1.- Una empresa tiene una función AWS Lambda que crea miniaturas (thumbnails) a partir de imágenes más grandes. Esta función Lambda necesita permisos de lectura y escritura en un bucket de Amazon S3 dentro de la misma cuenta de AWS.

¿Qué soluciones permitirán que la función Lambda tenga este acceso? (Elige dos opciones).

A. Crear un usuario IAM con acceso solo programático. Generar un nuevo par de claves de acceso. Agregar variables de entorno a la función Lambda con el ID de clave de acceso y la clave secreta. Modificar la función Lambda para que utilice estas variables de entorno durante la ejecución al comunicarse con Amazon S3.

B. Generar un par de claves para Amazon EC2. Almacenar la clave privada en AWS Secrets Manager. Modificar la función Lambda para que recupere la clave privada desde Secrets Manager y la use para comunicarse con Amazon S3.

**C. Crear un rol de IAM para la función Lambda. Adjuntar una política de IAM que permita el acceso al bucket de S3.**

**D. Crear un rol de IAM para la función Lambda. Adjuntar una política de bucket al bucket de S3 que permita el acceso. Especificar el rol de IAM de la función como el principal.**

E. Crear un grupo de seguridad. Asociar el grupo de seguridad a la función Lambda. Adjuntar una política de bucket que permita el acceso al bucket de S3 a través del ID del grupo de seguridad.

2.- Un ingeniero de seguridad está configurando un nuevo sitio web llamado example.com. El ingeniero desea asegurar las comunicaciones con el sitio web exigiendo que los usuarios se conecten a example.com mediante HTTPS.

¿Cuál de las siguientes es una opción válida para almacenar certificados SSL/TLS?

A.- Certificado SSL personalizado almacenado en AWS Key Management Service (AWS KMS)

B-. Certificado SSL predeterminado almacenado en Amazon CloudFront

**C. Certificado SSL personalizado almacenado en AWS Certificate Manager (ACM)**

D. Certificado SSL predeterminado almacenado en Amazon S3

3.- Un ingeniero de seguridad necesita desarrollar un proceso para investigar y responder ante posibles incidentes de seguridad en las instancias Amazon EC2 de una empresa. Todas las instancias EC2 están respaldadas por Amazon Elastic Block Store (Amazon EBS). La empresa utiliza AWS Systems Manager para gestionar todas las instancias EC2 y ha instalado el agente de Systems Manager (SSM Agent) en todas ellas.

El proceso que está desarrollando el ingeniero de seguridad debe cumplir con las mejores prácticas de seguridad de AWS y satisfacer los siguientes requisitos:

• Debe preservarse la memoria volátil y no volátil de cualquier instancia EC2 comprometida, para fines forenses.

• Se debe actualizar la metadata de la instancia comprometida con la información correspondiente al ticket del incidente.

• La instancia comprometida debe permanecer encendida durante la investigación, pero debe ser aislada para evitar la propagación de malware.

• Toda actividad de investigación durante la recolección de datos volátiles debe ser registrada como parte del proceso.

¿Qué combinación de pasos debe seguir el ingeniero de seguridad para cumplir estos requisitos con el menor esfuerzo operativo posible? (Elige tres opciones).

**A. Recolectar la metadata relevante de la instancia EC2 comprometida. Habilitar la protección contra terminación. Aislar la instancia actualizando los grupos de seguridad para restringir el acceso. Separar la instancia de cualquier grupo de Auto Scaling al que pertenezca. Anular el registro de la instancia en cualquier recurso de Elastic Load Balancing (ELB).**

B. Recolectar la metadata relevante de la instancia EC2 comprometida. Habilitar la protección contra terminación. Mover la instancia a una subred de aislamiento que deniegue todo el tráfico de origen y destino. Asociar la instancia a dicha subred para restringir el acceso. Separarla de cualquier grupo de Auto Scaling y anular su registro en recursos ELB.

**C. Usar Systems Manager Run Command para ejecutar scripts que recolecten datos volátiles.**

D. Establecer una sesión SSH en Linux o RDP en Windows con la instancia EC2 comprometida para ejecutar scripts que recolecten datos volátiles.

**E. Crear una snapshot del volumen EBS de la instancia EC2 comprometida para investigaciones posteriores. Etiquetar la instancia con la metadata e información del ticket del incidente.**

F.- Crear una asociación en Systems Manager State Manager para generar una snapshot del volumen EBS de la instancia comprometida. Etiquetar la instancia con la metadata e información del ticket del incidente.

4.- Una empresa tiene una organización en AWS Organizations. La empresa quiere usar AWS CloudFormation StackSets dentro de la organización para implementar varios patrones de diseño de AWS en diferentes entornos. Estos patrones incluyen instancias de Amazon EC2, balanceadores de carga de Elastic Load Balancing (ELB), bases de datos de Amazon RDS, y clústeres de Amazon EKS o Amazon ECS.

Actualmente, los desarrolladores de la empresa pueden crear sus propias pilas (stacks) de CloudFormation para aumentar la velocidad general de entrega. Un pipeline de CI/CD centralizado, ubicado en una cuenta de servicios compartidos, se encarga de desplegar cada stack de CloudFormation.

El equipo de seguridad de la empresa ya ha definido los requisitos para cada servicio, de acuerdo con los estándares internos. Si se detectan recursos que no cumplen con dichos estándares, el equipo de seguridad debe ser notificado para tomar las acciones necesarias. Además, la solución de notificación debe permitir que los desarrolladores mantengan la misma velocidad de entrega que tienen actualmente.

¿Qué solución cumplirá con estos requisitos de la forma más eficiente desde el punto de vista operativo?

A. Crear un tema de Amazon SNS. Suscribir las direcciones de correo del equipo de seguridad al tema. Crear una función personalizada en AWS Lambda que ejecute el comando aws cloudformation validate-template de la CLI de AWS sobre todas las plantillas de CloudFormation antes de la etapa de construcción en el pipeline de CI/CD. Configurar el pipeline para enviar una notificación al tema SNS si se detectan problemas.

**B. Crear un tema de Amazon SNS. Suscribir las direcciones de correo del equipo de seguridad al tema. Crear reglas personalizadas con CloudFormation Guard para cada tipo de recurso. En el pipeline de CI/CD, antes de la etapa de construcción, configurar una imagen de Docker para ejecutar el comando cfn-guard sobre la plantilla de CloudFormation. Configurar el pipeline (CI/CD) para enviar una notificación al tema SNS si se detectan problemas.**

C. Crear un tema de Amazon SNS y una cola de Amazon SQS. Suscribir las direcciones de correo del equipo de seguridad al tema SNS. Crear un bucket de Amazon S3 en la cuenta de servicios compartidos. Incluir una notificación de eventos para publicar en la cola SQS cuando se agreguen nuevos objetos al bucket. Requerir que los desarrolladores suban sus plantillas de CloudFormation a este bucket. Lanzar instancias EC2 que se escalen automáticamente según la profundidad de la cola SQS. Configurar las instancias EC2 para que usen CloudFormation Guard para analizar las plantillas y desplegarlas si no hay problemas. Configurar el pipeline de CI/CD para que envíe una notificación al tema SNS si se detectan problemas.

D. Crear un StackSet centralizado de CloudFormation que incluya un conjunto estándar de recursos que los desarrolladores puedan implementar en cada cuenta de AWS. Configurar cada plantilla de CloudFormation para que cumpla con los requisitos de seguridad. Para cualquier nuevo recurso o configuración, actualizar la plantilla de CloudFormation y enviarla al equipo de seguridad para revisión. Una vez completada la revisión, agregar el nuevo stack de CloudFormation al repositorio para que los desarrolladores puedan usarlo.

5.- Una empresa está migrando uno de sus sistemas heredados desde un centro de datos local hacia AWS. El servidor de aplicaciones se ejecutará en AWS, pero la base de datos debe permanecer en el centro de datos local por razones de cumplimiento.

La base de datos es sensible a la latencia de red. Además, los datos que viajan entre el centro de datos local y AWS deben estar cifrados con IPsec.

¿Qué combinación de soluciones de AWS cumplirá con estos requisitos? (Elige dos opciones).

**A. AWS Site-to-Site VPN**

**B. AWS Direct Connect**

C. AWS VPN CloudHub

D. Emparejamiento de VPC (VPC peering)

E. Gateway NAT

6.- Una empresa tiene una aplicación que utiliza docenas de tablas de Amazon DynamoDB para almacenar datos. Los auditores detectan que estas tablas no cumplen con la política de protección de datos de la empresa.

La política de retención de datos establece que todos los datos deben respaldarse dos veces al mes: una vez a medianoche del día 15 y otra vez a medianoche del día 25 de cada mes. Además, la empresa debe conservar los respaldos durante 3 meses.

¿Qué combinación de pasos debe seguir un ingeniero de seguridad para cumplir con estos requisitos? (Elige dos opciones).

A. Usar la capacidad de respaldo bajo demanda de DynamoDB para crear un plan de respaldo. Configurar una política de ciclo de vida para que los respaldos expiren después de 3 meses.

B. Usar AWS DataSync para crear un plan de respaldo. Agregar una regla de respaldo que incluya un período de retención de 3 meses.

**C. Usar AWS Backup para crear un plan de respaldo. Agregar una regla de respaldo que incluya un período de retención de 3 meses.**

**D. Establecer la frecuencia de respaldo usando una expresión de cron. Asignar cada tabla de DynamoDB al plan de respaldo.**

E. Establecer la frecuencia de respaldo usando una expresión de programación por intervalo (rate). Asignar cada tabla de DynamoDB al plan de respaldo.

7.- Una empresa necesita que un ingeniero de seguridad implemente una solución escalable para autenticación y autorización entre múltiples cuentas. La solución no debe agregar componentes arquitectónicos que los usuarios deban administrar. Se deben usar características nativas de AWS tanto como sea posible.

El ingeniero de seguridad ya ha configurado AWS Organizations con todas las funciones activadas y ha habilitado AWS IAM Identity Center (anteriormente AWS Single Sign-On).

¿Qué pasos adicionales debe seguir el ingeniero de seguridad para completar esta tarea?

A. Usar AD Connector para crear usuarios y grupos para todos los empleados que necesitan acceso a las cuentas de AWS. Asignar los grupos de AD Connector a las cuentas de AWS y vincularlos con roles de IAM según las funciones laborales y necesidades de acceso de los empleados. Indicar a los empleados que accedan a las cuentas de AWS mediante el portal de usuario de AWS Directory Service.

**B. Usar un directorio predeterminado de IAM Identity Center para crear usuarios y grupos para todos los empleados que necesitan acceso a las cuentas de AWS. Asignar grupos a las cuentas de AWS y vincularlos con conjuntos de permisos según las funciones laborales y necesidades de acceso de los empleados. Indicar a los empleados que accedan a las cuentas de AWS mediante el portal de usuario de IAM Identity Center.**

C. Usar un directorio predeterminado de IAM Identity Center para crear usuarios y grupos para todos los empleados que necesitan acceso a las cuentas de AWS. Vincular los grupos de IAM Identity Center con los usuarios de IAM existentes en todas las cuentas para heredar los permisos actuales. Indicar a los empleados que accedan a las cuentas de AWS mediante el portal de usuario de IAM Identity Center.

D. Usar AWS Directory Service para Microsoft Active Directory para crear usuarios y grupos para todos los empleados que necesitan acceso a las cuentas de AWS. Habilitar el acceso a la consola de administración de AWS en el directorio creado y especificar a IAM Identity Center como fuente de información para cuentas integradas y conjuntos de permisos. Indicar a los empleados que accedan a las cuentas de AWS mediante el portal de usuario de AWS Directory Service.

8.- Una empresa ha implementado Amazon GuardDuty y ahora quiere automatizar la respuesta ante posibles amenazas. La empresa ha decidido comenzar con los ataques por fuerza bruta RDP que provienen de instancias de Amazon EC2 dentro del entorno de AWS de la empresa.

Un ingeniero de seguridad necesita implementar una solución que bloquee la comunicación detectada desde una instancia sospechosa hasta que se pueda realizar una investigación y, si es necesario, aplicar medidas correctivas.

¿Qué solución cumplirá con estos requisitos?

A. Configurar GuardDuty para enviar el evento a un flujo de datos de Amazon Kinesis. Procesar el evento con una aplicación de Amazon Kinesis Data Analytics for Apache Flink que envíe una notificación a la empresa mediante Amazon SNS. Agregar reglas a la lista de control de acceso de red (NACL) para bloquear el tráfico hacia y desde la instancia sospechosa.

B. Configurar GuardDuty para enviar el evento a Amazon EventBridge. Implementar un ACL web de AWS WAF. Procesar el evento con una función de AWS Lambda que envíe una notificación a la empresa mediante Amazon SNS y que agregue una regla en el ACL web para bloquear el tráfico hacia y desde la instancia sospechosa.

**C. Habilitar AWS Security Hub para que reciba los hallazgos de GuardDuty y enviar el evento a Amazon EventBridge. Implementar AWS Network Firewall. Procesar el evento con una función de AWS Lambda que agregue una regla a una política de firewall de Network Firewall para bloquear el tráfico hacia y desde la instancia sospechosa.**

D. Habilitar AWS Security Hub para recibir los hallazgos de GuardDuty. Configurar un flujo de datos de Amazon Kinesis como destino de eventos de Security Hub. Procesar el evento con una función de AWS Lambda que reemplace el grupo de seguridad de la instancia sospechosa por uno que no permita ninguna conexión.

9.-Una empresa tiene una cuenta de AWS que aloja una aplicación en producción. La empresa recibe una notificación por correo electrónico de que Amazon GuardDuty ha detectado un hallazgo del tipo Impact:IAMUser/AnomalousBehavior en la cuenta.

Un ingeniero de seguridad necesita ejecutar el procedimiento de respuesta (playbook) para investigar este incidente de seguridad, y debe recopilar y analizar la información sin afectar la aplicación.

¿Qué solución permitirá cumplir con estos requisitos de la manera más rápida posible?

A. Iniciar sesión en la cuenta de AWS usando credenciales de solo lectura. Revisar el hallazgo de GuardDuty para obtener detalles sobre las credenciales de IAM utilizadas. Usar la consola de IAM para agregar una política DenyAll al principal de IAM.

**B. Iniciar sesión en la cuenta de AWS usando credenciales de solo lectura. Revisar el hallazgo de GuardDuty para determinar qué llamadas a la API generaron el hallazgo. Usar Amazon Detective para revisar las llamadas a la API en su contexto.**

C. Iniciar sesión en la cuenta de AWS usando credenciales de administrador. Revisar el hallazgo de GuardDuty para obtener detalles sobre las credenciales de IAM utilizadas. Usar la consola de IAM para agregar una política DenyAll al principal de IAM.

D. Iniciar sesión en la cuenta de AWS usando credenciales de solo lectura. Revisar el hallazgo de GuardDuty para determinar qué llamadas a la API generaron el hallazgo. Usar AWS CloudTrail Insights y AWS CloudTrail Lake para revisar las llamadas a la API en su contexto.

10.- La Empresa A tiene una cuenta de AWS llamada Cuenta A. Recientemente, la Empresa A adquirió a la Empresa B, que tiene una cuenta de AWS llamada Cuenta B. La Empresa B almacena sus archivos en un bucket de Amazon S3.

Los administradores necesitan dar a un usuario de la Cuenta A acceso completo al bucket de S3 en la Cuenta B.

Después de ajustar los permisos de IAM para el usuario en la Cuenta A para que pueda acceder al bucket en la Cuenta B, el usuario todavía no puede acceder a ningún archivo en el bucket de S3.

¿Qué solución resolverá este problema?

A. En la Cuenta B, crear una ACL del bucket para permitir que el usuario de la Cuenta A acceda al bucket de S3.

B. En la Cuenta B, crear una ACL de objetos para permitir que el usuario de la Cuenta A acceda a todos los objetos del bucket de S3.

**C. En la Cuenta B, crear una política de bucket que permita al usuario de la Cuenta A acceder al bucket de S3.**

D. En la Cuenta B, crear una política de usuario que permita al usuario de la Cuenta A acceder al bucket de S3

11.-Una empresa desea recibir una notificación por correo electrónico sobre hallazgos críticos en AWS Security Hub. La empresa no cuenta con una arquitectura existente que permita esta funcionalidad.

¿Qué solución cumplirá con este requisito?

A. Crear una función de AWS Lambda para identificar hallazgos críticos de Security Hub. Crear un tema de Amazon SNS como destino de la función Lambda. Suscribir una dirección de correo electrónico al tema de SNS para recibir los mensajes publicados.

B. Crear un flujo de entrega de Amazon Kinesis Data Firehose. Integrar el flujo con Amazon EventBridge. Crear una regla de EventBridge con un filtro para detectar hallazgos críticos de Security Hub. Configurar el flujo para enviar los hallazgos a una dirección de correo electrónico.

C. Crear una regla de Amazon EventBridge para detectar hallazgos críticos de Security Hub. Crear un tema de Amazon SNS como destino de la regla de EventBridge. Suscribir una dirección de correo electrónico al tema de SNS para recibir los mensajes publicados.

**D. Crear una regla de Amazon EventBridge para detectar hallazgos críticos de Security Hub. Crear un tema de Amazon SES como destino de la regla de EventBridge. Usar la API de SES para dar formato al mensaje. Elegir una dirección de correo electrónico como destinatario del mensaje.**

12.- Una empresa internacional ha establecido una nueva unidad de negocio en Corea del Sur. También ha creado una nueva cuenta de AWS para alojar la carga de trabajo correspondiente a esa región. La carga de trabajo se ha implementado en la nueva cuenta dentro de la región ap-northeast-2 (Seúl).

La carga de trabajo consiste en tres grupos de Auto Scaling de instancias EC2. Todas las cargas de trabajo que operan en esta región deben almacenar registros del sistema y de aplicaciones por un período de 7 años.

Un ingeniero de seguridad debe implementar una solución que asegure que no se pierdan los datos de registro (logs) de cada instancia durante actividades de escalado, y que también se mantengan los logs solo durante el período requerido de 7 años.

¿Qué combinación de pasos debe seguir el ingeniero de seguridad para cumplir con estos requisitos? (Elige tres opciones).

**A. Asegurarse de que el agente de Amazon CloudWatch esté instalado en todas las instancias EC2 que lanzan los grupos de Auto Scaling. Generar un archivo de configuración del agente de CloudWatch para reenviar los logs requeridos a Amazon CloudWatch Logs.**

**B. Establecer la retención de los grupos de logs deseados en 7 años.**

C. Adjuntar un rol de IAM a la configuración de lanzamiento o plantilla de lanzamiento que utilizan los grupos de Auto Scaling. Configurar el rol para proporcionar los permisos necesarios para reenviar los logs a Amazon CloudWatch Logs.

D. Adjuntar un rol de IAM a la configuración de lanzamiento o plantilla de lanzamiento que utilizan los grupos de Auto Scaling. Configurar el rol para proporcionar los permisos necesarios para reenviar los logs a Amazon S3.

E. Asegurarse de que haya una aplicación de reenvío de logs instalada en todas las instancias EC2 que lanzan los grupos de Auto Scaling. Configurar la aplicación para agrupar periódicamente los logs y enviarlos a Amazon S3.

F. Configurar una política de ciclo de vida de Amazon S3 en el bucket de destino para eliminar automáticamente los objetos después de 7 años.

13.- Un ingeniero de seguridad está diseñando una política de IAM para proteger las operaciones de la API de AWS. La política debe exigir el uso de autenticación multifactor (MFA) para que los usuarios de IAM puedan acceder a ciertos servicios en la cuenta de producción de AWS.

Además, cada sesión debe ser válida solo por 2 horas.

La versión actual de la política IAM es la siguiente:

¿Qué combinación de condiciones debe agregar el ingeniero de seguridad a la política IAM para cumplir con estos requisitos? (Elige dos opciones).

**A. "Bool": {"aws:MultiFactorAuthPresent": "true"}**

B. "Bool": {"aws:MultiFactorAuthPresent": "false"}

**C. "NumericLessThan": {"aws:MultiFactorAuthAge": "7200"}**

D. "NumericGreaterThan": {"aws:MultiFactorAuthAge": "7200"}

E. "NumericLessThan": {"MaxSessionDuration": "7200"}

14.- Una empresa utiliza AWS Organizations y tiene cargas de trabajo en producción distribuidas en múltiples cuentas de AWS. Un ingeniero de seguridad necesita diseñar una solución que permita monitorear de forma proactiva comportamientos sospechosos en todas las cuentas que contienen cargas de trabajo en producción.

La solución debe:

Automatizar la remediación de incidentes en todas las cuentas de producción.

Publicar una notificación en un tema de Amazon SNS cuando se detecte un hallazgo crítico de seguridad.

Enviar todos los registros de incidentes de seguridad a una cuenta dedicada.

¿Qué solución cumplirá con estos requisitos?

A. Activar Amazon GuardDuty en cada cuenta de producción. En una cuenta dedicada para registros, agregar todos los logs de GuardDuty desde cada cuenta de producción. Remediar los incidentes configurando GuardDuty para invocar directamente una función de AWS Lambda. Configurar la función Lambda para que también publique notificaciones en el tema de SNS.

B. Activar AWS Security Hub en cada cuenta de producción. En una cuenta dedicada para registros, agregar todos los hallazgos de Security Hub desde cada cuenta de producción. Remediar los incidentes usando AWS Config y AWS Systems Manager. Configurar Systems Manager para que también publique notificaciones en el tema de SNS.

**C. Activar Amazon GuardDuty en cada cuenta de producción. En una cuenta dedicada para registros, agregar todos los logs de GuardDuty desde cada cuenta de producción. Remediar los incidentes usando Amazon EventBridge para invocar una función personalizada de AWS Lambda a partir de los hallazgos de GuardDuty. Configurar la función Lambda para que también publique notificaciones en el tema de SNS.**

D. Activar AWS Security Hub en cada cuenta de producción. En una cuenta dedicada para registros, agregar todos los hallazgos de Security Hub desde cada cuenta de producción. Remediar los incidentes usando Amazon EventBridge para invocar una función personalizada de AWS Lambda a partir de los hallazgos de Security Hub. Configurar la función Lambda para que también publique notificaciones en el tema de SNS.

15.-Una empresa está diseñando una estructura multi-cuenta para sus equipos de desarrollo. Está utilizando AWS Organizations y AWS IAM Identity Center (anteriormente AWS Single Sign-On).

La empresa debe implementar una solución que cumpla con los siguientes requisitos:

Los equipos de desarrollo solo puedan usar regiones específicas de AWS.

Cada cuenta de AWS permita el acceso solo a servicios específicos.

¿Qué solución cumplirá con estos requisitos con el menor esfuerzo operativo posible?

A. Usar IAM Identity Center para configurar roles vinculados a servicios (service-linked roles) con políticas IAM que incluyan los elementos Condition, Resource y NotAction para permitir el acceso solo a las regiones y servicios necesarios.

B. Desactivar AWS STS (Security Token Service) en las regiones que los desarrolladores no tienen permitido usar.

**C. Crear Políticas de Control de Servicios (SCPs) que incluyan los elementos Condition, Resource y NotAction para permitir el acceso solo a las regiones y servicios requeridos.**

D. Para cada cuenta de AWS, crear políticas personalizadas basadas en identidad para IAM Identity Center, usando sentencias que incluyan los elementos Condition, Resource y NotAction para permitir acceso únicamente a las regiones y servicios necesarios.

16.- Una empresa está desarrollando una aplicación de comercio electrónico. La aplicación utiliza instancias de Amazon EC2 y una base de datos Amazon RDS MySQL. Por razones de cumplimiento, los datos deben estar protegidos tanto en tránsito como en reposo. La empresa necesita una solución que minimice el esfuerzo operativo y los costos.

¿Qué solución cumple con estos requisitos?

**A. Usar certificados TLS de AWS Certificate Manager (ACM) con un Application Load Balancer. Implementar certificados autofirmados en las instancias EC2. Asegurar que el software cliente de la base de datos use una conexión TLS con Amazon RDS. Habilitar el cifrado de la instancia de RDS. Habilitar el cifrado en los volúmenes de Amazon EBS que respaldan las instancias EC2.**

B. Usar certificados TLS de un proveedor externo con un Application Load Balancer. Instalar los mismos certificados en las instancias EC2. Asegurar que el software cliente de la base de datos use una conexión TLS con Amazon RDS. Usar AWS Secrets Manager para cifrado del lado del cliente de los datos de la aplicación.

C. Usar AWS CloudHSM para generar certificados TLS para las instancias EC2. Instalar los certificados TLS en las instancias EC2. Asegurar que el software cliente de la base de datos use una conexión TLS con Amazon RDS. Usar las claves de cifrado de CloudHSM para el cifrado del lado del cliente de los datos de la aplicación.

D. Usar Amazon CloudFront con AWS WAF. Enviar conexiones HTTP a las instancias EC2 de origen. Asegurar que el software cliente de la base de datos use una conexión TLS con Amazon RDS. Usar AWS Key Management Service (AWS KMS) para cifrar del lado del cliente los datos de la aplicación antes de almacenarlos en la base de datos RDS.

17.- Un ingeniero de seguridad está trabajando con una empresa para diseñar una aplicación de comercio electrónico. La aplicación se ejecutará en instancias Amazon EC2 dentro de un grupo de Auto Scaling detrás de un Application Load Balancer (ALB). La aplicación usará una instancia de Amazon RDS como base de datos.

La única conectividad requerida desde internet es para el tráfico HTTP y HTTPS hacia la aplicación. Sin embargo, la aplicación también debe comunicarse con un proveedor de pagos externo, el cual solo permite tráfico desde una lista blanca (allow list) preconfigurada de direcciones IP. La empresa debe asegurarse de que la comunicación con el proveedor de pagos externo no se interrumpa, incluso cuando el entorno se escale.

¿Qué combinación de acciones debe recomendar el ingeniero de seguridad para cumplir con estos requisitos? (Elige tres).

**A. Implementar un NAT Gateway en cada subred privada de cada Zona de Disponibilidad que se esté utilizando.**

B. Ubicar la instancia de base de datos en una subred pública.

**C. Ubicar la instancia de base de datos en una subred privada.**

D. Configurar el grupo de Auto Scaling para ubicar las instancias EC2 en una subred pública.

**E. Configurar el grupo de Auto Scaling para ubicar las instancias EC2 en una subred privada.**

F. Implementar el ALB en una subred privada.

18.- Una empresa utiliza varios stacks de AWS CloudFormation para gestionar el despliegue de un conjunto de aplicaciones. El líder del equipo de desarrollo de aplicaciones nota que algunos miembros del equipo reciben errores de permisos cuando intentan desplegar los stacks, mientras que otros pueden hacerlo sin problemas.

Los miembros del equipo acceden a la cuenta asumiendo un rol que tiene un conjunto específico de permisos necesarios para sus responsabilidades laborales. Todos los miembros tienen permisos para operar los stacks, pero aun así hay fallos.

¿Qué combinación de pasos garantizará el despliegue consistente de los stacks de forma más segura? (Elige tres).

A. Crear un rol de servicio que tenga un principal compuesto que incluya cada servicio que necesite los permisos necesarios. Configurar el rol para permitir la acción sts:AssumeRole.

**B. Crear un rol de servicio que tenga cloudformation.amazonaws.com como principal del servicio. Configurar el rol para permitir la acción sts:AssumeRole.**

C. Para cada conjunto de permisos requerido, agregar una política separada al rol para permitir dichos permisos. Agregar el ARN de cada stack de CloudFormation en el campo Resource de cada política.

**D. Para cada conjunto de permisos requerido, agregar una política separada al rol para permitir dichos permisos. Agregar el ARN de cada servicio que necesita los permisos en el campo Resource de la política correspondiente.**

**E. Actualizar cada stack para que use el rol de servicio.**

F. Agregar una política a cada rol de los miembros del equipo para permitir la acción iam:PassRole. Establecer el campo Resource de la política en el ARN del rol de servicio.

19.- Una empresa utilizó un enfoque de “lift-and-shift” para migrar desde sus centros de datos locales hacia la nube de AWS. La empresa migró máquinas virtuales (VMs) locales a instancias de Amazon EC2. Ahora, la empresa desea reemplazar algunos de los componentes que actualmente se ejecutan en EC2 por servicios administrados de AWS que ofrezcan funcionalidades similares.

Como primer paso, la empresa realizará la transición desde software de balanceo de carga que corre en EC2 hacia Elastic Load Balancers (ELB) de AWS. Un ingeniero de seguridad debe asegurarse de que, tras esta transición:

Todos los logs del balanceador de carga estén centralizados y sean consultables para auditoría.

Se generen métricas que indiquen qué cifrados (ciphers) están en uso.

¿Qué solución cumplirá con estos requisitos?

A. Crear un grupo de logs en Amazon CloudWatch Logs. Configurar los balanceadores de carga para que envíen logs a ese grupo. Usar la consola de CloudWatch Logs para buscar en los logs. Crear filtros de logs en CloudWatch para generar las métricas requeridas.

B. Crear un bucket de Amazon S3. Configurar los balanceadores de carga para que envíen los logs al bucket. Usar Amazon Athena para consultar los logs que están en el bucket. Crear filtros en Amazon CloudWatch sobre los archivos de log del bucket para generar las métricas requeridas.

**C. Crear un bucket de Amazon S3. Configurar los balanceadores de carga para que envíen los logs al bucket. Usar Amazon Athena para consultar los logs en el bucket. Crear consultas de Athena para obtener las métricas requeridas y publicar esas métricas en Amazon CloudWatch.**

D. Crear un grupo de logs en CloudWatch Logs. Configurar los balanceadores de carga para que envíen los logs al grupo. Usar la Consola de administración de AWS para consultar los logs. Crear consultas en Athena para las métricas requeridas y publicarlas en CloudWatch.

20.- Una empresa utiliza AWS Organizations para administrar un entorno multi-cuenta de AWS dentro de una sola región. La cuenta de administración de la organización se llama management-01. La empresa ha habilitado AWS Config en todas las cuentas de la organización y ha designado una cuenta llamada security-01 como administrador delegado de AWS Config.

Cada cuenta informa su estado de cumplimiento al administrador delegado (security-01) mediante un agregador de AWS Config. Además, cada administrador de cuenta puede configurar y gestionar sus propias reglas de AWS Config para manejar requisitos de cumplimiento específicos.

Un ingeniero de seguridad necesita implementar una solución que:

Implemente automáticamente un conjunto de 10 reglas de AWS Config en todas las cuentas existentes y futuras de la organización.

Active AWS Config automáticamente en el momento en que se crea una nueva cuenta.

¿Qué combinación de pasos cumplirá con estos requisitos? (Elige dos).

A. Crear una plantilla de AWS CloudFormation que contenga las 10 reglas requeridas de AWS Config. Implementar la plantilla usando CloudFormation StackSets desde la cuenta security-01.

**B. Crear un conformance pack que contenga las 10 reglas requeridas de AWS Config. Implementar el conformance pack desde la cuenta security-01.**

C. Crear un conformance pack que contenga las 10 reglas requeridas de AWS Config. Implementar el conformance pack desde la cuenta management-01.

D. Crear una plantilla de AWS CloudFormation que active AWS Config. Implementar la plantilla usando CloudFormation StackSets desde la cuenta security-01.

**E. Crear una plantilla de AWS CloudFormation que active AWS Config. Implementar la plantilla usando CloudFormation StackSets desde la cuenta management-01.**

21.- Una empresa tiene una aplicación heredada que se ejecuta en una única instancia de Amazon EC2. Una auditoría de seguridad revela que la aplicación ha estado usando una clave de acceso de IAM incrustada en el código para acceder a un bucket de Amazon S3 llamado DOC-EXAMPLE-BUCKET1, dentro de la misma cuenta de AWS.

Este par de claves de acceso tiene el permiso s3:GetObject para todos los objetos dentro solo de ese bucket. La empresa decide apagar la aplicación, ya que no cumple con las políticas de seguridad de la compañía para acceder a recursos de AWS desde instancias EC2.

Un ingeniero de seguridad confirma que AWS CloudTrail está habilitado en todas las regiones, y que está enviando logs a un bucket S3 llamado DOC-EXAMPLE-BUCKET2, que también está en la misma cuenta de AWS. Sin embargo, CloudTrail no ha sido configurado para enviar logs a Amazon CloudWatch Logs.

La empresa desea saber si algún objeto en DOC-EXAMPLE-BUCKET1 fue accedido con esa clave de acceso de IAM durante los últimos 60 días. En caso afirmativo, quiere saber si alguno de esos objetos con extensión .txt contiene información personal identificable (PII).

¿Qué combinación de pasos debe seguir el ingeniero de seguridad para obtener esta información? (Elige dos).

A. Usar Amazon CloudWatch Logs Insights para identificar cualquier objeto en DOC-EXAMPLE-BUCKET1 que contenga PII y que haya estado accesible mediante la clave de acceso.

B. Usar Amazon OpenSearch Service para consultar los logs de CloudTrail en DOC-EXAMPLE-BUCKET2 en busca de llamadas a la API que hayan utilizado la clave de acceso para acceder a objetos que contengan PII.

**C. Usar Amazon Athena para consultar los logs de CloudTrail en DOC-EXAMPLE-BUCKET2 y encontrar llamadas a la API que hayan utilizado la clave de acceso para acceder a objetos que contengan PII.**

D. Usar AWS IAM Access Analyzer para identificar llamadas a la API que hayan utilizado la clave de acceso para acceder a objetos con PII en DOC-EXAMPLE-BUCKET1.

**E. Configurar Amazon Macie para identificar objetos en DOC-EXAMPLE-BUCKET1 que contengan PII y que hayan estado accesibles mediante la clave de acceso.**

22.- Un ingeniero de seguridad crea una política de bucket de Amazon S3 que deniega el acceso a todos los usuarios. Unos días después, el ingeniero agrega una nueva instrucción a la política del bucket para permitir acceso de solo lectura a otro empleado. Sin embargo, después de actualizar la política, el empleado sigue recibiendo un mensaje de acceso denegado.

¿Cuál es la causa más probable de este rechazo de acceso?

A. Es necesario actualizar la ACL (lista de control de acceso) del bucket.

B. La política de IAM no permite al usuario acceder al bucket.

C. Las políticas de bucket tardan unos minutos en aplicarse.

**D. El permiso de allow (permitir) está siendo anulado por un deny (denegar).**

23.- Una empresa está utilizando Amazon Macie, AWS Firewall Manager, Amazon Inspector y AWS Shield Advanced en su cuenta de AWS. La empresa quiere recibir alertas si ocurre un ataque DDoS contra la cuenta.

¿Qué solución cumplirá con este requisito?

A. Usar Macie para detectar un evento DDoS activo. Crear alarmas de Amazon CloudWatch que respondan a los hallazgos de Macie.

B. Usar Amazon Inspector para revisar los recursos e invocar alarmas de CloudWatch para cualquier recurso vulnerable a ataques DDoS.

C. Crear una alarma de Amazon CloudWatch que supervise las métricas de Firewall Manager para detectar un evento DDoS activo.

**D. Crear una alarma de Amazon CloudWatch que supervise las métricas de Shield Advanced para detectar un evento DDoS activo.**

24.- Una empresa aloja una aplicación web en un servidor web Apache. La aplicación se ejecuta en instancias de Amazon EC2 que están dentro de un grupo de Auto Scaling. La empresa ha configurado las instancias EC2 para que envíen los logs del servidor Apache a un grupo de Amazon CloudWatch Logs, el cual está configurado para expirar después de 1 año.

Recientemente, la empresa descubrió en los logs de Apache que una dirección IP específica está enviando solicitudes sospechosas a la aplicación web. Un ingeniero de seguridad quiere analizar los logs de la última semana para determinar:

Cuántas solicitudes envió esa dirección IP, y Qué URLs solicitó.

¿Qué debe hacer el ingeniero de seguridad para cumplir con estos requisitos con el menor esfuerzo posible?

A. Exportar los datos del grupo de logs de CloudWatch a Amazon S3. Usar Amazon Macie para consultar los logs en busca de la dirección IP específica y las URLs solicitadas.

B. Configurar una suscripción de CloudWatch Logs para transmitir el grupo de logs a un clúster de Amazon OpenSearch Service. Usar OpenSearch para analizar los logs con respecto a la IP y las URLs.

**C. Usar CloudWatch Logs Insights con una consulta personalizada para analizar los logs de CloudWatch y buscar la dirección IP específica y las URLs solicitadas.**

D. Exportar los datos del grupo de logs de CloudWatch a Amazon S3. Usar AWS Glue para rastrear (crawl) el bucket de S3 buscando solo las entradas de log que contengan la dirección IP específica. Usar AWS Glue para ver los resultados.

25.- Mientras se aseguraba la conexión entre la VPC de una empresa y su centro de datos on-premises, un ingeniero de seguridad ejecutó un comando ping desde un host local (dirección IP 203.0.113.12) hacia una instancia de Amazon EC2 (dirección IP 172.31.16.139). El comando ping no obtuvo respuesta.

El registro de flujo (flow log) en la VPC mostró lo siguiente:

¿Qué acción debe realizarse para que el ping funcione?

A. En el grupo de seguridad de la instancia EC2, permitir tráfico ICMP entrante.

B. En el grupo de seguridad de la instancia EC2, permitir tráfico ICMP saliente.

C. En la lista de control de acceso a red (NACL) de la VPC, permitir tráfico ICMP entrante.

**D. En la lista de control de acceso a red (NACL) de la VPC, permitir tráfico ICMP saliente.**

26.- Una empresa desarrolló una aplicación utilizando AWS Lambda, Amazon S3, Amazon Simple Notification Service (Amazon SNS) y Amazon DynamoDB. Una aplicación externa coloca objetos en el bucket S3 de la empresa y etiqueta los objetos con fecha y hora. Una función Lambda extrae periódicamente datos del bucket S3 de la empresa basándose en esas etiquetas de fecha y hora, e inserta valores específicos en una tabla de DynamoDB para su posterior procesamiento.

Los datos incluyen información personal identificable (PII). La empresa debe eliminar los datos que tengan más de 30 días tanto del bucket S3 como de la tabla de DynamoDB.

¿Qué solución cumplirá este requisito con la mayor eficiencia operativa?

A. Actualizar la función Lambda para agregar una etiqueta TTL S3 a los objetos. Crear una política de ciclo de vida de S3 para eliminar los objetos que tengan más de 30 días utilizando esa etiqueta TTL.

**B. Crear una política de ciclo de vida de S3 para eliminar los objetos que tengan más de 30 días. Actualizar la función Lambda para agregar un atributo TTL en la tabla de DynamoDB. Habilitar TTL en la tabla para que elimine automáticamente los registros que tengan más de 30 días según ese atributo.**

C. Crear una política de ciclo de vida de S3 para eliminar objetos que tengan más de 30 días y que incluya todos los prefijos del bucket. Actualizar la función Lambda para eliminar manualmente las entradas que tengan más de 30 días.

D. Crear una política de ciclo de vida de S3 para eliminar objetos que tengan más de 30 días usando etiquetas de objeto. Actualizar la función Lambda para eliminar manualmente las entradas que tengan más de 30 días.

27.- ¿Cuáles son las formas MÁS seguras de proteger al usuario raíz de una cuenta de AWS recientemente creada? (Elige dos).

A. Usar las claves de acceso del usuario raíz de la cuenta de AWS en lugar de la Consola de administración de AWS.

B. Habilitar autenticación multifactor (MFA) para los usuarios de IAM que tengan la política administrada AdministratorAccess.

C. Usar AWS KMS para cifrar todas las claves de acceso del usuario raíz y de los usuarios de IAM, y configurar la rotación automática cada 30 días.

**D. No crear claves de acceso para el usuario raíz de la cuenta de AWS; en su lugar, crear usuarios de IAM.**

**E. Habilitar la autenticación multifactor (MFA) para el usuario raíz de la cuenta de AWS.**

28.- Una empresa está expandiendo su red de tiendas. El día que cada nueva tienda abre, la empresa quiere lanzar una aplicación web personalizada para esa tienda. Cada aplicación tendrá un entorno de producción y un entorno no productivo, y cada entorno será implementado en una cuenta de AWS diferente.

La empresa utiliza AWS Organizations y tiene una unidad organizativa (OU) que se utiliza únicamente para estas cuentas.

La mayor parte del trabajo de desarrollo se subcontrata a equipos externos. Un ingeniero de seguridad debe asegurarse de que cada equipo siga el plan de implementación de recursos en AWS definido por la empresa. Además, debe limitar el acceso a ese plan solo a los desarrolladores que realmente lo necesiten.

El ingeniero de seguridad ya ha creado una plantilla de AWS CloudFormation que implementa el plan de despliegue.

¿Qué debe hacer el ingeniero de seguridad a continuación para cumplir con los requisitos de la forma más segura posible?

**A. Crear un portafolio de AWS Service Catalog en la cuenta de administración de la organización. Subir la plantilla de CloudFormation. Agregar la plantilla a la lista de productos del portafolio. Compartir el portafolio con la OU.**

B. Usar la CLI de CloudFormation para crear un módulo a partir de la plantilla de CloudFormation. Registrar el módulo como una extensión privada en el registro de CloudFormation. Publicar la extensión. En la OU, crear una política de control de servicios (SCP) que permita acceso a esa extensión.

C. Crear un portafolio de AWS Service Catalog en la cuenta de administración de la organización. Subir la plantilla de CloudFormation. Agregar la plantilla a la lista de productos del portafolio. Crear un rol de IAM con una política de confianza que permita acceso entre cuentas al portafolio para los usuarios de las cuentas dentro de la OU. Adjuntar la política administrada AWSServiceCatalogEndUserFullAccess al rol.

D. Usar la CLI de CloudFormation para crear un módulo a partir de la plantilla de CloudFormation. Registrar el módulo como una extensión privada en el registro de CloudFormation. Publicar la extensión. Compartir la extensión con la OU.

29.- Un equipo está utilizando AWS Secrets Manager para almacenar la contraseña de la base de datos de una aplicación. Solo un número limitado de entidades de IAM dentro de la cuenta puede acceder al secreto. Los usuarios que requieren acceso cambian con frecuencia.

Un ingeniero de seguridad debe crear una solución que maximice la flexibilidad y escalabilidad.

¿Qué solución cumplirá con estos requisitos?

A. Usar un enfoque basado en roles, creando un rol de IAM con una política de permisos inline que permita acceso al secreto. Actualizar la política de confianza del rol para agregar o quitar los usuarios según sea necesario.

B. Implementar un punto de enlace (endpoint) de VPC para Secrets Manager. Crear y adjuntar una política de endpoint que especifique qué entidades IAM pueden acceder al secreto. Actualizar la lista de usuarios IAM según se requiera.

C. Usar un enfoque basado en etiquetas, adjuntando una política de recurso al secreto. Aplicar etiquetas (tags) tanto al secreto como a los usuarios IAM. Usar las claves de condición aws:PrincipalTag y aws:ResourceTag para controlar el acceso.

**D. Usar un enfoque de denegación por defecto, utilizando políticas de IAM para denegar explícitamente el acceso al secreto. Adjuntar estas políticas a un grupo de IAM. Agregar a todos los usuarios IAM a ese grupo. Quitar temporalmente a los usuarios del grupo cuando necesiten acceso y volver a agregarlos cuando ya no se les deba permitir.**

30.- Una empresa está alojando una aplicación web en instancias Amazon EC2 que están detrás de un Application Load Balancer (ALB). La aplicación se ha convertido en el objetivo de un ataque de denegación de servicio (DoS). Los registros de la aplicación muestran que las solicitudes provienen de un pequeño número de direcciones IP de cliente, pero estas direcciones cambian con frecuencia.

La empresa necesita bloquear el tráfico malicioso con una solución que requiera el menor esfuerzo continuo posible.

¿Qué solución cumple con estos requisitos?

**A. Crear una regla basada en tasa (rate-based rule) en AWS WAF y adjuntarla al ALB.**

B. Actualizar el grupo de seguridad adjunto al ALB para bloquear las direcciones IP atacantes.

C. Actualizar la lista de control de acceso a red (NACL) de la subred del ALB para bloquear las direcciones IP atacantes.

D. Crear una regla basada en tasa en AWS WAF y adjuntarla al grupo de seguridad de las instancias EC2.