguridad, ordenados por nivel de gravedad. Puede revisar estos hallazgos directamente o como parte de informes de evaluación detallados, que están disponibles a través de la Consola de administración de AWS o la API.

Para más información, consulte Amazon Inspector en https://aws.amazon.com/inspector

Beneficios de seguridad al usar Amazon Inspector

Entre los beneficios de seguridad de Amazon Inspector se incluyen los siguientes:

Automatice tareas para responder a los problemas de seguridad:
Al utilizar eventos de Amazon EventBridge con Amazon Inspector, puede automatizar tareas que le ayuden a responder a los problemas de seguridad que revelen los hallazgos de Amazon Inspector.

Supervisión periódica de sus recursos:
Amazon Inspector ayuda a encontrar vulnerabilidades de seguridad en las aplicaciones y desviaciones de las prácticas recomendadas de seguridad. El servicio detecta estos problemas antes de que su aplicación se implemente y mientras se ejecuta en producción. Esto mejora la seguridad general de sus aplicaciones alojadas en AWS.

Conocimientos de seguridad de AWS:
Amazon Inspector incluye una base de conocimientos de reglas trazadas según las prácticas recomendadas de seguridad comunes y las definiciones de vulnerabilidades. AWS actualiza constantemente las prácticas recomendadas y las reglas de seguridad.

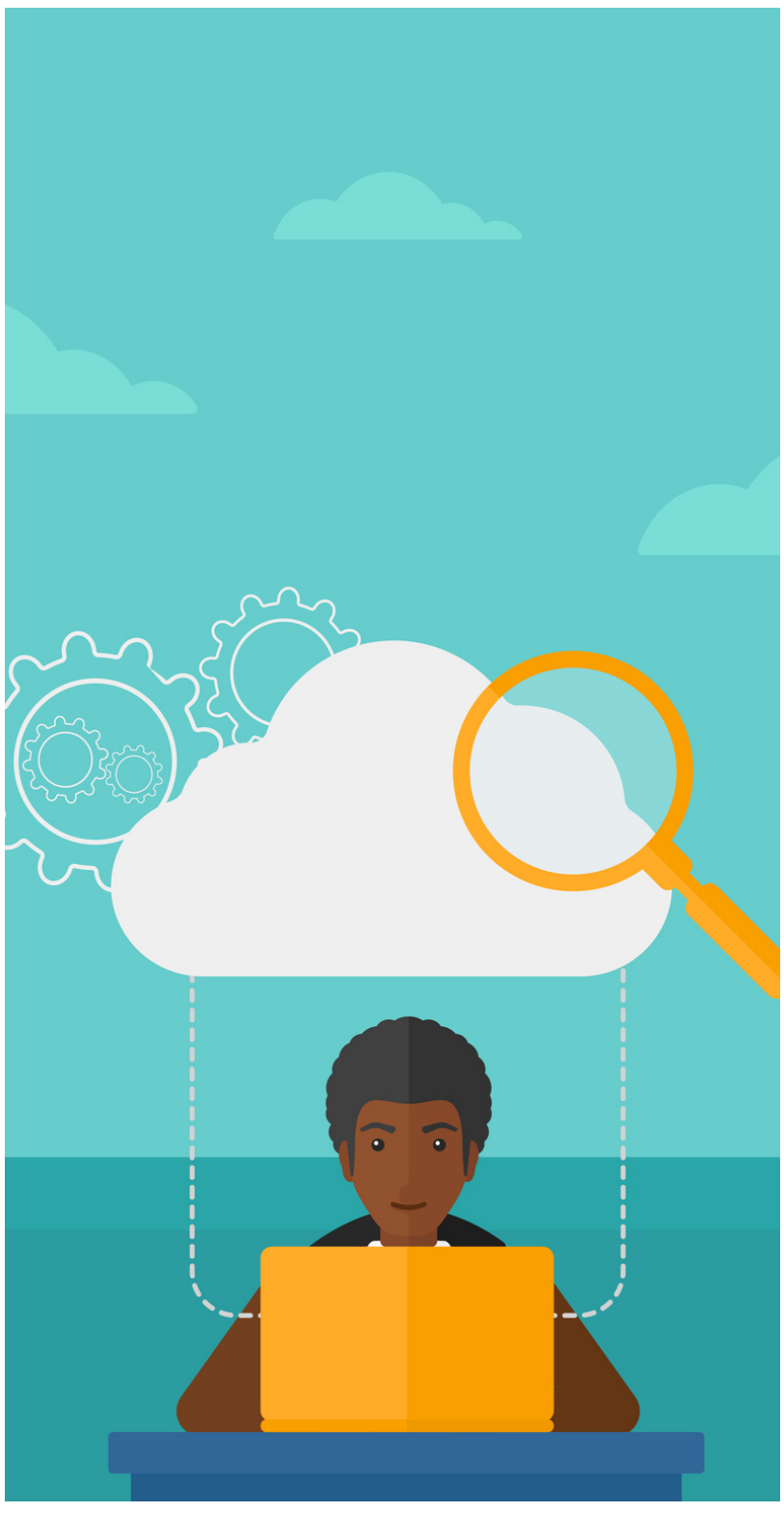
Integración de la seguridad en DevOps:
Amazon Inspector es un servicio vinculado a la API que analiza las configuraciones de red en su cuenta de AWS. Además, el servicio utiliza un agente opcional para la visibilidad de las instancias de EC2. El agente puede ayudarle a integrar las evaluaciones de Amazon Inspector en su proceso DevOps existente. Esto le ayuda a capacitar tanto a los equipos de desarrollo como a los de operaciones para hacer de las evaluaciones de seguridad una parte esencial del proceso de implementación.

AWS Systems Manager

Amazon Inspector utiliza el ampliamente implementado agente AWS Systems Manager (agente SSM) para recopilar el inventario de software y las configuraciones de sus instancias de EC2.

AWS Systems Manager le ofrece visibilidad y control de su infraestructura en AWS. Systems Manager proporciona una interfaz de usuario unificada para que pueda ver los datos operativos de varios servicios de AWS. El servicio incluye funciones que le ayudan a automatizar las tareas de administración. Puede recopilar el inventario del sistema, aplicar parches del sistema operativo, mantener actualizadas las definiciones antivirus y configurar sistemas operativos y aplicaciones a escala. Systems Manager ayuda a mantener la conformidad de los sistemas con las políticas de configuración que haya definido.

Estos son algunos de los aprendizajes clave de esta sección de la unidad



Amazon Inspector es un servicio automatizado de seguridad que ayuda a mejorar la seguridad y la conformidad de las aplicaciones implementadas en AWS.

Systems Manager le ofrece visibilidad y control de su infraestructura en AWS.

Analice periódicamente sus recursos informáticos en busca de vulnerabilidades y aplique los parches que correspondan. Puede automatizar esta tarea utilizando servicios de AWS como Lambda y Systems Manager.